Information Security (CP3404)

Chapter 14 – Risk Mitigation

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

- Explain how to control risk
- List the ways in which security policies can reduce risk
- Describe how awareness and training can provide increased security

Outline

Preface

- Risk is at heart of information security
- Some risks have small impact and can be easily managed, other risks can threaten very existence of business
- Multifaceted approach to managing risk in information security:
  - Control Risk
  - Reducing Risk Through Policies
  - Awareness and Training

Controlling Risk

Controlling Risk

- Risk – Situation that involves exposure to some type of danger
- Not all events that first appear to be risk may actually result in a risk:
  - False positive – Event considered be a risk yet turns out not to be one
  - False negative – Event that does not appear to be risk but actually turns out to be one

Risks can be divided into several classifications —see Table 14-1

Controlling Risk

Risk category	Description	Example
Strategic	Action that affects the long-term goals of the organization	Theft of intellectual property, not pursuing a new opportunity, loss of a major account, competitor entering the market
Compliance	Following (or not following) a regulation or standard	Breach of contract, not responding to the introduction of new laws
Financial	Impact of financial decisions or market factors	Increase in interest rates, global financial crisis
Operational	Events that impact the daily business of the organization	Fire, hazardous chemical spill, power blackout
Environmental	Actions related to the surroundings	Tornado, flood, hurricane
Technical	Events that affect information technology systems	Denial of service attack, SQL injection attack, virus
Managerial	Actions related to the management of the organization	Long-term illness of company president, key employee resigning

Table 14-1 Risk classifications

Controlling Risk

Controlling Risk — Approaches

- Several different approaches used to reduce risk
- Can modify the response to the risk instead of merely accepting the risk
- Different risk responses:
  - Transference – Make third party responsible for the risk
  - Risk avoidance – Identifying the risk and making the decision not engage in activity.
  - Mitigation – Address the risk by making it less serious

Controlling Risk

Controlling Risk — Approaches (Simple Risk Model)

- Simple Risk Model organizes risks as (see Table 14-2):
  - Preventive – Considered most effective since they minimize possibility of loss by preventing the risk from occurring
  - Detective – Least effective but most often used that identify event after has occurred
  - Corrective – Minimize impact by restoring system to its state at point before event; may still result in some degree of loss

Controlling Risk

Element	Description	Example
Preventive	These are controls that prevent the loss or harm from occurring based on the risk.	A preventive control requires the installation of firewalls in a network.
Detective	Detective controls monitor activity to identify instances where practices or procedures were not followed.	A detective control requires a continual review of log files to detect any abnormal activity on a system.
Corrective	Corrective controls restore the system back to its prior state before a malicious event occurred.	A corrective control restores a data backup after a virus infected a system.

Table 14-2 Simple Risk Model

Controlling Risk

Controlling Risk — Types

- Management risk control types – Administrative in their nature and are laws, regulations, policies, practices, and guidelines that govern overall requirements and controls
- Technical risk control types – Enforcing technology to control risk (Examples: antivirus software, firewalls, encryption)
- Operational risk control types – Cover operational procedures to limit risk; may include using video surveillance systems and barricades to limit access to secure sites

Controlling Risk

Controlling Risk — Managerial Perspective

- A Final approach to controlling risks looks at mitigating risk from a managerial perspective
- Three (3) of the most common elements in this approach are:
  1. Privilege Management
  2. Change Management
  3. Incident Management

Controlling Risk

Controlling Risk — Managerial Perspective (Privilege)

- Privilege management – Process of assigning and revoking privileges to objects and covers procedures of managing object authorizations
- Privilege auditing – One element of privilege management that is periodic review of subject's privileges over object
- Auditing IT security functions serve to verify that organization's security protections being enacted and that corrective actions can be swiftly implemented before an attacker exploits vulnerability (see Figure 14-1)

Controlling Risk

Review of User Access Rights

- User access rights will be reviewed on a regular basis by the IT Security Manager. External audits of access rights will be carried out at least once per year.
- The organization will institute a review of all network access rights every six months in order to positively confirm all current users. Any lapsed accounts that are identified will be disabled immediately and deleted within three business days unless they can be positively reconfirmed.
- The organization will institute a review of access to applications once per year. This will be done in cooperation with the application owner and will be designed to positively and deleted within three business days unless they can be positively reconfirmed. This review will be conducted as follows:

  1. The IT Security Manager will generate a list of users, by application.
  2. The appropriate list will be sent to each application owner who will be asked to confirm that all users identifier are authorized to have access to the application.
  3. The IT Security Manager will ensure that a response is received within 10 business days.
  4. Any user not confirmed will have his/her access to the system disabled immediately and deleted within three business days.
  5. The IT Security Manager will maintain a permanent record of list that were distributed to application owners, application owner responses, and a record of any action taken.

Figure 14-1 Sample user access rights review

Controlling Risk

Controlling Risk — Managerial Perspective (Change)

- Change management – Methodology for making modifications and keeping track of changes
- Ensures proper documentation of changes so future changes have less chance of creating a vulnerability
- Involves all types of changes to information systems
- Two (2) major types of changes that need proper documentation:
  1. Changes to system architecture
  2. Changes to file or document classification

Controlling Risk

Controlling Risk — Managerial Perspective (Change)

- Change management team (CMT) – Body responsible for overseeing the changes
- Composed of representatives from all areas of IT, network security, and upper-level management
- Proposed changes must first be approved by CMT
- CMT duties:
  - Review proposed changes
  - Ensure risk/impact planned change are understood
  - Recommend approval, disapproval, or deferral
  - Communicate proposed and approved changes to co-workers

Controlling Risk

Controlling Risk — Managerial Perspective (Incident)

- Incident response – Components required to identify, analyze, and contain an incident
- Incident handling – Planning, coordination, and communications functions needed to resolve incident in efficient manner
- Incident management – The *framework* and functions required to enable incident response and incident handling within an organization
- Objective of incident management is to restore normal operations quickly with least possible impact on business or users

Controlling Risk

Controlling Risk — Risk Calculation

- Qualitative risk calculation – Uses an *educated guess* based on observation
- Quantitative risk calculation – Attempts to create *hard* numbers associated with risk of an element in system by using historical data
- Quantitative risk calculations can be divided into:
  - Risk Liklihood
  - Risk Impact

Controlling Risk

Controlling Risk — Risk Calculation (Liklihood)

- Historical data valuable in providing information on risk likelihood (see Table 14-3)
- Mean Time To Failure (MTTF) – Basic measure of reliability for systems that cannot be repaired and is average amount of time expected until first failure of equipment
- Failure In Time (FIT) – Can report number of expected failures per one billion hours of operation for device
- Annualized Rate of Occurrence (ARO) – Likelihood of risk occurring within one year

Controlling Risk

Source	Explanation
Police departments	Crime statistics on the area of facilities to determine the probability of vandalism, break-ins, or dangers potentially encountered by personnel
Insurance companies	Risks faced by other companies and the amounts paid out when these risks became reality
Computer incident monitoring organizations	Data regarding a variety of technology-related risks, failures, and attacks

Table 14-3 Historical data sources

Controlling Risk

Controlling Risk — Risk Calculation (Impact)

- Single Loss Expectancy (SLE) – Expected monetary loss every time a risk occurs; computed by multiplying Asset Value (AV) by Exposure Factor (EF), which is proportion of an asset's value that is likely to be destroyed by particular risk, i.e.,

$$SLE = AV \times EF$$

- Annualized Loss Expectancy (ALE) – Expected monetary loss be expected for asset due to risk over a one-year period; computed by multiplying SLE by ARO, which is the probability that a risk will occur in a particular year, i.e.,

$$ALE = SLE \times ARO$$

Reducing Risk Through Policies

Reducing Risk Through Policies

- Another means of reducing risks is through a risk policy
- Important related concepts are:
  - What Is a Security Policy?
  - Balancing Trust and Control
  - Designing a Security Policy
  - Types of security Policies

Reducing Risk Through Policies

What Is a Security Policy?

- Security policy – Written document states how an organization plans to protect company's information technology assets
- Outlines protections that should be enacted to ensure that organization's assets face minimal risks
- Security policy can serve several functions

Reducing Risk Through Policies

What Is a Security Policy? — Security Policy Functions

- Documents management's overall intention and direction
- Details specific risks and how to address them
- Provides controls to direct employee behavior
- Helps create a security-aware organizational culture
- Helps ensure employee behavior is directed and monitored

Reducing Risk Through Policies

Balancing Trust and Control

- Approaches to trust:
  - Trust everyone all of the time
  - Trust no one at any time
  - Trust some people some of the time
- Security policy attempts to provide right amount of trust
- Trust some people some of the time
- Builds trust over time
- Level of control must also be balanced

Reducing Risk Through Policies

Designing a Security Policy — Definition

- Standard – Collection of requirements specific to system or procedure that must be met by everyone
- Guideline – Collection of suggestions that should be implemented
- Policy – Document that outlines specific requirements that must be met

Reducing Risk Through Policies

Designing a Security Policy — Definition (cont.)

- A policy generally has these characteristics:
  - Communicates a consensus of judgment
  - Defines appropriate user behavior
  - Identifies needed tools and procedures
  - Provides directives for Human Resource action in response to inappropriate behavior
  - Helps if necessary to prosecute violators

Reducing Risk Through Policies

Designing a Security Policy — Security Policy Cycle

- The security policy cycle is a never-ending process of three (3) phases (see Figure 14-2):
  1. Vulnerability assessment – consists of asset identification, threat evaluation, vulnerability appraisal, risk assessment, and risk mitigation
  2. Creating the policy – using the information from risk management study
  3. Review the policy for compliance – because new assets are continually being added to the organization

Reducing Risk Through Policies

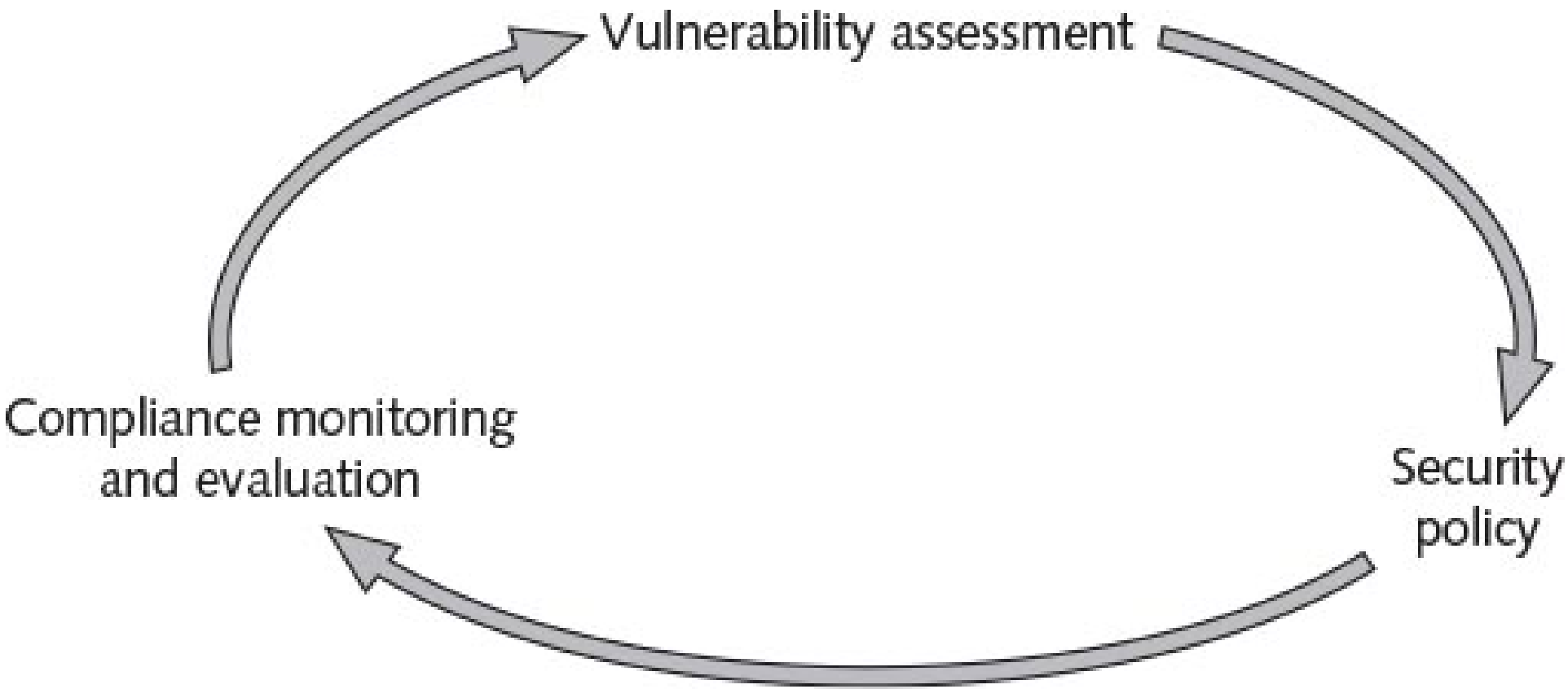

Figure 14-2 Security policy cycle

Reducing Risk Through Policies

Designing a Security Policy — Steps in Development

- When designing a policy, bear in mind what a policy must do and what a policy should do (see Table 14-4)
- Security policy design should be the work of a team
- Development team representatives:
  - Senior level administrator
  - Member of management who can enforce the policy
  - Member of the legal staff
  - Representative from the user community
- Team should first decide on policy goals and scope and how specific the policy should be

Reducing Risk Through Policies

Security policy *must*	Security policy *should*
Be implementable and enforceable	State reasons why the policy is necessary
Be concise and easy to understand	Describe what is covered by the policy
Balance protection with productivity	Outline how violations will be handled

Table 14-4 Policy *must* and *should* statements

Reducing Risk Through Policies

Designing a Security Policy — Steps in Development (Due Care)

- Due care – Obligations imposed on owners and operators of assets
- Owners must exercise reasonable care of assets and take precautions to protect them
- Examples of due care policy statements:
  - Employees should exercise due care in opening attachments received from unknown sources
  - Technicians will exercise due care when installing new operating system on an existing computer
  - Students will exercise due care when using computers in a crowded lab setting

Reducing Risk Through Policies

Designing a Security Policy — Steps in Development (Guidelines)

- Notify users in advance of development of and reasons for a new security policy
- Provide affected users an opportunity to review and comment on policy prior to deployment
- Give users with responsibility the authority to carry out their responsibilities

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer:

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

2. Which risk calculation approach uses an *educated guess* based on observation?
   Answer:

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

2. Which risk calculation approach uses an *educated guess* based on observation?
   Answer: Qualitative risk calculation

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

2. Which risk calculation approach uses an *educated guess* based on observation?
   Answer: Qualitative risk calculation

3. The likelihood of a risk occurring within a year is known as the _____.
   Answer:

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

2. Which risk calculation approach uses an *educated guess* based on observation?
   Answer: Qualitative risk calculation

3. The likelihood of a risk occurring within a year is known as the _____.
   Answer: Annualized Rate of Occurrence (ARO)

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

2. Which risk calculation approach uses an *educated guess* based on observation?
   Answer: Qualitative risk calculation

3. The likelihood of a risk occurring within a year is known as the _____.
   Answer: Annualized Rate of Occurrence (ARO)

4. At its core, a _____ is a written document that states how an organization plans to protect the company's information technology assets.
   Answer:

Quick Quiz

1. An attempt to address a risk by making it less serious is known as _____.
   Answer: risk mitigation

2. Which risk calculation approach uses an *educated guess* based on observation?
   Answer: Qualitative risk calculation

3. The likelihood of a risk occurring within a year is known as the _____.
   Answer: Annualized Rate of Occurrence (ARO)

4. At its core, a _____ is a written document that states how an organization plans to protect the company's information technology assets.
   Answer: security policy

Reducing Risk Through Policies

Types of Security Policies

- Because a security policy is so comprehensive, it is often broken down into subpolicies
- The term security policy then becomes an umbrella term for all the subpolcies included within it
- In addition to the security policies listed in Table 14-5, most organizations have security policies that address acceptable use, privacy, data, security-related human resources, ethics, and password management and complexity

Reducing Risk Through Policies

Name of security policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Antivirus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments, investigate incidents, ensure conformance to security policies, or monitor user activity
Automatically forwarded email policy	Prescribes that no email will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Demilitarized zone (DMZ) security policy	Defines standards for all networks and equipment located in the DMZ
Email policy	Creates standards for using corporate email
Email retention policy	Helps employees determine what information sent or received by email should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations to access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organization's information in a manner appropriate to its level of security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security configuration for servers
VPN security policy	Establishes requirements for remote access virtual private network (VPN) connections to the organization's network
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

Table 14-5 Types of security policies

Reducing Risk Through Policies

Types of Security Policies — Acceptable Use Policy (AUP)

- Acceptable Use Policy (AUP) – Policy that defines actions users may perform while accessing systems
- Users include employees, vendors, contractors, and visitors
- Typically covers all computer use
- AUPs are generally considered to be the most important information security policies

Reducing Risk Through Policies

Types of Security Policies — Privacy Policy

- Privacy policy – Outlines how organization uses personal information it collects

  A typical privacy policy for consumers is shown in Figure 14-3

Reducing Risk Through Policies

In general, you can visit us on the Internet without telling us who you are and without giving any personal information about yourself. There are times, however, when we or our partners may need information from you. You may choose to give us personal information in a variety of situations. For example, you may want to give us information, such as your name and address or e-mail, to correspond with you, to process an order, or to provide you with a subscription. You may give us your credit card details to buy something from us or a description of your education and work experience in connection with a job opening for which you wish to be considered. We intend to let you know how we will use such information before we collect it from you. You may tell us that you do not want us to use this information to make further contact with you beyond fulfilling your request. If you give us personal information about somebody else, such as a spouse or work colleague, we will assume that you have their permission to do so.

Figure 14-3 Sample privacy policy

Reducing Risk Through Policies

Types of Security Policies — Data Policies

- Data policies – Address different aspects of how data should be handled within an organization
- Data storage policy – Set of procedures designed to control and manage data within organization by specifying data collection and storage
- Data retention policy – Outlines how to maintain information in user's possession for predetermined length of time
- Data wiping and disposing policy – Addresses how and when data will ultimately be erased

Reducing Risk Through Policies

Types of Security Policies — Security-Related Human Resource Policy

- Security-related human resource policy – Include statements regarding how an employee's information technology resources will be addressed
- May include statements regarding:
  - Due process – The principle of treating all accused persons in an equal fashion, using established rules and procedures
  - Due diligence – Any investigation into suspicious employee conduct will examine all material facts
- Covers actions to be taken if employee terminated

Reducing Risk Through Policies

Types of Security Policies — Ethics Policy

- Ethics – Study of what group of people understand be good and right behavior and how people make those judgments
- Morals – Values are attributed to system of beliefs that help individual distinguish right from wrong
- Ethics policy – Attempts to establish culture of openness, trust, and integrity in business practices
- Ethics policies contain topics of executive commitment to ethics, employee commitment to ethics, how to maintain ethical practices, and penalties for unethical behavior

Reducing Risk Through Policies

Types of Security Policies — Password Management and Complexity Policy

- Password management and complexity policy – Address how passwords are created and managed
- Cover implementing controls through technology (such as setting passwords to expire after 60 days and not allowing them to be recycled)
- Also include reminder to users on how to select and use passwords
- Information regarding weak passwords can be included in the security policy (see Figure 14-4)

Reducing Risk Through Policies

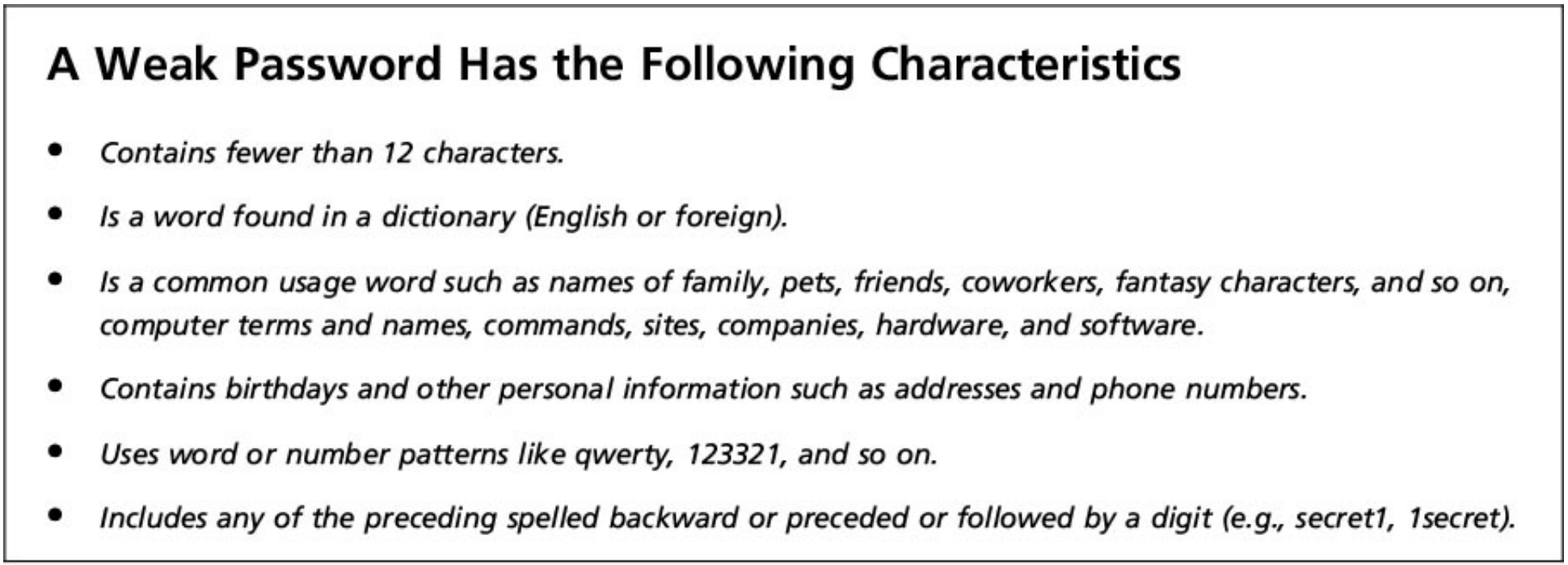

Figure 14-4 Weak password characteristics

Awareness and Training

Awareness and Training

- Providing users with security awareness training is key defense in information security
- All computer users in organization have shared responsibility to protect assets of organization
- Cannot be assumed that all users have knowledge and skill to protect assets
- Awareness and training involves instruction regarding:
  - Compliance
  - User Practices
  - Threat Awareness

Awareness and Training

Awareness and Training — Compliance

- Users should be informed regarding:
  - Security policy training and procedures
  - Personally identifiable information
  - Information classification
  - Data labeling, handling, and disposal
  - Compliance with laws, best practices, and standards

Awareness and Training

Awareness and Training — User Practices

- Helping users understand how their normal practices can impact the security of the organization (see Table 14-6)

Awareness and Training — Threat Awareness

- It is not uncommon for users to be unaware of the security threats
- Two (2) common examples are:
  1. Peer-to-Peer (P2P) Networks
  2. Social Networking

Awareness and Training

Category	Instruction
Password behaviors	Creating strong passwords that are unique for each account and properly protecting them serve as a first line of defense that all employees must practice.
Data handling	No sensitive data may leave the premises without prior authorization. All data that is temporarily stored on a laptop computer must be encrypted.
Clean desk policy	Employees are required to clear their workspace of all papers at the end of each business day.
Prevent tailgating	Never allow another person to enter a secure area along with you without displaying their ID card.
Personally owned devices	No personally owned devices, such as USB flash drives or portable hard drives, may be connected to any corporate equipment or network.

Table 14-6 User practices

Awareness and Training

Threat Awareness — Peer-to-Peer (P2P) Networks

- Peer-to-peer (P2P) networks – Users connect directly to each other —semilar to instant messaging (IM)
- Typically used for sharing audio, video, data files
- Tempting targets for attackers
- Viruses, worms, Trojans, and spyware can be sent using P2P
- Most organizations prohibit use of P2P due to high risk of infection and legal consequences

Awareness and Training

Threat Awareness — Social Networking

- Social networking – Grouping individuals based on some sort of affiliation
- Web sites that facilitate social networking called social networking sites
- Social networking sites carry risks (see Table 14-7):
  - Personal data can be used maliciously.
  - Users may be too trusting
  - Accepting friends may have unforeseen consequences
  - Social networking security is lax or confusing

Awareness and Training

Feature	Description	Risks
Games and applications	When your Facebook friends use games and applications, these can request information about friends like you, even if you do not use the application.	Information such as your biography, photos, and places where you check in can be exposed.
Social advertisements	A "social ad" pairs an advertisement with an action that a friend has taken, such as "liking" it.	Your Facebook actions could be associated with an ad.
Places	If you use Places, you could be included in a "People Here Now" list once you check in to a location.	Your name and Facebook profile picture appear in the list, which is visible to anyone who checks in to the same location, even if he is not a friend.
Web search	Entering your name in a search engine like Google can display your Facebook profile, profile picture, and information you have designated as public.	Any web user can freely access this information about you.
Photo albums	Photos can be set to be private but that may not include photo albums.	The albums Profile Pictures, Mobile Uploads, and Wall Photos are usually visible to anyone.

Table 14-7 Facebook features and risks

Awareness and Training

Threat Awareness — Social Networking (Defenses)

- Users should be cautious about what information posted
- Users should be cautioned regarding who can view their information
- Users should be instructed to pay close attention to information about new or updated security settings
- Good idea to disable options and then enable them only as necessary (see Table 14-8)

Awareness and Training

Option	Recommended setting	Explanation
Profile	Only my friends	Facebook networks can contain hundreds or thousands of users, and there is no control over who else joins the network to see the information.
Photos or photos tagged of you	Only my friends	Photos and videos have often proven to be embarrassing. Only post material that would be appropriate to appear with a resume or job application.
Status updates	Only my friends	Because changes to status such as "Going to Florida on January 28" can be useful information for thieves, only approved friends should have access to it.
Online status	No one	Any benefits derived by knowing who is online are outweighed by the risks.
Friends	Only my friends (minimum setting)	Giving unknown members of the community access to a list of friends may provide attackers with opportunities to uncover personal information through friends.

Table 14-8 Recommended Facebook profile settings

Awareness and Training

Training Techniques

- All users need continus training in the new security defenses
- Opportunities for security education and training can be at any of the following times:
  - When new employee is hired
  - After computer attack has occurred
  - When employee promoted
  - During annual department retreat
  - When new user software is installed
  - When user hardware is upgraded

Awareness and Training

Training Techniques — Traits of Learning

- Learner traits impact how people learn (see Table 14-9)
- Training styles (see Table 14-10):
  - Pedagogical approach – Classic teaching method
  - Andragogical approach – Art of helping an adult learn
- There are different learning styles, such as, Visual, Auditory, and kinesthetic
- Role-based training – Specialized training customized to specific role an employee holds

Awareness and Training

Year born	Traits	Number in U.S. population
Prior to 1946	Patriotic, loyal, faith in institutions	75 million
1946–1964	Idealistic, competitive, question authority	80 million
1965–1981	Self-reliant, distrustful of institutions, adaptive to technology	46 million
1982–2000	Pragmatic, globally concerned, computer literate, media savvy	76 million

Table 14-9 Traits of learners

Awareness and Training

Subject	Pedagogical approach	Andragogical approach
Desire	Motivated by external pressures to get good grades or pass on to next grade	Motivated by higher self-esteem, more recognition, desire for better quality of life
Student	Dependent on teacher for all learning	Self-directed and responsible for own learning
Subject matter	Defined by what the teacher wants to give	Learning is organized around situations in life or at work
Willingness to learn	Students are informed about what they must learn	A change triggers a readiness to learn or students perceive a gap between where they are and where they want to be

Table 14-10 Approaches to training

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer:

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

2. Grouping individuals and organizations into clusters or groups based on some sort of affiliation is called _____.
   Answer:

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

2. Grouping individuals and organizations into clusters or groups based on some sort of affiliation is called _____.
   Answer: social networking

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

2. Grouping individuals and organizations into clusters or groups based on some sort of affiliation is called _____.
   Answer: social networking

3. The _____ policy typically contains statements regarding actions to be taken when an employee is terminated.
   Answer:

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

2. Grouping individuals and organizations into clusters or groups based on some sort of affiliation is called _____.
   Answer: social networking

3. The _____ policy typically contains statements regarding actions to be taken when an employee is terminated.
   Answer: security-related human resource

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

2. Grouping individuals and organizations into clusters or groups based on some sort of affiliation is called _____.
   Answer: social networking

3. The _____ policy typically contains statements regarding actions to be taken when an employee is terminated.
   Answer: security-related human resource

4. _____ learners learn through taking notes, being at the front of the class, and watching presentations.
   Answer:

Quick Quiz

1. A policy that outlines how to maintain information in the user's possession for a predetermined length of time is known as a(n) _____.
   Answer: data retention policy

2. Grouping individuals and organizations into clusters or groups based on some sort of affiliation is called _____.
   Answer: social networking

3. The _____ policy typically contains statements regarding actions to be taken when an employee is terminated.
   Answer: security-related human resource

4. _____ learners learn through taking notes, being at the front of the class, and watching presentations.
   Answer: Visual