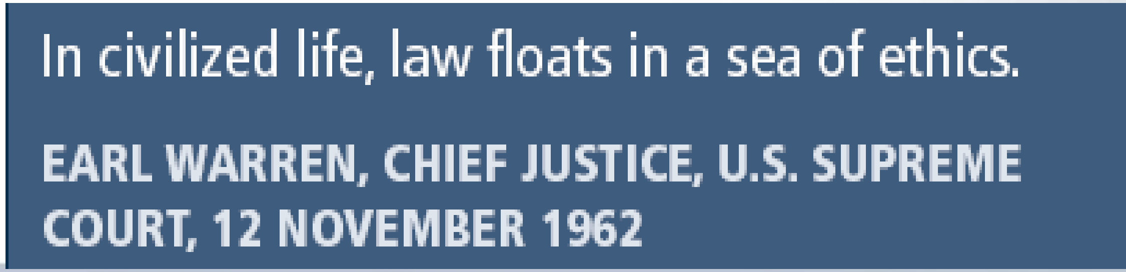
EE5084
Cyber Security

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

- Describe the functions of and relationships among laws, regulations, and professional organizations in information security
- Explain the differences between laws and ethics
- 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

Threats from Lawyers (1)

- Lawyers take **legal action** against an individual or organization

- Legal action may be on behalf of employees, customers, business partners, shareholders, or government

- These risks result from:
  - the failure to protect customer data,
  - the illegal, irresponsible, ignorant or unethical behavior of employees

Threats from Lawyers (2)

- While the potential for damage from hackers is <u>more evident</u>,
  hackers do not file lawsuits for:
  - harassment or discrimination,
  - privacy invasion,
  - disclosure of confidential information,
  - copyright infringement, or
  - investment fraud.

Liability Exposure

- Liability exposure refers to unnecessary risk that an organization exposes itself to when it fails to take action to prevent harm.

- Risk cannot be eliminated. It can only be minimized

Sources of liability exposure

- networked computers
- email and instant messaging
- ecommerce Websites
- client records on databases
- automated transactions
- digital signatures
- electronic contracting

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain behaviour and are enforced by the state
- Ethics: regulate and define socially acceptable behaviour
- Cultural mores: fixed moral attitudes or customs of a particular group

- Laws carry the authority of a governing authority; ethics do not.

Policy Versus Law

- Policies: managerial directives that specify acceptable and unacceptable employee behaviour 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 defence.

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.

Relevant Singapore Laws

Computer Misuse and Cybersecurity Act
(CHAPTER 50A)
(Original Enactment: Act 19 of 1993)

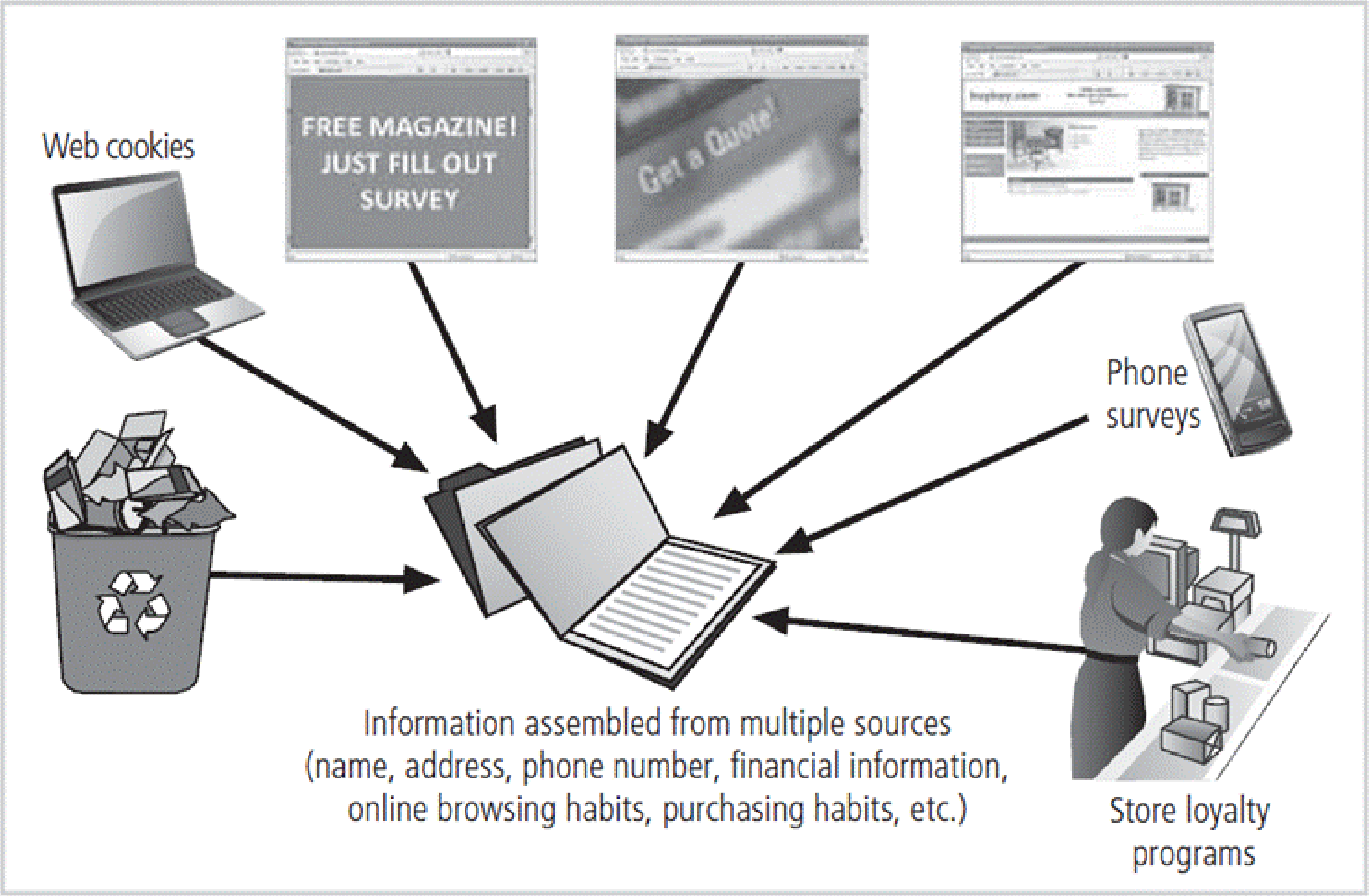
REVISED EDITION 2007
(31st July 2007)

