Law & Ethics, Policies & Guidelines, and Security Awareness

CSE 4471: Information Security

Instructor: Adam C. Champion, Ph.D.

Reading: Chaps. 3, 5 in textbook

Introduction

- You need to understand an organization's legal, ethical responsibilities
- To minimize liabilities and reduce risks, the information security practitioner must:
  - Understand current legal environment
  - Stay current with laws and regulations
  - Watch for emerging issues

Terminology (1)

- See also page 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"
  - Expectations that define 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 showing due care, due diligence)
  - Minimize damages/awards
  - Help you respond effectively 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 regarding open records law
  - Increased accountability, sanctions against money laundering
  - National Security Letters: administrative subpoenas with permanent gag orders
- Telecommunications Deregulation and Competition Act of 1996
- Communications Decency Act of 1996 (CDA) (partly 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" (including 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 (IP) protection in U.S., other countries
- Copyright law extends to electronic formats
- With citations, you can include brief portions of others' work as reference ("fair use")
- U.S. Copyright Office website: http://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 at state, local levels
- Information security professional responsible for understanding applicable regulations, compliance
- 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:
  - International task force oversees Internet security functions for standardized international technology laws
  - Attempts to improve effectiveness of international investigations into breaches of technology law
- General Data Protection Regulation (GDPR): requires website disclosure about data collection, user consent (Europe)

United Nations Charter

- Makes provisions, to a degree, for information security during information warfare (IW)
- IW uses information technology to conduct organized and lawful military operations
- IW is fairly 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 ethical behavior
- 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 considered piracy

Ethics and Education

- Education levels ethical perceptions within a small group of people
- Employees must be trained in expected behaviors, especially regarding 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 “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 training to support computer, networking, and info. security professionals
- Argued for adoption of ethical behavior among info. security professionals

Key U.S. Federal Agencies

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

Policy, Standards and Practices

- Communities of interest need to consider policies as starting point for 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

Policy Management

- Policies management needed due to change
- To remain viable, security policies must have:
  - People responsible for reviews
  - A schedule of reviews
  - Method for recommending reviews
  - Specific policy issuance and revision date

Information Classification

- Information classification an important aspect of policy (*e.g.*, public, internal, classified)
- Specific company policies may be classified, but general guidelines shared among companies
- A clean desk policy stipulates that at end of business day, classified information is properly secured
- Questions:
  - Feasibilities?
  - Benefits?

Security Education, Training, and Awareness Program

- Security education, training and awareness (SETA) implementation should follow security policy
  - Designed to reduce accidental security breaches
  - Training builds on general knowledge employees need for their jobs (focused on security aspects)

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

Spheres of Security (Fig. 5-15)

