Law & Ethics, Policies & Guidelines, and Security Awareness

Modifications by Prof. Dong Xuan and
Adam C. Champion

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
- Describe management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines

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
- Read Ch. 3, 5 of the textbook

Terminology (1)

- See also p. 89 of textbook
- ***Cultural mores:*** fixed morals or customs of a group of people, form basis of ethics
- ***Ethics:*** Rules that define socially acceptable behavior, not necessarily criminal, not enforced (via authority/courts)
- ***Laws:*** Rules that mandate or prohibit behavior, enforced by governing authority (courts)
  - Laws carry sanctions of governing authority, ethics do not
- ***Policy:*** "Organizational laws"
  - Body of expectations that defines acceptable workplace behavior
  - General and broad, not aimed at specific technologies or procedures
  - To be enforceable, policy must be distributed, readily available, easily understood, and acknowledged by employees

Terminology (2)

- ***Standards, guidelines, best practices:*** define what must be done to comply with policy, how to do so
- ***Jurisdiction:*** a court's right to hear a case if a wrong was committed in its territory or against its citizens
- ***Long-arm jurisdiction:*** court's ability to "reach far" and apply law (another state, country)
- ***Case law:*** documentation about application of law in various cases
- ***Liability:*** legal obligation beyond what's required by law, increased if you fail to take due care
- ***Due care:*** has been taken when employees know what is/isn't acceptable, what the consequences are
- ***Due diligence:*** sustained efforts to protect others

Types of Law

- Civil: laws governing nation or state
- ***Criminal:*** harmful actions to society, prosecuted by the state
- Tort: individual lawsuits as recourse for “wrongs”, prosecuted by individual attorneys
- Private: includes family, commercial, labor law
- Public: includes criminal, administrative, constitutional law

Law and Information Security

- In practice, you can be sued for almost anything; no "absolute" protection against litigation
- Information security practices can:
  - Reduce likelihood that incidents result in lawsuits
  - Reduce likelihood that you lose (by demonstrating due care and due diligence)
  - Minimize damages/awards
  - Help you respond effectively and efficiently to incidents
- We'll focus on *criminal* laws. Know Table 3-1 in the book; FERPA, HIPAA, DMCA.

Relevant Federal Laws (General)

- Computer Fraud and Abuse Act of 1986 (CFAA)
- National Information Infrastructure Protection Act of 1996
- USA PATRIOT Act of 2001 (made permanent in 2006)
  - Broadens reach of law enforcement agencies
  - Broadens "protected" information re. open records law
  - Increased accountability, sanctions against money laundering
  - National Security Letters: cannot be contested before a judge, permanent gag order
- Telecommunications Deregulation and Competition Act of 1996
- Communications Decency Act of 1996 (CDA) (*struck down*)
- Computer Security Act of 1987: sets minimal federal government security standards

Relevant Federal Laws (Privacy)

- Federal Privacy Act of 1974: Federal government
- Electronic Communications Privacy Act of 1986: Regulates interception of electronic communications
- ***Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA):*** Requires privacy policies in healthcare and financial industries, restricts sharing & use of customer info
- Family Education Rights and Privacy Act (FERPA): Restricts distribution of "student academic records" such as names and grades
- Freedom of Information Act of 1966: can request info from gov't, some info is protected
- FACTA Red Flag regulation of 2009 (ID theft)

Relevant Federal Laws (Copyright)

- Intellectual property recognized as protected asset in the U.S.; copyright law extends to electronic formats

- With proper acknowledgement, permissible to include portions of others' work as reference

- U.S. Copyright Office website: www.copyright.gov

- ***Digital Millennium Copyright Act of 1998 (DMCA):*** criminalizes circumvention of technological copyright protection measures (some exceptions)

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
- State of Ohio:
  - Ohio Rev. Code §1347: notify data breach victims
  - Open records, anti-spam laws