An Act to make provision for securing computer material against unauthorised access or modification, to require or authorise the taking of measures to ensure cybersecurity, and for matters related thereto.

https://sso.agc.gov.sg/Act/CMA1993#legis

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

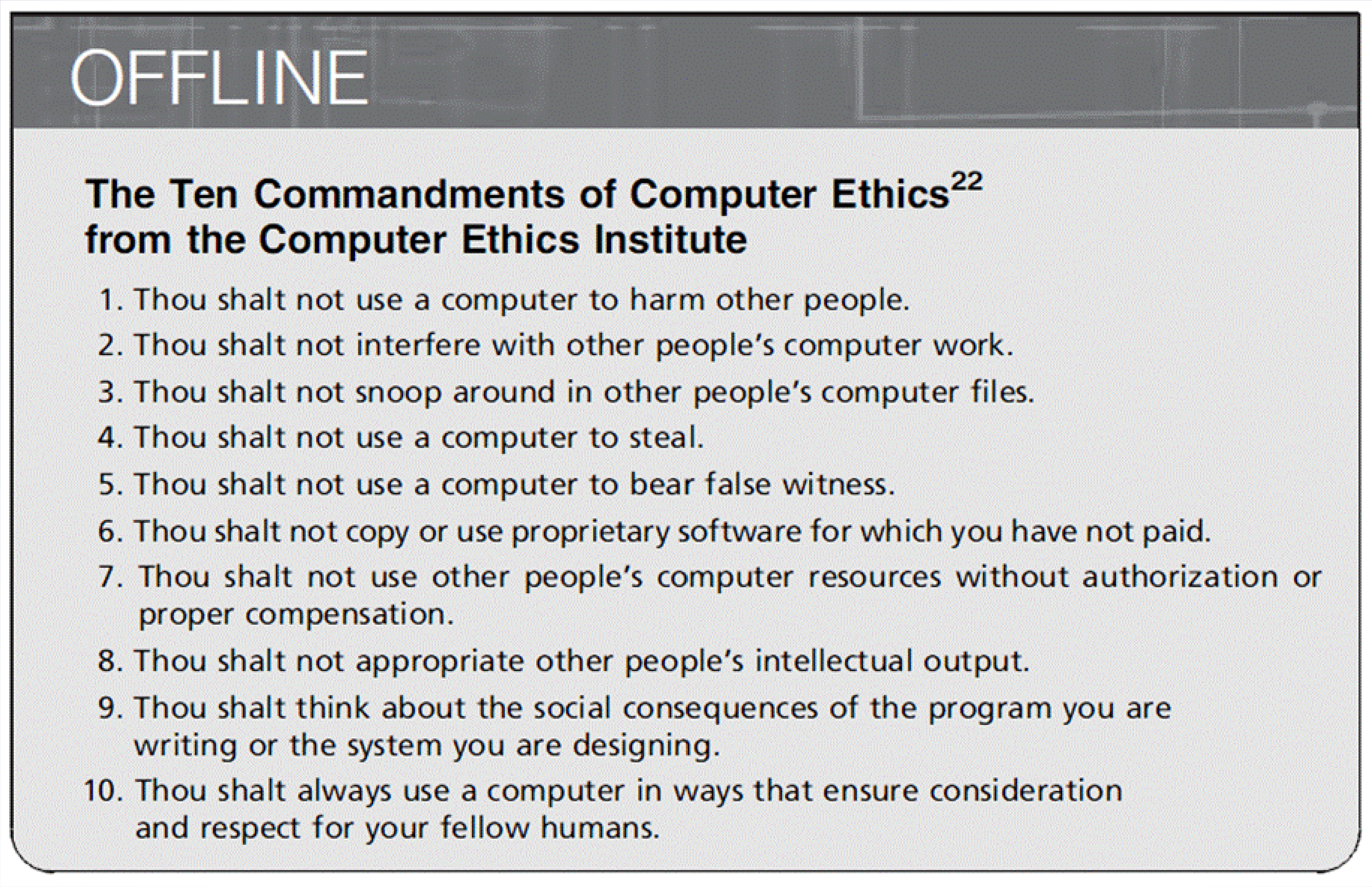
Singapore
Personal Data Protection Acts

- The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data.
- It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

International Laws and Legal Bodies

- When organizations do online business, they do so 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.
- Such international laws are important but are limited in their enforceability.



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.

Deterring Unethical and Illegal Behavior

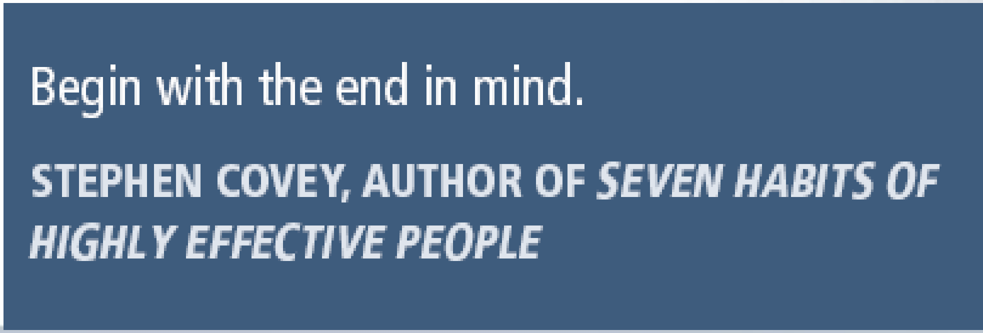
- Causes of unethical and illegal behaviour: ignorance, accident, intentional
- Deterrence: best method for preventing an illegal or unethical activity; for example, laws, policies, technical controls
- Laws and policies only deter if these conditions are present:
  - Fear of penalty
  - Probability of being apprehended
  - Probability of penalty being applied

Summary

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

EE 8084
Cyber Security

Planning for Security



Begin with the end in mind.