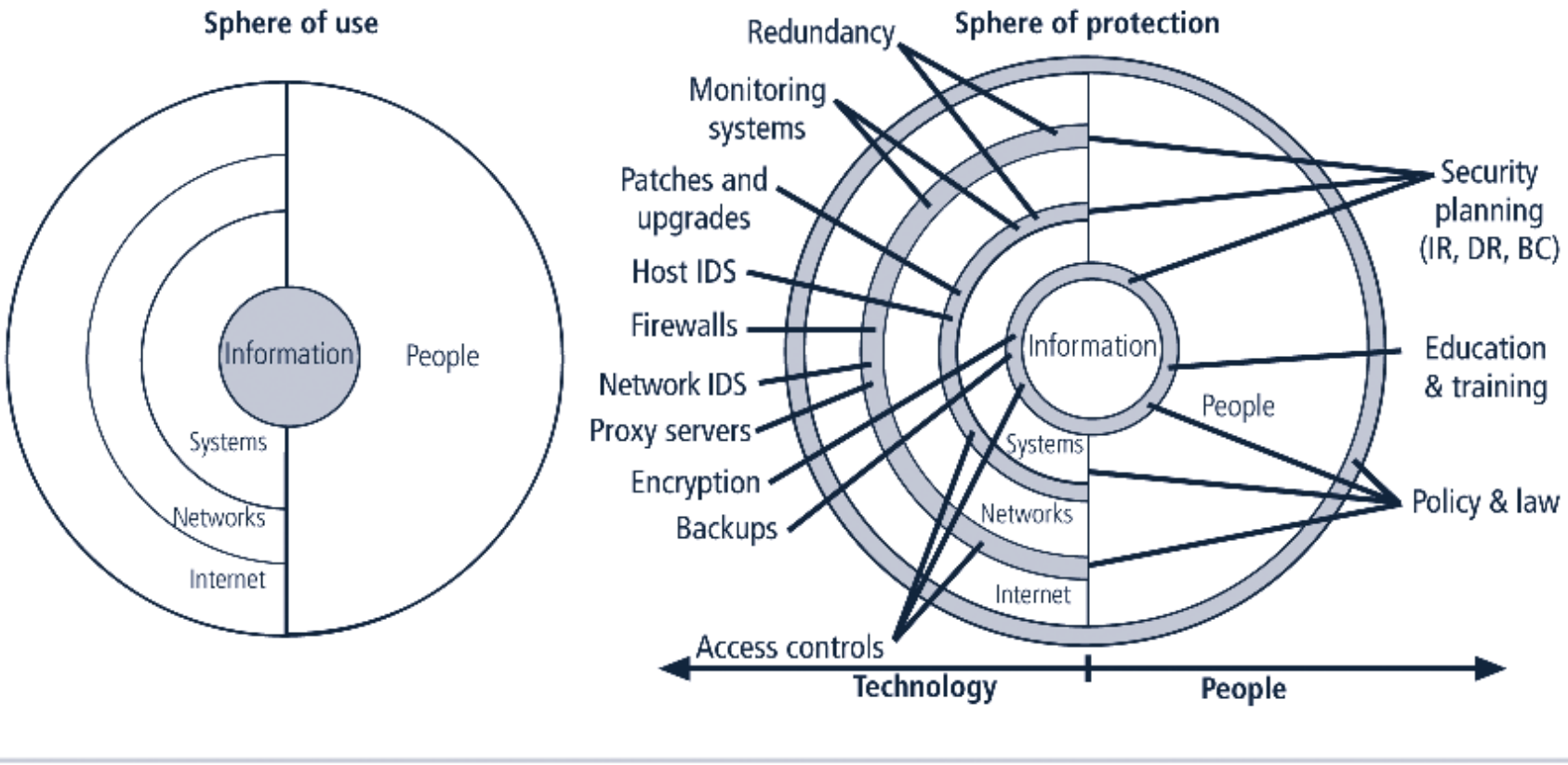

FIGURE 5-15 Spheres of Security

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

Security Technology Components

- Firewall: device that selectively allows information into/out of organization
- Demilitarized Zone (DMZ): “no-man’s land” between inside, outside networks; some companies place Web servers here
- Intrusion Detection Systems (IDSs): detects unauthorized (strange) activity on organizational network, individual machines, or both

Network Security Architecture (Fig. 5-18)

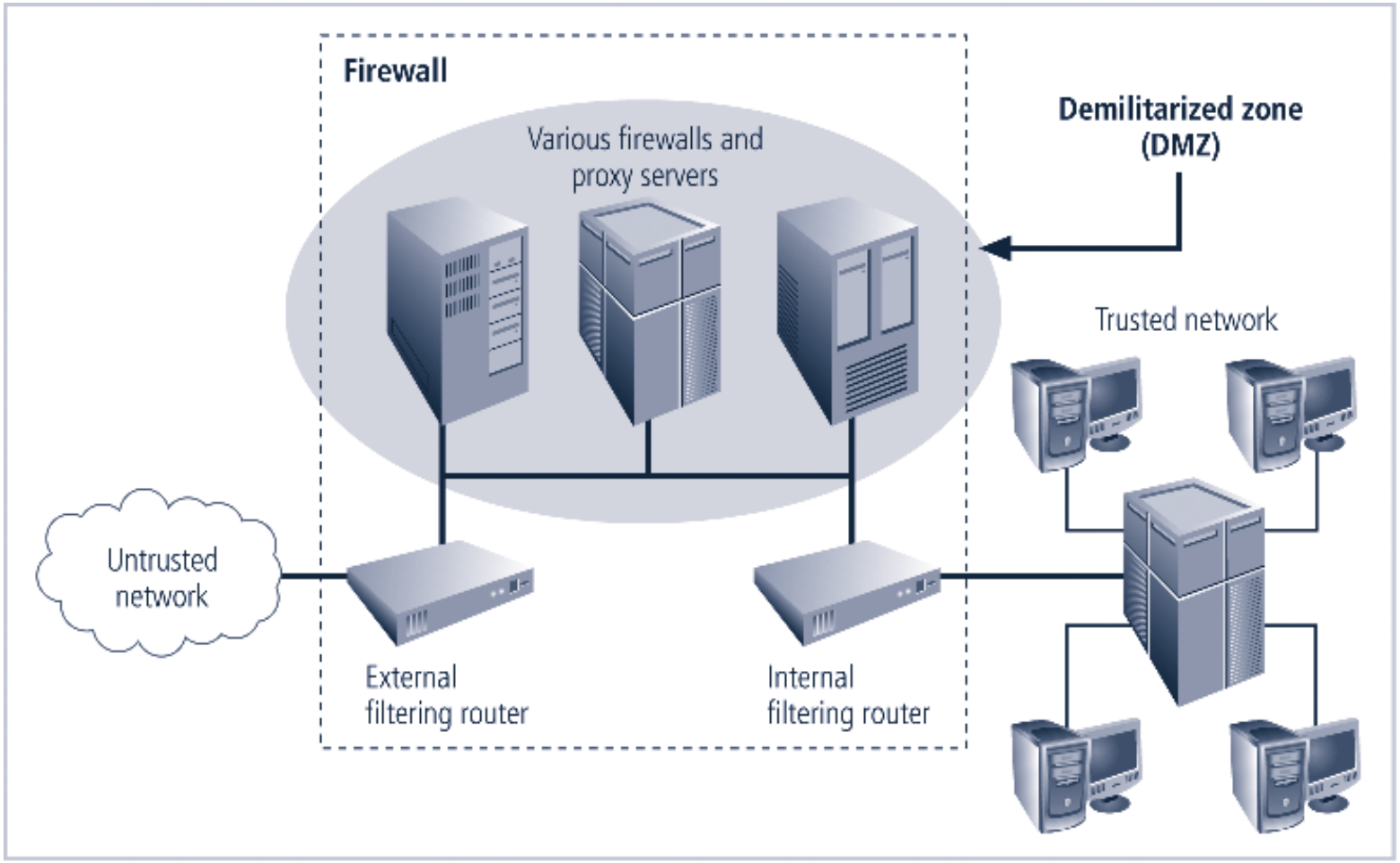

FIGURE 5-18 Firewalls, Proxy Servers, and DMZs

Summary

- Laws: state-enforced rules that mandate or prohibit certain behavior; drawn from ethics
- Ethics: define socially acceptable behaviors (may vary among groups)
- Policies: organizational laws
- Management needs to “set tone” for security practices, support their deployment