COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fifth Edition

Chapter 3

Legal, Ethical, and Professional Issues in Information Security

In civilized life, law floats in a sea of ethics.

EARL WARREN, CHIEF JUSTICE, U.S. SUPREME COURT, 12 NOVEMBER 1962

Learning Objectives

- Upon completion of this material, you should be able to:
  - Describe the functions of and relationships among laws, regulations, and professional organizations in information security
  - Explain the differences between laws and ethics
  - Identify major national laws that affect the practice of information security
  - Discuss the role of culture as it applies to ethics in information security

Introduction

- You must understand the scope of an organization’s legal and ethical responsibilities.
- To minimize liabilities/reduce risks, the information security practitioner must:
  - Understand the current legal environment
  - Stay current with laws and regulations
  - Watch for new and emerging issues

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain behavior and are enforced by the state
- Ethics: regulate and define socially acceptable behavior
- Cultural mores: fixed moral attitudes or customs of a particular group
- Laws carry the authority of a governing authority; ethics do not.

Organizational Liability and the Need for Counsel

- Liability: the legal obligation of an entity extending beyond criminal or contract law; includes the legal obligation to make restitution
- Restitution: the legal obligation to compensate an injured party for wrongs committed
- Due care: the legal standard requiring a prudent organization to act legally and ethically and know the consequences of actions
- Due diligence: the legal standard requiring a prudent organization to maintain the standard of due care and ensure actions are effective

Organizational Liability and the Need for Counsel (cont’d)

- Jurisdiction: court’s right to hear a case if the wrong was committed in its territory or involved its citizenry
- Long-arm jurisdiction: application of laws to those residing outside a court’s normal jurisdiction; usually granted when a person acts illegally within the jurisdiction and leaves

Policy Versus Law

- Policies: managerial directives that specify acceptable and unacceptable employee behavior in the workplace
- Policies function as organizational laws; must be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone
- Difference between policy and law: Ignorance of a policy is an acceptable defense.

Policy Versus Law (cont’d)

- Criteria for policy enforcement:
  - Dissemination (distribution)
  - Review (reading)
  - Comprehension (understanding)
  - Compliance (agreement)
  - Uniform enforcement

Types of Law

- Civil: governs nation or state; manages relationships/conflicts between organizations and people
- Criminal: addresses activities and conduct harmful to society; actively enforced by the state
- Private: family/commercial/labor law; regulates relationships between individuals and organizations
- Public: regulates structure/administration of government agencies and their relationships with citizens, employees, and other governments

Relevant U.S. Laws

- The United States has been a leader in the development and implementation of information security legislation.
- Information security legislation contributes to a more reliable business environment and a stable economy.
- The United States has demonstrated understanding of the importance of securing information and has specified penalties for individuals and organizations that breach civil and criminal law.

General Computer Crime Laws

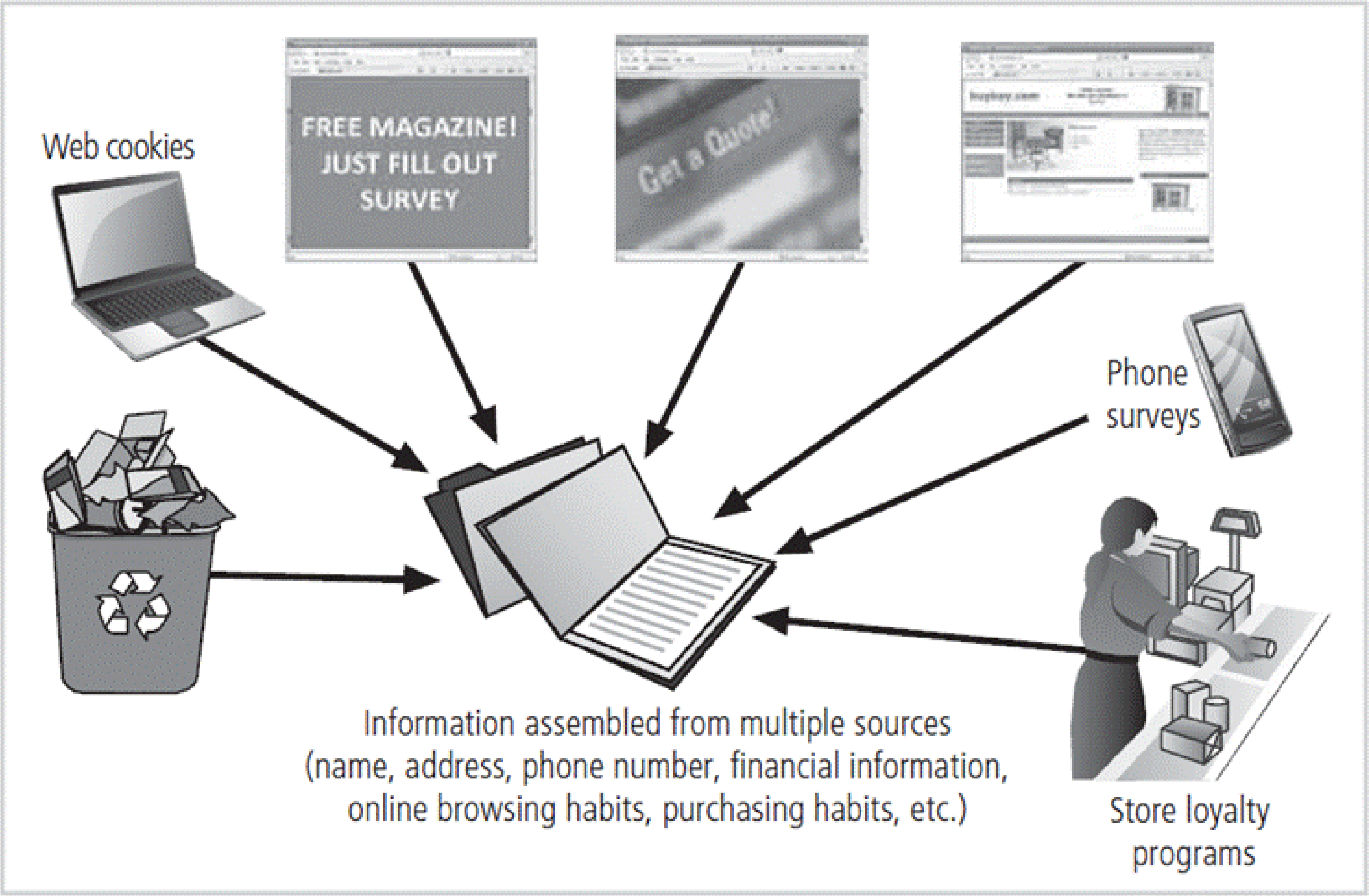
- Computer Fraud and Abuse Act of 1986 (CFA Act): Cornerstone of many computer-related federal laws and enforcement efforts
- National Information Infrastructure Protection Act of 1996:
  - Modified several sections of the previous act and increased the penalties for selected crimes
  - Severity of the penalties was judged on the value of the information and the purpose
    - For purposes of commercial advantage
    - For private financial gain
    - In furtherance of a criminal act

General Computer Crime Laws (cont’d)

- USA PATRIOT Act of 2001: Provides law enforcement agencies with broader latitude in order to combat terrorism-related activities
- USA PATRIOT Improvement and Reauthorization Act: Made permanent fourteen of the sixteen expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity
- Computer Security Act of 1987: One of the first attempts to protect federal computer systems by establishing minimum acceptable security practices.

Privacy

- One of the hottest topics in information security
- Right of individuals or groups to protect themselves and personal information from unauthorized access
- Ability to aggregate data from multiple sources allows creation of information databases previously impossible
- The number of statutes addressing an individual’s right to privacy has grown.


Web cookies
FREE MAGAZINE! JUST FILL OUT SURVEY
Get a Quote!
Phone surveys
Store loyalty programs
Information assembled from multiple sources (name, address, phone number, financial information, online browsing habits, purchasing habits, etc.)

© Cengage Learning 2015

Figure 3-2 Information aggregation

Privacy (cont'd)

- U.S. Regulations
  - Privacy of Customer Information Section of the common carrier regulation
  - Federal Privacy Act of 1974
  - Electronic Communications Privacy Act of 1986
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA), aka Kennedy-Kassebaum Act
  - Financial Services Modernization Act, or Gramm-Leach-Bliley Act of 1999

Identity Theft

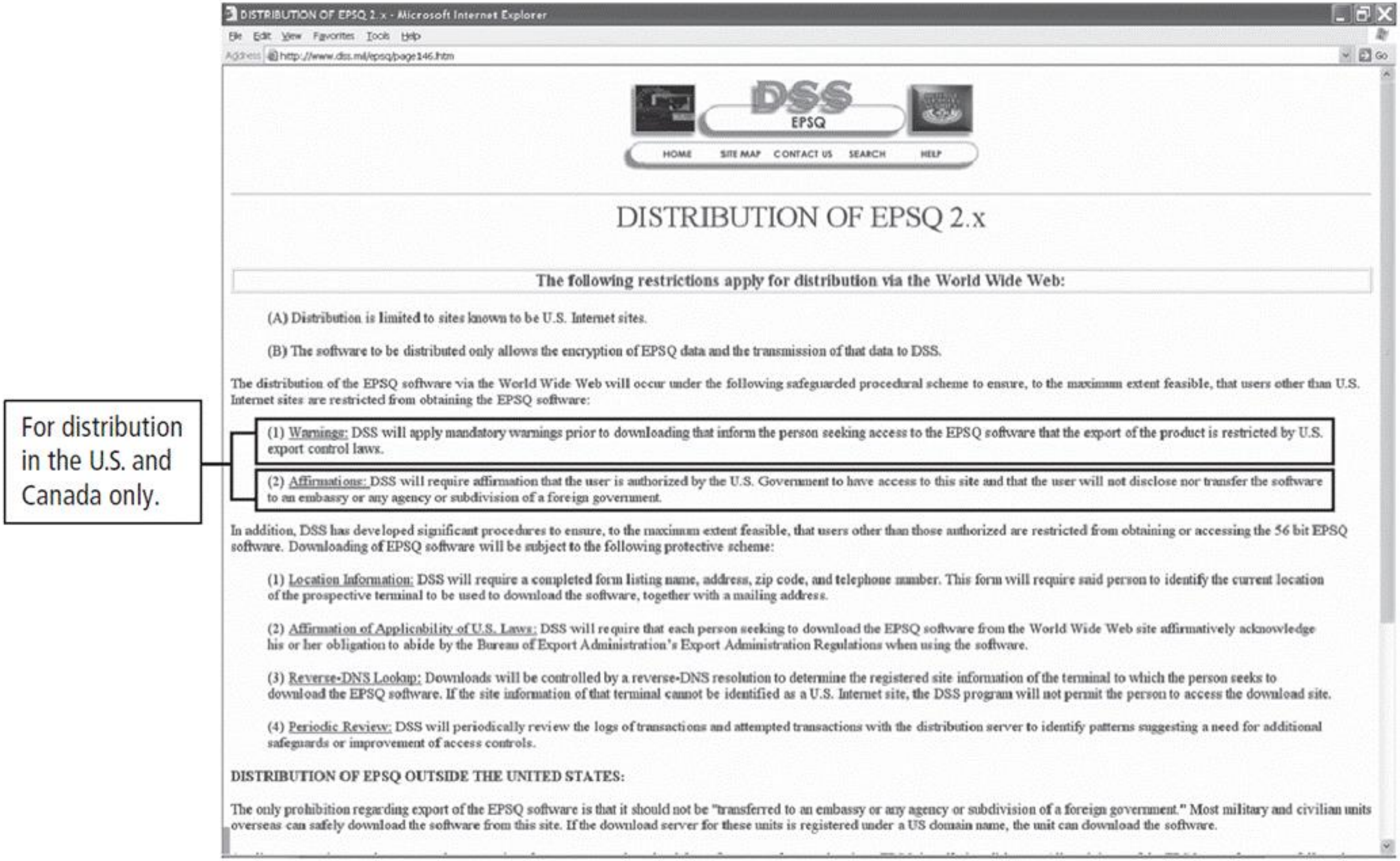
- It can occur when someone steals victim’s personally identifiable information (PII) and poses as victim to conduct actions/make purchases.
- Federal Trade Commission oversees efforts to foster coordination, effective prosecution of criminals, and methods to increase victim’s restitution.
- Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information (Title 18, U.S.C. § 1028)

Identity Theft (cont'd)

- If someone suspects identity theft:
  - Report to one of the three national credit reporting companies and request initial fraud alert.
  - Order credit reports and examine for fraud activity; contact the fraud department in the organization holding the suspect account.
  - Create an identity theft report through FTC's identity theft affidavit.
  - Document all calls/letters/communications during the process.

Export and Espionage Laws

- Economic Espionage Act of 1996 (EEA)
- Security and Freedom through Encryption Act of 1999 (SAFE)
- The acts include provisions about encryption that:
  - Reinforce the right to use or sell encryption algorithms, without concern of key registration.
  - Prohibit the federal government from requiring it.
  - Make it not probable cause to suspect criminal activity.
  - Relax export restrictions.
  - Additional penalties for using it in a crime.


DISTRIBUTION OF EPSQ 2.x - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.dss.mil/epsq/page146.htm
Go
DSS
EPSQ
HOME
SITE MAP
CONTACT US
SEARCH
HELP

DISTRIBUTION OF EPSQ 2.x

The following restrictions apply for distribution via the World Wide Web:

(A) Distribution is limited to sites known to be U.S. Internet sites.

(B) The software to be distributed only allows the encryption of EPSQ data and the transmission of that data to DSS.

The distribution of the EPSQ software via the World Wide Web will occur under the following safeguarded procedural scheme to ensure, to the maximum extent feasible, that users other than U.S. Internet sites are restricted from obtaining the EPSQ software:

(1) Warnings: DSS will apply mandatory warnings prior to downloading that inform the person seeking access to the EPSQ software that the export of the product is restricted by U.S. export control laws.

(2) Affirmations: DSS will require affirmation that the user is authorized by the U.S. Government to have access to this site and that the user will not disclose nor transfer the software to an embassy or any agency or subdivision of a foreign government.

For distribution in the U.S. and Canada only.

In addition, DSS has developed significant procedures to ensure, to the maximum extent feasible, that users other than those authorized are restricted from obtaining or accessing the 56 bit EPSQ software. Downloading of EPSQ software will be subject to the following protective scheme:

(1) Location Information: DSS will require a completed form listing name, address, zip code, and telephone number. This form will require said person to identify the current location of the prospective terminal to be used to download the software, together with a mailing address.

(2) Affirmation of Applicability of U.S. Laws: DSS will require that each person seeking to download the EPSQ software from the World Wide Web site affirmatively acknowledge his or her obligation to abide by the Bureau of Export Administration's Export Administration Regulations when using the software.

(3) Reverse-DNS Lookup: Downloads will be controlled by a reverse-DNS resolution to determine the registered site information of the terminal to which the person seeks to download the EPSQ software. If the site information of that terminal cannot be identified as a U.S. Internet site, the DSS program will not permit the person to access the download site.

(4) Periodic Review: DSS will periodically review the logs of transactions and attempted transactions with the distribution server to identify patterns suggesting a need for additional safeguards or improvement of access controls.

DISTRIBUTION OF EPSQ OUTSIDE THE UNITED STATES:

The only prohibition regarding export of the EPSQ software is that it should not be "transferred to an embassy or any agency or subdivision of a foreign government." Most military and civilian units overseas can safely download the software from this site. If the download server for these units is registered under a US domain name, the unit can download the software.

© Cengage Learning 2015

Figure 3-4 Export and espionage

U.S. Copyright Law

- Intellectual property was recognized as a protected asset in the United States; copyright law extends to electronic formats.
- With proper acknowledgment, it is permissible to include portions of others' work as reference.
- U.S. Copyright Office Web site: www.copyright.gov

Financial Reporting

- Sarbanes-Oxley Act of 2002
- Affects the executive management of publicly traded corporations and public accounting firms
- Seeks to improve the reliability and accuracy of financial reporting and increase the accountability of corporate governance in publicly traded companies
- Penalties for noncompliance range from fines to jail terms.

Freedom of Information Act of 1966 (FOIA)

- Allows access to federal agency records or information not determined to be matter of national security
- U.S. government agencies are required to disclose any requested information upon receipt of written request.
- Some information is protected from disclosure; this act does not apply to state/local government agencies or private businesses/individuals.

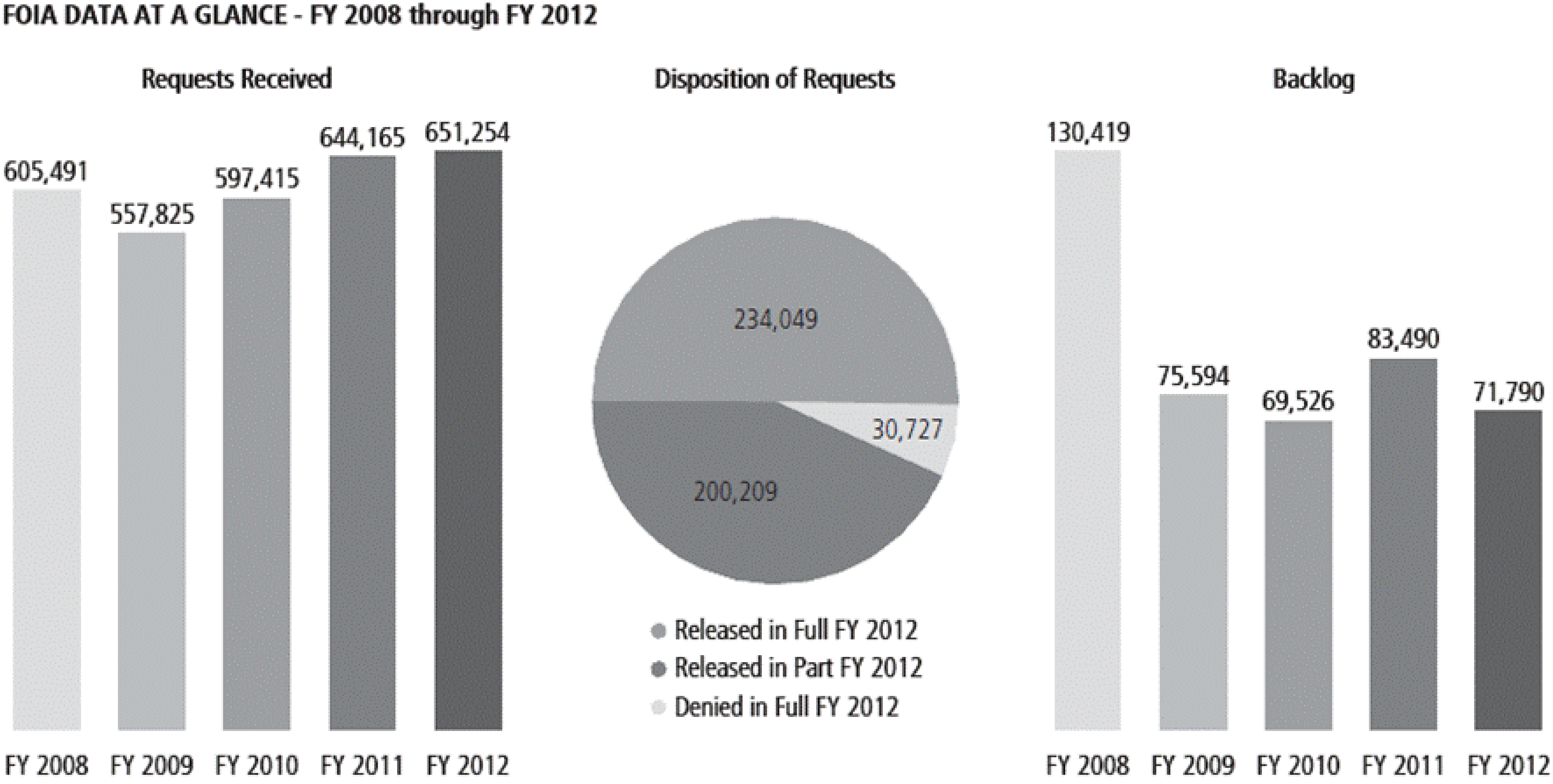


Figure 3-5 U.S. government FOIA requests and processing

Source: www.foia.gov.

Payment Card Industry Data Security Standards (PCI DSS)

- PCI Security Standards Council offers a standard of performance to which organizations processing payment cards must comply.
- Designed to enhance security of customer's account data
- Addresses six areas:
  - Build and maintain secure networks/systems
  - Protect cardholder data
  - Maintain vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain information security policy

State and Local Regulations

- Federal computer laws are mainly written specifically for federal information systems; they have little applicability to private organizations.
- Information security professionals are responsible for understanding state regulations and ensuring that organization is in compliance with regulations.

International Laws and Legal Bodies

- When organizations do business on the Internet, they do business globally.
- Professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries.
- Because of the political complexities of relationships among nations and differences in culture, few international laws cover privacy and information security.
- These international laws are important but are limited in their enforceability.

Council of Europe Convention on Cybercrime

- Created international task force to oversee Internet security functions for standardized international technology laws
- Attempts to improve effectiveness of international investigations into breaches of technology law
- Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution
- Lacks realistic provisions for enforcement

Agreement on Trade-Related Aspects of Intellectual Property Rights

- Created by World Trade Organization (WTO)
- The first significant international effort to protect intellectual property rights
- Outlines requirements for governmental oversight and legislation providing minimum levels of protection for intellectual property

Agreement on Trade-Related Aspects of Intellectual Property Rights (cont'd)

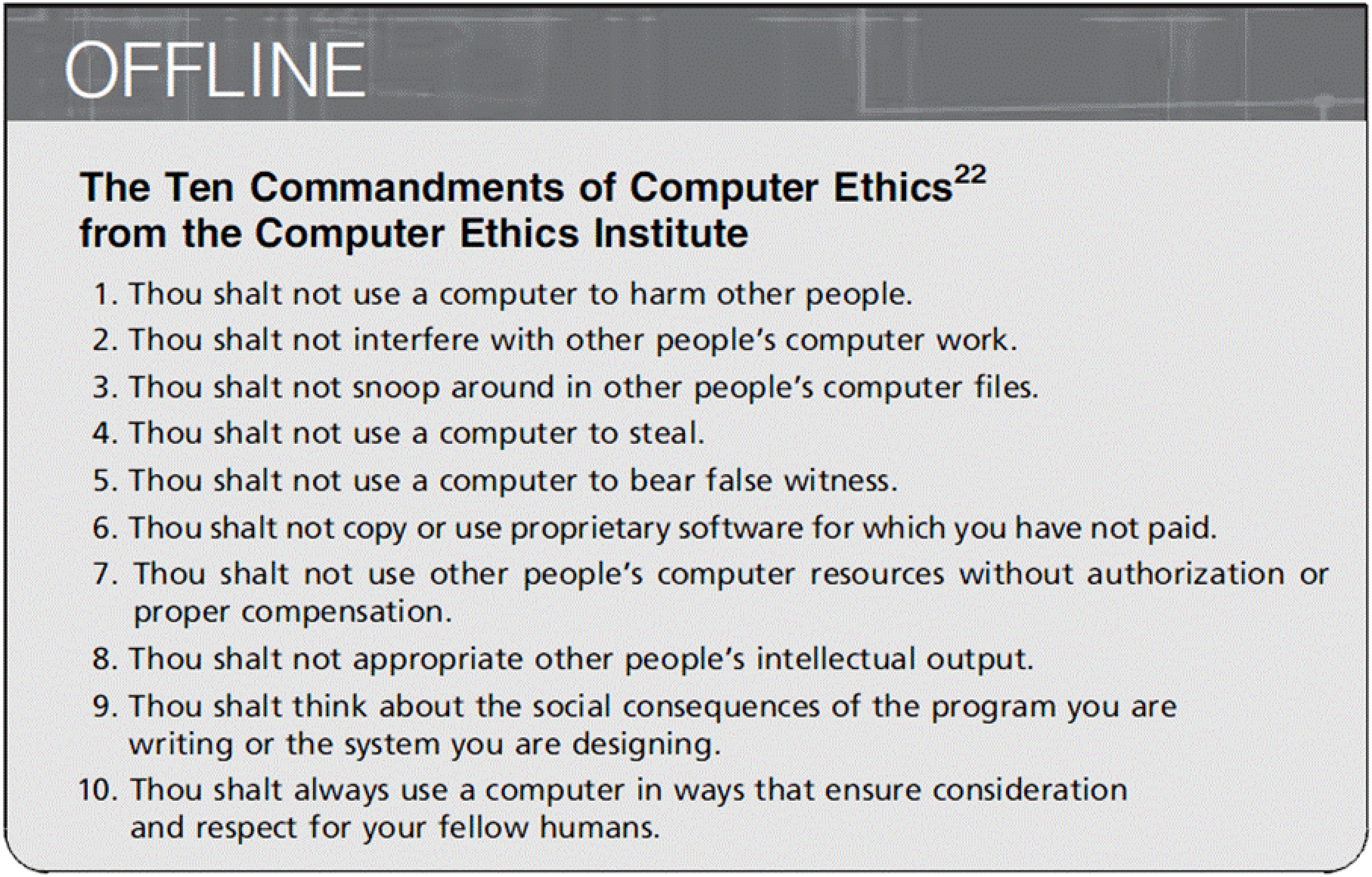
- Agreement covers five issues:
  - Application of basic principles of trading system and international intellectual property agreements
  - Giving adequate protection to intellectual property rights
  - Enforcement of those rights by countries within their borders
  - Settling intellectual property disputes
  - Transitional arrangements while new system is being introduced

Digital Millennium Copyright Act (DMCA)

- U.S. contribution to international effort to reduce impact of copyright, trademark, and privacy infringement
- A response to European Union Directive 95/46/EC
- Prohibits
  - Circumvention of protections and countermeasures
  - Manufacture and trafficking of devices used to circumvent such protections
  - Altering information attached or imbedded in copyrighted material
- Excludes ISPs from some copyright infringement

Ethics and Information Security

- Many professional disciplines have explicit rules governing the ethical behavior of members.
- IT and IT security do not have binding codes of ethics.
- Professional associations and certification agencies work to maintain ethical codes of conduct.
  - Can prescribe ethical conduct
  - Do not always have the ability to ban violators from practice in field



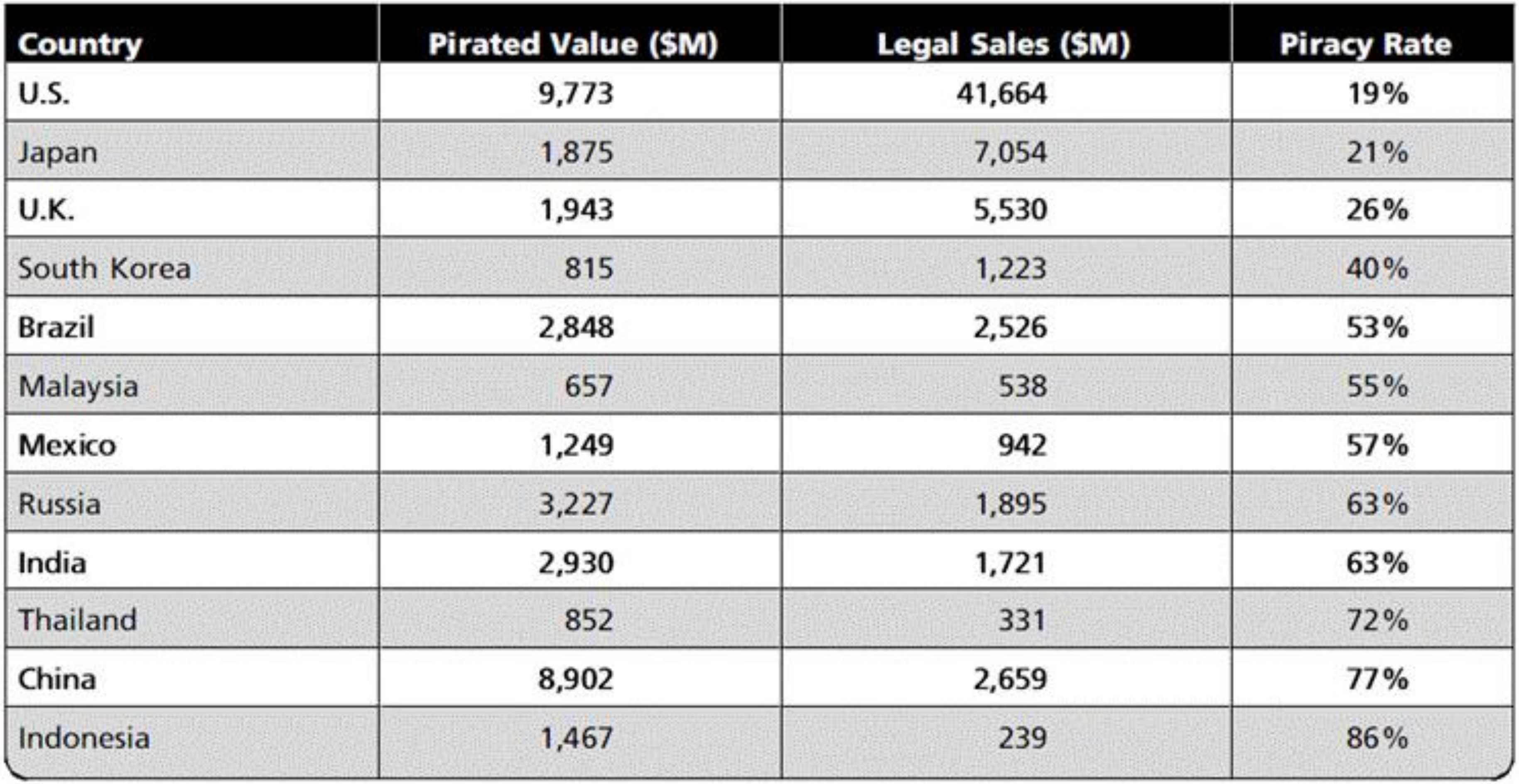
OFFLINE

The Ten Commandments of Computer Ethics[22] from the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical.
- Difficulties arise when one nationality’s ethical behavior conflicts with the ethics of another national group.
- Scenarios are grouped into:
  - Software license infringement
  - Illicit use
  - Misuse of corporate resources
- Cultures have different views on the scenarios.



Country	Pirated Value ($M)	Legal Sales ($M)	Piracy Rate
U.S.	9,773	41,664	19%
Japan	1,875	7,054	21%
U.K.	1,943	5,530	26%
South Korea	815	1,223	40%
Brazil	2,848	2,526	53%
Malaysia	657	538	55%
Mexico	1,249	942	57%
Russia	3,227	1,895	63%
India	2,930	1,721	63%
Thailand	852	331	72%
China	8,902	2,659	77%
Indonesia	1,467	239	86%

Table 3-2 International Piracy Rates

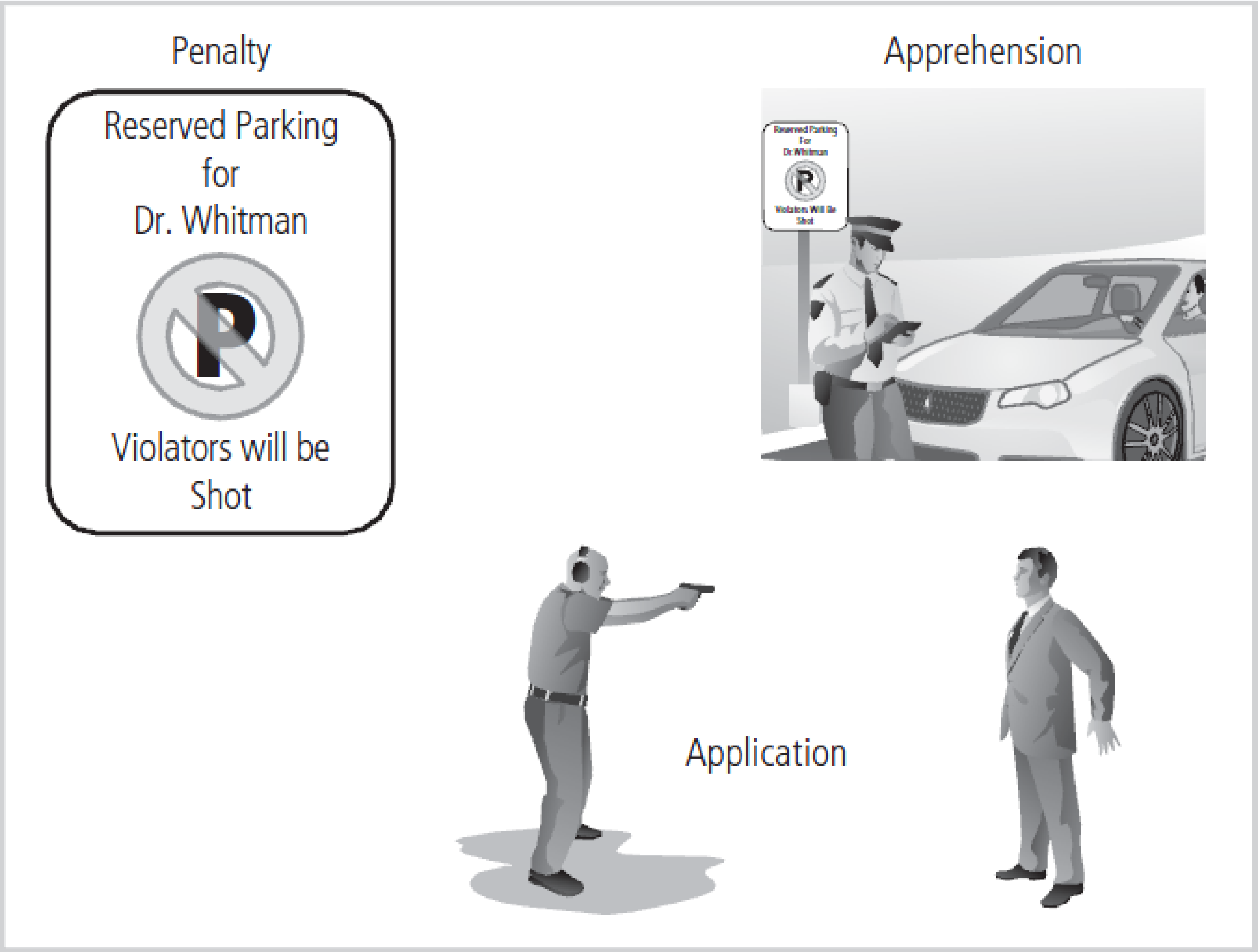
BSA, 2012.[24]

Ethics and Education

- Education is the overriding factor in leveling ethical perceptions within a small population.
- Employees must be trained and kept aware of the expected behavior of an ethical employee, as well as many other information security topics.
- Proper ethical training is vital to creating informed and a well-prepared system user.

Deterring Unethical and Illegal Behavior

- Three general causes of unethical and illegal behavior: ignorance, accident, intent
- Deterrence: best method for preventing an illegal or unethical activity; for example, laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - Probability of being apprehended
  - Probability of penalty being applied

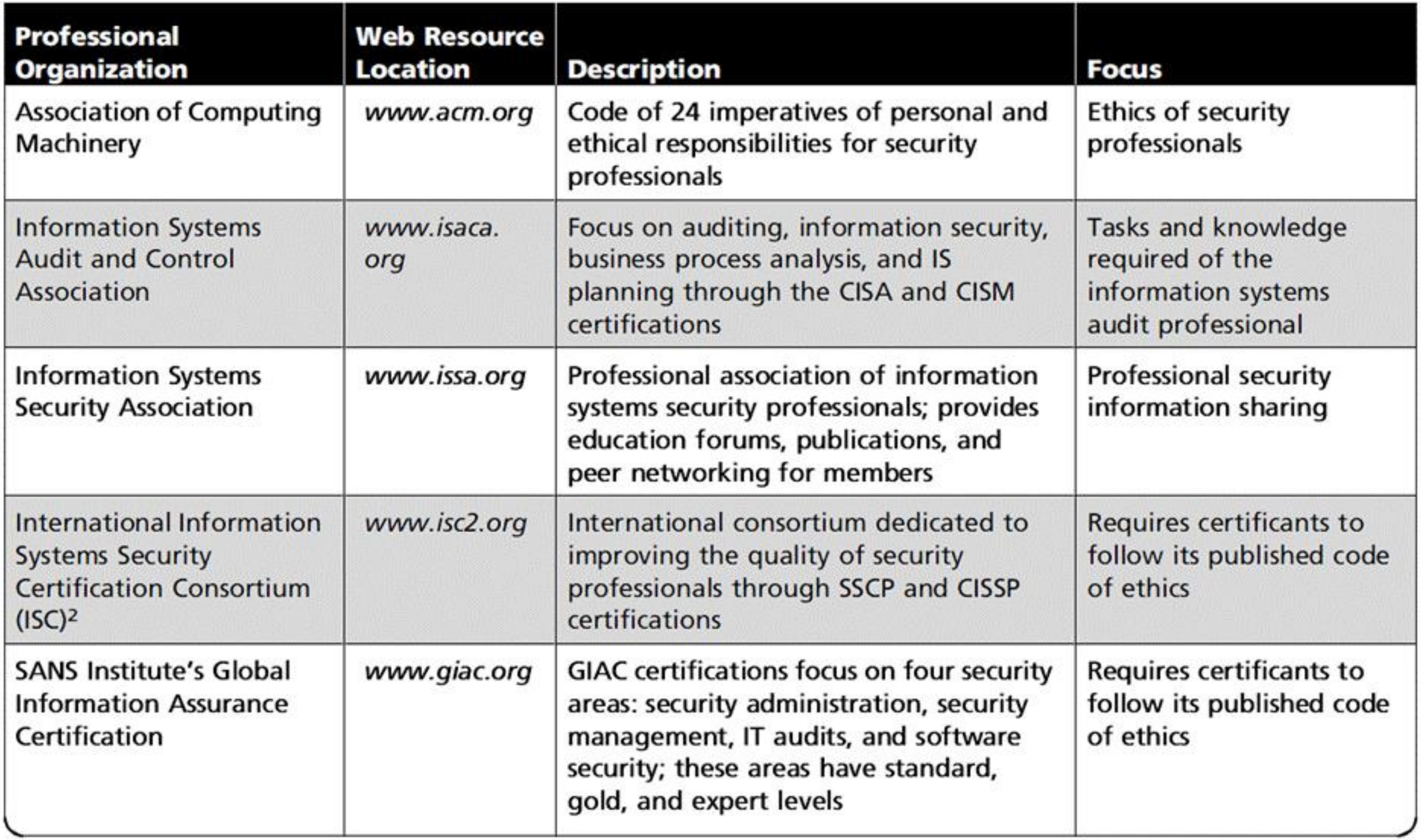


© Cengage Learning 2015

Figure 3-7 Deterrents to illegal or unethical behavior

Codes of Ethics and Professional Organizations

- Many professional organizations have established codes of conduct/ethics.
- Codes of ethics can have a positive effect; unfortunately, many employers do not encourage joining these professional organizations.
- Responsibility of security professionals is to act ethically and according to the policies of the employer, the professional organization, and the laws of society.



Professional Organization	Web Resource Location	Description	Focus
Association of Computing Machinery	*www.acm.org*	Code of 24 imperatives of personal and ethical responsibilities for security professionals	Ethics of security professionals
Information Systems Audit and Control Association	*www.isaca.org*	Focus on auditing, information security, business process analysis, and IS planning through the CISA and CISM certifications	Tasks and knowledge required of the information systems audit professional
Information Systems Security Association	*www.issa.org*	Professional association of information systems security professionals; provides education forums, publications, and peer networking for members	Professional security information sharing
International Information Systems Security Certification Consortium (ISC)^2	*www.isc2.org*	International consortium dedicated to improving the quality of security professionals through SSCP and CISSP certifications	Requires certificants to follow its published code of ethics
SANS Institute's Global Information Assurance Certification	*www.giac.org*	GIAC certifications focus on four security areas: security administration, security management, IT audits, and software security; these areas have standard, gold, and expert levels	Requires certificants to follow its published code of ethics

Table 3-3 Professional Organizations of Interest to Information Security Professionals

Major IT Professional Organizations

- Association of Computing Machinery (ACM)
  - Established in 1947 as “the world’s first educational and scientific computing society”
  - Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others’ privacy, and respecting others’ intellectual property and copyrights.

Major IT Professional Organizations (cont’d)

- International Information Systems Security Certification Consortium, Inc. $(ISC)^2$
  - Nonprofit organization focusing on the development and implementation of information security certifications and credentials
  - Code is primarily designed for the information security professionals who have certification from $(ISC)^2$.
  - Code of ethics focuses on four mandatory canons.

Major IT Professional Organizations (cont'd)

- SANS (originally System Administration, Networking, and Security Institute)
  - Professional organization with a large membership dedicated to the protection of information and systems
  - SANS offers a set of certifications called Global Information Assurance Certification (GIAC).

Major IT Professional Organizations (cont'd)

- ISACA (originally Information Systems Audit and Control Association)
  - Professional association with focus on auditing, control, and security
  - Concentrates on providing IT control practices and standards
  - ISACA has a code of ethics for its professionals.

Major IT Professional Organizations (cont'd)

- Information Systems Security Association (ISSA)
  - Nonprofit society of information security (IS) professionals
  - Primary mission to bring together qualified IS practitioners for information exchange and educational development
  - Promotes code of ethics similar to $(ISC)^2$, ISACA, and ACM

Key U.S. Federal Agencies

- Department of Homeland Security (DHS)
  - Made up of five directorates, or divisions
  - Mission is to protect the citizens as well as the physical and informational assets of the United States
  - US-CERT provides mechanisms to report phishing and malware.
- U.S. Secret Service
  - In addition to protective services, it is charged with safeguarding the nation’s financial infrastructure and payments system to preserve integrity of the economy.

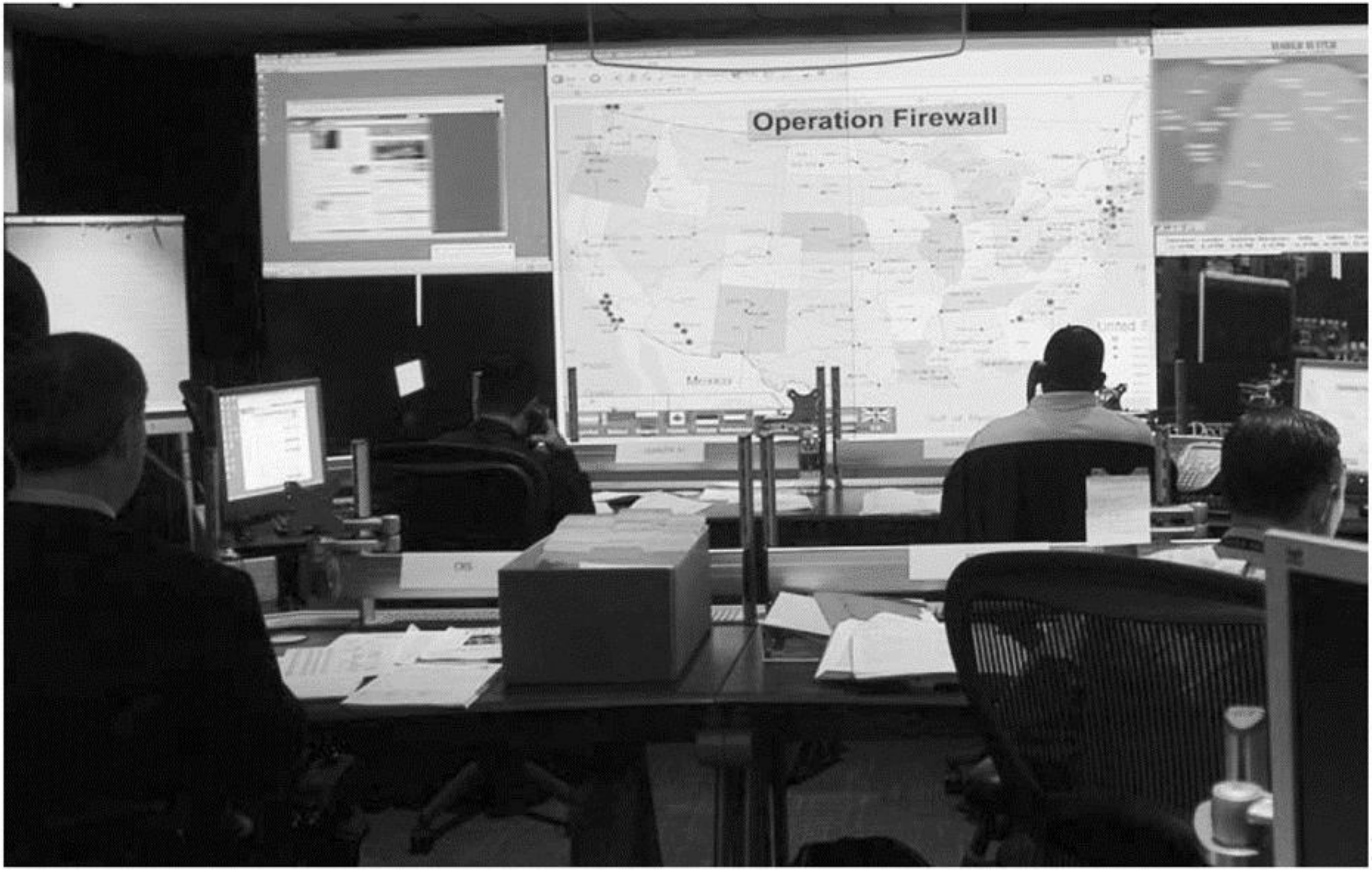
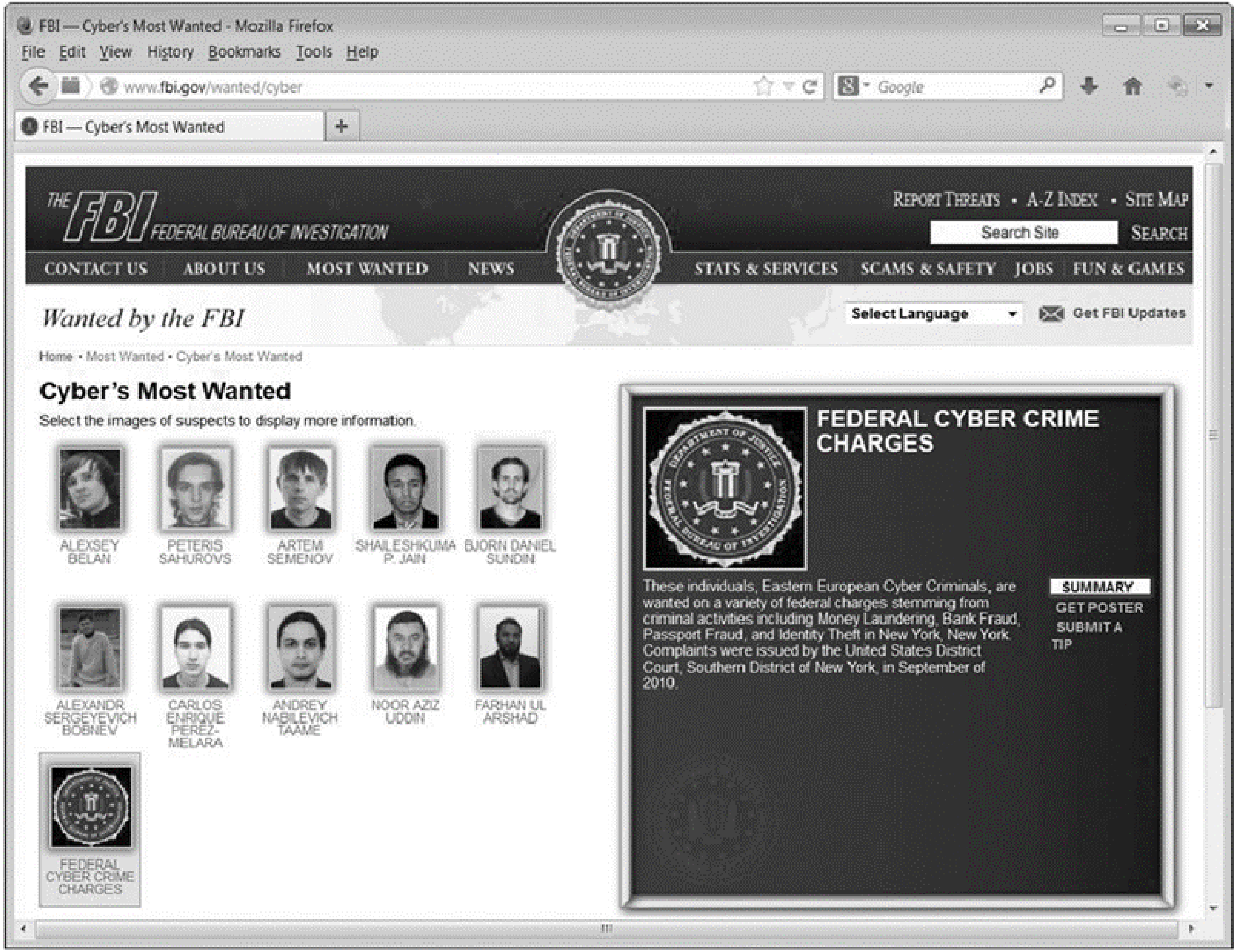


Figure 3-10 U.S. Secret Service Operation Firewall

Source: USSS.[36]

Key U.S. Federal Agencies (cont'd)

- Federal Bureau of Investigation
  - Primary law enforcement agency; investigates traditional crimes and cybercrimes
  - Key priorities include computer/network intrusions, identity theft, and fraud
  - Federal Bureau of Investigation's National InfraGard Program
    - Maintains an intrusion alert network
    - Maintains a secure Web site for communication about suspicious activity or intrusions
    - Sponsors local chapter activities
    - Operates a help desk for questions



FBI — Cyber's Most Wanted - Mozilla Firefox
File Edit View History Bookmarks Tools Help
www.fbi.gov/wanted/cyber
Google
FBI — Cyber's Most Wanted
THE FBI FEDERAL BUREAU OF INVESTIGATION
REPORT THREATS • A-Z INDEX • SITE MAP
Search Site
SEARCH
CONTACT US
ABOUT US
MOST WANTED
NEWS
STATS & SERVICES
SCAMS & SAFETY
JOBS
FUN & GAMES
Wanted by the FBI
Select Language
Get FBI Updates
Home • Most Wanted • Cyber's Most Wanted

Cyber's Most Wanted

Select the images of suspects to display more information.

ALEXSEY BELAN
PETERIS SAHUROVS
ARTEM SEMENOV
SHAILESHKUMA P. JAIN
BJORN DANIEL SUNDIN
ALEXANDR SERGEYEVICH BOBNEV
CARLOS ENRIQUE PEREZ-MELARA
ANDREY NABILEVICH TAAME
NOOR AZIZ UDDIN
FARHAN UL ARSHAD
FEDERAL CYBER CRIME CHARGES

FEDERAL CYBER CRIME CHARGES

These individuals, Eastern European Cyber Criminals, are wanted on a variety of federal charges stemming from criminal activities including Money Laundering, Bank Fraud, Passport Fraud, and Identity Theft in New York, New York. Complaints were issued by the United States District Court, Southern District of New York, in September of 2010.

Figure 3-12 FBI Cyber's Most Wanted list

Key U.S. Federal Agencies (cont'd)

- National Security Agency (NSA)
  - Is the nation's cryptologic organization
  - Responsible for signal intelligence and information assurance (security)
  - Information Assurance Directorate (IAD) is responsible for the protection of systems that store, process, and transmit information of high national value.

Summary

- Laws: rules that mandate or prohibit certain behavior in society; drawn from ethics
- Ethics: define socially acceptable behaviors, based on cultural mores (fixed moral attitudes or customs of a particular group)
- Types of law: civil, criminal, private, public

Summary (cont'd)

- Relevant U.S. laws:
  - Computer Fraud and Abuse Act of 1986 (CFA Act)
  - National Information Infrastructure Protection Act of 1996
  - USA PATRIOT Act of 2001
  - USA PATRIOT Improvement and Reauthorization Act
  - Computer Security Act of 1987
  - Title 18, U.S.C. § 1028

Summary (cont'd)

- Many organizations have codes of conduct and/or codes of ethics.
- Organization increases liability if it refuses to take measures known as due care.
- Due diligence requires that organizations make a valid effort to protect others and continually maintain that effort.