STEPHEN COVEY, AUTHOR OF *SEVEN HABITS OF HIGHLY EFFECTIVE PEOPLE*

Announcement - dates for the quizzes

1. Quiz 1 - 16 Sep 5pm
2. Quiz 2 - 28 Oct 5pm

- ✓ They will be conducted via EEE OASIS physically in the lab.
- ✓ We will inform you later about the lab allocation.
- ✓ More details will be released later.

- ✓ **IMPORTANT: Please email me if you cannot attend the quizzes physically due to SHN or you cannot be in Singapore due to the COVID-19 situation.**
- ✓ Please also note that attendance is compulsory;
- ✓ and we will not accept any other reasons for missing the quizzes unless you have an official LOA from your school.

Learning Objectives

- Management’s role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Institutionalizes policies, standards, and practices using education, training, and awareness programs
- Contingency planning and how it relates to incident response planning, disaster recovery planning, and business continuity plans

Introduction

- Policies, standards, and practices are the foundation for information security architecture and blueprint.
- Coordinated planning is required to create and maintain these elements.
- Strategic planning for the management of allocation of resources
- Contingency planning for the preparation of uncertain business environment

Information Security Planning and Governance (1)

- Planning levels help translate organization's strategic plans into tactical objectives.
- Planning and the CISO
- Information Security Governance
  - Governance:
    - Set of responsibilities and practices exercised by the board and executive management
    - Goal to provide strategic direction, establishment of objectives, and measurement of progress toward objectives
    - Also verifies/validates that risk management practices are appropriate and assets used properly

Information Security Planning and Governance (2)

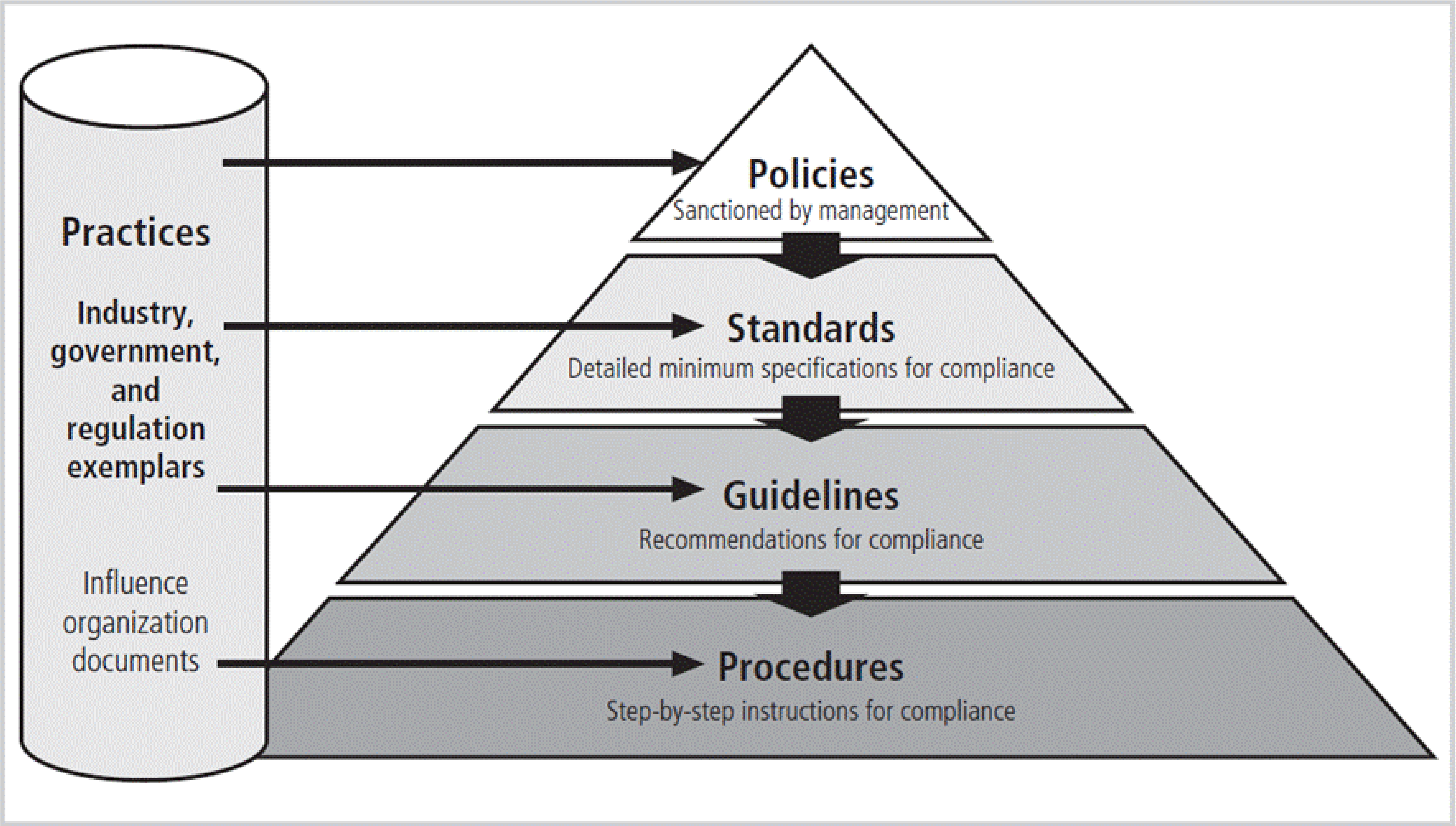
- Information Security Governance outcomes
  - Five goals:
    - Strategic alignment
    - Risk management
    - Resource management
    - Performance measures
    - Value delivery

Policy, Standards, and Practice (1)

- Policies is the basis for all information security planning, design, and deployment.
- Direct how issues should be addressed and technologies used.
- Should never contradict law, must be able to stand up in court, and must be properly administered.
- Policies are the least expensive controls to execute but most difficult to implement properly.

