# Chapter 3: Information Security Principles of Success

# Objectives

- Build an awareness of 12 basic principles of information security
- Distinguish between the three main security goals
- Learn how to design and apply the principle of "Defense in Depth"
- Explain the difference between functional and assurance requirements

# Objectives cont.

- Comprehend the fallacy of security through obscurity
- Comprehend the importance of risk analysis and risk management tools and techniques

# Introduction

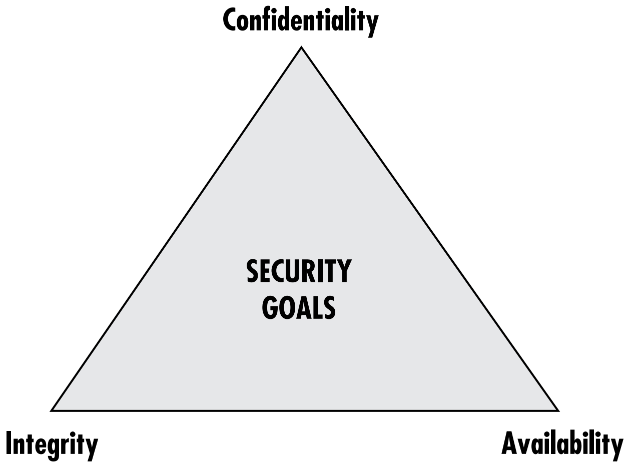
- Imperative to rely on **principle-based analysis and decision making**
  - No two systems or situations are identical, and there are no cookbooks to consult on how to solve security problems

# Information Security Principles:
# #1 There Is No Such Thing as Absolute Security

- Given enough time, tools, skills, and inclination, a hacker can break through any security measure

# Information Security Principles:
# #2 Three Security Goals (CIA triad)

- Protect the *confidentiality* of data
  - Confidentiality models are primarily intended to assure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible



© Pearson Education Information Security: Principles and Practices

# Information Security Principles:
# #2 Three Security Goals cont.

- Preserve the *integrity* of data
  - Integrity models keep data pure and trustworthy by protecting system data from intentional and accidental changes
- Promote the *availability* of data for authorized use
  - Availability models keep data and resources available for authorized use

# Information Security Principles:
# #3 Defense in Depth as Strategy

- Defense in depth
  - Security implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response
  - The weaknesses of one security layer are offset by the strengths of two or more layers

# Information Security Principles:
# #4 When Left on Their Own, People Tend to Make the Worst Security Decisions

- Takes little to convince someone to give up their credentials in exchange for trivial or worthless goods
- Many people are easily convinced to double-click on the attachment

Subject: Here you have, ;o)
Message body: Hi: Check This!
Attachment: AnnaKournikova.jpg.vbs

# Information Security Principles:
# #5 Functional and Assurance Requirements

- Functional requirements
  - Describe what a system should do
- Assurance requirements
  - Describe how functional requirements should be implemented and tested

*Does the system do the right things in the right way?*

- ***Verification**: the process of confirming that one or more predetermined requirements or specifications are met*
- ***Validation**: a determination of the correctness or quality of the mechanisms used in meeting the needs*

# Information Security Principles:
# #6 Security Through Obscurity Is Not an Answer

- Many people believe that if hackers don’t know how software is secured, security is better
  - Although this seems logical, it’s actually **untrue**
- Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all

# Information Security Principles:
# #7 Security = Risk Management

- Security is not concerned with eliminating all threats within a system or facility but with **eliminating known threats and minimizing losses** if an attacker succeeds in exploiting a vulnerability
- **Risk analysis and risk management are central themes** to securing information systems
- Risk assessment and risk analysis are concerned with **placing an economic value on assets to best determine appropriate countermeasures** that protect them from losses

# Information Security Principles:
# #7 Security = Risk Management cont.

- Vulnerability
  - A known problem within a system or program
- Exploit
  - A program or a “cookbook” on how to take advantage of a specific vulnerability
- Attacker
  - The link between a vulnerability and an exploit

# Information Security Principles:
# #7 Security = Risk Management cont.

| Likelihood | Consequences | | | | |
|---|---|---|---|---|---|
| | 1. Insignificant | 2. Minor | 3. Moderate | 4. Major | 6. Catastrophic |
| A (almost certain) | High | High | Extreme | Extreme | Extreme |
| B (likely) | Moderate | High | High | Extreme | Extreme |
| C (moderate) | Low | Moderate | High | Extreme | Extreme |
| D (unlikely) | Low | Low | Moderate | High | Extreme |
| E (rare) | Low | Low | Moderate | High | High |

© Pearson Education Information Security:
Principles and Practices

# Information Security Principles: #8 Security Controls: Preventative, Detective, and Responsive

- A security mechanism serves a purpose by **preventing a compromise**, **detecting that a compromise or compromise attempt** is underway, or **responding to a compromise** while it is happening or after it has been discovered

# Information Security Principles:
# #9 Complexity Is The Enemy of Security

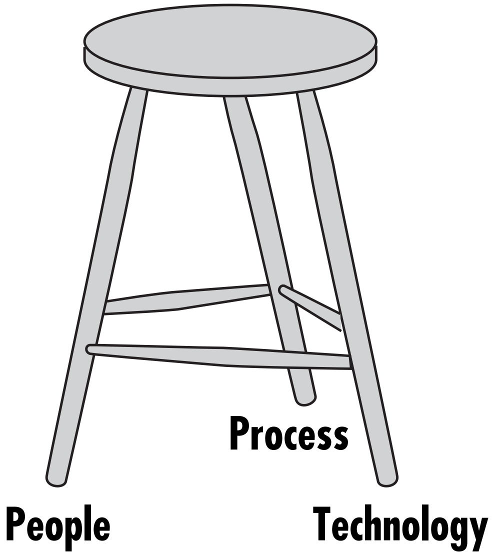
- The more complex a system gets, the harder it is to secure

# Information Security Principles:
# #10 Fear, Uncertainty, and Doubt (FUD) Do Not Work in Selling Security

- Information security managers must justify all investments in security using techniques of the trade
- When spending resources can be justified with good, solid business rationale, security requests are rarely denied

# Information Security Principles: #11 People, Process and Technology Are All Needed

- **People, process, and technology controls are essential elements of security practices** including operations security, applications development security, physical security, and cryptography



# Information Security Principles:
# #12 Open Disclosure of Vulnerabilities Is Good for Security

- Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security
- The need to know trumps the need to keep secrets in order to give users the right to protect themselves

# Summary

- Computer security specialists must not only know the technical side of their jobs but also must understand the principles behind information security
- These principles are mixed and matched to describe why certain security functions and operations exist in the real world of IT