UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

Lecture 13: Risk Mitigation

Objectives

- Explain how to control risk
- List the types of security policies
- Describe how awareness and training can provide increased security

INTRODUCTION

Risk management is one of the concept at the heart of information security

Multifaceted approach to information security

1. Control risk through different management techniques
2. Develop a security policy
3. User awareness and training

Controlling Risk

THREAT	Type of action that has potential to cause harm
THREAT AGENT	Person or element with power to carry out a threat
VULNERABILITY	Flaw or weakness that allows threat agent to bypass security
RISK	Possibility threat agent will exploit the vulnerability

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 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 that are related to the management of the organization	Long-term illness of company president, key employee resigning

Risk classifications

Controlling Risk

PRIVILAGE

Subject's access level over an object, such as a file

PRIVILAGE MANAGEMENT

Process of assigning and revoking privileges to objects

PRIVILAGE AUDITING

- Periodically reviewing a subject's privileges over an object
- **Objective**: determine if subject has the correct privileges

Controlling Risk

CHANGE MANEGEMENT

- 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 major types of changes that need proper documentation
  - –Changes to system architecture
  - –Changes to file or document classification

CHANGE MANEGEMENT TEAM

- Body responsible for overseeing the changes
- Composed of representatives from all areas of IT, network security, and upper management
- Proposed changes must first be approved by CMT
- CMT duties
  - –Review proposed changes
  - –Ensure risk and impact of planned change are understood
  - –Recommend approval, disapproval, deferral, or withdrawal of a requested change
  - –Communicate proposed and approved changes to coworkers

Controlling Risk

INCIDENT RESPONSE

- Components required to identify, analyze, and contain an incident.

INCIDENT HANDLING

- Planning, coordination, communications, and planning functions needed to resolve incident

INCIDENT MANAGEMENT

- Response to an unauthorized incident
- Components required to identify, analyze, and contain an incident

INCIDENT MANAGEMENT OBJECTIVE

- Restore normal operations as quickly as possible with least impact to business or users

Reducing Risk Through Policies

SECURITY POLICY

- Another means of reducing risks
- A security policy must identify all of a company's assets as well as all the potential threats to those assets.

Important **considerations** regarding security policies
–Understanding what it is
–Knowing how to balance trust and control
–Understanding the process for designing a policy
–Knowing what the different types of policies are

WHAT is Security Policy

- Written document that states how an organization plans to protect the company's information technology assets.

Higher level definition

Set of management statements that define organization's philosophy of how to safeguard information

Lower level definition

Rules for computer access and how the rules are carried out

WHAT is Security Policiy

Security Policy Function

- 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

Balancing Trust and Control

Three 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
  - –Influenced by security needs and organization's culture

Designing a Security Policy

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

Characteristics of a policy

–Communicates a consensus of judgment

–Defines appropriate user behavior

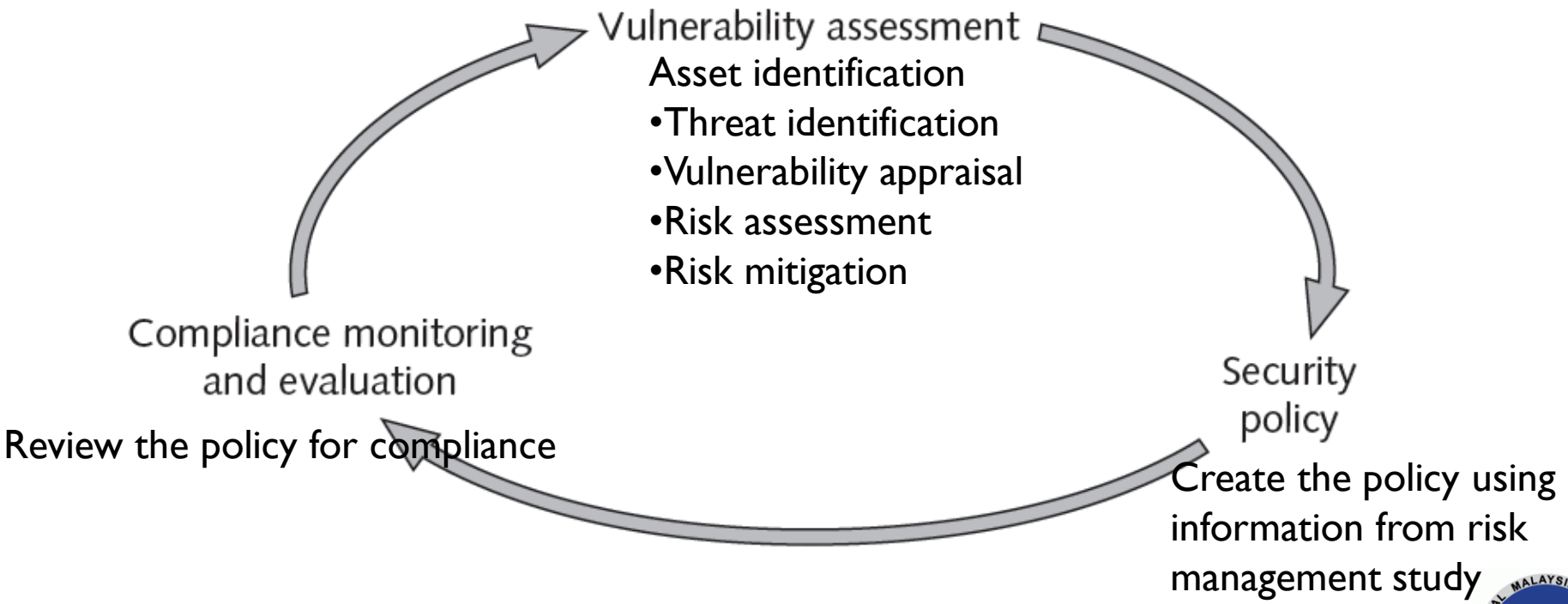
–Identifies needed tools and procedures

–Provides directives for Human Resource action in response to inappropriate behavior