Policy, Standards, and Practice (2)

- Policy is the organizational law that dictates acceptable and unacceptable behavior.
- Standards are more detailed statements of what must be done to comply with policy
- Practices, procedures, and guidelines effectively explain how to comply with policy.
- For a policy to be effective, it must be properly disseminated, read, understood, and agreed to by all members of the organization, and uniformly enforced.


Practices
Industry, government, and regulation exemplars
Influence organization documents
Policies
Sanctioned by management
Standards
Detailed minimum specifications for compliance
Guidelines
Recommendations for compliance
Procedures
Step-by-step instructions for compliance

© Cengage Learning 2015

Figure 4-2 Policies, standards, guidelines, and procedures

Policy Management

- Policies must be managed as they constantly change.
- To remain viable, security policies must have:
  - A responsible manager
  - A schedule of reviews
  - A method for making recommendations for reviews
  - A policy issuance and revision date
  - Automated policy management

Security Models

- The ISO 27000 Series

  One of the most widely referenced security models

  http://www.27000.org/

- NIST Security Models

  Another possible approach described in the documents available from Computer Security Resource Center of NIST

  https://www.nist.gov

Design of Security Architecture (1)

- Spheres of security: foundation of the security framework
- Levels of controls:
  - Management controls set the direction and scope of the security processes and provide detailed instructions for its conduct.
  - Operational controls address personnel and physical security, and the protection of production inputs/outputs.
  - Technical controls are the tactical and technical implementations related to designing and integrating security in the organization.

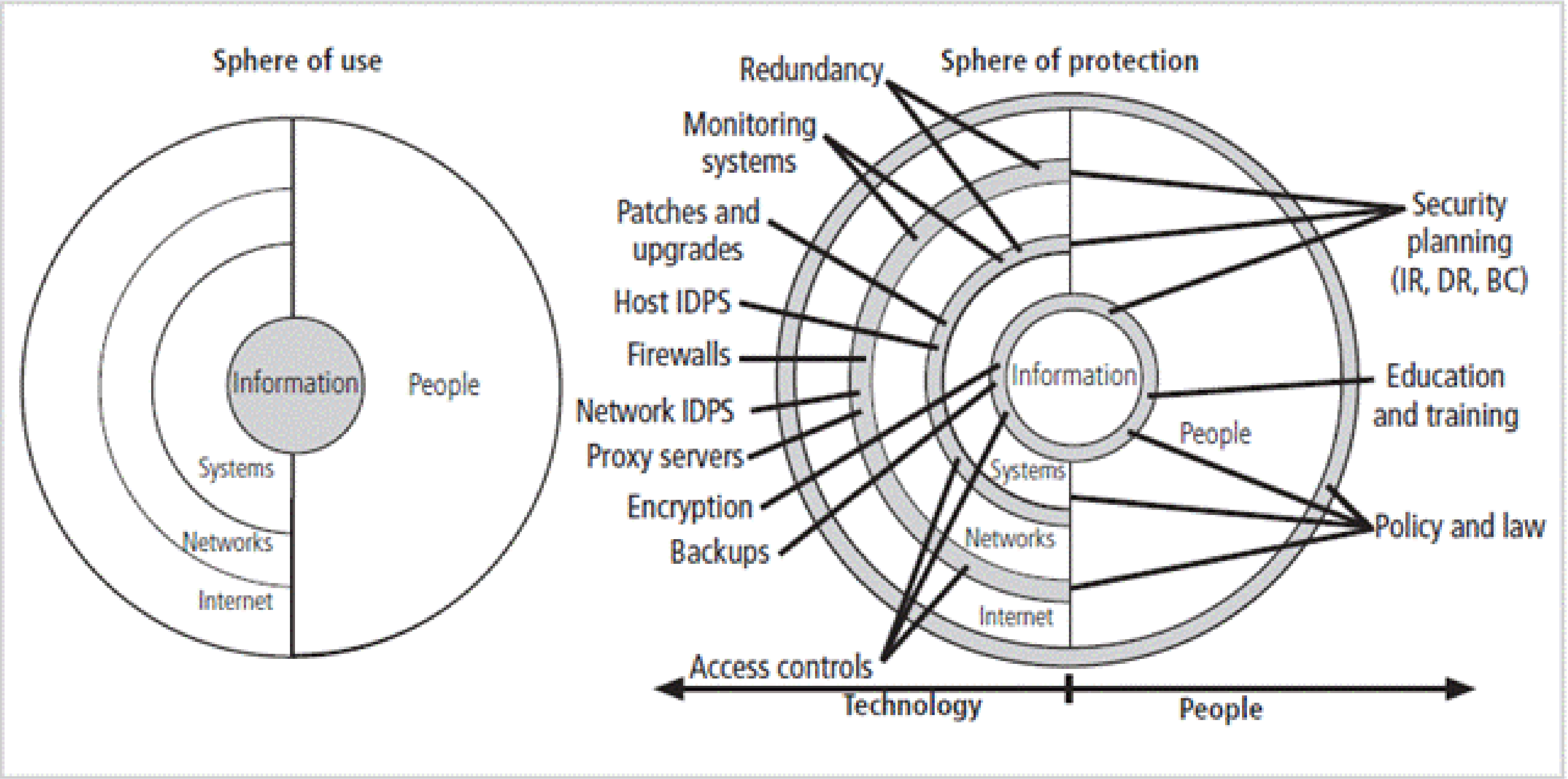
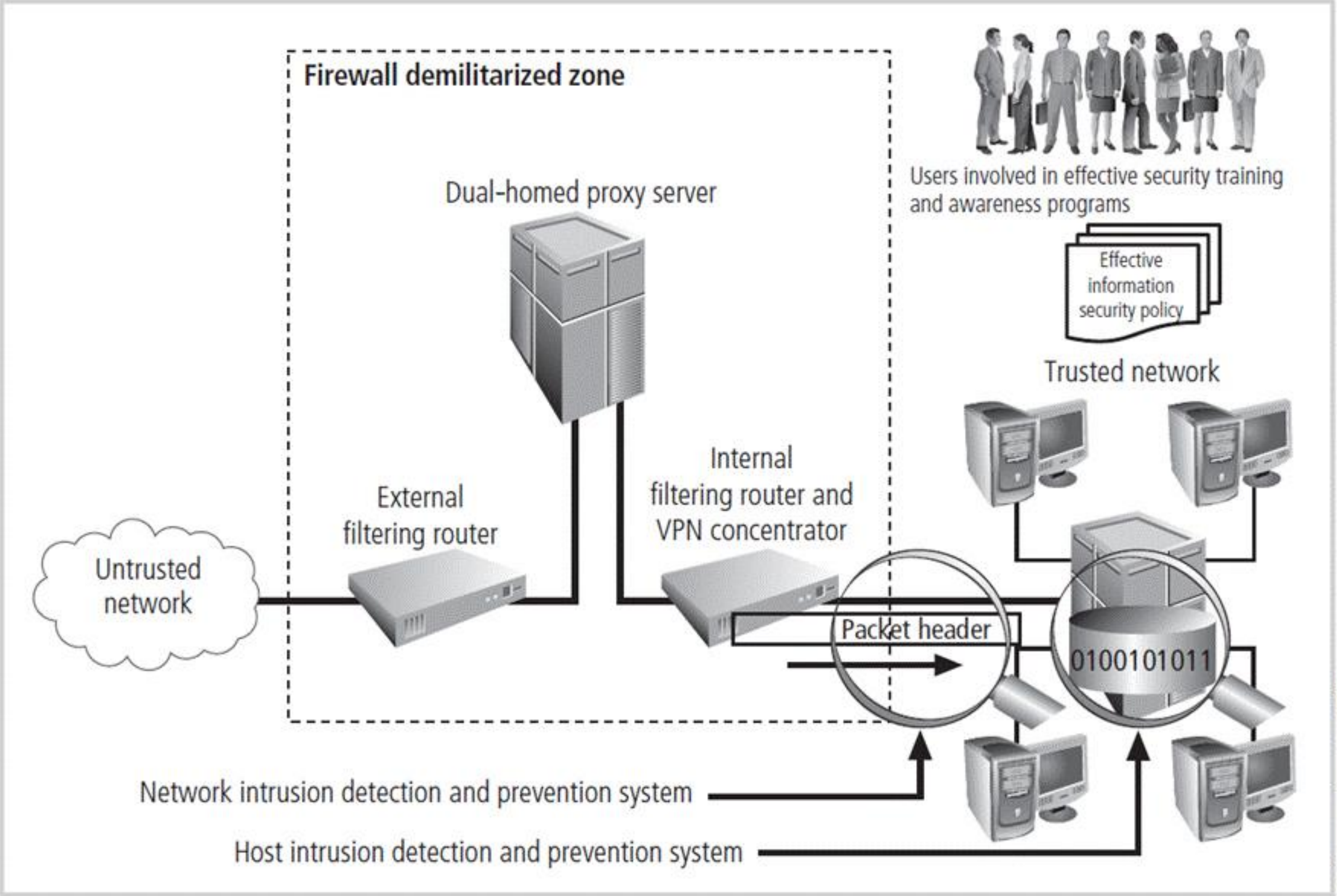


