

PART FOUR

INFORMATION SECURITY AND GOVERNMENT POLICIES

CHAPTER 1. INTRODUCTION

CHAPTER 2. PROTECTING GOVERNMENT SYSTEMS

CHAPTER 3. THE ROLE OF LAW AND GOVERNMENT POLICY

VIS A VIS THE PRIVATE SECTOR

CHAPTER 4. GOVERNMENT CYBER-SECURITY POLICIES

CHAPTER 1. INTRODUCTION

As in other areas affecting the Internet, government policy has an important role to play in the promotion of IT Security. There is a paradox, however: a sound public policy framework can enhance security, but ill-considered government regulation can do more harm than good. Technology is changing so rapidly and new cyber threats are emerging with such swiftness that government regulation can become a straitjacket, impeding the development and deployment of innovative responses. It is important therefore to achieve the right balance of regulatory and non-regulatory measures. In seeking that balance, policymakers should appreciate some defining characteristics of the Internet. Compared with earlier information and communications technologies, cyberspace is uniquely decentralized. The Internet's power comes in part from the fact that it has no gatekeepers. Most functionality is at the edges rather than at the center of the network. Government cyber-security policies must take into account these features of the Internet. Within this context, there is a range of steps governments can take to improve computer security, without interfering with technical design decisions.¹⁰⁸

While the picture varies from country to country, in most countries some or all components of the communications network and many of the critical infrastructures based on computer systems (banking, transportation, energy, manufacturing, etc.) are owned and operated by the private sector. Therefore, much of the responsibility for ensuring the security of these systems lies with the private sector.¹⁰⁹ However, these systems are critical to the national well-being and are interdependent in ways that implicate broader public interests and justify government attention. Also, of course, the government has its own computer systems, including those that are crucial to national security, emergency services, health care, and other critical functions. These systems, in turn, often depend in part on privately owned communications networks. By and large,

many of the computer systems of private companies and government agencies rely on the same hardware and software, designed and built by private companies. Thus, the picture is one of mutual interdependencies.

For all of these reasons, responsibility for computer security is shared between the government sector and the private sector. As a first priority, the government has a responsibility to "get its own house in order" – that is, to implement sound security practices for its own systems. In addition, it is universally recognized that the government should use the power of the criminal law to punish and deter intentional attacks on private sector as well as on government computers. Beyond that, a growing number of governments are concluding that they must undertake additional responsibilities to promote sound computer security practices in the private sector. The challenge is to adopt government policies that maximize the benefits of government involvement without stifling innovation through overbearing regulation and technology mandates. Within a framework of partnership, the solution can be found in a balanced approach that includes:

- Market forces that encourage private enterprises to address the security of their computer systems in order to protect their profitability;
- The government's research and awareness-building functions;
- Computer crime laws protecting both government and privately-owned computers and networks;
- Traditional concepts of legal liability translated to the computer context; and
- Laws, regulations, and government policies that are specifically focused on promoting computer security.

The issue of cybersecurity policy can be viewed as one component of the larger issue of the role of law in fostering trust online. Creating an environment of trust in cyberspace requires the adoption of laws and government policies in other areas in addition to cyber-security. These other areas include consumer protection, data and

¹⁰⁸ The following discussion draws upon the detailed surveys compiled by the American Bar Association's Privacy & Computer Crime Committee: Jody R. Westby, ed., *International Guide to Combating Cybercrime*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, 2003 (Westby Guide), <http://www.abanet.org/abapubs/books/cybercrime/>; Jody R. Westby, ed., *International Strategy for Cyberspace Security*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, 2003 (Westby Strategy). See also *International Critical Information Infrastructure Protection Handbook*, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

¹⁰⁹ In some countries, privatization is quite recent, meaning that operators, regulators and policymakers are struggling with the new problem of security at the same time they are grappling with the full range of transitional problems associated with privatization.

communications privacy, intellectual property rights, and the framework for e-commerce. In the offline world, the law weaves a web of rules and protections around commercial and consumer transactions. Much of that same law applies to cyberspace, but countries seeking to promote development of ICT need to assess whether there are gaps in their laws that fail to promote trust in ways that are special to cyberspace. Indeed, countries eager to promote e-commerce may find that their laws for financial services, intellectual property, and consumer protection do not provide sufficient confidence or protection for offline transactions. The process of cyberlaw reform may occur as part of broader legal reforms. This Handbook focuses on those laws and policies that directly concern attacks on computer systems, leaving to other resources (some of which are cited in Part 3 and the Annexes) the questions of the broader enabling framework for ICT and e-commerce.¹¹⁰

This Part, while it discusses initiatives taken in developing and transitional countries, focuses in some detail on the programs and policies adopted by the most highly developed countries and by multi-national organizations. To a large degree, this is where the action has been to date. However, this focus on resources and models from developed countries and international bodies should not deter “the rest of the world.” It is important that all countries develop, promote, and implement the necessary framework for e-security. The budgetary and human resources available are of course different, and developing countries may have to approach the issues at a more basic level, but the principles outlined here are global in relevance. Cyberspace and cyber-insecurity are not limited by state boundaries.

The Concept of Critical Infrastructures

In a number of countries, the development of government responses to the problem of computer security has been conceptualized in terms of “critical infrastructures.” A critical infrastructure is some network of physical assets and operating systems that serves a function of critical importance to the economic or governmental well-being of a country. The financial services network, for example, is a

critical infrastructure, consisting of all the private banks, the central bank, the securities exchange and commodities markets, the payment clearinghouses, and other entities involved in the flow of money and credit. In virtually every country in the world, these functions are dependent upon computers. The transportation network is another critical infrastructure, consisting of roads, bridges, canals, railroads, and airports. The transportation infrastructure is largely physical and mechanical, but it too is increasingly dependent on computers to operate traffic lights, to open and close bridges, to switch trains, and to control air traffic.

There is no common definition of critical infrastructure categories, and the list of “critical infrastructures” used by policymakers varies from country to country and from time to time. The U.S. government cyber-security strategy issued in February 2003 identifies thirteen critical infrastructure categories: 1) agriculture; 2) food; 3) water; 4) public health; 5) emergency services; 6) government; 7) defense industrial base; 8) information and telecommunications; 9) energy; 10) transportation; 11) banking and finance; 12) chemicals and hazardous material; and 13) postal and shipping.¹¹¹ By comparison, Canada’s critical infrastructure protection strategy uses only six categories: 1) communications; 2) government, 3) energy and utilities; 4) services (within which Canada includes financial services, food distribution and health care); 5) safety; and 6) transportation.¹¹² How a country defines “critical infrastructure” is not as important as the recognition of the concept itself.

The concept of critical infrastructures is important for several reasons. First, it can help crystallize why computer security is important: policymakers may better grasp the cyber-security problem if they understand that money will be frozen in banks, trains will not be able to leave their stations, and drinking water will not be pumped if certain computers fail. Second, infrastructure categories are important insofar as they help define lines of responsibility and communities of shared interest that need to work together to improve security. For example, the electric

¹¹⁰ The Global Internet Policy Initiative has a host of resources on the full range of policy issues affecting ICT development: <http://www.internetpolicy.net>.

¹¹¹ *The National Strategy to Secure Cyberspace* [United States], February 2003 <http://www.whitehouse.gov/pcip/b/>; http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

¹¹² Office of Critical Infrastructure Protection and Emergency Preparedness [Canada] http://www.ocipep.gc.ca/home/index_e.asp. For descriptions of how various other countries have responded to critical infrastructure protection, see “International Critical Information Infrastructure Protection Handbook,” edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

power industry and its government regulators can work together to good effect in addressing computer vulnerabilities of the electric power system. Computer security measures, including the identification of best practices and the sharing of information about vulnerabilities, can, to some extent, be developed and implemented within the context of existing institutions created along industry lines. In the private sector, these institutions include trade associations, standards bodies, and other self-regulatory bodies for various industries. On the government side, many nations implement their cybersecurity policies through existing ministries and regulatory agencies that were created along sectoral lines many years ago (such as those that have traditionally regulated the banking, telecommunications, and energy sectors).

Currently there are a number of broad initiatives to stimulate a greater degree of cross-border cooperation in these areas. For example, in May of 2003, the G8 adopted eleven principles to consider when developing a strategy for reducing risks to critical information infrastructure:

(See http://www.cybersecuritycooperation.org/documents/G8_CIIIP_Principles.pdf.)

- I. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.
- II. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.
- III. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
- IV. Countries should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
- V. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
- VI. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.
- VII. Countries should facilitate tracing attacks on critical information infrastructures and, where

appropriate, the disclosure of tracing information to other countries.

VIII. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

IX. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

X. Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

XI. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Computer security is characterized by interrelationships across sectors, including similar or identical hardware and software and dependency on a common communications network. Therefore, governments must design policies that ensure sharing of information about vulnerabilities and solutions across infrastructure categories. This can be greatly facilitated by the designation of centralized leadership within the government to coordinate cyber-security policies and programs; we will return to this point later.

CHAPTER 2. PROTECTING GOVERNMENT SYSTEMS

All of the issues pertaining to small and medium sized enterprises that are covered in Part 3 are equally applicable to government systems. Just as an enterprise needs to protect itself, its suppliers, and its customers, the government must protect its systems and its citizens from security threats, both physically and in cyberspace. Local and national governments cannot afford to have major crises such as interruption of operations that are based on computers, loss of confidential data, or theft of computing resources. Security incidents that are well-publicized lead to a diminution of public trust and present an obstacle to promotion of e-government initiatives. Therefore, government's first responsibility in terms of computer security is probably to "get its own house in order," meaning that government agencies at all levels (national, provincial, and local) must protect the computer systems that they own and operate. These include the computer systems used by government agencies or ministries, including national defense authorities, law enforcement, public health and safety and emergency response agencies, and central banks. Government-owned infrastructures that are dependent on computers may also include water systems, hydroelectric dams, the air traffic control system, and other facilities, depending on what is privatized and what is government owned.

Leadership and Organization

Computer security poses leadership and organizational challenges within government. For purposes of defining responsibilities within government, is computer security

an economic, national security, or law enforcement problem?

- Canada has put much of the authority for cyber-security in its Ministry National Defence.¹¹³
- In the United Kingdom, the Home Office, which is mainly a law enforcement ministry, has the lead.¹¹⁴
- The United States has put the issue within the newly created Department of Homeland Security, but consciously left the Computer Security Division of the National Institute of Standards and Technology under the Commerce Department.¹¹⁵
- Australia has created an E-Security Coordination Group to coordinate cybersecurity policy,, an inter-agency body chaired by the National Office for the Information Economy, which is an Executive Agency¹¹⁶ under the Minister for Communications, Information Technology and the Arts.
- Italy has established an Interministerial Committee for Responsible Use of the Internet, managed by the Department of Innovation and Technologies in the Prime Minister's Office.
- In Japan, in 2000, the Prime Minister established a branch for IT security in the Cabinet Office in order to better coordinate security policy and measures among ministries and agencies. The branch is composed of experts from concerned ministries and agencies and from the private sector.¹¹⁷

The choice of where within government to place cyber-security leadership can be significant. For example, the issues surrounding the sharing of information about cyber-security vulnerabilities and when to disclose vulnerabilities to the public require a balancing of interests. Placing responsibility for cyber-security within the

¹¹³ Canada's Office of Critical Infrastructure Protection and Emergency Preparedness is a civilian organization operating within the Ministry of National Defence.

¹¹⁴ The U.K.'s Home Office has created a National Infrastructure Security Coordination Centre (NISCC) to coordinate critical infrastructure protection issues, provide alerts and attack response assistance, and facilitate public-private relationships to protect infrastructure. Within NISCC, there is a Computer Emergency Response Team, known as UNIRAS. An Electronic Attack Response Group (EARG) is also within NISCC to provide assistance to critical infrastructure organizations and government departments that suffer an attack. UNIRAS will provide an early warning and alert service to all UK businesses. The NISCC website (<http://www.niscc.gov.uk>) provides detailed information on the British government's approach.

¹¹⁵ In some ways, the United States is a complex model of coordination, and may therefore be of limited utility as an example for developing countries. The Homeland Security Act of 2002 places responsibility for security of both government and private sector computer systems in the Department of Homeland Security, but the Federal Information Security Management Act of 2002 gives the Office of Management and Budget in the White House responsibility for overseeing security of government computer systems, and a Homeland Security Council in the White House also has responsibility for coordinating cybersecurity policy.

¹¹⁶ Under Australian law, Executive Agencies are non-statutory bodies established by the Governor-General when a degree of independence within the governmental structure is needed and when the functions of the agency require a government-wide approach. The head of an Executive Agency is appointed by, and directly accountable to a Minister, in this case the Minister for Communications, Information Technology and the Arts. See http://www.noie.gov.au/Projects/confidence/Protecting/nat_agenda.htm.

¹¹⁷ See <http://www.kantei.go.jp/foreign/it/security/2000/0519taisei.html>.

defense ministry, which likely has a tradition of national security secrecy, may hamper information sharing and produce a policy that does not sufficiently promote public awareness. Since public-private partnership is a major component of what we believe to be the most effective computer security strategy, leadership for cyber-security may better be placed within an economic affairs agency or an intergovernmental body under the nation's chief executive.

But more important than the question of which agency or agencies should be given responsibility for computer security is the point that some national leadership should be designated to ensure that computer security will receive government-wide attention. There are important organizational questions to be considered when it comes to getting powerful existing ministries to address computer security. If the agency with cyber-security leadership is granted only the powers of persuasion and publicity, its ability to improve security in other ministries may be limited. Therefore, mechanisms should be considered that give the office charged with cyber-security leadership the authority to require other ministries and departments to address the security of their own systems. The ultimate power to require ministries to comply with computer security standards may be the authority to disapprove those government agencies' computer purchases that do not meet security standards.

To some extent, the United States has taken this approach, giving its Office of Management and Budget in the Office of the President authority to approve or disapprove expenditure of funds for computer systems based on various considerations, including security. Other less drastic measures include requiring ministries and government agencies to conduct annual cyber-security audits and report the results to the cyber-security office. Whatever structures are chosen, leadership from the office of the president or prime minister will probably be needed to ensure that all departments are taking the issue seriously.

Another organizational challenge for government is the problem of human resources: Governments may find it hard to attract and retain well-qualified computer security personnel. Effective responses may include college

scholarships for computer security studies, where the scholarships require graduates to work a certain number of years for the government. A short-term solution may be a secondment program with the private sector whereby corporate cyber-security experts are loaned to the government but paid in whole or in part by their private sector employers. For both developed and developing countries, the problem of human resources in cyber-security may be a manifestation of the government's broader difficulty in paying salaries competitive with the private sector in order to attract qualified, committed employees.

Developing a National Cyber-Security Strategy

The process of developing a "national cyber-security strategy" can be an effective means of deciding what a nation's cyber-security vulnerabilities are, what the government's responsibilities should be, and what policies and legal reforms need to be adopted. A national cyber-security strategy can also define the relationship of the government to the private sector. Here we will focus mainly on the elements of a cyber-security strategy that concern protecting the government's own computers. Later on in Part 4, we will discuss the role of the government in improving the security of private sector systems. The U.S. strategy explains the reason for the distinction:

"In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government response is most appropriate and justified. Looking inward, providing continuity of government requires ensuring the safety of [the government's] own cyber infrastructure and those assets required for supporting its essential missions and services. Externally, a government role in cyber-security is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under provisioning of critical shared resources; and raising awareness."¹¹⁸

¹¹⁸ The National Strategy to Secure Cyberspace [United States], February 2003, p. ix, <http://www.whitehouse.gov/pcipb/>; http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

To date, the United States has had probably the most extensive and most transparent process of developing a national cyber-security strategy, but the same themes emerge in the initiatives of other countries and international bodies. While details of the process and of the resulting organizational structures and laws will vary from country to country, the process of developing a cyber-security strategy is similar to that which many countries have undertaken in developing national ICT strategies.¹¹⁹ Indeed, security is best seen as a component of a nation's ICT strategy, and a cyber-security strategy can be developed with the same institutions and mechanisms used to develop a nation's basic program for ICT development. Japan, for example, has incorporated cyber-security into its "e-Japan Priority Policy Program" of March 2001.¹²⁰

Looking at the experiences of those countries that have developed national cyber-security strategies, some common elements or phases emerge:

1. Assessment of national vulnerabilities and issuance of a public report that conceptualizes the issue and raises awareness of policymakers and the public;
2. Creation of a leadership structure within the executive branch to oversee the development and implementation of policy;
3. Drafting of a detailed national plan based on dialogue with the private sector;
4. Adoption of legislation and guidelines addressing such questions as information sharing and accountability.

The first phase is to broadly assess vulnerabilities and raise awareness. Australia, for example, published the report "Australia's National Information Infrastructure: Threats and Vulnerabilities" in 1997. The report, prepared by the Defence Signals Directorate, concluded that Australian society was vulnerable to significant disruption due to vulnerabilities in computer networks

and that no formal structure existed for the coordination and implementation of government policy for protecting critical infrastructures.¹²¹ In the United States, to study the issue, the President appointed a board of corporate and government officials, known as the President's Critical Infrastructure Protection Board in 1996. The board had no regulatory powers and was not a permanent body. It conducted hearings, interviews, and research and issued a report that described the problem and drew the attention of policymakers, corporate officials, the media and the public. The Board presented its report in October 1997, calling for closer cooperation between the private sector and the government and making numerous specific recommendations.

The second phase is to create some permanent structure within the executive branch to coordinate policy development and implementation. In Canada, for example, following the issuance of an assessment by an inter-departmental Critical Infrastructure Protection Task Force, the government created an Information Protection Coordination Centre to collect information, assess threats, and analyze incidents and an Office of Critical Infrastructure Protection and Emergency Preparedness to provide national leadership on critical infrastructure protection issues.¹²²

In the United States, Presidents Clinton and Bush issued a series of executive directives establishing policymaking and oversight bodies within the executive branch of the federal government. The directives called for the development of a national plan for infrastructure protection.¹²³ These Presidential orders did not give federal agencies authority over the systems of the private sector; instead, they emphasized public-private partnership and information sharing. Other leadership structures are discussed above under "Leadership and Organization."

¹¹⁹ For descriptions of how various other countries developed their cyber-security strategies, see International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

¹²⁰ <http://www.kantei.go.jp/foreign/it/network/priority-all/index.html>.

¹²¹ See International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002), p. 18, <http://www.isn.ethz.ch/crn>.

¹²² Office of Critical Infrastructure Protection and Emergency Preparedness [Canada], http://www.ocipep.gc.ca/critical/nciap/disc_e.asp.

¹²³ President Clinton issued Presidential Decision Directive (PDD) 63: Critical Infrastructure Protection, May 22, 1998, <http://www.fas.org/irp/offdocs/pdd-63.htm> and PDD 62: Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998, <http://www.fas.org/irp/offdocs/pdd-62.htm>. In the aftermath of September 11, 2001, President Bush signed two executive orders reallocating functions and creating new entities within the executive branch responsible for critical infrastructure protection. E.O. 13228, Establishing the Office of Homeland Security and the Homeland Security Council, October 8, 2001, <http://fas.org/irp/offdocs/eo/eo-13228.htm>; E.O. 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001, <http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>.

The third phase involves the development of the strategy itself. As noted above, a national cyber-security strategy can be a free-standing document or it can be part of the nation's overall ICT strategy. A key to this process is dialogue between government and the private sector. In Japan, which has incorporated cyber-security into its overall ICT strategy, the process was carried out jointly by the "IT Strategy Headquarters" established within the Cabinet and the "IT Strategy Council," made up of 20 opinion leaders, which was established in order to combine private- and public-sector strengths.¹²⁴ In the United States, the cyber-security strategy is a free-standing document.

Development of the U.S. cyber-security strategy involved a lengthy process of public dialogue, managed by the staff of the National Security Council. The first version of the strategy was issued in 2000. A revised plan was published in draft in the fall of 2002 and in final form in February 2003.¹²⁵ At all stages of the process, the U.S. plans were drafted on the basis of extensive consultations within government and between the government and the private sector. Ten public meetings were held in major cities around the country to gather input on the development of the strategy. Civil society groups, trade associations and

corporations were consulted. Other national cyber strategies include that of Australia.¹²⁶

Other strategy efforts have been undertaken at a regional level. The European Union has developed a cyber-security strategy not in a single document, but rather in a series of Communications and proposals from the Commission and a Council resolution, issued over a period of years.¹²⁷ The Asia Pacific Economic Cooperation (APEC) forum has adopted a regional cyber-security strategy, drafted by the Telecommunications and Information Working Group (TEL) with active participation of the private sector.¹²⁸ The Organization of American States (OAS) has undertaken regional work as well.¹²⁹ In June 2003, the OAS General Assembly approved a resolution calling for development of an inter-American strategy against threats to computer information systems and networks.¹³⁰ The Organization for Economic Cooperation and Development (OECD) has issued a set of Guidelines that constitute a roadmap for governments (and private enterprises) in developing cybersecurity strategies.¹³¹

A consistent set of themes emerges from these national, regional and international cyber-security strategies:

¹²⁴ "e-Japan Priority Policy Program," March 29, 2001, <http://www.kantei.go.jp/foreign/it/network/priority-all/index.html>.

¹²⁵ The final version is The National Strategy to Secure Cyberspace, Feb. 14, 2003:

http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf. The National Strategy to Secure Cyberspace was supplemented by The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, released March 4, 2003, http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf. Both of these documents are implementing components of The National Strategy for Homeland Security, issued by the White House on July 16, 2002.

¹²⁶ E-Security National Agenda [Australia], September 2001

http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm.

¹²⁷ European Commission, Proposal for a Regulation of the European Parliament and of the Council - Establishing the European Network and Information Security Agency, Feb. 11, 2003, COM(2003) 63 final, 2003/0032 (COD),

http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf; Council of the European Union, Council Resolution of 28

January 2002 on a common approach and specific actions in the area of network and information security, (2002/C 43/02),

http://www.europa.eu.int/information_society/eeurope/action_plan/safe/netsecres_en.pdf; European Commission, Proposal for a Council Framework

Decision on attacks against information systems, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf;

European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach, June 6, 2001, COM (2001) 298 final, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm;

European Commission, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee on the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Jan. 26, 2001, COM(2000) 890 final, <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>.

¹²⁸ Available at: http://www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html. In October 2002, APEC Ministers underscored the importance of protecting the integrity of APEC's communications and information systems while allowing the free flow of information. In responding to this challenge, they supported the TEL cyber-security strategy and instructed officials to implement it.

http://203.127.220.67/apec/ministerial_statements/annual_ministerial/2002_14th_apec_ministerial.html#policies.

¹²⁹ The OAS's initial work focused on cybercrime. See material compiled at http://www.oas.org/juridico/english/cyber_experts.htm.

¹³⁰ Development of an Inter-American Strategy to Combat Threats to Cybersecurity, AG/RES. 1939 (XXXIII-0/03) (Resolution adopted at the fourth plenary session, held on June 10, 2003)

<http://www.oas.org/main/main.asp?sLang=E&sLink=http://www.oas.org/documents/eng/documents.asp>.

¹³¹ Organization for Economic Cooperation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, July 25, 2002, <http://www.oecd.org/pdf/M00034000/M00034292.pdf>; "Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, DSTI/ICCP/REG(2002)6/FINAL, Jan. 21, 2003, [http://www.ois.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg\(2002\)6-final](http://www.ois.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)6-final).

- **Public-Private Partnership:** Effective cybersecurity requires a public-private partnership.¹³² The private sector has primary responsibility for ensuring the security of its systems and networks.
- **Public Awareness:** “Participants in a network, whether as developer, owner, operator, or individual user, must be aware of the threats to and vulnerabilities of the network and assume responsibility for protecting that network according to their position and role.”¹³³
- **Best Practices, Guidelines and International Standards:** Cybersecurity should be based on the growing number of voluntary, consensus-based standards and best practices being developed through international standards bodies and cooperative institutions. These standards are crucial guides to governments’ internal policies. Governments need not and should not mandate technical standards for the private sector.¹³⁴
- **Information Sharing:** It is widely recognized that cyber-security efforts have been hampered by system operators’ reluctance to disclose vulnerabilities and attacks. Sharing of information should be encouraged among private sector entities, between the private sector and the government, and internationally.
- **Training and Education:** The APEC Strategy states, “The development of the human resources is critical to the success of efforts to improve security. In order to achieve cybersecurity, governments and corporations must have personnel trained in the complex technical and legal issues raised by cybercrime and critical infrastructure protection.
- **Respect for Privacy:** ICT networks transmit and store communications and personal information of the most sensitive character. Privacy is a crucial component of trust in cyberspace and cybersecurity strategies must be implemented in ways compatible with the essential values of a democratic society.¹³⁵
- **Vulnerability Assessment, Warning and Response:** As the APEC strategy puts it: “Successfully combating cybercrime and protecting information infrastructures depends upon economies having in place systems for evaluating threats and vulnerabilities and issuing required warnings and patches. By identifying and sharing information on a threat before it causes widespread harm, networks...can be better protected.”¹³⁶ The United States Strategy calls for the creation of a National Cyberspace Security Response System to rapidly identify attacks on computer networks.

¹³⁰ Development of an Inter-American Strategy to Combat Threats to Cybersecurity, AG/RES. 1939 (XXXIII-0/03) (Resolution adopted at the fourth plenary session, held on June 10, 2003)

<http://www.oas.org/main/main.asp?sLang=E&sLink=http://www.oas.org/documents/eng/documents.asp>.

¹³¹ Organization for Economic Cooperation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, July 25, 2002, <http://www.oecd.org/pdf/M00034000/M00034292.pdf>; “Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,” Organization for Economic Cooperation and Development, Working Party on Information Security and Privacy, DSTI/ICCP/REG(2002)6/FINAL, Jan. 21, 2003, [http://www.oalis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg\(2002\)6-final](http://www.oalis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)6-final).

¹³² See, e.g., APEC, “Statement on the Security of Information and Communications Infrastructure,” Fifth APEC Ministerial Meeting on Telecommunications and Information Industry, Shanghai, China, May 29-30, 2002, http://www.apecsec.org.sg/virtualib/minismtg/telminAnnexB_SICI.html. Canada’s *National Critical Infrastructure Assurance Program Discussion Paper* emphasizes public/private sector interaction and cooperation.

http://www.ocipep.gc.ca/critical/nciap/disc_e.asp (Draft), Nov. 1, 2002. Article 7 of Japan’s Basic Law on the Formation of an Advanced Information and Telecommunications Network Society specifies that the private sector is to take the lead in forming an advanced information and telecommunications network, with the state and local governments implementing supportive measures to ensure the private sector can exert its full potential. Basic Law on the Formation of an Advanced Information and Telecommunications Network Society, Law No. 144 of 2000, Nov. 2000, http://www.kantei.go.jp/foreign/it/it_basicalaw/it_basicalaw.html.

¹³³ APEC Cybersecurity Strategy, http://www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html. See also, Council of the European Union, *Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security*, (2002/C 43/02), http://www.europa.eu.int/information_society/eeurope/action_plan/safe/netsecres_en.pdf. Awareness is a major theme as well of the OECD guidelines and the work of the G8.

¹³⁴ For example, while the U.S. strategy addresses both government systems and privately owned and operated infrastructures, it concludes that the government should not dictate security standards for private sector systems. *The National Strategy to Secure Cyberspace*, February 2003, pp. 11, 15, <http://www.whitehouse.gov/pcipb/>; http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

¹³⁵ Principle 5 of the OECD Guidelines is “Democracy.” *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, July 25, 2002, <http://www.oecd.org/pdf/M00034000/M00034292.pdf>. Protection of privacy and civil liberties is a guiding principle of the U.S. strategy. *The National Strategy to Secure Cyberspace* [United States], February 2003, p. 4, <http://www.whitehouse.gov/pcipb/>; http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

¹³⁶ APEC Cybersecurity Strategy, http://www.apecsec.org.sg/content/apec/apec_groups/working_groups/telecommunications_and_information.html.

- **International Cooperation:** Governments should work together to develop compatible cybercrime laws and law enforcement cooperation and should work through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting promoting a global “culture of security.”¹³⁷

The process of developing and implementing a cyber-security strategy for a government has many of the same elements as the development and implementation of a computer security program for a corporate enterprise:

- Assess vulnerabilities.
- Raise awareness.
- Designate program leadership to serve as policy coordinator and for oversight.
- Develop a risk management program.
- Adopt appropriate security guidelines.
- Structure accountability.
- Periodically reassess and continuously improve.

The fourth phase (focusing for the moment on the security of government systems) is the promulgation of guidelines or the enactment of any necessary laws addressing cyber-security issues. Some countries, such as Japan and Italy, have approached this issue through guidelines. In July 2000, the IT Security Promotion Committee at the Cabinet level issued “Guidelines for IT Security Policy,” requiring all offices and ministries by FY2003 to implement an assessment of IT security policies and to take other steps to raise the level of security. In March 2001, Japan’s Inter-Ministerial Council for Promoting the Digitization of Public Administration issued security guidelines for all IT government procurements.¹³⁸ In the United States, where the Congress concluded that the Executive Branch was not adequately improving the security of

government computer systems, Congress adopted the Federal Information Security Management Act (FISMA) of 2002, strengthening requirements and oversight mechanisms within the federal government.¹³⁹ A similar approach has been followed in Tunisia, where the government in 2002 adopted security regulations that require government agencies to perform an annual security audit of their computer systems.

Structuring Responsibility: Implementing a Cyber-Security Strategy for Government Systems – The U.S. Approach

In the United States, policy for addressing the security of the federal government’s own information systems is defined in greater detail and implemented through the Federal Information Security Management Act, adopted in 2002.¹⁴⁰ The law illustrates some of the ways in which accountability can be built into implementation of cyber-security across multiple agencies.

The stated purpose of FISMA is to provide government-wide management and oversight of computer security, including coordination of information security efforts throughout the civilian, national security, and law enforcement agencies, and to provide for the development and maintenance of minimum controls required to protect government information systems. The law acknowledges that commercially developed products offer dynamic and effective computer security solutions for the government. It leaves to individual agencies the selection of specific technical hardware and software security solutions from among commercially developed products.

FISMA requires the head of each agency to develop, document, and implement an agency-wide Information Security Program for the information systems that support the operations of the agency, including those provided or managed by contractors.¹⁴¹ The program must include:

¹³⁷ International cooperation has been a major theme of the G8, see Presidents’ Summary: Meeting of G8 Ministers of Justice and Home Affairs, Paris, May 5, 2003, <http://www.g8.utoronto.ca/justice/justice030505.htm>, and of the OECD as well.

¹³⁸ <http://www.kantei.go.jp/foreign/it/network/priority-all/7.html>. Italy’s Minister for Innovation and technologies issued “The government’s guidelines for the development of the information society” in June 2002.

http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf. The audit office of New South Wales, Australia has issued a checklist for governments called “Implementing e-Government - Being Ready,” <http://www.audit.nsw.gov.au/guides-bp/e-govt-BPG.pdf>, which includes a chapter on security.

¹³⁹ Federal Information Security Management Act, Title III of the E-Government Act of 2002, Pub. Law 107-347, <http://csrc.nist.gov/policies/FISMA-final.pdf>. FISMA is discussed further below.

¹⁴⁰ Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347, <http://csrc.nist.gov/policies/FISMA-final.pdf> and <http://www.fedcirc.gov/library/legislation/FISMA.html>. Parts of FISMA are codified in Titles 40 and 44 of the United States Code.

¹⁴¹ Title 44, United States Code, section 3544.

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems.
- Policies and procedures that:
 - o are based on the risk assessments;
 - o cost-effectively reduce information security risks;
 - o ensure that information security is addressed throughout the life cycle of each agency information system; and
 - o ensure compliance with OMB requirements and security standards.
- Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.
- Security awareness training for agency personnel, contractors, and other users of information systems that support the operations of the agency.
- Periodic testing and evaluation (not less than annually) of the effectiveness of information security policies, procedures and practices, which includes testing of management, operational, and technical controls.
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Procedures for detecting, reporting, and responding to security incidents.
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Each agency is required to submit an annual report to the Director of the Office of Management and Budget (OMB, part of the Executive Office of the President) and to Congressional committees on the adequacy and effectiveness of information security policies, procedures and

practices and on compliance with each element of the required agency-wide Information Security Program. Additionally, the adequacy and effectiveness of information security policies, procedures, and practices must be addressed in a number of other plans and reports, including those relating to annual agency budgets, program performance, financial management, and internal accounting and administrative controls. Any deficiencies in policies, procedures, and practices that are identified must be reported to OMB and the Congress.¹⁴²

Annually, each agency must have an independent security evaluation performed to determine the effectiveness of its information security program and practices. Each evaluation must include testing of the effectiveness of information security policies, procedures and practices of a representative subset of the agency's information systems, and an assessment of compliance with relevant information security policies, procedures, standards, and guidelines.¹⁴³

FISMA requires the Director of OMB to oversee the development and implementation of all information security policies and practices. FISMA also vests authority in the National Institute of Science and Technology to develop standards and guidelines for minimum information security requirements¹⁴⁴ and requires the Director of OMB to oversee agency compliance with these requirements and to review at least annually agency information security programs. The OMB Director is charged with reporting annually to Congress on the agencies' performance.¹⁴⁵

¹⁴² Id.

¹⁴³ Title 44, United States Code, section 3545.

¹⁴⁴ Title 40, United States Code, section 11331.

¹⁴⁵ Title 44, United States Code, section 3543.

CHAPTER 3. THE ROLE OF LAW AND GOVERNMENT POLICY VIS-À-VIS THE PRIVATE SECTOR

Traditional Legal Responsibilities Translated to Cyberspace

Businesses have an incentive to maintain the security of their information systems because their profitability depends on it. In a variety of ways, if a company does not protect itself against cyber failures, it could suffer losses that directly affect its profitability. Cyber-security breaches can result in substantial interruption of a company's business and tarnish its reputation. An attack on a corporation's computer network may shut down operations or result in damage to or loss of information such as customer data or trade secrets. Any company that fails to provide security may lose customers to competitors that do take security seriously. If makers of computers and software build insecure products, they risk losing customers.

In addition to pure market forces, many legal principles can create incentives for cyber-security.¹⁴⁶ Corporations are subject to a web of legal responsibilities arising from traditional concepts of corporation or company law, contracts, and civil liability for intentional or negligent infliction of loss, to name a few. Corporations are also subject to relatively more modern regulatory obligations related to the registration and sale of securities on public exchanges and to unfair and deceptive trade practices, for example. Increasingly, attention is being given to how these traditional legal responsibilities might apply to cyber-security issues. Regulatory agencies are already determining by rulemaking or case-by-case adjudication that regulatory systems of fair trade or public disclosure apply to computer security issues as well as traditional misconduct or vulnerabilities. In legal systems where judges have authority to extend general legal concepts to new situations, judges could resolve lawsuits involving cyber-security by deciding that a traditional legal concept (such as negligence or the duties of contractual performance) applies to computer failures.

While this area of the law is barely emerging even in developed countries, part of the legal and policy debate in any nation concerning cyber-security should include consideration of how traditional legal concepts apply to the risks and responsibilities of computer security.

In this section, we discuss the ways in which legal policies of general applicability are being extended to cyber-security. In Chapter 4, we discuss governmental policies that are specifically designed to promote cyber-security in the private sector.

Laws Regarding Corporate Governance, the Registration and Sale of Corporate Securities, and Accounting

Under company/corporate law, an entity's officers and directors may have a fiduciary obligation to the corporation and its shareholders to use reasonable care in overseeing the corporation's business operations. Increasingly, it is being recognized that this duty extends to matters of computer security. Some writers have noted that where corporate officers and directors are negligent in failing to take appropriate steps to assess the threat of cyber-security breaches and to insist that management protect the corporation accordingly, the directors may be liable for damages in lawsuits brought by shareholders.¹⁴⁷

In the United States, this kind of legal obligation, arising from general rules of corporate law (promulgated at the state level), has been strengthened by federal statutory obligations. The Sarbanes-Oxley Act of 2002 imposes a number of new requirements on the sale of corporate securities, prompted in large part by accounting scandals. Congress determined that cyber-security had become vital to the soundness of a corporation's financial data. Therefore, Congress included a requirement that a corporation's auditors publicly attest to the security of the corporations' information systems.¹⁴⁸

¹⁴⁶ See the excellent article by Thomas J. Smedinghoff, "The Developing U.S. Legal Standard for Cyber-security," Baker & McKenzie, Chicago (May 3, 2003), <http://www.bmck.com/ecommerce/us%20cyber-security%20standards.pdf>

¹⁴⁷ Benjamin Wright, "The Legal Risks of Computer Pests and Hacker Tools," *Password* (the ISSA Magazine), Feb. 2002, http://www.tecmetrics.com/legal_risks.htm.

¹⁴⁸ Sarbanes-Oxley Act of 2002, Pub. Law 107-204.

Also under the law in various companies, publicly traded corporations must undergo annual financial audits by independent accounts. As accountants recognize that cyber-vulnerabilities may threaten the financial viability of a company, accountants increasingly including cyber-security in the scope of their audits. A number of organizations have developed standards or guidelines for use by auditors.¹⁴⁹

Contract Law

Businesses may also have a responsibility under contract law to protect the data of their customers from unauthorized access or destruction resulting from a cyber-security breach. Applying basic contract law principles in the cyber context, a company that represents that its system is secure, whether in a service contract or a privacy and security promise appearing on its website, could arguably be deemed to have entered into an agreement with a customer who has agreed to the contract or has proceeded to interact with the company in reliance on those assurances.¹⁵⁰ This company may be subject to claims for breach of contract if the security of customer information is compromised in a cyber attack. Companies that offer web-based services may also have contractual responsibilities to consumers to maintain the availability of these services. If a site is rendered inoperable by a denial of service attack, the company may be subject to customer claims for breach of contract.¹⁵¹

Tort Law

Theoretically, the legal doctrine of torts (civil liability for the intentional or negligent causing of injury) could have application to various kinds of computer security failures.¹⁵² For example, applying traditional tort theory to the cyber context, if a company fails to take reasonable measures to protect a customer's information from unauthorized disclosure as a result of a cyber-attack,

the company could be subject to a claim for negligence. Where a company's computers are used to launch a cyber attack against a third party, there may be potential for tort liability if the company failed to take widely-accepted measures to prevent its computers from being hijacked. Where an attack is launched by a company employee, victims may be able to obtain relief by showing that the defendant company engaged in negligent hiring or supervisory practices.¹⁵³

For now, this is an area of the law that remains undeveloped, even in the United States, where tort lawsuits are common for a wide range of injuries. So far, courts have not held that there is a general legal duty to maintain one's network secure. However, it may be just a matter of time before traditional theories of liability are applied to the field of computer security. At such time, courts could find the standard of care for computer security in industry "best practices," guides and manuals issued by regulators or trade associations, and standards adopted by self-regulatory bodies.¹⁵⁴

¹⁴⁹ See, e.g., the Information Systems Audit and Control Association, <http://www.isaca.org>.

¹⁵⁰ See, e.g., Michael Nugent, *It Can't Happen Here*, Wall Street Technology Association, Ticker, A Technology Magazine For Industry Profession (2003) (Nugent), http://www.wsta.org/publications/articles/0402_article03.html.

¹⁵¹ Id.

¹⁵² Margaret Jane Radin, "Distributed Denial of Service Attacks: Who Pays?", http://www.mazunetworks.com/white_papers/radin-print.html; Sarah Scalet, "See You in Court," CIO Magazine, Nov. 1, 2001, http://www.cio.com/archive/110101/court_content.html.

¹⁵³ Id., Michael Nugent, *It Can't Happen Here*, Wall Street Technology Association, Ticker, A Technology Magazine For Industry Profession (2003), http://www.wsta.org/publications/articles/0402_article03.html.

¹⁵⁴ As is made clear throughout this handbook, there is a growing body widely accepted computer security standards, ranging from the Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems to the information security standards adopted by non-governmental standards bodies. See, e.g., Nugent, *supra* note ____ (43).

CHAPTER 4. GOVERNMENT CYBER-SECURITY POLICIES

Increasingly, governments are recognizing that they need to adopt policies that specifically address the issue of computer security in the private sector. This may include the adoption of legislation imposing certain duties on private sector corporations. Experience has shown that tailoring the level of regulatory intervention to the particular facts and circumstances at hand is a key ingredient to successful regulation.¹⁵⁵ With this caution in mind, governments are beginning to impose duties on private sector, without mandating particular technologies or standards. In Europe, responsibility for computer security is imposed across all sectors by the Data Protection Directive.¹⁵⁶ In Singapore, the government has made computer security a component of the regulatory requirements for the financial sector, broadly defined. In the United States, in recent years, federal legislation has been adopted imposing explicit computer security responsibilities on the banking industry and the health care industry.¹⁵⁷ We discuss these more fully below, but first we emphasize some of the important roles the government can play vis-à-vis the private sector without regulation.

Non-regulatory Roles of Government

There are a number of ways in which government can directly influence the security of privately owned and operated computer systems. Not all of these policy options are regulatory; many of the most effective options may be non-regulatory in nature.

Research: An important role for the government is in conducting and funding research on computer security. The U.S. National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the

U.S. Commerce Department. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

NIST's Computer Security Division works to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities, and protection requirements;
- Researching, studying, and advising agencies about IT vulnerabilities;
- Devising techniques for the cost-effective security of sensitive Federal systems;
- Developing standards, metrics, tests, and validation programs to promote, measure, and validate security in systems and services;
- Establishing minimum security requirements for Federal systems; and
- Developing guidance to increase secure IT planning, implementation, management and operation.¹⁵⁸

In sharing research publicly, government agencies may need to overcome a tradition of secrecy. The normally super-secret National Security Agency in the United States has posted on its public web site its Security Recommendation guides.¹⁵⁹

Standards: The government is also an important participant in private sector standards setting processes. Standards processes are non-regulatory, voluntary, and consensus-based, but government experts may make important contributions, especially if the government supports its own computer security research.

Awareness, Education, and Capacity-Building:

Another major non-regulatory role of the government is to educate the public and work with the private sector to promote awareness of vulnerabilities and

¹⁵⁵ See, Smedinghoff, *supra* note ____ (39).

¹⁵⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281/31, Nov. 23, 1995, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett.

¹⁵⁷ Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, <http://aspe.hhs.gov/admsimp/pl104191.htm>; Financial Services Modernization Act of 1999, Pub. Law 106-102, Nov. 12, 1999, 15 U.S.C. Section 6801 *et seq.*, <http://www4.law.cornell.edu/uscode/15/6801.html>; <http://www.ftc.gov/privacy/glbact/>.

¹⁵⁸ NIST's Computer Security Resource Center (CSRC) publishes information on a broad range of security topics, including cryptographic standards and applications, security testing, security research, system certification and accreditation guidelines, return on security investments, small business computer security, and federal agency security practices. <http://csrc.nist.gov/>. NIST publications are available at <http://csrc.nist.gov/publications/index.html>.

¹⁵⁹ National Security Agency, Security Recommendation Guides, <http://nsa1.www.conxion.com/>.

responses.¹⁶⁰ Special studies and reports of the kind described above are one means of accomplishing this goal. The European Commission has called on Member States to launch public education and awareness campaigns, including mass media and efforts targeted at all stakeholders. Convening of expert bodies and issuance of reports and strategy documents help raise awareness. Education also includes scholarship and human resources development programs. The European Commission has recommended that education systems of Member States should give more emphasis to courses focused on computer security.

Information Sharing: Another important government role is to promote information sharing about computer security vulnerabilities, warnings of new viruses and attacks, and recommendations on solutions, patches, and best practices.¹⁶¹ The government may fund such information sharing centers, such as the CERT (Computer Emergency Response Team) coordination centers that are being established around the globe. For example, the U.S. CERT at Carnegie Mellon University is a federally funded research and development center that provides assistance in handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing security information and training materials.¹⁶² Other countries that have established or are establishing CERT centers include Malaysia, Japan, Australia, and Korea. Mcert is a CERT for small and medium sized enterprises in Germany, created as a public-private partnership by Germany's ICT Association BITKOM,

seven industry sponsors and the German Government. Multinational structures are being created to promote information sharing regionally and internationally. In June 2001, the European Commission issued a Communication calling for a strengthening of the CERT system in Europe and better coordination among the CERTs operating in Member States.¹⁶³ In February 2003, the Commission took a further step, announcing its intent to establish a Network and Information Security Agency to build on national efforts regarding cybersecurity and to serve as a coordinating and advisory entity.¹⁶⁴ APEC has launched an initiative for a regional CERT aimed at providing in-country training to enhance CERT capabilities in developing countries in the region and to develop CERT guidelines.¹⁶⁵ The G8 has created a network of "24x7 contacts" – round-the-clock duty offices at law enforcement agencies to facilitate information sharing and cooperation in criminal investigations of cybercrimes. Non-G8 nations may participate¹⁶⁶.

Alternatively, the government may promote the creation of privately funded, voluntary information sharing systems, such as the Information Sharing and Analysis Centers (ISACs) that are operating in various forms around the globe. For instance, the United States has established industry ISACs for certain sectors (such as the financial services sector, the telecommunications sector, and the electrical power industry), and other countries, such as Canada, Germany, Japan, and the Netherlands, have ISACs as well. The UK is pursuing the WARP Concept (Warning, Advice & Reporting Point), an initiative to establish a 'network' across the UK to

¹⁶⁰ Awareness is the first principle in the OECD's computer security guidelines. Organization for Economic Cooperation and Development, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, July 25, 2002, <http://www.oecd.org/pdf/M00034000/M00034292.pdf>. The G8 has recommended that countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructure, and the role each must play in protecting them. In addition, the G8 has recommended that countries conduct training to enhance their response capabilities. Presidents' Summary: Meeting of G8 Ministers of Justice and Home Affairs, Paris, May 5, 2003, <http://www.g8.utoronto.ca/justice/justice030505.htm>.

¹⁶¹ Information sharing has been a major theme of most international initiatives, including those of the G8, OAS and APEC. ¹⁵⁸ NIST's Computer Security Resource Center (CSRC) publishes information on a broad range of security topics, including cryptographic standards and applications, security testing, security research, system certification and accreditation guidelines, return on security investments, small business computer security, and federal agency security practices. <http://csrc.nist.gov/>. NIST publications are available at <http://csrc.nist.gov/publications/index.html>.

¹⁶² National Security Agency, Security Recommendation Guides, <http://nsa1.www.conxion.com/>.

¹⁶³ European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach, June 6, 2001, COM(2001) 298 final, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm. ¹⁶¹ Information sharing has been a major theme of most international initiatives, including those of the G8, OAS and APEC.

¹⁶⁴ European Commission, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Network and Information Security Agency, Feb. 11, 2003, COM(2003) 63 final, 2003/0032 (COD), http://europa.eu.int/information_society/eeurope/action_plan/safe/documents/nisa_en.pdf.

¹⁶⁵ "Protecting Developing Economies from Cyber Attack – Assistance to Build Regional Cyber-security Preparedness," APEC Media Release, Mar. 18, 2003, http://www.apecsec.org.sg/whatsnew/press/PressRel_ProtectgFromCyberAttack_180303.html.

¹⁶⁶ G8, Meeting of Justice and Interior Ministers - Action Plan, Dec. 10, 1997, <http://birmingham.g8summit.gov.uk/prebham/washington.1297.shtml>.

provide better and more timely advice and warnings relating to electronic attack, and for receiving incident reports.

The government may also form public-private committees or fora for exchange of security-related information. An example is the U.S. National Security Telecommunications Advisory Committee (NSTAC), which is composed of 30 chief executives representing major communications and network service providers and information technology companies and government officials responsible for national security and emergency communications systems.¹⁶⁷ NSTAC provides industry-based advice to the President on issues and problems related to implementing national security and emergency preparedness communications policy.

Criminal Law

Another way in which the government protects private systems is through the criminal law. International and regional institutions have recommended that every nation, as part of the legal framework promoting trust and confidence in cyberspace, should adopt basic criminal laws against activities that attack the confidentiality, integrity, or availability of computer data and computer systems.¹⁶⁸ The framework of applicable criminal law comprises both substantive as well as procedural law, implicating search and seizure as well as privacy concepts that may have unique application in the cyber context.

The UN was perhaps the first international body to recognize the importance of addressing cybercrime.¹⁶⁹ In December 2000 and January 2002, the UN General Assembly adopted Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of *Information Technologies*.¹⁷⁰ Resolution 55/63 declares that states should review their laws to eliminate “safe havens” for those who carry out cybercrime. Resolution 55/63 recommends, *inter alia*, that states take appropriate measures to prevent the criminal misuse of information technologies, international cooperation in investigation

and enforcement efforts, and the preservation and timely sharing of electronic data and evidence. Resolution 55/63 also recommends educating law enforcement authorities and the general public on cybercrime issues.

Substantive Criminal Law Offenses

There are various ways to conceptualize cybercrimes, and various names exist for specific offenses, but in general, laws addressing cybercrime issues have crystallized around four kinds of activity:

- **Data interception:** intentional interception, without right, of non-public transmissions of computer data. This covers interception of email of another person, for example, and is aimed at protecting the confidentiality of communications. Some legal frameworks already make it a crime to intercept telephone conversations without legal authorization, for example. This well-known concept in the telecom world could have analogous application in the cyber context.
- **Data interference:** intentional damage to, deletion, degradation, alteration, or suppression of data in someone else's computer without right. This covers, for example, intentionally sending viruses that delete files, or hacking a computer and changing or deleting data, or hacking a web site and changing its appearance. The element of intent is important to distinguish criminal activity from mere production of defective software or unintentionally forwarding viruses .
- **System interference:** intentionally causing serious hindrance, without right, to the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. This covers things like denial of service attacks or introducing viruses into a system in ways that interfere with its normal usage. “Serious harm” is an element of this offense that distinguishes criminal activity from other, ordinary online behavior, such as sending one or just a few unsolicited emails.

¹⁶⁷ See <http://www.ncs.gov/NSTAC/attf.html>

¹⁶⁸ International bodies recommending adoption of cybercrime laws include the UN, EU, COE, G8, APEC, and OAS. For an extended discussion of the activities and recommendations of these and other international bodies regarding cybercrime, see, Westby Guide, *supra* note ____.

¹⁶⁹ In 1995, the UN issued under its International Review of Criminal Policy the *United Nations Manual on the Prevention and Control of Computer-Related Crime* (1995) <http://www.uncjin.org/Documents/EighthCongress.html>.

¹⁷⁰ UN General Assembly, Resolution 55/63, Combating the criminal misuse of information technologies, Dec. 4, 2000, http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf ; UN General Assembly, Resolution 56/121, *Combating the criminal misuse of information technologies*, Jan. 23, 2002, http://www.unodc.org/pdf/crime/a_res_56/121e.pdf . See also UN Resolution 57/239 (2002).

- **Illegal access:** intentionally accessing, without right, the computer system of another. It can be thought of as the cyberspace equivalent of trespass. (Looked at another way, illegal access is an offense against the confidentiality of stored data and therefore is analogous to illegal interception, which is an offense against the confidentiality of data in transit.) In some legal systems, the definition of the crime of illegal access is limited to situations in which confidential information (medical or financial information) is taken, copied or viewed or where there is an intent to obtain confidential information or where access is obtained only by defeating security measures.

The Council of Europe has adopted a Convention that addresses these points.¹⁷¹

Articles 2-5 of the Council of Europe Convention on Cybercrime address these four basic cybercrimes. However, in the Convention itself these provisions are drafted in broad terms that could cover a wide range of common behavior. The Convention also has an Explanatory Report that aids in interpreting the Convention. Article 2 of the Convention calls upon states to establish as a criminal offense “when committed intentionally, the access to the whole or any part of a computer system *without right*” (emphasis added). On its face, this provision could arguably make it a crime to send an unsolicited email, since the sender of an unsolicited email “accesses” the recipient’s computer (or the mail server of the recipient’s ISP) without right. Nations following the Therefore it is key in interpreting the Council of Europe Convention on Cybercrime to clarify whether “without right” is meant to include common activities inherent in the Internet. The Explanatory Report states, “legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized.” (Para. 38.)

These would include, for example, sending electronic mail without it having been first solicited by the recipient; accessing a web page, directly or through hypertext links; or using “cookies” or “bots” to collect information. (Para. 46, 48.)¹⁷²

Computer-facilitated Crime

Discussions of computer crime often extend into activities that are not crimes against computers, but are crimes *facilitated* by the use of computers. For example, theft and fraud are crimes in virtually every legal system whose laws were crafted in the “offline” world. But theft and fraud can equally take place in the “on-line” world. Similarly, crimes such as infringement of intellectual property rights or dissemination of child pornography, also are not limited to computer crimes – but they are crimes that may be facilitated by use of a computer. In many cases, existing criminal sanctions apply to offenses committed online. A critical analysis of a multiplicity of factors would need to be taken into account to assess not only whether existing criminal laws apply both online and offline, but also whether special, separate offenses for computer-related crime or crime facilitated by a computer would be necessary.

Articles 7-10 of the Council of Europe Convention on Cybercrime depart from this principle, and reach more broadly, covering crimes involving the use of a computer to engage in conduct that is normally already a crime offline (i.e., forgery, fraud, and the distribution, production or possession of child pornography, and copyright infringement to name a few). Adopting special provisions for computer-facilitated offenses may be unnecessary in some legal systems and might improperly suggest that a crime committed online is worse than the same crime committed offline.¹⁷³

¹⁷¹ The treaty, ETS no. 185, is online at <http://conventions.coe.int/treaty/EN/cadreprincipal.htm> along with an extensive Explanatory Report. It is very important that nations looking to the convention as a model also carefully consider the Explanatory Report, which has extensive explanations of the meaning of the treaty’s sometimes cryptic provisions. The convention, which has not taken effect as of August 2003, has some positive and some negative elements. The convention is very broad, reaching far beyond computer crime as such. And while it requires signatories to adopt laws giving the government access to computer data (for all crimes) and while it states that such powers must be subject to procedural safeguards protecting privacy, the treaty fails to specify such procedural safeguards. Accordingly, developing countries should be cautious in approaching the Council of Europe convention as a model. A major section of the treaty aims to require governments to cooperate with other countries seeking to search and seize computers, compel disclosure of data stored in computers, and carry out real-time interceptions – in all kinds of criminal cases – in other countries. It also covers extradition for computer crimes as defined under the treaty.

¹⁷² Further point of caution: the Explanatory Report also states that the phrase “without right” may refer to conduct undertaken without contractual authority. This interpretation seems unwise, for it could make violations of a service provider’s terms of service into a criminal offense.

¹⁷³ That said, child pornography, which is internationally condemned, is easily facilitated by computers and governments should be sure that their laws adequately prohibit the production and dissemination of such material, lest they become havens for its production or online hosting. Likewise, protection of intellectual property is one of the important building blocks of cyberlaw.

Application of basic criminal law concepts

Nations may also want to consider how common concepts of the criminal law such as “aiding and abetting” or “attempt” apply to cybercrime. Thus, if a law has the concept of an attempted offense, then that concept might apply to cybercrime. For example, launching a virus with intent to disrupt service might be a crime under the concept of intent even if the virus didn’t work as intended. Similarly, if a nation’s law has the concept of aiding and abetting, that might be applied to cyber-crime, such that one who intentionally produces a virus and provides it to another knowing or intending that it will be used to destroy data or interfere with a system may be guilty of data or network interference caused by the virus even if the virus was introduced into a network by someone else.

Privacy Protections

Consideration of cybercrime often leads to questions about the standards under which the government is authorized to obtain access to the electronic communications and computer data that may constitute evidence of cybercrime and other types of crime. Many countries have procedural laws granting the government investigative powers to access information stored in computers. These include judicial orders for the disclosure of stored data and warrants for the immediate search and seizure of computers and computerized data. Many countries also allow real-time interception of communications and the traffic data or transactional data that shows the origin and destination of communications. A major part of the Council of Europe Convention on Cybercrime requires governments to adopt laws on search and seizure of computer evidence, disclosure to governments of computerized records of any kind, and electronic interception of communications – for all kinds of crimes.

Government seizures or compelled disclosures of data stored in computers and government interceptions of communications and traffic data constitute an intrusion on personal privacy and therefore need to be subject to procedural safeguards.¹⁷⁴ As the OECD states in its Guidelines for the Security of Information Systems and Networks, “Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.”¹⁷⁵ The European Commission has stated, “Protection of privacy is a key policy objective in the European Union. It was recognized as a basic right under Article 8 of the European Convention on human rights. Articles 7 and 8 of the Charter of Fundamental Rights of the EU also provide the right to respect for family and private life, home and communications and personal data.”¹⁷⁶ Especially in developing and transitional societies, unregulated government surveillance can seriously undermine trust in the Internet.

UN Resolution 55/63 (December 2000) provides that states, as they adopt laws regarding investigative access to communications and computer data, should protect individual freedoms and privacy. In 1990, the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders issued a series of recommendations concerning the adoption of investigative procedures, evidentiary rules, forfeiture, and international cooperation in cyber-crime investigations.¹⁷⁷ In 1995, the UN published its *Manual on the Prevention and Control of Computer-Related Crime*.¹⁷⁸ This extensive document examines a wide range of issues related to crime and technology, including procedural law, substantive criminal law, international cooperation, data protection, security, and privacy.

¹⁷⁴ The right to privacy is recognized as a fundamental human right under the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights.

¹⁷⁵ http://www.oecd.org/document/42/0,2340,en_2649_201185_15582250_1_1_1_1,00.html

¹⁷⁶ European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach*, June 6, 2001, COM (2001) 298 final, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm.

¹⁷⁷ *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Havana, Aug. 27-Sept. 7, 1990, report prepared by the Secretariat, UN publication, Sales No. E.91.IV.2, chap I. For the text of these recommendations, see United Nations Commission on Crime Prevention and Criminal Justice, Report on the Eighth Session, Apr. 27-May 6, 1999, E/CN.15/1999/12, <http://www.un.org/documents/ecosoc/docs/1999/e1999-30.htm>.

¹⁷⁸ UN, *International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-Related Crime*, <http://www.uncjin.org/Documents/EighthCongress.html>.

¹⁷⁹ Another valuable resource is the report of UN Economic and Social Council’s Commission on Crime Prevention and Criminal Justice effectively summarizes UN and other international work in the cybercrime and cyber-security area. *Effective measures to prevent and control computer-related crime*, E/CN.15/2002/8, Report of the Secretary-General, United Nations, Economic and Social Council, Commission on Crime Prevention and Criminal Justice, Eleventh Session, Vienna, Apr. 16-25, 2002, <http://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf>.

Likewise, the Council of Europe Convention on Cybercrime explicitly requires that interceptions of communications and searches and seizures for stored data be conducted pursuant to the privacy principles set forth in the European Convention on Human Rights. Article 15 of the Cybercrime Convention provides:

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms...and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

Surveillance Standards

The Council of Europe Convention on Cybercrime itself does not spell out specific surveillance procedures that would comply with the European Convention of Human Rights. Those are found instead in the decisions of the European Court of Human Rights (summarized below), as well as in the surveillance laws of countries like Canada and the United States that have strong traditions of an independent judiciary and protection of privacy. Especially in developing and transitional societies, which may not have a fully defined set of rules for searches and seizure and surveillance in the offline world, it is important to give close attention to the development of strong standards for government surveillance in the digital context.

Under most advanced legal systems, interception of electronic communications is permissible, but only in accordance with clear standards in the law, requiring justification and prior independent approval, which in many legal systems means approval by a judge.

Governments addressing interception and data access issues must be sure to address the procedural standards for government access to communications and computer data. An emerging body of international experience provides useful guidance. Based upon developing national and international standards,¹⁸⁰ it is possible to identify the following procedural safeguards regulating the interception of communications:

- The standards for interception are transparent, fully and clearly spelled out in legislation available to the public, with sufficient precision to protect against arbitrary application and so that citizens are aware of the circumstances and conditions under which public authorities are empowered to carry out such surveillance.
- Approval is obtained from an independent official (preferably a judge),¹⁸¹ based on a written application giving reasons and setting forth facts justifying the intrusion, and the approval should be manifested in written order.
- Surveillance is limited only to the investigation of specified serious offenses.
- Approval is granted only upon a strong factual showing of reason to believe that the target of the search is engaged in criminal conduct.
- Approval is granted only when it is shown that other less intrusive techniques will not suffice.
- Each surveillance order should cover only specifically designated persons or accounts – generalized monitoring is not permitted.
- The rules are technology neutral – all one-to-one communications are treated the same, whether they involve voice, fax, images or data, wire line or wireless, digital or analog.
- The scope and length of time of the interception are limited, and in no event is the surveillance extended longer than is necessary to obtain the needed evidence.

¹⁸⁰ Perhaps the most developed body of international law on communications interception can be found in Europe, where the basic privacy principle in Article 8 of the European Convention of Human Rights has been given greater definition by the European Court of Human Rights (ECHR). The principles outlined here are drawn from the case law of the ECHR. *Kopp v. Switzerland*, Mar. 25, 1998, 27 EHRR 91; *Klass v. Germany*, 6 September 1978, 2 EHRR 214; *Khan v. U.K.*, May 12, 2000, Reports of Judgments and Decisions, ECtHR, 2000-V; *Halford v. U.K.*, June 25, 1997, Reports of Judgments and Decisions, ECtHR 1997-III; *Huvig v. France*, Apr. 24, 1990, 12 EHRR 528; *Kruslin v. France*, Apr. 24, 1990, 12 EHRR 547.

¹⁸¹ *Klass v. Germany*, 6 September 1978, 2 EHRR 214 (“The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.”).

- The surveillance is conducted in such a way as to reduce the intrusion on privacy to an unavoidable minimum necessary to obtain the needed evidence.
- The enabling legislation describes the use to which seized or intercepted material could be put; information obtained for criminal investigative purposes may not be used for other ends.
- The law specifies procedures for drawing up summary reports for a judge's review and precautions to be taken in order to permit inspection of the recordings by the judge and by the defense.
- In criminal investigations, all those who have been the subject of interception should be notified after the investigation concludes, whether or not charges results.
- Personal redress is provided for violations of the privacy standards.

Many of the same provisions are also applicable to search and seizure orders for computer data.

Data Retention and Other Government Design Mandates

A number of developed countries (including the United States) have imposed design mandates on telephone common carriers (and, in some countries, ISPs), requiring that communications networks be designed to support government surveillance. In addition, some countries have adopted, or are debating the adoption of, laws requiring service providers to retain traffic data on all communications for a specified period of time (a mandate referred to as "data retention"). These mandates have been very controversial and have been criticized for threatening the privacy of citizens and the security of networks and for imposing considerable costs on service providers. A fuller consideration of design

mandates for surveillance is beyond the scope of this report. However, it should be noted that the Council of Europe Convention on Cybercrime does not impose design mandates, technical standards, or data retention requirements on service providers. The treaty only establishes procedures for preserving, seizing, or accessing whatever data is otherwise available for business purposes, using whatever current technical capabilities companies may have. It does not require changes in technology or business practices.¹⁸² The European Union in 2002 adopted a directive on privacy in the communications sphere that permits but does not require member countries to adopt data retention requirements.¹⁸³

Anonymity

The Council of Europe Convention on Cybercrime also recognizes another important privacy right: the legitimacy of anonymous communications. The Explanatory Report makes it clear that the convention does not impose on service providers any obligation to keep records of their subscribers. Thus, under the Convention, a service provider would not be required to register identity information of users of prepaid cards for telephone service, nor is it obliged to verify the identity of subscribers or to resist the use of pseudonyms by users of its services.¹⁸⁴ In 2003, the Council of Europe issued a Declaration on Freedom of Communication on the Internet in which it expressly stated, "In order to...enhance the free expression of information and ideas, member states should respect the will of users not to disclose their identity."¹⁸⁵ Likewise, the European Commission, in its 2001 Communication on Creating a Safer Information Society, recognized the value of anonymity, stating, "An increasing variety of authentication mechanisms is required to meet our different needs in the environments in which we interact. In some environments, we may need or wish

¹⁸² Articles 20 and 21 of the Council of Europe convention specifically state that the real-time interception laws required under the convention shall empower competent authorities to "compel a service provider, *within its existing technical capability*," to collect or record, or to co-operate and assist the competent authorities in the collection or recording of, traffic data and communications content. The Explanatory Report states: "The article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Para. 221.

¹⁸³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*), Article 4(1), Official Journal L 201/37, July 31, 2002, at 37-47 (replacing EU Directive 97/66/EC),

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett. Also available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

¹⁸⁴ Convention, Para. 181.

¹⁸⁵ Declaration on freedom of communication on the Internet (Strasbourg, 28.05.2003) (Adopted by the Committee of Ministers at the 840th meeting of the Ministers' Deputies) http://www.coe.int/T/E/Communication_and_Research/Press/News/2003/20030528_declaration.asp

to remain anonymous.”¹⁸⁶ Also, in its 2001 Communication on Network and Information Security, the Commission stated, “authentication must also include the possibility for anonymity, as many services do not need to identify the user...”¹⁸⁷

Encryption

Strong encryption is an important tool used in securing the Internet. As the European Commission noted in 2001, “The use of encryption technologies...[is] becoming indispensable, particularly with the growth in wireless access.”¹⁸⁸ Recognizing this, the general trend in national policies regarding cryptography has been to reduce or eliminate rules limiting the import, export, and use of encryption. In recent years, most developed countries, which previously sought to control encryption, have concluded that, on balance, the general availability of encryption will improve security, not interfere with it. The 1997 OECD Guidelines on Cryptography Policy and a 1998 European Commission report expressed strong support for the unrestricted availability of encryption products and services.

Based on these statements, in the late 1990s Canada, Germany, Ireland, and Finland announced national cryptography policies based on the OECD Guidelines, favoring the free use of encryption. France, which had long restricted encryption, reversed that policy in January 1999 and announced that encryption could be used in France without restrictions. In December 1997, Belgium amended its 1994 law to eliminate the provision restricting cryptography. The United States, which had sought to limit use of encryption by limiting trade in cryptographic products and services, lifted almost all restrictions on the export of encryption in 2000.¹⁸⁹

Regulation and Legislation

In a growing number of countries, policymakers are concluding that market forces alone are not sufficient to ensure adequate mitigation of cyber-security risks. As the European Commission has noted, action by governments is required because the market offers imperfect incentives for security: market prices do not always accurately reflect the costs and benefits of investment in security; often neither providers nor users bear all the consequences of inaction; control over the Internet is dispersed and given the complexity of networks, it may be difficult for users to assess potential dangers. Many of the critical infrastructures heavily dependent on computer systems have a long history of regulation in the public interest – regulation of safety, competition, and environmental impact, among other issues. Increasingly, regulators are adding cyber-security to the list of concerns meriting government attention.

Regulation, however, carries risks. In some respects, the Internet has flourished as a relatively unregulated communications medium. The global trend over the past two decades has been towards deregulation of communications networks generally. Competition and innovation supports development of new services and technologies, drives down prices, and expands access to communications technology. When technology is rapidly changing, government regulation may hinder the adoption of innovative security solutions.

So a key question is: what are the best means to achieve the desired results of improved computer security? By and large, as a fundamental principle, government should not impose technology mandates on private sector operators of critical infrastructures. There is widespread recognition that technology mandates are likely to be ineffective and even counterproductive.

¹⁸⁶ European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee on the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, Jan. 26, 2001, COM(2000) 890 final, <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>.

¹⁸⁷ European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach*, June 6, 2001, COM (2001) 298 final, http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm.

¹⁸⁸ European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee on the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, Jan. 26, 2001, COM(2000) 890 final, <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>.

¹⁸⁹ See “Cryptography and Liberty 2000: An International Survey of Encryption Policy,” Electronic Privacy Information Center, <http://www2.epic.org/reports/crypto2000>; see also “Commercial Encryption Export Controls,” Bureau of Industry and Security, U. S. Dep’t of Commerce, <http://www.bxa.doc.gov/Encryption/Default.htm>.

Instead, one approach is to impose a general requirement to protect security. This approach was taken in Europe, growing out of the concept of privacy protection, where a general duty to protect security is imposed on all entities that collect or process personally identifiable data. Another approach is to focus only on certain economic sectors. The United States for example, in imposing privacy obligations on the financial services and health care industries, also imposed a requirement for companies in those sectors to protect the security of personal data. Singapore has also focused on the financial services sector, but not in the context of privacy protection – Singapore’s e-security guidelines for financial services firms grow directly out of security concerns, not privacy concerns. There are also different approaches to translating a general security requirement into specific security steps. One approach for government cyber-security regulation is to address processes, not technologies. Another approach is to develop guidelines. These approaches can be complimentary.

Europe has started by imposing security obligations on all entities that collect and process personal information. Article 17 of the EU Data Protection Directive requires that controllers of personal information take “appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”¹⁹⁰ The Directive further states “such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be processed.” Canada takes a similar approach, requiring in general terms under its Personal Information Protection and Electronic Documents Act that private sector companies take security measures to protect personal information they hold.

The European Union has issued a somewhat more detailed directive specifically addressing obligations regarding the protection of information in the electronic communications industry.¹⁹¹ Article 4 specifies that a provider of electronic communications service providers must take steps to safeguard the security of “its services, as opposed to personal data, if necessary in conjunction with the provider of the public communications network with respect to network security.” Second, providers of publicly available electronic communications must inform subscribers of a particular risk of a breach of security, and “where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.”¹⁹²

How should these general requirements be translated into practice? Singapore offers one model, where the Monetary Authority of Singapore (MAS) has spelled out a comprehensive set of cyber-security recommendations in its Technology Risk Management Guidelines for Financial Institutions.¹⁹³ The guidelines are aimed at promoting sound processes in managing technology risks and the implementation of security practices, but they are not mandatory. Instead, as the guidelines state, “MAS intends to incorporate these guidelines into supervisory expectations for the purpose of assessing the adequacy of technology risk controls and security measures adopted by financial institutions. Each institution can expect that MAS will take a keen interest as to how and what extent it has achieved compliance with these guidelines...Financial institutions are encouraged to use their best endeavors to ensure compliance with these guidelines.”¹⁹⁴ The guidelines are careful to state that they do not affect and should not be regarded as a statement of the standard of care that institutions owe to their customers.¹⁹⁵ An appendix lists security practices for financial institutions, stating that financial institutions “should” adopt the practices.

¹⁹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281/31, Nov. 23, 1995, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett.

¹⁹¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Article 4(1), Official Journal L 201/37, July 31, 2002, at 37-47, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett. Also available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

¹⁹² *Id.* at Article 4(2).

¹⁹³ *Technology Risk Management Guidelines for Financial Institutions*, Monetary Authority of Singapore, Draft Nov. 11, 2002, <http://www.mas.gov.sg/display.cfm?id=94D063CD-5EB6-4636-82B5A725F9F6E9F5>

¹⁹⁴ *Id.*, para. 7.0.1, p. 11.

¹⁹⁵ *Id.* at p. 25.

The practices include the following guidelines:

- Systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of enhancements, updates and patches recommended by system vendors;
- All default passwords for new systems should be changed immediately upon installation as they are mostly known by intruders at large;
- Firewalls should be installed between internal and external networks as well as between geographically separate sites; and
- Anti-virus software should be implemented.¹⁹⁶

The United States has taken a different approach, focusing on processes, not technological practices. Thus, the Financial Services Modernization Act of 1999 (known popularly by its lead sponsors in the Congress as the Gramm-Leach-Bliley Act) recognized that “each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”¹⁹⁷ Under the Act, regulators of financial institution were required to issue regulations for administrative, technical, and physical safeguards for information security.¹⁹⁸ The crucial point is this: the regulations that were issued do not say what the technical components of a safeguards program must be. Instead the regulations leave it up to the businesses to decide what specific security measures are best for them.

Under the Act, the rules issued by the regulatory agencies for the financial services industry require banks to adopt security plans. The rules do not state what technical measures those plans must contain. The security program must:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and
- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risk.¹⁹⁹

Information security programs must be designed to control risks, commensurate with the sensitivity of the information and the complexity and scope of activities. The regulations require that certain fairly broad categories of security measures must be considered and, if appropriate, adopted:

- access controls on customer information systems (authentication and authorization);
- access restrictions at physical locations;
- encryption of electronic customer information;
- change management procedures;
- dual control procedures (segregation of duties and background checks) for employees with access to customer information;
- intrusion monitoring systems;
- intrusion response programs; and
- measures to protect against destruction, loss, or damage of customer information.

Additionally, under the regulations, staff must be trained in the implementation of the security program. Regular testing of the key controls, systems, and procedures must take place, with appropriate adjustments made to account for relevant changes in technology, the sensitivity of customer information, internal or external threats to information, and changing business

¹⁹⁶ Id., Appendix C, p. 21. For further information on financial security, see Thomas Glaessner, Tom Kellermann, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues*, The World Bank, June 2002, [http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/\(attachmentweb\)/E-security-RiskMitigationversion3/\\$FILE/E-security-Risk+Mitigation+version+3.pdf](http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationversion3/$FILE/E-security-Risk+Mitigation+version+3.pdf); Thomas Glaessner, Tom Kellermann, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions—Summary of Recent Research and Global Dialogues*, The World Bank, May 2003, http://www.worldbank.org/wbi/B-SPAN/sub_e-security.htm

¹⁹⁷ Gramm-Leach Bliley Act, Title 15, United States Code, section 6801.

¹⁹⁸ Gramm-Leach Bliley Act, Title 15, United States Code, section 6805.

¹⁹⁹ “Appendix B to Part 570—Interagency Guidelines Establishing Standards for Safeguarding Customer Information,” Part III, <http://www.occ.treas.gov/fr/fedregister/66fr8616.htm>.

²⁰⁰ Id.

arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements²⁰⁰ The rules also require the Boards of Directors of financial institutions to approve their institutions' written security programs and oversee the development, implementation, and maintenance of the program, including assigning specific responsibility for implementation and reviewing reports from management.

Similar rules issued by the Federal Trade Commission require that financial institutions under its purview must develop a plan in which the institution must:

- (1) designate one or more employees to coordinate the safeguards;
- (2) identify and assess the risks to customers information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- (3) design and implement a safeguards program, and regularly monitor and test it;
- (4) select appropriate service providers and contract with them to implement safeguards; and
- (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firms business arrangements or operations, or the results of testing and monitoring of safeguards.²⁰¹

A similar approach can be seen in the United States' Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires healthcare institutions to institute security measures to ensure patient information that is stored electronically remains confidential and free from unauthorized access. The security rule adopted under the Act requires the maintenance of reasonable and appropriate administrative, physical, and technical safeguards to protect the integrity and confidentiality of personal medical information and to protect against reasonably anticipated threats or hazards to the security or integrity of medical data or its unauthorized use or disclosure.²⁰³ The rule applies to data both while in storage and in transit. It has 28 "standards" and 41

"implementation specifications."²⁰⁴ It states that security practices should take into account technical capabilities of record systems, costs of security measures, the need for personnel training, and the value of audit trails in computerized record systems. The security rule identifies safeguards that are "required" and those that are "addressable."

The core principles of the Security Rule require covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not required under the Security Rule.
- Ensure compliance with the Security Rule by its workforce.²⁰⁵

The Rule, however, allows flexibility:

- Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications.
- In deciding which security measures to use, a covered entity must take into account the following factors:
 - (i) The size, complexity, and capabilities of the covered entity.
 - (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

²⁰¹ See "Financial Institutions and Customer Data: Complying with the Safeguards Rule," <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>; see also Standards for Safeguarding Customer Information, 67 Fed. Reg. 36484-94, May 23, 2000, (codified at 16 Code of Federal Regulations Part 314), <http://www.ftc.gov/os/2002/05/67fr36585.pdf>.

²⁰² 45 Code of Federal Regulations sections 160, 162, 164; <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>

²⁰³ See HIPAA, Title 42, United States Code section 1320d-2(d)(2).

²⁰⁴ Linda A. Malek and Brian R. Krex, "HIPAA's security rule becomes effective 2005," *The National Law Journal*, Mar. 31, 2003 at B14.

²⁰⁵ 45 Code of Federal Regulations Section 164.306(a).

- (iii) The costs of security measures.
- (iv) The probability and criticality of potential risks to electronic protected health information.²⁰⁶

Another approach is to require companies to publicly disclose vulnerabilities and breaches, both in order to inform the public and to prompt system operators to improve security. EU law obligates the providers of publicly available telecommunications services to inform their subscribers of particular risks of a breach of security of the network and any possible remedies, including the costs involved. For example, in the State of California, a law took effect on July 1, 2003 requiring any company that owns, licenses, or maintains personal information of California residents to notify those residents if a security breach enables an unauthorized person to gain access to the residents' personal information.²⁰⁷

²⁰⁶ 45 Code of Federal Regulations Section 164.306(b).

²⁰⁷ Security Breach Information Act (SB 1386), added to the California Civil Code as Section 1798.29; Thomas J. Smedinghoff, "Cybersecurity Disclosure Requirements: A New Trend?" Baker & McKenzie, Chicago (October 3, 2003), <http://www.bmck.com/ecommerce/cybersecurity-disclosure-requirements.pdf>.