–Helps if necessary to prosecute violators

Designing a Security Policy

Three phases of the security policy cycle



Designing a Security Policy

Security policy must	Security policy should
Be implementable and enforceable	State reasons 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

- 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

–Also how specific the policy should be

Designing a Security Policy

- 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

–Students will exercise due care when using computers in a crowded lab setting

Designing a Security Policy

POLICY DEVELOPMENT GUIDELINE

- 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
- Provide a sample of people affected by the policy with an opportunity to review and comment on the policy.
- Give users with responsibility the authority to carry out their responsibilities

Types of Security Policy

Security policies often broken down into sub 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

Types of security policies

Types of Security Policy

- Acceptable use policy
- Privacy policy
- Security-related human resource policy
- Password management and complexity policy
- Disposal and destruction policy
- Classification of information policy
- Ethics policy

Types of Security Policy

Acceptable use policy

- Policy that defines actions users may perform while accessing systems
- Users include employees, vendors, contractors, and visitors
- Typically covers all computer use
- Generally considered most important information security policy

Privacy policy

- Also called personally identifiable information policy
- Outlines how organization uses personal information it collects

Types of Security Policy

Security-related human resource policy

- Includes statements about how an employee's information technology resources will be addressed
- Typically presented at employee orientation session after employee is hired
- May include statements regarding due process and/or due diligence
- May include statements regarding actions to be taken when employee is terminated

Password management and complexity policy

- Addresses how passwords are created and managed
- Reminds users of differences between strong and weak passwords

Types of Security Policy

Weak Passwords Have the Following Characteristics

- *The password contains fewer than 12 characters.*
- *The password is a word found in a dictionary (English or foreign).*
- *The password is a common usage word such as names of family, pets, friends, coworkers, fantasy characters, and so on, or computer terms and names, commands, sites, companies, hardware, and software.*
- *Birthdays and other personal information such as addresses and phone numbers.*
- *Word or number patterns like qwerty, 123321, and so on.*
- *Any of the preceding spelled backward or preceded or followed by a digit (e.g., secret1, 1secret).*

Weak password information

Strong Passwords Have the Following Characteristics

- *Contain both uppercase and lowercase characters (a–z, A–Z)*
- *Have digits and punctuation characters as well as letters (0–9, !@#$%^& *()_+={}[]*
- *Are at least 12 characters long*
- *Are not words in any language, slang, dialect, or jargon*
- *Are not based on personal information*

Strong password information

Types of Security Policy

Disposal and destruction policy

- Addresses disposal of confidential resources
- Describes how to dispose of equipment, records, and data

Classification of information policy

- Designed to produce standardized framework for classifying information assets
- Generally involves creating classification categories
  -Example: high, medium, low

Types of Security Policy

Ethics

Study of what a group of people understand to be good and right behavior

Moral

Values attributed to a belief system that helps individuals distinguish right from wrong

Values

A person's fundamental beliefs and principles

Ethics Policy

- Written code of conduct
- Guides employees in decision making
- Serves as a communication tool to reflect organization's commitments

Awareness and Training

- Providing users with security awareness training
  - –Key defense in information security
- Awareness and training topics
  - –Compliance
  - –Secure user practices
  - –Awareness of threats

- 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

User Practices

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 policies	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

User practices

Threat Awareness

- Peer-to-peer (P2P) networks
  - –Similar to instant messaging
  - –Users connect directly to each other
  - –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
  - –High risk of infection
  - –Legal consequences

Threat Awareness

- Social networking
  - –Grouping individuals based on some sort of affiliation
  - –Can be physical or online
- Web sites that facilitate social networking called social networking sites
  - –Increasingly becoming prime targets of attacks
- Reasons social networking sites are popular with attackers
  - –Lots of personal data is available
  - –Users are generally trusting
  - –Sites are confusing
- Security tips for using social networking sites
  - –Consider carefully who is accepted as a friend
  - –Show limited friends a reduced version of your profile
  - –Disable options and reopen only as necessary

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.

Facebook features and risks

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

Recommended Facebook profile settings

Training Techniques

- **Opportunities for security education and training**
  - –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

- Learner traits impact how people learn
- Examples of learning styles
  - –Visual
  - –Auditory
  - –Kinesthetic

Summary

- A risk is the likelihood that a threat agent will exploit a vulnerability
- Privilege management and change management are risk management approaches
- A security policy states how an organization plans to protect its information technology assets
- Development and maintenance of a security policy follows a three-phase cycle

- Security policies are often broken into subpolicies

–Acceptable use policy
–Privacy policy
–Password management and complexity policy
–Disposal and destruction policy
–Classification of information policy

- Ongoing awareness training provides users with knowledge and skills necessary to support information security