Figure 4-8 Spheres of security

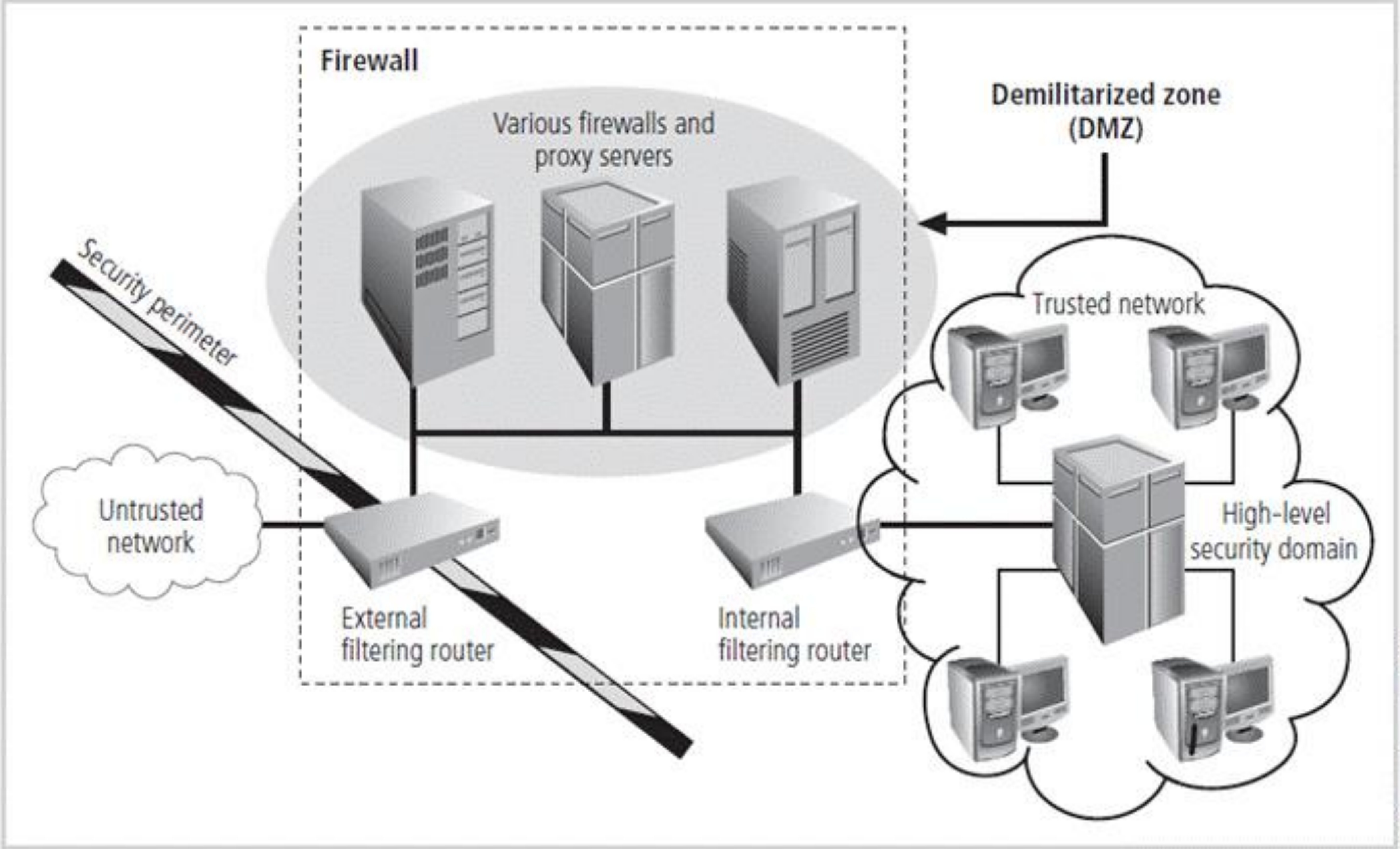
Design of Security Architecture (2)