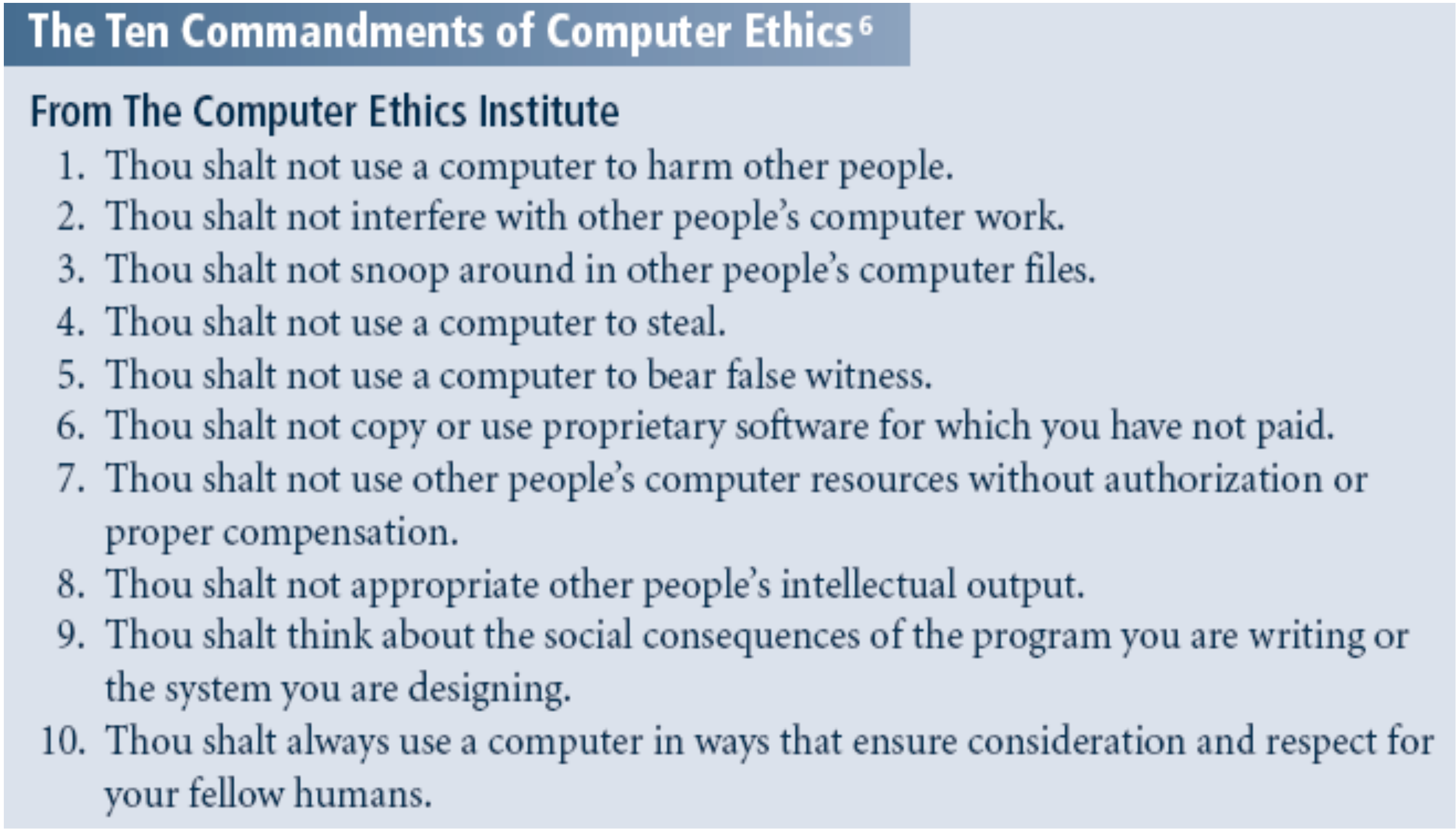
International Laws and Legal Bodies

- 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

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

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 ways in which Asian cultures use computer technology is software piracy

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

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

Computer Security Institute (CSI)

- Provides information and training to support computer, networking, and information security professionals

- Though without a code of ethics, has argued for adoption of ethical behavior among information security professionals

Key U.S. Federal Agencies

- Department of Homeland Security (DHS)
- Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC)
- National Security Agency (NSA)
- U.S. Secret Service

