

http://www



THE BUSINESS ROUNDTABLE



http://www



BUILDING SECURITY
IN THE DIGITAL ECONOMY
AN EXECUTIVE RESOURCE

BUILDING SECURITY IN THE DIGITAL ECONOMY



THE BUSINESS ROUNDTABLE
1615 L STREET, NW
SUITE 1100
WASHINGTON, DC 20036
202.872.1260
WWW.BRT.ORG

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

CYBER SECURITY GUIDELINES 3

 CORPORATE GUIDELINES 4

 TECHNOLOGY GUIDELINES 6

 BUSINESS GUIDELINES 8

 PUBLIC POLICY GUIDELINES 10

CYBER SECURITY FRAMEWORK 12

CYBER SECURITY EMERGENCY CONTACTS 14

CYBER SECURITY INFORMATION 16





THE BUSINESS ROUNDTABLE

CHAIRMAN

John T. Dillon, Chairman & CEO, *International Paper*

PRESIDENT

John J. Castellani

DIGITAL ECONOMY TASK FORCE

CHAIRMAN

Richard H. Brown, Chairman and CEO, *EDS*

VICE CHAIRMAN

Scott G. McNealy, Chairman and CEO, *Sun Microsystems*

WITH SPECIAL THANKS TO

The Digital Economy Task Force's Cyber Security Experts Group

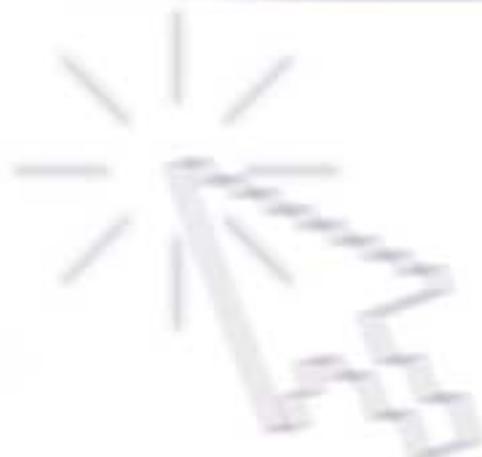
William R. Sweeney, *EDS*

Christopher G. Hankin, *Sun Microsystems*

Liesyl I. Franz, *EDS*

The Business Roundtable is an association of chief executive officers of leading corporations with a combined workforce of more than 10 million employees in the United States and \$3.7 trillion in annual revenues. The chief executives are committed to advocating public policies that foster vigorous economic growth and a dynamic global economy.

EXECUTIVE SUMMARY



EXECUTIVE SUMMARY

Securing the movement of our goods, information, and people has never before possessed the urgency and enormity that it does today. American ingenuity created the digital economy in which we live and work, and the benefits of that economy are evident in the increased efficiencies and productivity gains we have seen as a result. In such a networked society, however, the threat of a cyber attack is more pervasive than ever, and surveys done each year reveal the increasing number of cyber security breaches that do occur.

In this environment, The Business Roundtable believes that cyber security is a critical issue that requires CEO vision, leadership, planning, and participation. Therefore, the BRT's Digital Economy Task Force has developed this Executive Resource to help CEOs and their senior executives develop a robust, effective program to help protect their business as they increasingly incorporate sophisticated information systems into their operations.

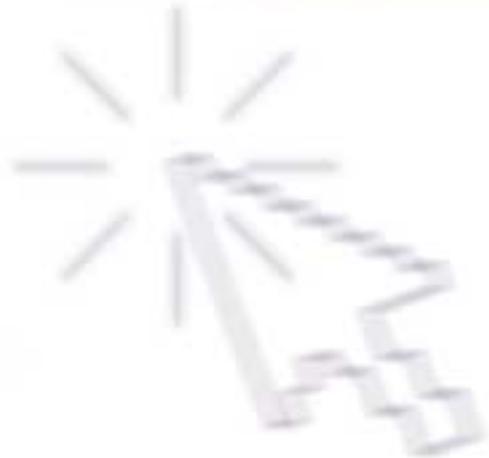
This Resource is comprised of several parts, each of which provides elements to incorporate into a corporate cyber security strategy.

- **A SET OF GUIDELINES FOR ACHIEVING SECURITY IN THE DIGITAL ECONOMY**
This part of the Resource provides a comprehensive set of recommendations for building or furthering corporate cyber security programs. It represents the top-down, horizontal approach necessary to achieve a company's cyber security goals.
- **THE BRT'S FRAMEWORK FOR SECURING THE MOVEMENT OF GOODS, INFORMATION, AND PEOPLE IN THE DIGITAL ECONOMY**
As the Digital Economy Task Force focuses on cyber security, it is important to demonstrate that technology cannot stand alone in a successful program. Corporate issues, business issues, and public policy issues are equally important to the process, which this illustration and corresponding statement depicts. This Framework serves as the basis for the guidelines in this Resource.
- **LIST OF KEY GOVERNMENT AGENCIES WITH RESPONSIBILITY FOR CYBER SECURITY**
This list provides government contacts and Web sites for more information on cyber security, and provides information on whom to contact in the event of a cyber incident.

Our intent is for CEOs and their senior management team to use this Resource to involve and integrate the cross-section of departments in their company that are each crucial to establishing policies and processes in the development of an effective cyber security program. The Resource will assist in:

- Identifying key executives from relevant functions within your organization — which may include operations, human resources, legal, sales and marketing, finance, government affairs, security, information technology, and risk management — to take part in an effective, enterprise-wide cyber security program;
- Developing a top-down and cross-departmental approach that elevates and strengthens accountability for security;
- Taking steps to assess what components of a cyber security program will be best suited to the organization;
- Establishing a set of policies and processes that can be appropriately communicated to all employees, partners, suppliers, business units, and boards of directors; and
- Evaluating the technology tools available.

CYBER SECURITY GUIDELINES



CYBER SECURITY

GUIDELINES

In today's networked environment, every company is susceptible to those who can use digital technology to exploit vulnerabilities to access proprietary data and cause major business disruption. Cyber attacks involving money laundering, economic sabotage, and the destruction of proprietary databases occur across all industry sectors. Cyber criminals are even using the interconnectedness of computer networks to facilitate devastating attacks on other systems.

An effective cyber security program involves not only the information technology department, but requires that the CEO break down the functional silos within a corporation and assemble a cross-departmental senior team to develop and implement the cyber security strategy that will work for that company and its culture. The team of key executives must integrate corporate policies, technology tools, business/economic assessments, and public policy into the cyber security program. This will enable companies to better anticipate, detect, and prevent cyber terrorism and cyber sabotage.

These guidelines are organized into four key issue areas that illustrate the comprehensive and interconnected framework necessary for an effective cyber security program.

- **CORPORATE** — Establish strong and appropriate security policies involving senior executive participation that identify, and mitigate vulnerabilities, and establish corporate-wide practices that will enhance cyber security.
- **TECHNOLOGY** — Working closely with IT providers, develop technology policies that utilize interoperable tools and processes that incorporate security, promote ease of use, and prevent unauthorized access.
- **BUSINESS** — Assess threats and vulnerabilities through business policies that provide analysis of the risks and impact of cyber incidents, balanced against the cost of implementing effective cyber security preventative and detection programs.
- **PUBLIC POLICY** — Adopt public policy guidelines that recognize the balance between the free flow of information, privacy, civil liberties, and security.

CORPORATE GUIDELINES

AN ORGANIZATION'S OPTIMAL CYBER SECURITY GOAL SHOULD BE TO INTEGRATE SECURITY INTO ITS CORE PROCESSES, BUDGETING CYCLES, AND STRATEGIC PLANNING. ALL OFFICERS AND MANAGERS — NOT JUST THE SECURITY OR INFORMATION TECHNOLOGY DEPARTMENT — NEED TO SHARE RESPONSIBILITY AND BE AWARE OF THEIR STAKE IN THE CORPORATION'S SECURITY. COMPANIES MUST NOT ONLY DEPLOY PROVEN TECHNOLOGIES THAT ARE APPROPRIATE TO THEIR ORGANIZATION, BUT ALSO STRIVE TO ENGAGE ALL LEVELS OF EMPLOYEES IN THE PROCESS OF MAKING INFORMATION SECURITY PART OF THEIR EVERYDAY ROUTINE. THE END GOAL MUST BE TO CREATE WHAT A NUMBER OF PUBLIC OFFICIALS ARE CALLING A "CULTURE OF SECURITY."

- The CEO and senior executive staff should lead by example — e.g., take visible steps that evidence good security practices in their daily environment, including wearing corporate badges where they can be seen and implementing the company’s security protections/procedures on their own computer systems.
- Integrate physical, personnel, and network security across the entire organization.
- Incorporate security and privacy reviews and input into the corporate strategy and planning process to identify implications of strategy or business changes.
- Identify the responsibility of officers, leaders, managers, and relevant team members throughout the organization, and encourage them to offer valuable insight, facilitate information dissemination, and provide leverage to achieve cyber security goals.
- Conduct threat, vulnerability, and risk assessments (reviewed at least annually), and adopt practical and enforceable security policies that support those assessments.
- Develop a transparent communication process that reports to the Board regularly on the cyber security program.
- Communicate security policies to all personnel in an easily accessible manner — detailing compliance procedures, priorities, sensitivity levels, off-site storage, e-mail, and instant messenger procedures.
- Review the security policy at least annually, ensuring that it is flexible and dynamic enough to stay current with emerging threats, laws, regulations, and technologies.
- Build ongoing and annual cyber security education, training, and certification into the human resources training system and hiring procedures. When policies and procedures are updated, employees should be required to read and sign a statement attesting to their understanding and compliance.
- Develop security procedures that recognize the organization’s network interconnectivity and external cyber security threats and vulnerabilities from its trusted partners, suppliers, vendors, franchisees, and/or customers.
- Make certain that corporate officers participate in appropriate standards-setting organizations involved in security, including the International Information Systems Security Certification Consortium (ISC²) and the Information Security Management Standard ISO 17799.¹

¹ See: ISC2: www.isc2.org and ISO 17799: www.iso.ch/iso/en/ISOOnline.frontpage.

TECHNOLOGY GUIDELINES

WHILE PEOPLE AND PROCESSES ARE CRITICAL TO DEVELOPING AN EFFECTIVE CYBER SECURITY PROGRAM, THE USE OF TECHNOLOGY IS ALSO AN ESSENTIAL COMPONENT. THE MOST EFFECTIVE TECHNOLOGY SOLUTIONS INCLUDE CONTINUOUSLY UPDATED SECURITY AND ANTI-VIRUS SOFTWARE, AND THE SECURING OF REMOTE CONNECTIONS. ANY SUCH TECHNOLOGY SHOULD BE ABLE TO BE USED WITH EXISTING SOFTWARE AND HARDWARE, BE ABLE TO GROW WITH THE ORGANIZATION, AND ADAPT TO CHANGING BUSINESS NEEDS.

- Evaluate different authentication technologies and procedures as appropriate to the enterprise. This may include authentication tokens, perimeter defenses, smart cards, and/or biometrics to gain access to critical facilities and networks.
- Establish an effective system that monitors and controls access. These technologies should supplement individual-user password procedures that further protect against unauthorized access.
- Incorporate technology providers as an integral part of a cyber security program to ensure that flexible and dynamic security tools are built into the systems at the outset.
- Incorporate automatic “timeout” features when systems are unattended or after a number of unsuccessful login attempts.
- Implement remote/portable telecommunications policies that restrict or protect off-site connections. Remote access, however, should also be viewed as a means of fortifying business continuity and disaster recovery capabilities.
- Recognize that newer technologies, such as wireless devices (PDAs, cell phones, etc.), instant messaging, and high-speed access for home offices, are introducing new vulnerabilities that must be addressed.
- Continuously monitor networks and systems for unauthorized activity, vulnerabilities, or unauthorized modification of systems or files.
- Incorporate security redundancy to ensure that one failure will not compromise the entire network and that the operation is resilient enough to react quickly to new threats.
- Place backup data and mission-critical systems off-site, and periodically test how quickly they can be brought on-line if needed.
- Keep informed of security vulnerabilities, such as software weakness announcements, and maintain a robust process to apply fixes and configuration changes to appropriate software.
- Recognize that every new technology integrated into the system will have an impact on vulnerabilities. Alter the risks and necessitate a reevaluation of the security policies in place. Set policies for the addition of new applications to the system.
- Develop a robust identity-management process that centralizes employee and user information, what users are authorized to access on a system, and authentication procedures.
- Develop a plan that identifies and secures the most vital, sensitive, and/or valuable data when it is not possible to secure the entire network.

BUSINESS GUIDELINES

ALL SENIOR EXECUTIVES MUST BALANCE SECURITY COSTS, THE IMPACT ON PRODUCTION OR SERVICE, AND THE OVERALL EFFICIENCIES OF THE ORGANIZATION AGAINST THE ECONOMIC HARM ASSOCIATED WITH A CYBER SECURITY ATTACK. AN ORGANIZATION SHOULD ALSO CONSIDER HOW BEST TO ABSORB THE COSTS — SOME CALL IT A “SECURITY TAX” — ASSOCIATED WITH IMPROVING THEIR CYBER SECURITY. IN ORDER TO ACHIEVE ULTIMATE INTEGRATION INTO THE COMPANY’S BUSINESS MODEL, THE CYBER SECURITY PROGRAM CANNOT BE TOO EXPENSIVE, COMPLEX, OR RIGID TO RESPOND TO CHANGING TECHNOLOGIES OR NEW CYBER THREATS. A SUCCESSFUL ENTERPRISE-WIDE CYBER SECURITY PLAN WILL REDUCE DOWNTIME AND SYSTEM OUTAGES, AVOID PRODUCTIVITY LOSSES, AND BOOST PROFITS.

-
- Balance potential threats and risk against the organization's desire to maintain product/service quality. Also factor in other considerations such as speed, convenience, and ease of use.
 - Pay particular attention to the vulnerability of the company's proprietary property, including trade secrets, patents, and other sensitive intellectual property that could be at risk from internal or external attack.
 - Develop business continuity and disaster recovery/contingency plans for response to any cyber incidents — or the collateral damage from physical incidents. Emergency communications networks should be created to stabilize mission-critical systems in times of crisis or disaster.
 - Work and communicate with colleagues across your organization, suppliers, customers, partners, and even competitors in the adoption of security standards that protect without creating business barriers. Share approaches being used to deal with common threats and cyber incidents.
 - Utilize management metrics to gauge acceptable levels of risk when evaluating the level of security needed to determine the most effective and beneficial procedures in relation to their return on investment and the anticipated economic impact if an incident occurs.

PUBLIC POLICY GUIDELINES

THE COMPONENTS OF A SUCCESSFUL CYBER SECURITY PROGRAM CANNOT CONSIST SOLELY OF CORPORATE, TECHNOLOGY, AND BUSINESS ISSUES. THE RELEVANT FEDERAL, STATE, AND FOREIGN GOVERNMENT PRIVACY LAWS AND REGULATIONS THAT AFFECT IMPLEMENTATION MUST BE FACTORED INTO SECURITY PROCEDURES. PENDING LEGISLATION SHOULD BE REVIEWED FOR ANY ADVERSE IMPACT ON A COMPANY'S ABILITY TO ESTABLISH CYBER SECURITY PROGRAMS THAT FIT ITS LEGAL OBLIGATIONS AND ADDRESS ITS BUSINESS NEEDS.

- Understand that a balance may have to be struck between preventing and prosecuting those who engage in cyber security attacks, while protecting the legitimate privacy and civil liberties of individuals.
- Know the organization’s legal and contractual requirements, and what federal, state, and foreign government regulations require, including the Financial Modernization “Gramm-Leach-Bliley” Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Patriot Act, the European Union Data Privacy Directive, the Council of Europe’s Convention on Cybercrime, cryptography export controls, and the Basel Accords.²
- Recognize that each new federal, state, or foreign security/privacy law, treaty, or regulation mandates obligations that a company must follow — including new response capabilities, new audit records, new senior management responsibilities, and, in some instances, new financial models. Pay special attention to how such laws and regulations might affect the way a company handles data pertaining to its own employees, partners, and customers.
- Be aware (and when /where appropriate, be involved in the development) of new security standards issued by private and public sector organizations and agencies.
- Encourage officers and managers to communicate and share incident and vulnerability information with trusted peers, trade associations, and relevant Information Sharing Analysis Centers (ISACs). Lines of communication could be established with and among appropriate internal departments /facilities, other like-sector businesses, cross-sector information security officials, and government officials.

² See: GLBA - www.senate.gov/~banking/conf/; HIPAA - www.hhs.gov/news/press/2002pres/hipaa.html; EU Data Privacy Directive - www.europa.eu.int/comm/internal_market/en/dataprot/index.htm; Council of Europe’s Convention on Cybercrime - www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/Convention/The_Convention.asp#; Cryptography Export Controls - www.bis.doc.gov; The U.S. Patriot Act - <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.3162>; and The Basel Accords - www.bis.org/bcbs/publ.htm.

CYBER SECURITY FRAMEWORK

CYBER SECURITY FRAMEWORK

An enduring principle of the United States has been that a strong economy is fundamental to our national security. The ability of enterprises in all industry sectors — not just *high-tech* companies — to incorporate sophisticated information technology innovations and advancements into every aspect of their business operations will further fuel our overall national and global economic well-being. Crucial to the continued growth and productivity of our world-leading digital economy is the private sector’s ability to securely move and deliver their products, services, goods, people, and information. Implementing a strong cyber security plan, which provides for the protection of facilities, persons, borders, networks, and systems, was as necessary before September 11, 2001, as it is today.

BRT members are aware that securing the movement of goods, information, and people is an evolving, constant process that is built on a strong cyber security platform to address a variety of cyber attacks and other threats. Four issue pillars of a cyber security platform can provide internal and external safeguards for companies to anticipate, detect, and deter terrorism, criminal behavior, and even negligence. The pillars are:

- **CORPORATE ISSUES**

Equally important to a successful cyber security plan are the human component, which requires employee education and training; CEO and cross-departmental responsibility; establishing best practices and effective communication mechanisms; conducting internal assessments; incorporating risk management; and developing within and throughout the enterprise a strong “culture of security.”

- **TECHNOLOGY ISSUES**

Incorporate, as appropriate to the enterprise, interoperable technology tools that provide for authentication and access, such as ID systems, passwords, and firewalls, as well as the linking of databases.

- **BUSINESS ISSUES**

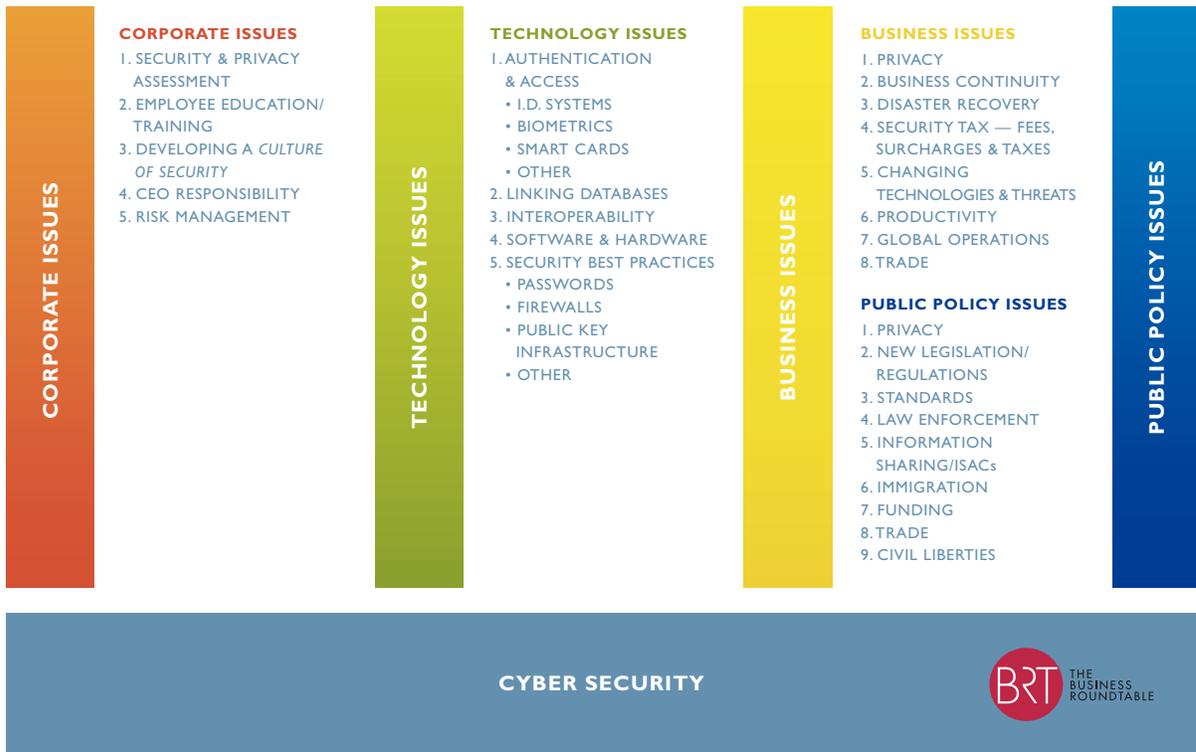
Social, political, and economic considerations must be taken into account in the development of a successful cyber security plan, including cost of implementation, privacy concerns, national borders and divergent legal regimes, ever-changing technologies, never-contemplated threats, business continuity, disaster recovery, and the impact of security measures on productivity.

- **PUBLIC POLICY ISSUES**

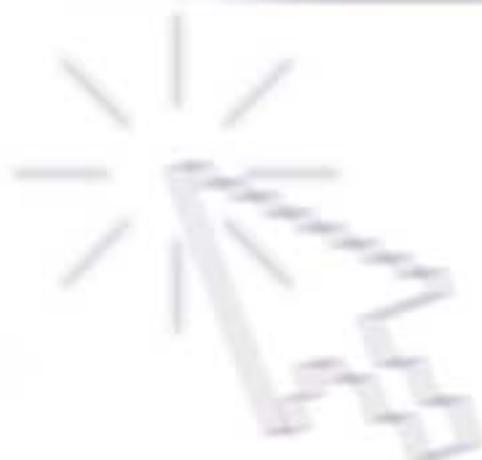
The majority of applications, systems, and networks are built, owned, and operated by the private sector, but the government can play a role in developing standards; funding law enforcement; helping to deter, detect, and prosecute cyber criminals/terrorists; providing for internal government information security; and eliminating obstacles to information-sharing on cyber attacks, threats, and intrusions.

The Business Roundtable's Digital Economy Task Force is working to establish this strong cyber security foundation between BRT CEOs and the public sector. This includes business education and fostering cooperative partnerships between government and industry to meet the information security challenges before us. If implemented, strong and effective cyber security policies and technologies will instill a sense of trust and confidence in the overall security of our nation's infrastructure and further stimulate the robust growth and productivity of the economy.

**SECURING THE MOVEMENT OF GOODS, INFORMATION,
AND PEOPLE IN THE DIGITAL ECONOMY**



CONTACTS



CYBER SECURITY

EMERGENCY CONTACTS

The following agencies provide information on whom to contact (in many cases anonymously, if necessary) in the event your organization's systems are impacted in any way by a cyber incident (e.g., hacking, a virus attack, or other intrusions). Following such an intrusion, the appropriate official responsible for cyber security oversight should be contacted and the company's internal security/incident response procedures should be immediately implemented, including but not limited to, isolating/containing all individual systems affected by the attack.

- If your organization's network or system has been breached, contact the **COMPUTER EMERGENCY RESPONSE TEAM COORDINATING CENTER (CERT) AT CARNEGIE MELLON UNIVERSITY**. It provides various resources on Internet security, including advisories on vulnerabilities and computer security incidents.
 - www.cert.org
 - Forms available to report a breach, incident, or vulnerability: www.cert.org/reporting/incident_form.txt or www.cert.org/reporting/vulnerability_form.txt
 - 24-Hour Phone Hotline: 412.268.7090
- The next appropriate step after contacting CERT is to contact (if you are a member) the appropriate **INFORMATION SHARING ANALYSIS CENTER (ISAC)**.
 - For further information on ISACs and the individual sector groups go to: www.nipc.gov/infosharing/infosharing6.htm

If the circumstances are deemed appropriate, you may want to notify the relevant law enforcement agency or agencies. Agencies that handle cyber incident reports and investigations include:

- **NATIONAL INFRASTRUCTURE PROTECTION CENTER (NIPC)** — NIPC operates out of the FBI's headquarters in Washington, D.C. The group, along with state, local, and private partnerships, provides threat assessment, warning, investigation, and response to threats or attacks against telecommunications, energy, emergency services, and other infrastructures for the U.S. government. The site has information on alerts and cyber threats.
 - www.nipc.gov
 - Incident Reporting forms can be obtained at www.nipc.gov/incident/incident.htm.
 - Phone: 202.323.3205

-
- **COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION OF THE CRIMINAL DIVISION OF THE DEPARTMENT OF JUSTICE** — Consists of about two dozen lawyers who advise federal prosecutors and law enforcement agents, comment upon and propose legislation, coordinate international efforts to combat computer crime, litigate cases, and train all law enforcement groups.

- www.cybercrime.gov or www.usdoj.gov/criminal/cybercrime/reporting.htm — (site explains how to report an incident)

- Phone: 202.514.1026

- **FEDERAL BUREAU OF INVESTIGATION (FBI)** — The FBI has specialists in computer intrusion (i.e., computer hacker) cases. The FBI hosts the National Infrastructure Protection Center. Most field offices also have cyber security specialists.

- www.fbi.gov

- Hyperlink to field offices: www.fbi.gov/contact/fo/fo.htm

- Phone: 202.324.3000

CYBER SECURITY INFORMATION

A number of private and public sector trade associations, organizations, agencies, and issue-specific publications have issued standards, best practices, and other relevant background information that can help companies manage risks associated with cyber security and aid organizations in developing cyber security programs and procedures.

- **CRITICAL INFRASTRUCTURE ASSURANCE OFFICE (CIAO)** — CIAO was created to coordinate federal government initiatives across industry sectors and ensure a cohesive approach to achieving continuity in delivering critical infrastructure services.
 - www.ciao.gov
 - Phone: 202.482.7473
- **THE PRESIDENT’S CRITICAL INFRASTRUCTURE PROTECTION BOARD (CIPB)** — The Board has developed, in close collaboration with the private sector, the “National Strategy to Secure Cyberspace” an important resource for “Level 2 — Large Organizations” desiring more information, resources, and activities.
 - www.whitehouse.gov/pcipb and www.securecyberspace.gov
 - Phone: 202.456.9351
- **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) — INFORMATION TECHNOLOGY OFFICE** — NIST’s Computer Security Resource Center Web site has a number of reference points to help organizations with IT risks, vulnerabilities, and protection requirements.
 - www.itl.nist.gov and csrc.ncsl.nist.gov
 - Phone: 301.975.2900
- **FEDERAL TRADE COMMISSION (FTC)** — The FTC has created a Web site for consumers and businesses as a source of information about computer security and safeguarding personal information.
 - www.ftc.gov/infosecurity
 - See also recent remarks by FTC Commissioner Orson Swindle on creating a “culture of security.” www.ftc.gov/bcp/online/edcams/infosecurity/popups/clevelandspeech_swindle.htm
- **ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD)** — The OECD Council adopted in the summer of 2002 “Guidelines for the Security of Information Systems and Networks” to help organizations establish a “culture of security.”
 - www.oecd.org/pdf/M00034000/M00034292.pdf

-
- **NATIONAL ASSOCIATION OF ATTORNEYS GENERAL — COMPUTER CRIME POINT-OF-CONTACT LIST** — A list of prosecutors and investigators from state and local law enforcement agencies who are responsible for the investigation and prosecution of computer and computer-related crime within their respective jurisdictions.

- www.naag.org/issues/20010724-cc_list_bg.php

NOTES

