COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fourth 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
  - Differentiate between laws and ethics
  - Identify major national laws that affect the practice of information security
  - Explain 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 (cont'd.)

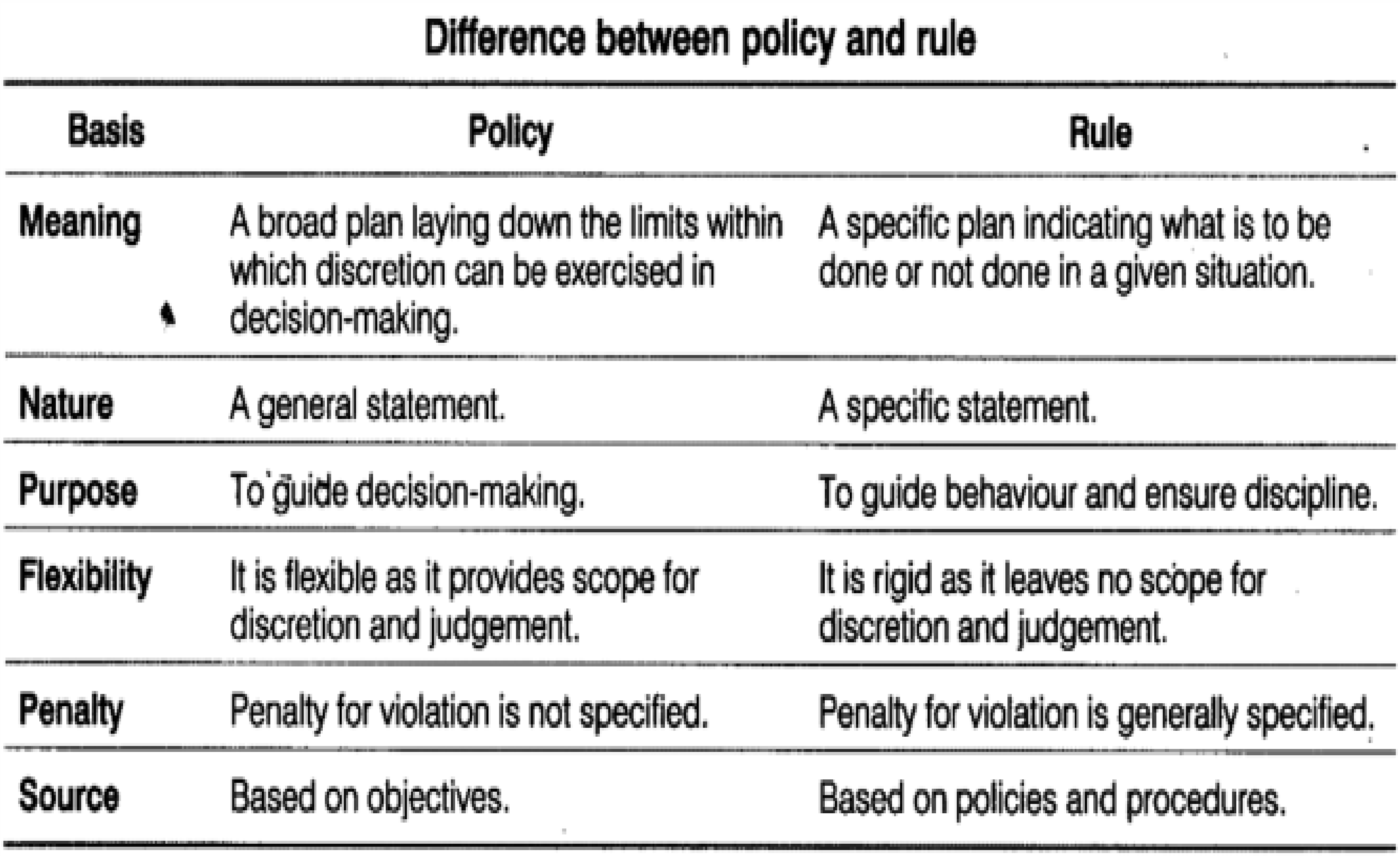
- Jurisdiction: court's right to hear a case if the wrong was committed in its territory or involved its citizenry
- Long arm jurisdiction: right of any court to impose its authority over an individual or organization if it can establish jurisdiction

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

Policy versus Law (cont'd.)

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



Difference between policy and rule

Basis	Policy	Rule
Meaning	A broad plan laying down the limits within which discretion can be exercised in decision-making.	A specific plan indicating what is to be done or not done in a given situation.
Nature	A general statement.	A specific statement.
Purpose	To guide decision-making.	To guide behaviour and ensure discipline.
Flexibility	It is flexible as it provides scope for discretion and judgement.	It is rigid as it leaves no scope for discretion and judgement.
Penalty	Penalty for violation is not specified.	Penalty for violation is generally specified.
Source	Based on objectives.	Based on policies and procedures.

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): 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 penalties judged on 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
- Is a “state of being free from unsanctioned intrusion”
- 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

Privacy (cont'd.)

- US 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

Privacy (cont’d.)

- 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)

Privacy (cont'd.)

- If someone suspects identity theft
  - Report to the three dominant consumer reporting companies that your identity is threatened
  - Account
    - Close compromised account
    - Dispute accounts opened without permission
  - Register your concern with the FTC(Federal Trade Commission)
  - Report the incident to either your local police or police in the location where the identity theft occurred

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange
- Consumer control of medical information
- Boundaries on the use of medical information
- Accountability for the privacy of private information
- Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
- Security of health information

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 in criminal activity
  - Relax export restrictions
  - Additional penalties for using it in a crime

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

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

Agreement on Trade-Related Aspects of Intellectual Property Rights

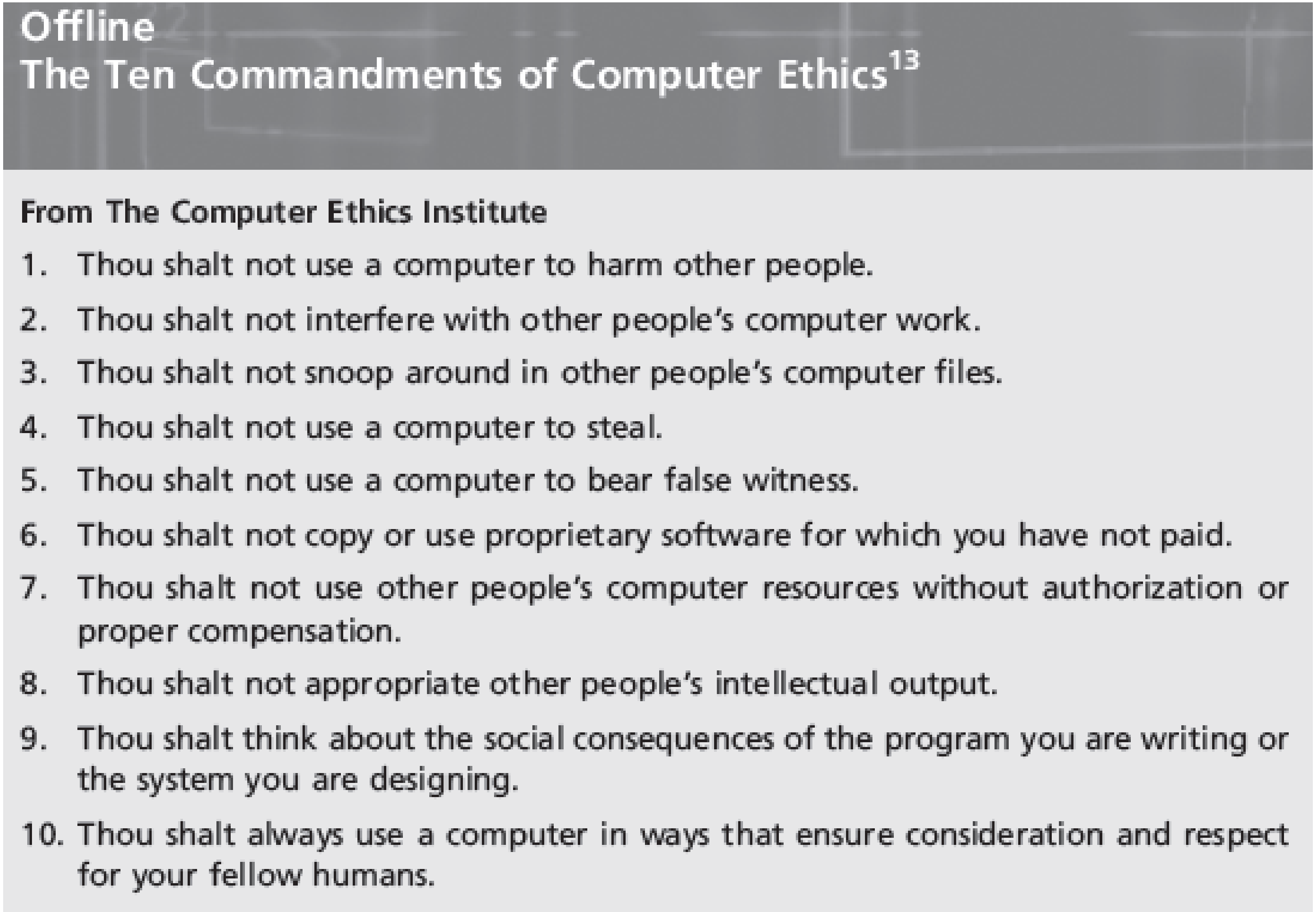
- Created by World Trade Organization (WTO)
- First significant international effort to protect intellectual property rights
- Outlines requirements for governmental oversight and legislation providing minimum levels of protection for intellectual property

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 in their own territories
  - Settling intellectual property disputes
  - Transitional arrangements while new system is being introduced

Ethics and Information Security

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



Offline
The Ten Commandments of Computer Ethics[13]

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
- Scenarios are grouped into:
  - Software License Infringement
  - Illicit(forbidden) Use
  - Misuse of Corporate Resources
- Cultures have different views on the scenarios

Ethics and Education

- Overriding factor in levelling 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 is vital to creating informed, well prepared, and low-risk 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; 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

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

Major IT Professional Organizations (cont'd.)

- 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

Major IT Professional Organizations (cont'd.)

- 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)

Major IT Professional Organizations (cont’d.)

- 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

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 people as well as the physical and informational assets of the US
- 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

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

- National Security Agency (NSA)
  - Is the Nation's cryptologic organization
  - Protects US information systems
  - Produces foreign intelligence information
  - Responsible for signal intelligence and information system security
- U.S. Secret Service
  - In addition to protective services, charged with the detection and arrest of persons committing a federal office relating to computer fraud or false identification