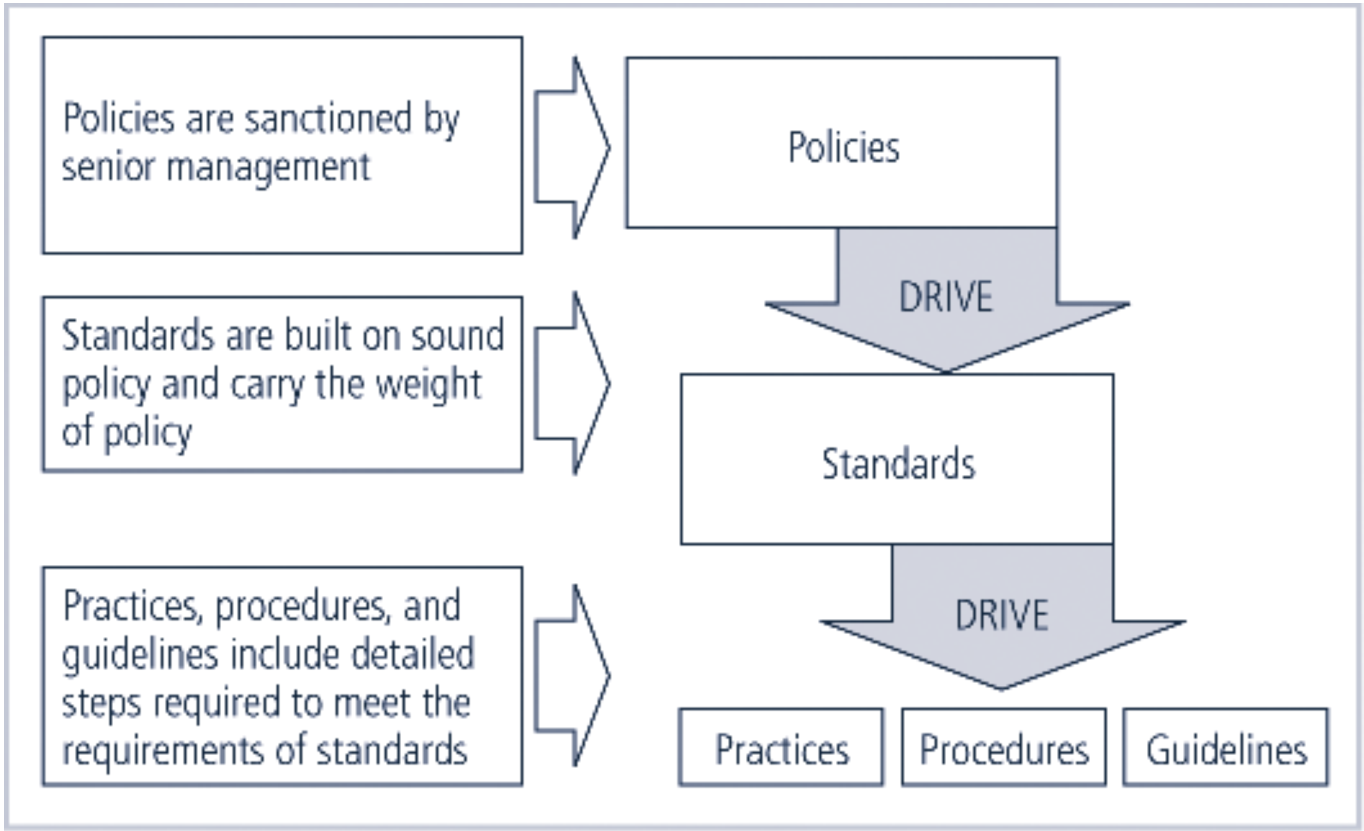
Information Security Policy, Standards and Practices

- Communities of interest must consider policies as basis for all information security efforts
- Policies direct how issues should be addressed and technologies used
- Security policies are least expensive controls to execute but most difficult to implement
- Shaping policy is difficult

OSU Policies and Standards

- Policies
  - Responsible Use of University Computing & Network Resources
  - Archives & Retention
  - Merchant Services & Use of Credit Cards
  - Deployment, Use of Wireless Data Networks
  - Public Records
  - Data Policy
  - Personal Info Disclosure

- Standards
  - University Computer Security Standards:
    - Min. Computer Security
    - Critical Server Security
    - Web Server Security
    - DB Server Security
  - Local Administrative Privilege Standard
- See http://ocio.osu.edu for more details



Policies are sanctioned by senior management

Standards are built on sound policy and carry the weight of policy

Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards

FIGURE 5-1 Policies, Standards, and Practices

Policy Management

- Policies must be managed as they constantly change
- To remain viable, security policies must have:
  - Individual responsible for reviews
  - A schedule of reviews
  - Method for making recommendations for reviews
  - Specific policy issuance and revision date

Information Classification

- Classification of information is an important aspect of policy, *e.g.*, public, internal, classified
- Policies are classified
- A clean desk policy stipulates that at end of business day, classified information must be properly stored and secured
- In today' s open office environments, may be beneficial to implement a clean desk policy

Security Education, Training, and Awareness Program

- As soon as general security policy exist, policies to implement security education, training and awareness (SETA) program should follow
- SETA is a control measure designed to reduce accidental security breaches
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness

Security Education

- Everyone in an organization needs to be trained and aware of information security; not every member needs formal degree or certificate in information security