- Defense in depth
  - Implementation of security in layers
  - Organization establish multiple layers of security controls and safeguards
- Security perimeter
  - Border of security protecting internal systems from outside threats
  - Does not protect against internal attacks from employee threats or onsite physical threats


Firewall demilitarized zone
Users involved in effective security training and awareness programs
Effective information security policy
Dual-homed proxy server
Trusted network
Internal filtering router and VPN concentrator
External filtering router
Untrusted network
Packet header
0100101011
Network intrusion detection and prevention system
Host intrusion detection and prevention system

© Cengage Learning 2015

Figure 4-9 Defense in depth


Firewall
Demilitarized zone (DMZ)
Various firewalls and proxy servers
Security perimeter
Trusted network
High-level security domain
Untrusted network
External filtering router
Internal filtering router

© Cengage Learning 2015

Figure 4-10 Security perimeters and domains

Security Education, Training, and Awareness Program

- After setting policy, we need to implement security education, training, and awareness (SETA) program
- SETA is a control measure designed to reduce accidental security breaches.
- Consists of security education, security training, and security awareness.
- Enhances security by improving awareness, developing skills, and knowledge, and building in-depth knowledge

Security Education

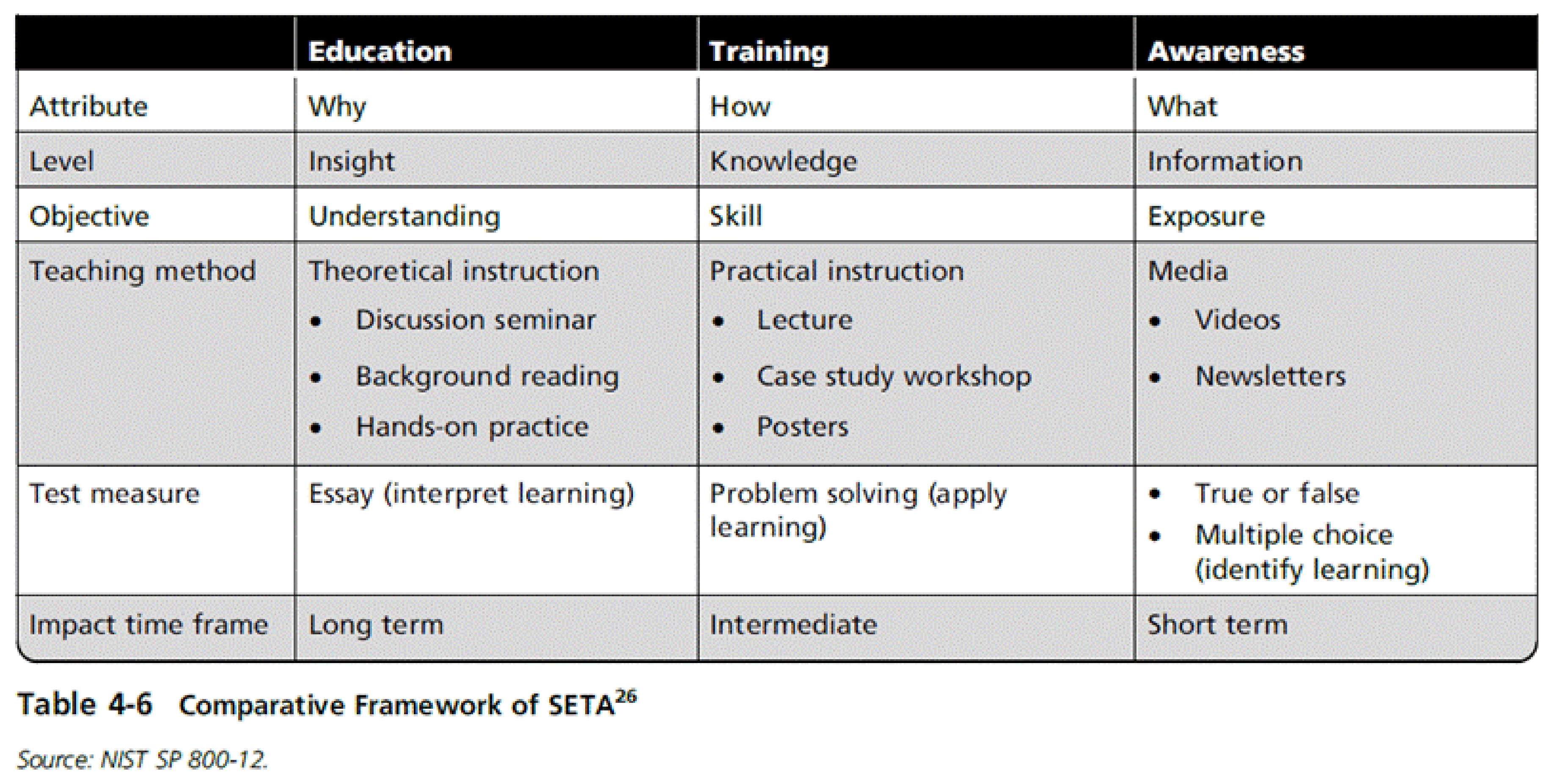
- Everyone in an organization needs to be trained and aware of information security
- When formal education is deemed appropriate, an employee can investigate courses in continuing education from local institutions of higher learning.
- A number of universities have formal coursework in information security.

Security Training

- Provide employees with detailed information and hands-on instruction to prepare them to perform their duties securely
- Develop customized in-house training or outsource the training program.
- Alternatives to formal training include conferences and programs offered through professional organizations.

Security Awareness

- One of the least frequently implemented but most beneficial programs is the security awareness program.
- Designed to keep information security at the forefront of users’ minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees may begin to neglect security matters, and risk of employee accidents and failures are likely to increase.



	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact time frame	Long term	Intermediate	Short term

Table 4-6 Comparative Framework of SETA[26]

Source: NIST SP 800-12.

Continuity Strategies (1)

- Incident response plans (IRPs); disaster recovery plans (DRPs); business continuity plans (BCPs)
- Primary functions of above plans:
  - IRP focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP.
  - DRP typically focuses on restoring systems after disasters occur; as such, it is closely associated with BCP.
  - BCP occurs concurrently with DRP when damage is major or ongoing, requiring more than simple restoration of information and information resources.

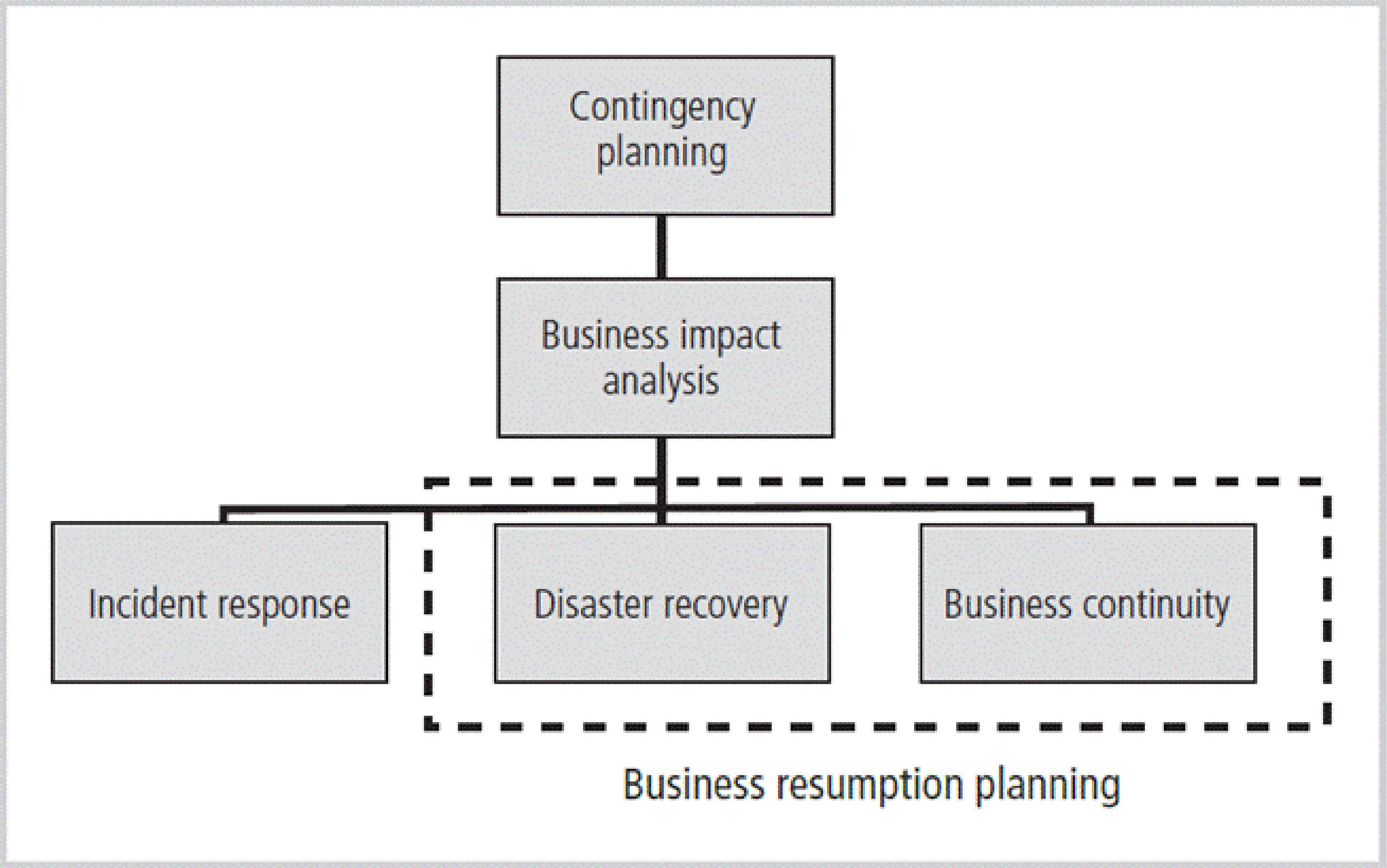


Figure 4-12 Components of contingency planning

Continuity Strategies (2)

- Before planning can actually begin, a team has to start the process.
- Champion: high-level manager to support, promote, and endorse findings of the project
- Project manager: leads project and ensures sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed
- Team members: should be managers, or their representatives, from various communities of interest: business, IT, and information security

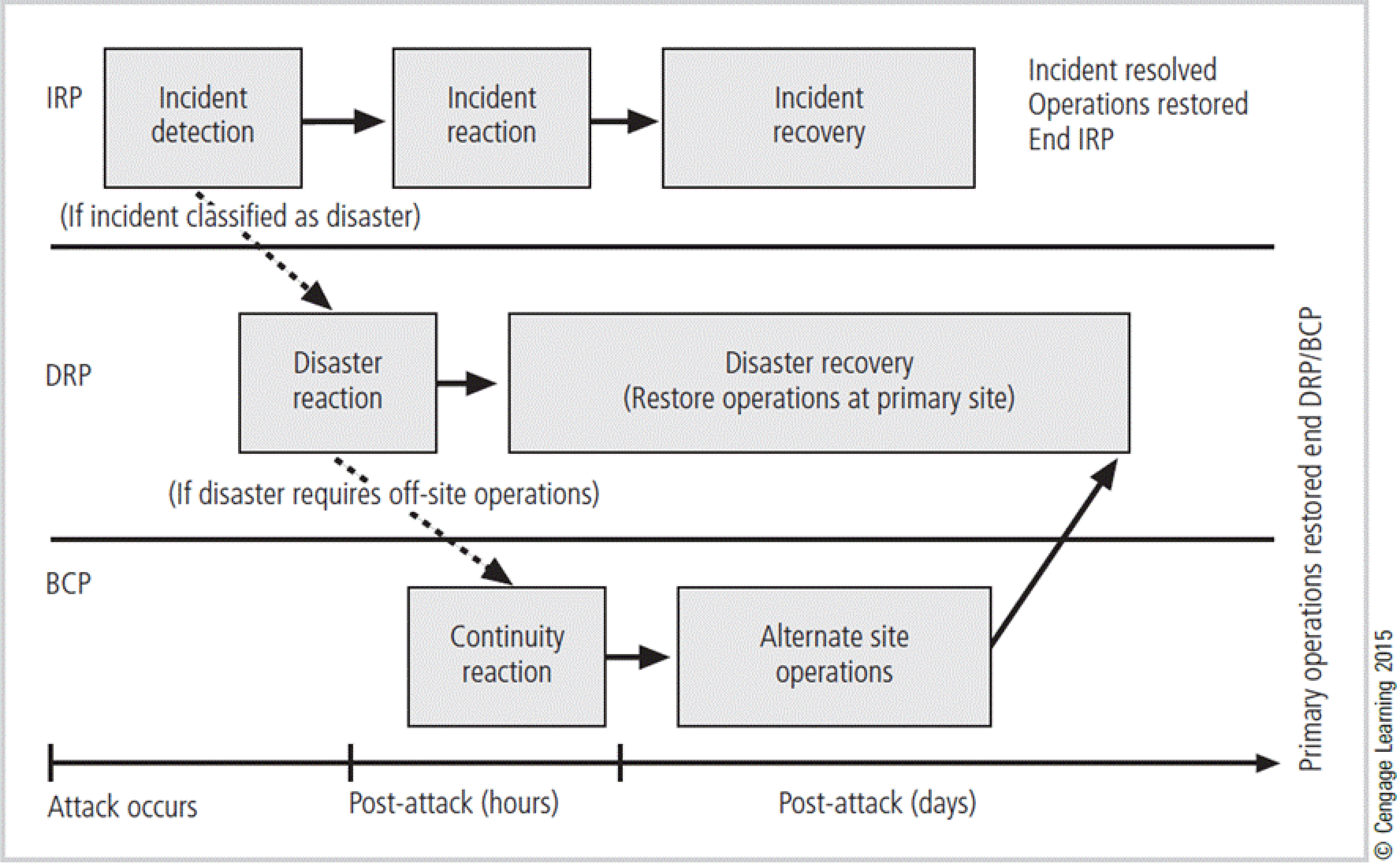


Figure 4-13 Contingency planning timeline

Contingency Planning (CP) Process

- Includes the following steps:
  - Develop CP policy statement
  - Conduct business impact analysis
  - Identify preventive controls
  - Create contingency strategies
  - Develop contingency plan
  - Ensure plan testing, training, and exercises
  - Ensure plan maintenance

CP Policy

- Should contain the following sections:
  - Introductory statement of philosophical perspective
  - Statement of scope/purpose
  - Call for periodic risk assessment/BIA
  - Specification of CP’s major components
  - Call for/guidance in the selection of recovery options
  - Requirement to test the various plans regularly
  - Identification of key regulations and standards
  - Identification of key people responsible for CP operations
  - Challenge to the organization members for support
  - Administrative information

Business Impact Analysis (BIA)

- Investigation and assessment of various adverse events that can affect organization
- Assumes security controls have been bypassed, have failed, or have proven ineffective, and attack has succeeded
- Organization should consider scope, plan, balance, knowledge of objectives, and follow-ups
- Three stages:
  - Determine mission/business processes and recovery criticality
  - Identify recovery priorities for system resources
  - Identify resource requirements

Incident Response Planning (IRP)

- Includes identification of, classification of, and response to an incident.
- Attacks classified as incidents if they:
  - Are directed against information assets
  - Have a realistic chance of success
  - Could threaten confidentiality, integrity, or availability of information resources
- More reactive than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident.

Disaster Recovery Planning

- Disaster recovery planning (DRP) is preparation for and recovery from a disaster.
- The contingency planning team must decide which actions constitute disasters and which constitute incidents.
- When situations are classified as disasters, plans change as to how to respond; take action to secure most valuable assets to preserve value for the longer term.
- DRP strives to reestablish operations at the primary site.

Business Continuity Planning

- Prepares the organization to reestablish or relocate critical business operations during a disaster that affects operations at the primary site
- If disaster has rendered the current location unusable, there must be a plan to allow business to continue functioning.
- Development of BCP is somewhat simpler than IRP or DRP.
  - Consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

Crisis Management

- Actions taken in response to an emergency to minimize injury/loss of life, preserve organization’s image/market share, and complement disaster recovery/business continuity processes
- What may truly distinguish an incident from a disaster are the actions of the response teams.
- Disaster recovery personnel must know their roles without any supporting documentation.
  - Preparation
  - Training
  - Rehearsal

The Consolidated Contingency Plan

- Single document set approach combines all aspects of contingency policy and plan, incorporating IR, DR, and BC plans.
- Often created and stored electronically, it should be easily accessible by employees in time of need.
  - Small- and medium-sized organizations may also store hard copies of the document.

Summary

- Development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Information security education, training, and awareness (SETA) is a control measure that reduces accidental security breaches and increases organizational resistance to many other forms of attack.
- Contingency planning (CP) is made up of three components: incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP).