3

Legal, Ethical, and Professional Issues in Information Security

PRINCIPLES of 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:

- Use this chapter as a guide for future reference on laws, regulations, and professional organizations
- Differentiate between laws and ethics
- Identify major national laws that relate to the practice of information security
- Understand the role of culture as it applies to ethics in information security

Introduction

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

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain societal behavior
- Ethics: define socially acceptable behavior
- Cultural mores: fixed moral attitudes or customs of a particular group; ethics based on these
- Laws carry sanctions of a governing authority; ethics do not

Organizational Liability and the Need for Counsel

- Liability: legal obligation of an entity extending beyond criminal or contract law; includes legal obligation to make restitution
- Restitution: to compensate for wrongs committed by an organization or its employees
- Due care: insuring that employees know what constitutes acceptable behavior and know the consequences of illegal or unethical actions
- Due diligence: making a valid effort to protect others; continually maintaining level of effort

Organizational Liability and the Need for Counsel (continued)

- Jurisdiction: court's right to hear a case if the wrong was committed in its territory or involved its citizenry
- Long arm jurisdiction: right of any court to impose its authority over an individual or organization if it can establish jurisdiction

Policy versus Law

- Policies: body of expectations that describe acceptable and unacceptable employee behaviors in the workplace
- Policies function as laws within an organization; must be crafted carefully to ensure they are complete, appropriate, fairly applied to everyone
- Difference between policy and law: ignorance of a policy is an acceptable defense
- 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 organizational entities and people
- Criminal: addresses violations harmful to society; actively enforced by the state
- Private: regulates relationships between individuals and organizations
- Public: regulates structure/administration of government agencies and relationships with citizens, employees, and other governments

Relevant U.S. Laws

- United States has been a leader in the development and implementation of information security legislation
- Implementation of information security legislation contributes to a more reliable business environment and a stable economy
- U.S. has demonstrated understanding of problems facing the information security field; has specified penalties for individuals and organizations failing to follow requirements set forth in U.S. civil statutes

General Computer Crime 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

Privacy

- One of the hottest topics in information security
- Is a “state of being free from unsanctioned intrusion”
- Ability to aggregate data from multiple sources allows creation of information databases previously unheard of

Privacy of Customer Information

- 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

- Federal Trade Commission: “occurring when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes”
- Fraud And Related Activity In Connection With Identification Documents, Authentication Features, And Information (Title 18, U.S.C. § 1028)

Export and Espionage Laws

- Economic Espionage Act of 1996 (EEA)
- Security And Freedom Through Encryption Act of 1999 (SAFE)

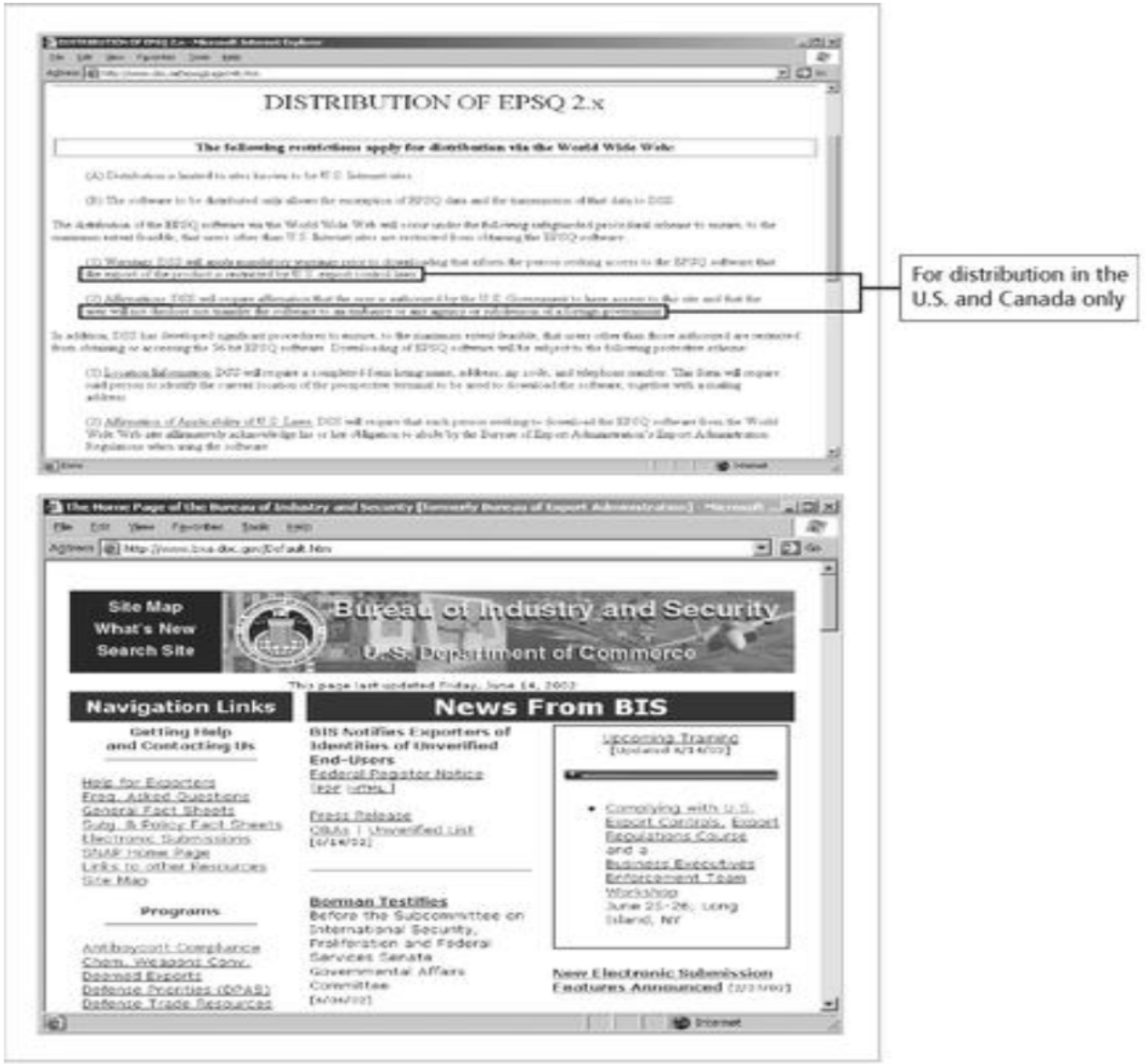

FIGURE 3-2 Export and Espionage

U.S. Copyright Law

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

FIGURE 3-2 The U.S. Copyright Office Web Site

Financial Reporting

- Sarbanes-Oxley Act of 2002
- Affects executive management of publicly traded corporations and public accounting firms
- Seeks to improve 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 required to disclose any requested information upon receipt of written request
- Some information protected from disclosure

State and Local Regulations

- Restrictions on organizational computer technology use exist at international, national, state, local levels
- Information security professional responsible for understanding state regulations and ensuring organization is compliant with regulations

International Laws and Legal Bodies

- IT professionals and IS practitioners should realize that when organizations do business on the Internet, they do business globally
- Professionals must be sensitive to laws and ethical values of many different cultures, societies, and countries
- Because of political complexities of relationships among nations and differences in culture, there are few international laws relating to privacy and information security
- These international laws are important but are limited in their enforceability

European Council Cyber-Crime Convention

- Establishes international task force overseeing 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

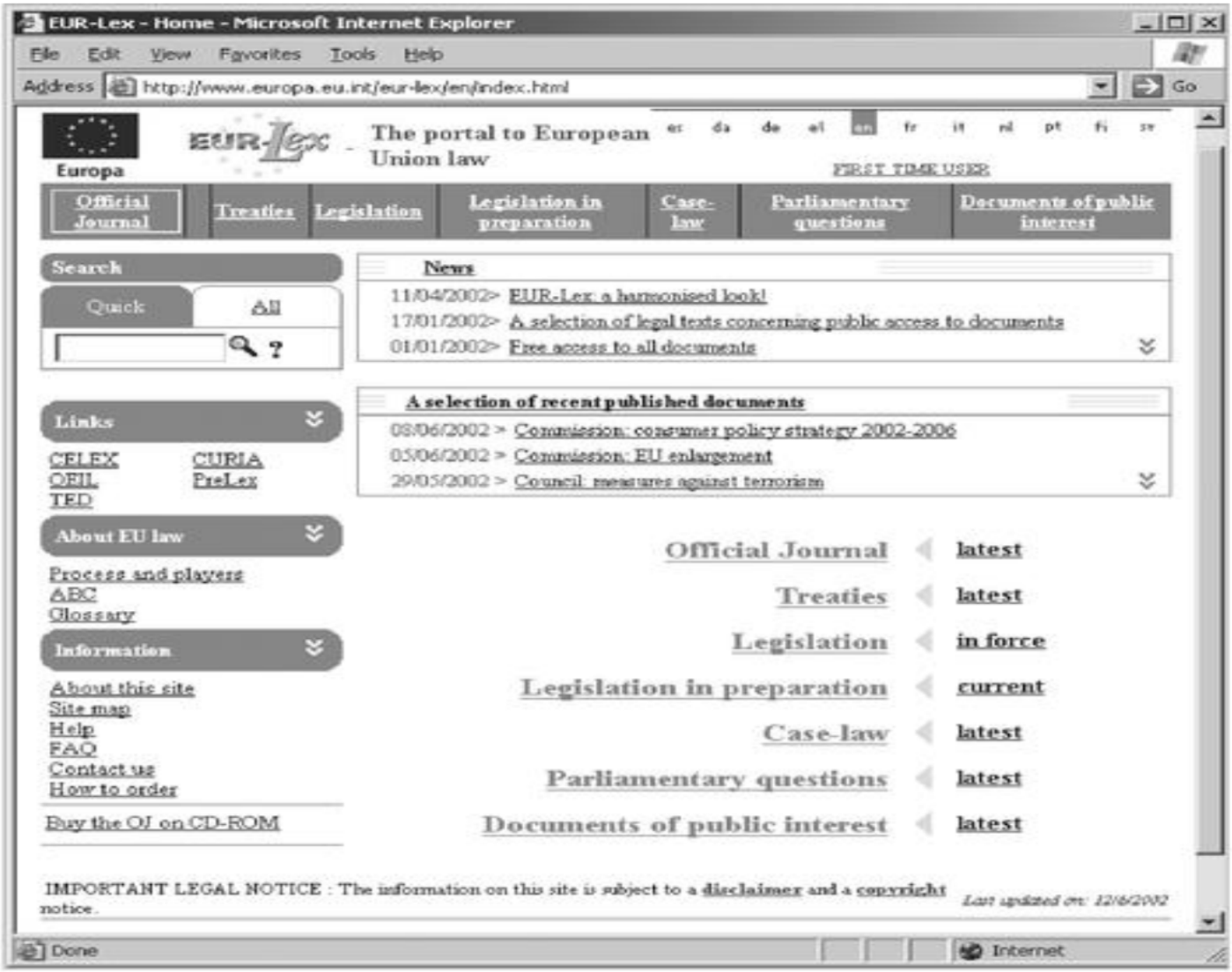

FIGURE 3-5 EU Law Portal

Agreement on Trade-Related Aspects of Intellectual Property Rights

- Created by World Trade Organization (WTO)
- First significant international effort to protect intellectual property rights
- 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 in their own territories
  - 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, which adds protection to individuals with regard to processing and free movement of personal data

United Nations Charter

- Makes provisions, to a degree, for information security during information warfare (IW)
- IW involves use of information technology to conduct organized and lawful military operations
- IW is relatively new type of warfare, although military has been conducting electronic warfare operations for decades

FIGURE 3-6 UN International Law Web site

Ethics and Information Security

The Ten Commandments of Computer Ethics [6]

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 ethics of another national group
- Example: many of the ways in which Asian cultures use computer technology is considered software piracy by other nations

Ethics and Education

- Overriding factor in leveling ethical perceptions within a small population is education
- Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security
- Proper ethical training vital to creating informed, well prepared, and low-risk system user

Deterrence to 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; e.g., laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - Probability of being caught
  - Probability of penalty being administered

Codes of Ethics and Professional Organizations

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

Association of Computing Machinery (ACM)

- 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

International Information Systems Security Certification Consortium, Inc. $(ISC)^2$

- Nonprofit organization focusing on development and implementation of information security certifications and credentials
- Code primarily designed for information security professionals who have certification from $(ISC)^2$
- Code of ethics focuses on four mandatory canons

System Administration, Networking, and Security Institute (SANS)

- Professional organization with a large membership dedicated to protection of information and systems
- SANS offers set of certifications called Global Information Assurance Certification (GIAC)

Information Systems Audit and Control Association (ISACA)

- Professional association with focus on auditing, control, and security
- Concentrates on providing IT control practices and standards
- ISACA has code of ethics for its professionals

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)
- Federal Bureau of Investigation's National InfraGard Program
- National Security Agency (NSA)
- U.S. Secret Service

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 (continued)

- 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

Summary (continued)

- 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 organization make valid effort to protect others and continually maintain that effort