- When formal education for individuals in security is needed, an employee can identify curriculum available from local institutions of higher learning or continuing education

- A number of universities have formal coursework in information security

Security Training

- Involves providing members of organization with detailed information and hands-on instruction designed to prepare them to perform their duties securely

- Management of information security can develop customized in-house training or outsource the training program

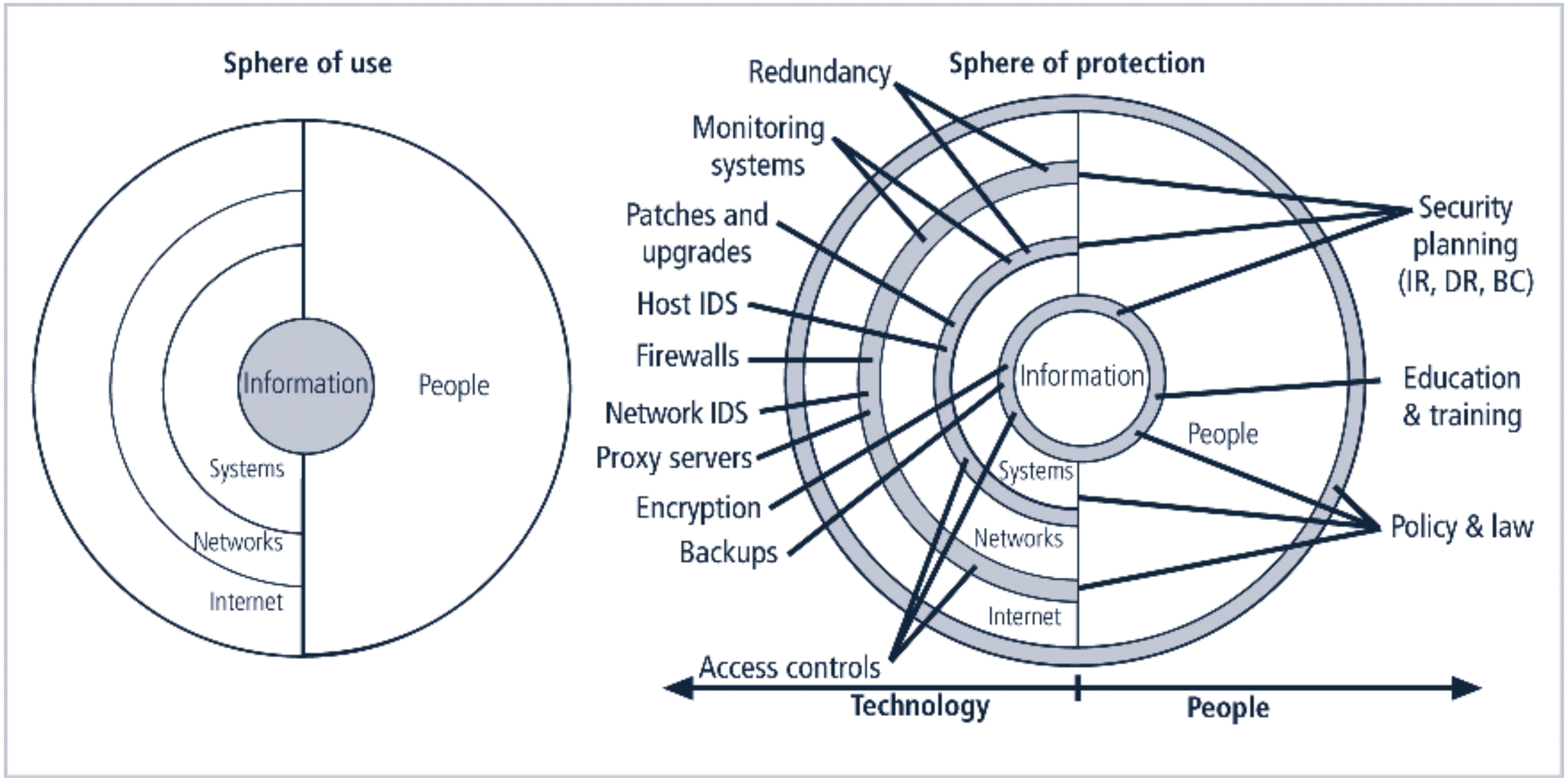


FIGURE 5-15 Spheres of Security

Design of Security Architecture

- Defense in depth
  - Implementation of security in layers
  - Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls
- Security perimeter
  - Point at which an organization’s security protection ends and outside world begins
  - Does not apply to internal attacks from employee threats or on-site physical threats

Key Technology Components

- Firewall: device that selectively discriminates against information flowing into or out of organization
- Demilitarized zone (DMZ): no-man’s land between inside and outside networks where some organizations place Web servers
- Intrusion Detection Systems (IDSes): in effort to detect unauthorized activity within inner network, or on individual machines, organization may wish to implement an IDS

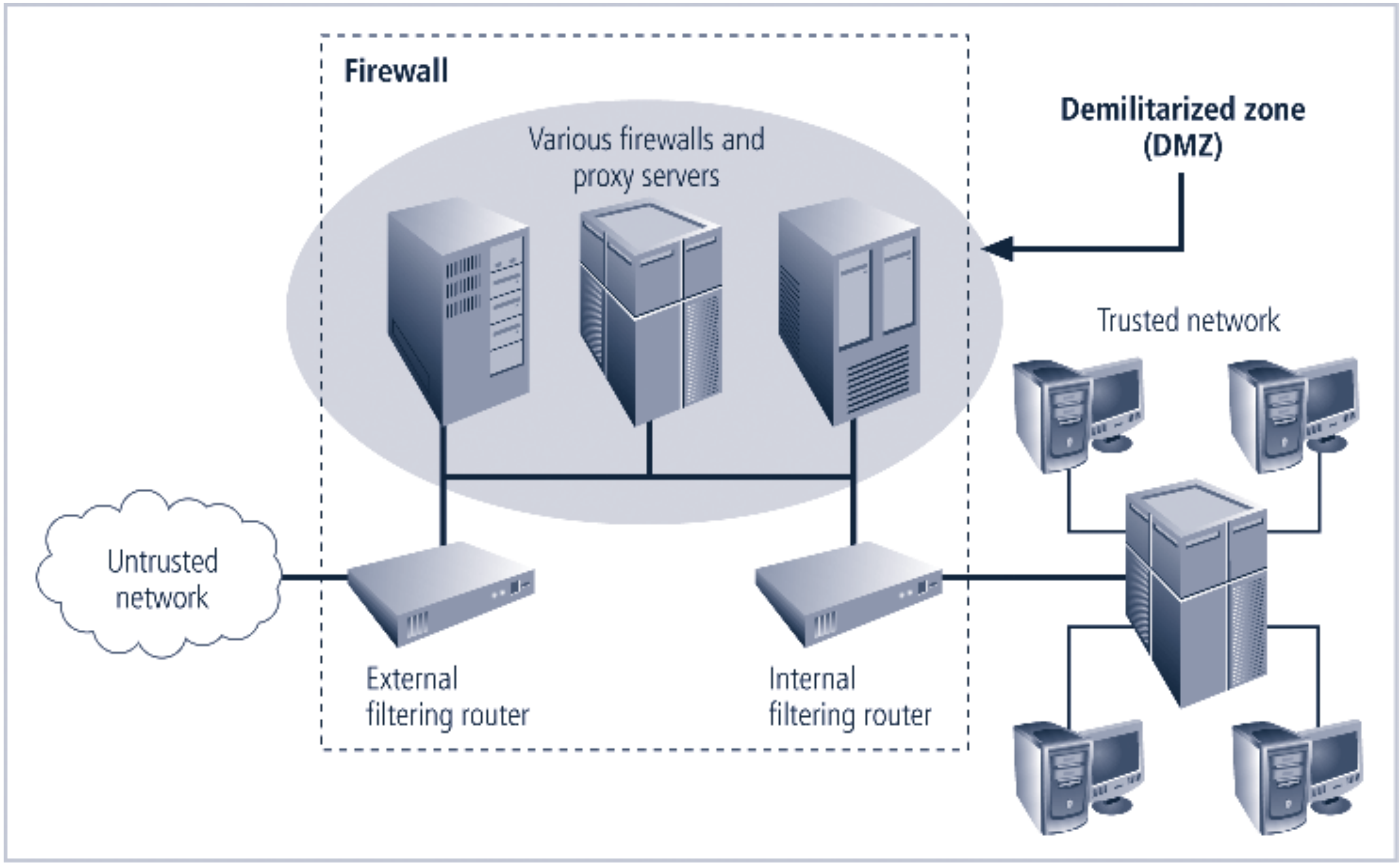

Firewall
Various firewalls and proxy servers
Demilitarized zone (DMZ)
Trusted network
Untrusted network
External filtering router
Internal filtering router

FIGURE 5-18 Firewalls, Proxy Servers, and DMZs

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, tort law, private, public
- Management has essential role in development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines