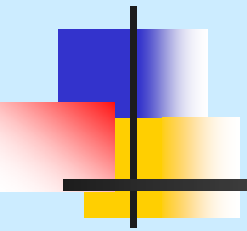


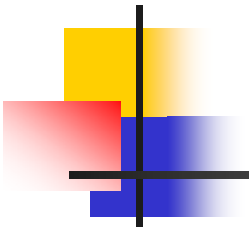
Chapter 9: Risk and Security Management

Objectives

- I - Risk Management
  - Define Risk
  - Identify the Risk to an Organization
  - Measure Risk

Objectives (cont.)

- II - Security Management :
  - Define identity management
  - Secur systems through privilege management
  - Plan for change management
  - Define digital rights management
  - Acquire effective training and education

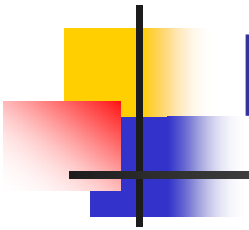


I - Managing Risk

Security is about Managing Risk

Managing Risk

- Without an understanding of the security risks to an organization's information assets, too many or not enough resources might be used or used in the wrong way.
- Risk management also provides a basis for the valuing of information assets
- By identifying risk, you learn the value of particular types of information and the value of the systems that contain that information.



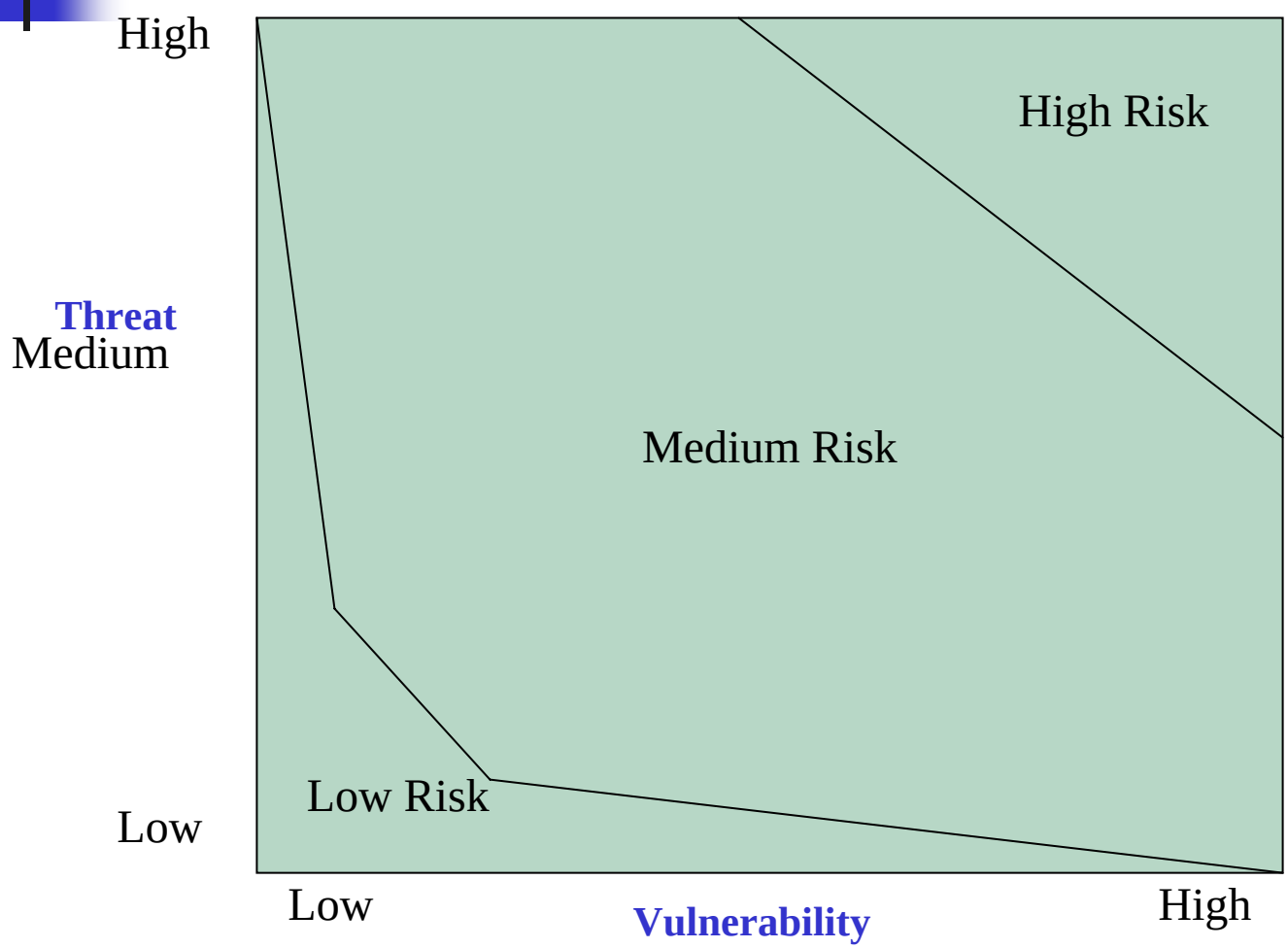
Risk

- Risk is the underlying concept that forms the basis for what we call “security”
- Risk is the potential for loss that requires protection
- If there is no risk, there is no need for security
- Risk is better understood in the insurance industry
  - A person purchases insurance because a danger is felt – accidents – theft
  - The insurance company sets the premiums on how much the car repair is likely to cost and the car usage profile

Components of Risk

- Vulnerability
  - The money that the insurance company has to pay in case of an accident is the vulnerability of the insurance company
- Threat
  - The likelihood of the insurance bearer to get into an accident...this will cause the vulnerability to be exploited (the payment of the cost of repair)

The Relation Between Vulnerability and Threat



Vulnerability

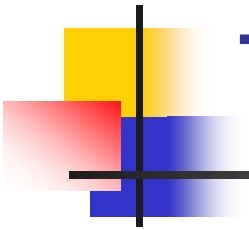
- Is a potential avenue of attack
- In computer systems
  - allowing the system to be open to a technical attack
- In administrative procedures
  - Allowing the environment to be open to social engineering attacks
- A vulnerability is characterized by the difficulty and the level of technical skill that is required to exploit it
- The result of the exploitation should also be taken into account

Vulnerability Categories

- High-danger vulnerability
  - A vulnerability that is easy to exploit and that allows the attacker to gain complete control over a system
- Low-danger vulnerability
  - A vulnerability that would require the hacker to invent significant resources for equipment and people and would only allow the attacker to gain access to information that was not considered particularly sensitive

Threat

- A threat is an action or event that might violate the security of an information systems environment.
- There are three components of threat :
  - Targets – the aspect of security that might be attacked
  - Agents – The people or organizations originating the threat
  - Events – the type of action that poses the threat

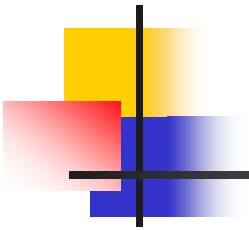


Targets

- Confidentiality – disclosure of information to unauthorized individuals
- Integrity – when the threat wishes to change information
- Availability – performance of DoS attack.

  Such attacks can target the availability of information, applications, systems, or infrastructure. Can be *short-term* or *long-term.*

Note : a threat may have multiple targets.

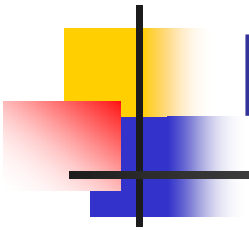


Agents

- The agents of threat are the people who wish to harm an organization.
- To be a credible part of a threat, an agent must have three characteristics:
  - Access - the ability to get to the target, e.g. an account on the system
  - Knowledge – the level of knowledge an agent has about the target e.g. passwords, network addresses, security procedures
  - Motivation – the reasons an agent might have for posing a threat to the target e.g. challenge, greed, or malicious intent

Agents to Consider

- Employees
- Ex-employees
- Hackers
- Commercial rivals
- Terrorists
- Criminals
- The general public
- Companies and supply services
- Customers
- Visitors
- Disasters



Events

- Events are the ways in which an agent of threat may cause the harm to an organization.
- Events that should be considered include :
  - Misuse of authorized access to information
  - Malicious or accidental alteration of information
  - Unauthorized access to information
  - Malicious or accidental destruction of information
  - Passive eavesdropping of communications
  - Theft of hardware or software
  - Natural physical events that may interfere with systems
  - Introduction of malicious software to systems

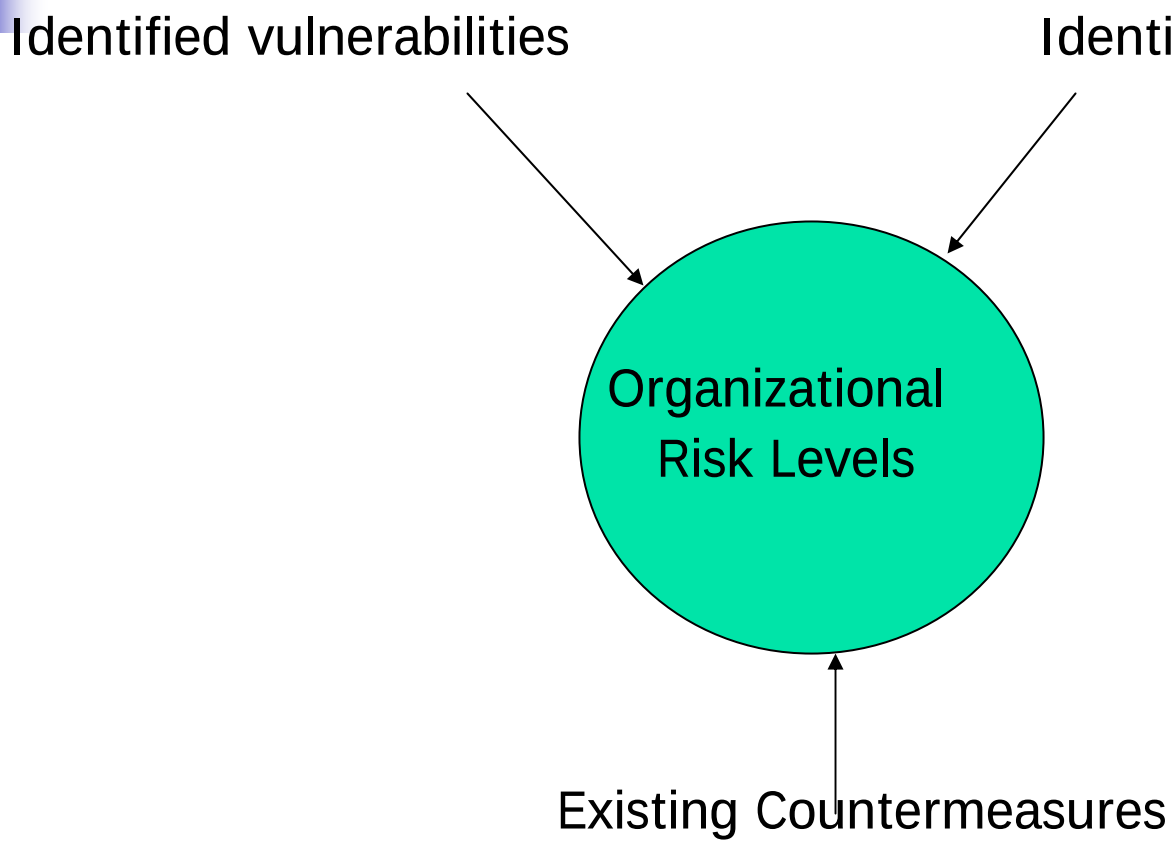
RISK

- Threat + Vulnerability = Risk
- Risk can be qualitatively defined in three levels:
  - High – vulnerability poses a real danger. Actions should be taken immediately to remove this vulnerability
  - Medium - vulnerability poses a significant level of risk and there is a real possibility that this may occur . Action to remove this vulnerability is advisable.
  - Low - vulnerability poses a level of risk though it is unlikely to occur. Action to remove this vulnerability should be taken if possible, but the cost of this action should be weighed against the small reduction in risk.

Identifying the Risk to an Organization

- Identifying Vulnerabilities :
  - Internet connections
  - Remote access points
  - Connections to other organizations
  - Physical access to facilities
  - User access points
  - Wireless access points
- For each of these access points, identify the information and systems that are accessible.
- Then identify how the information and systems may be accessed
- Include any known vulnerabilities in OS and applications.

Components of an Organizational Risk Assessment



Identifying Real Threats

- Threat assessment is a very detailed, time-consuming and difficult task.
- True threats will attempt to remain hidden from view
- True, targeted threats may not show themselves until an event has occurred.
- A targeted threat is the combination of a known agent having known access with a known motivation performing a known event against a known target.
  - E.g. a disgruntled employee (the agent) who desires knowledge of the latest designs an organization is working on (the motivation). This employee has access to the organization's information systems (access) and knows where the information is located (knowledge). The employee is targeting confidentiality of the new designs and may attempt to force his way into the files he wants (the event)
- An alternative to identifying targeted threats is to assume a generic level of threat in the world, this threat would be comprised of anyone with potential access to an organization's systems and information
- If we assume generic threat we can examine the vulnerabilities within an organization that may allow the access to occur
- Any such vulnerability then translates into risk since we assume there is a threat that may exploit the vulnerability.

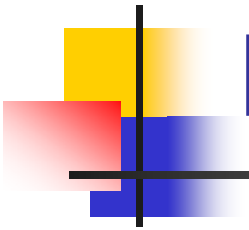
Examining Countermeasures

- Firewalls
- Anti-virus software
- Access controls
- Two factor authentication systems
- Badges
- Biometrics
- Card readers for access to facilities
- Guards
- File access controls
- Encryption
- Conscientious , well-trained employees
- Intrusion detection systems
- Automated patch and policy management systems

For each access point within an organization, countermeasures should be identified.

Identifying Risk

- Given the identified access points with the existing countermeasures, what could someone do to the organization through each access point?
- We take the likely threats for each access point and examine the potential targets through each access point. Based on the damage that can be done each risk is then rated : High , Medium , or Low.
- Note : the same vulnerability may pose different levels of risk based on the access point.
  - E.g Mail system vulnerability :
    - Internet firewall – low risk
    - Internal employees have access – medium risk



Measure Risk

- To be valuable, a risk assessment must identify the costs to the organization if an attack is successful
- Risk can never be completely removed. Risk must be managed.

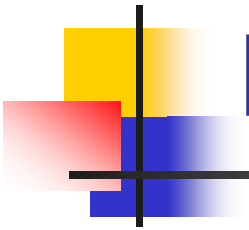
Qualitatively Assessing Risk

Impact

High Impact/Low probability	**High Impact/High probability**
Low Impact/Low probability	**Low Impact/High probability**

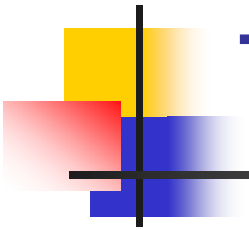
Probability

Binary Assessment



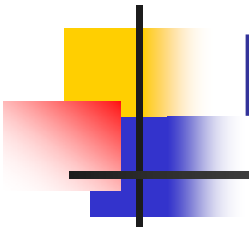
Money

- The most obvious way to measure risk is by the amount of money a successful penetration of an organization might cost. This includes :
  - Lost productivity (most difficult to estimate)
  - Stolen equipment or money
  - Cost of investigation
  - Cost of repair to the system
  - Cost of experts to assist
  - Employee overtime



Time

- Time is a measurement that is difficult to quantify.
- It may include the amount of time a technical staff member is unavailable to perform normal tasks due to a security event.
- But what about the time that other staff may be waiting for their computer to be fixed?
- Time may also mean the downtime of a key system.
- The delay in a product or service should be determined.
- Clearly, time, or perhaps lost time, must be included in the measurement of risk.

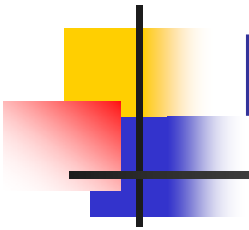


Resources

- Resources can be people, systems, communication lines, applications, or access.
- The monetary cost of using a resource to correct a situation if an attack occurs, can be computed.
- However , how is the non-monetary cost of not having a particular staff person available to perform other duties measured? Assigning a dollar value to this situation is not easy.
- The same issue exists for defining the cost of a slow network connection.

Reputation

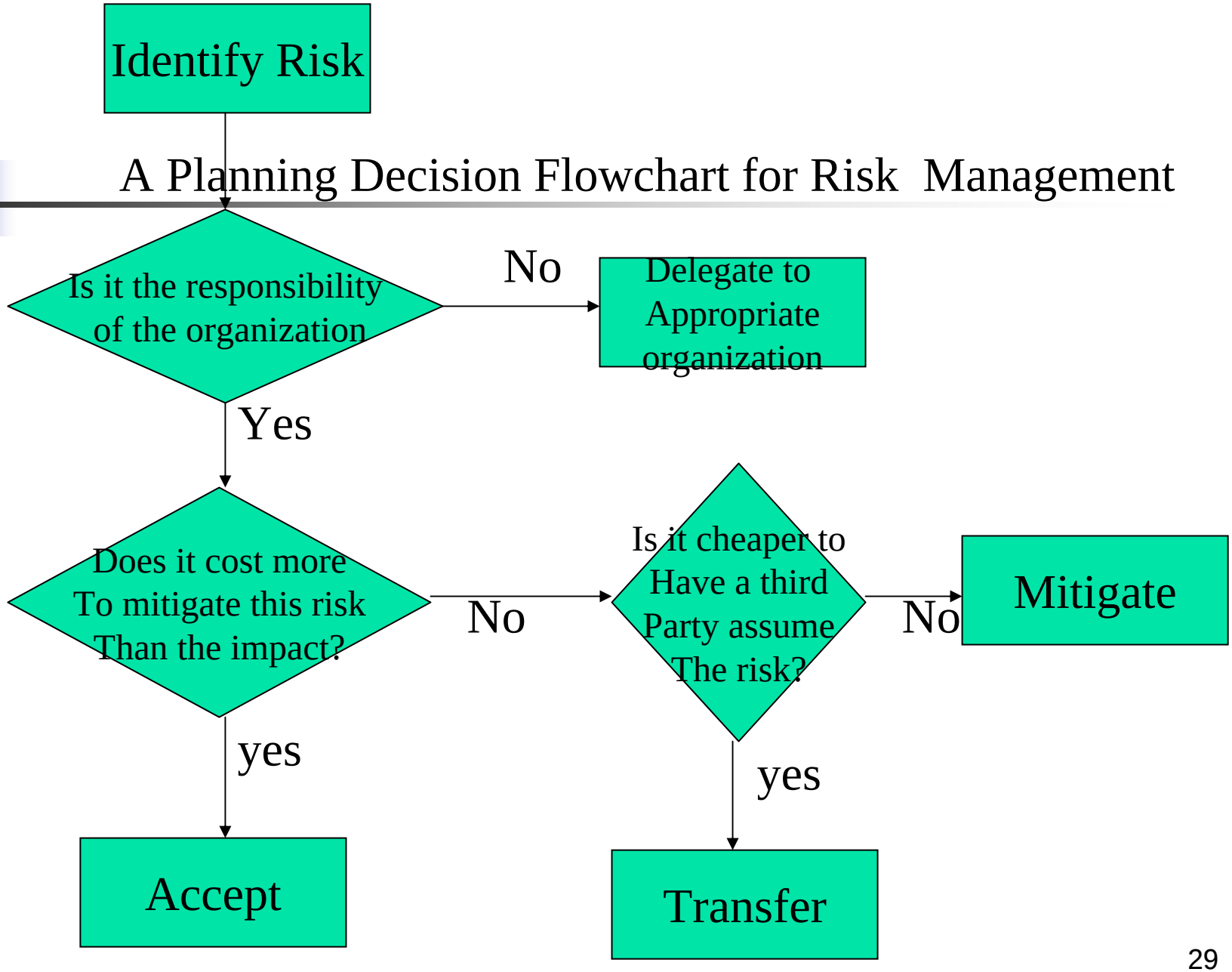
- The loss or degradation od an organization's reputation is a critical cost.
- However, the measurement of such loss is difficult.
- Reputation can be considered equivalent to trust.
  - For a bank- if people lose trust in a bank they will not put their money in the bank

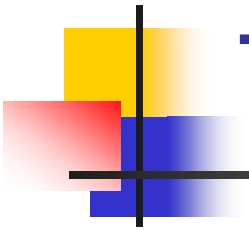


Lost Business

- Lost business is unrealized potential.
- It is possible to show how projected revenues or sales were not achieved, but how was the failure to achieve linked to security risk? Can the realization of the risk impact the organization so that business is lost?
  - E.g. an organization sells products over the Internet. The organization's web-site is down four days. Four days of sales did not occur.

A Planning Decision Flowchart for Risk Management





TOOLS

- Many tools can be used to enhance the risk management process.
  - Affinity grouping
  - Baseline identification and analysis
  - Cause and effect analysis
  - Cost/benefit analysis
  - Gantt charts
  - Interrelationship digraphs
  - Pareto charts
  - PERT charts
  - Risk management plan

II - Security Management

- A strong security infrastructure must be properly managed so it can continually ward off attackers.
- Security management must have the support from the highest levels of the organization to ensure that all users are aware of the importance of security and the key role that it plays in today's organizations.

Understanding Identity Management

- Identity management attempts to address problems and security vulnerabilities associated with users identifying and authenticating themselves across multiple accounts
- Solution may be found in identity management
  - A user's single authenticated ID is shared across multiple networks or online businesses

Understanding Identity Management (cont.)

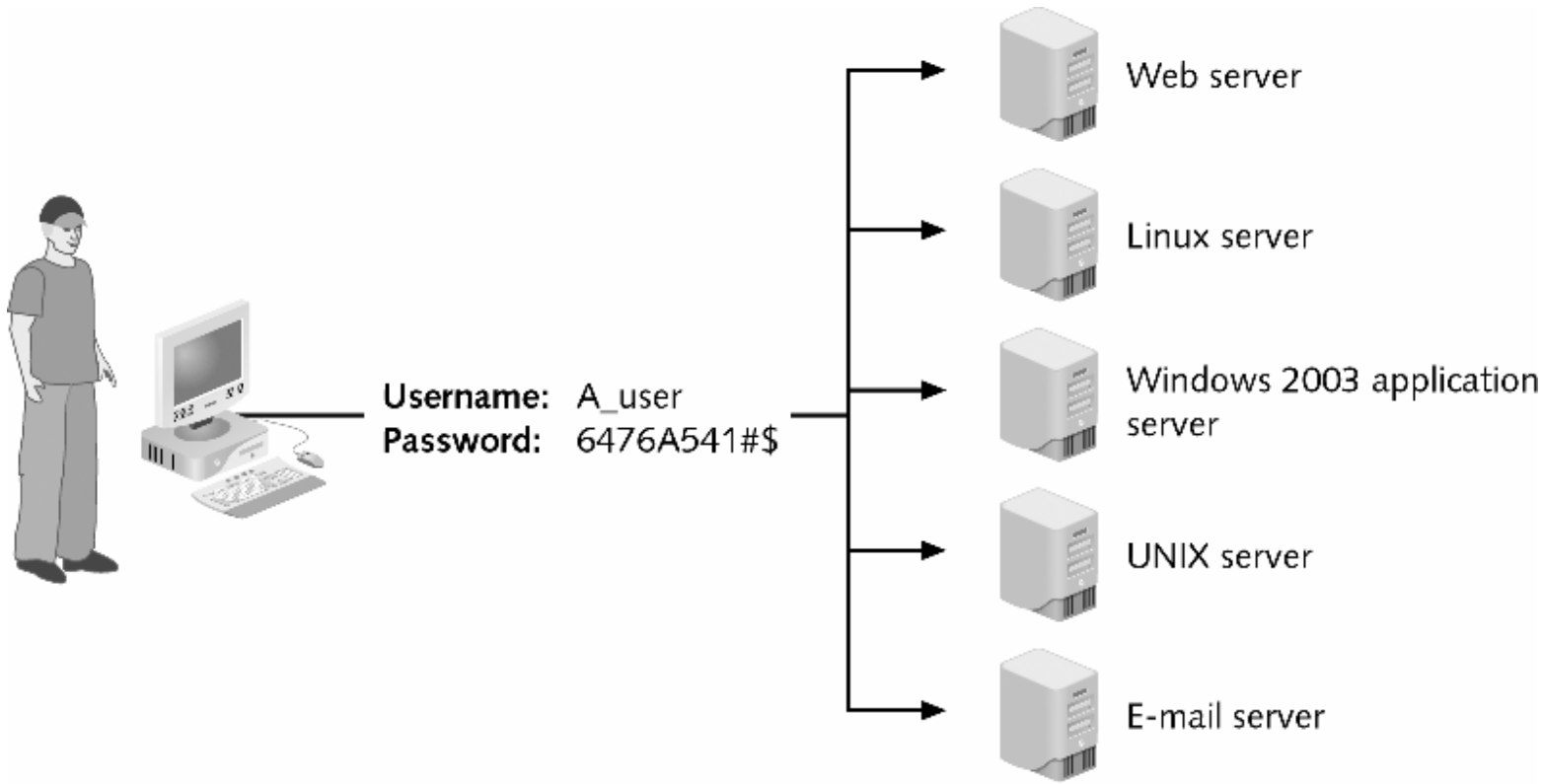


Fig 1 12-2 Identity management

Understanding Identity Management (cont.)

- Four key elements:
  - Single sign-on (SSO)
  - Password synchronization
  - Password resets
  - Access management

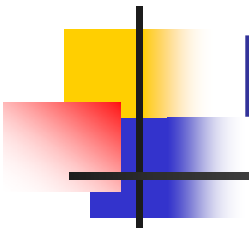
Understanding Identity Management (continued)

- SSO allows user to log on **one time** to a network or system and access multiple applications and systems based on that single password
- **Password synchronization** also permits a user to use a single password to log on to multiple servers
  - Instead of keeping a repository of user credentials, password synchronization ensures the password is the same for every application to which a user logs on

Understanding Identity Management (cont.)

- Password resets reduce costs associated with password-related help desk calls
  - *Identity management systems let users reset their own passwords and unlock their accounts without relying on the help desk*
- Access management software controls who can access the network while managing the content and business that users can perform while online

Hardening Systems Through Privilege Management



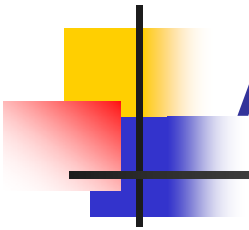
- Privilege management attempts to simplify assigning and revoking access control (privileges) to users

Centralized Or Decentralized Responsibility

- Responsibility can be centralized or decentralized
- Consider a chain of fast-food restaurants
  - Each location could have complete autonomy—it can decide whom to hire, when to open, how much to pay employees, and what brand of condiments to use
  - This decentralized approach has several advantages, including flexibility
  - A national headquarters tells each restaurant exactly what to sell, what time to close, and what uniforms to wear (**centralized approach**)

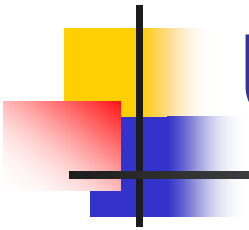
Centralized Or Decentralized Responsibility (cont.)

- Responsibility for privilege management can likewise be either centralized or decentralized
- In a centralized structure, one unit is responsible for all aspects of assigning or revoking privileges
- A decentralized organizational structure delegates authority for assigning or revoking privileges to smaller units, such as empowering each location to hire a network administrator to manage privileges



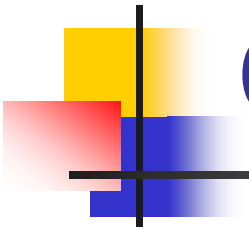
Assigning Privileges

- Privileges can be assigned by:
  - The user
  - The group to which the user belongs
  - The role that the user assumes in the organization



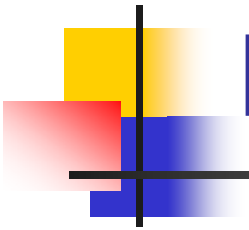
User Privileges

- If privileges are assigned by user,
  - the needs of each user should be closely examined to determine what privileges they need over which objects
- When assigning privileges on this basis,
  - the best approach is to have a baseline security template that applies to all users and then modify as necessary



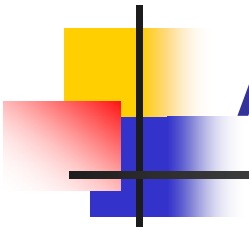
Group Privileges

- Instead of assigning privileges to each user, a group can be created and privileges assigned to the group
- As users are added to the group, they inherit those privileges



Role Privileges

- Instead of setting permissions for each user or group, you can assign permissions to a position or role and then assign users and other objects to that role
- The users inherit all permissions for the role



Auditing Privileges

- You should regularly audit the privileges that have been assigned
- Without auditing, it is impossible to know if users have been given too many unnecessary privileges and are creating security vulnerabilities

Usage Audit

- Process of reviewing activities a user has performed on the system or network
- Provides a detailed history of every action, the date and time, the name of the user, and other information

Usage Audits (cont.)

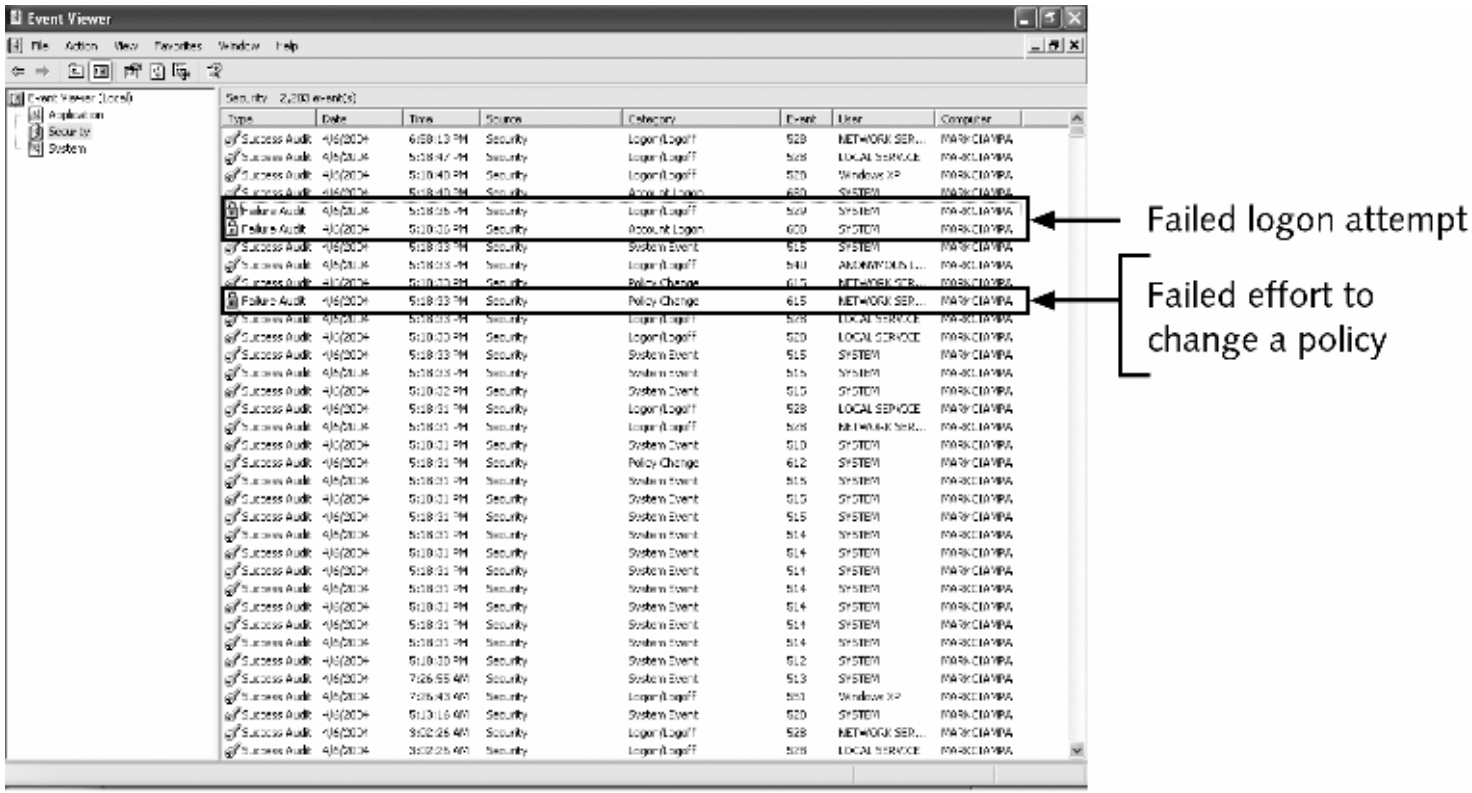
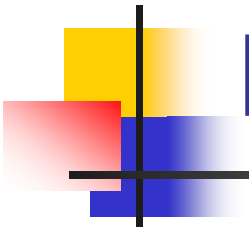
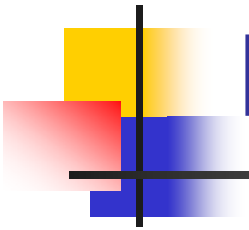


Fig. 2 12-3 Windows usage audit



Privilege Audit

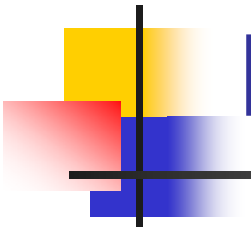
- Reviews privileges that have been assigned to a specific user, group, or role
- Begins by developing a list of the expected privileges of a user



Escalation Audits

- Reviews of usage audits to determine if privileges have unexpectedly escalated
- Privilege escalation attack:
  - attacker attempts to escalate her privileges without permission

Planning for Change Management



- Change management refers to a methodology for making changes and keeping track of those changes
- Change management involves identifying changes that should be documented and then making those documentations

Change Management Procedures

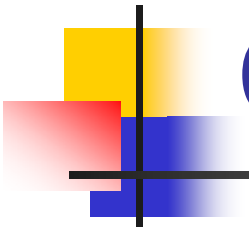
- Because changes can affect all users, and uncoordinated changes can result in
  - unscheduled service interruptions,
  - many organizations create a Change Management Team (CMT) to supervise the changes

Duties of the CMT

- Review proposed changes
- Ensure that the risk and impact of the planned change is clearly understood. It may be necessary to request additional information and clarification.
- Vote to recommend approval, disapproval, deferrals, or withdrawals of requested change.
- Communicate proposed and approved changes to co-workers in their areas.

Change Management Procedures (cont.)

- Process normally begins with a user or manager completing a Change Request form
- Although these forms vary widely, they usually include the information shown on the following slides:



Change Request Form

- Change Identifier
- Requester
- Team leader/manager
- Agency
- Change description
- Change reasons
- Change date

Change Request Form (cont.)

- Change components
- Impact category
- Help desk
- Management checklist
- Evaluation results

Changes That Should Be Documented

- Although change management involves all types of changes to information systems, two major types of security changes need to be properly documented
- First, any change in system architecture, such as new servers, routers, or other equipment being introduced into the network

Changes that Should Be Documented (cont.)

- Other changes that affect the security of the organization should also be documented:
  - Changes in user privileges
  - Changes in the configuration of a network device
  - Deactivation of network devices
  - Changes in client computer configurations
  - Changes in security personnel

Documenting Changes

- Decisions must be made regarding how long the documentation should be retained after it is updated
- Some security professionals recommend all documentation be kept for at least three years after any changes are made
- At the end of that time, documentation should be securely shredded or disposed of so that it could not be reproduced

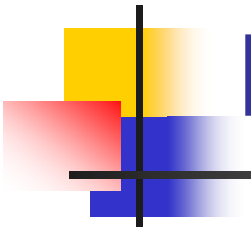
Understanding Digital Rights Management (DRM)

- Most organizations go to great lengths to establish a security perimeter around a network or system to prevent attackers from accessing information
- Information security can also be enhanced by building a security fence around the information itself
- Goal of DRM is to provide another layer of security:
  - *an attacker who can break into a network still faces another hurdle in trying to access information itself*

Content Providers

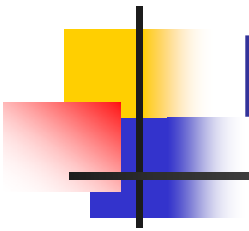
- Data theft is usually associated with stealing an electronic document from a company or credit card information from a consumer
- Another type of electronic thievery is illegal electronic duplication and distribution of intellectual property, which includes books, music, plays, paintings, and photographs
  - *Considered theft because it deprives the creator or owner of the property of compensation for their work (known as royalties)*

Enterprise Document Protection



- Protecting documents through DRM can be accomplished at one of two levels
- First level is file-based DRM; focuses on protecting content of a single file
  - Most document-creation software now allows a user to determine the rights that the reader of the document may have
  - Restrictions can be contained in metadata (information about a document)

Enterprise Document Protection (cont.)



- Server-based DRM is a more comprehensive approach
  - Server-based products can be integrated with Lightweight Directory Access Protocol (LDAP) for authentication and can provide access to groups of users based on their privileges

Enterprise Document Protection (cont.)

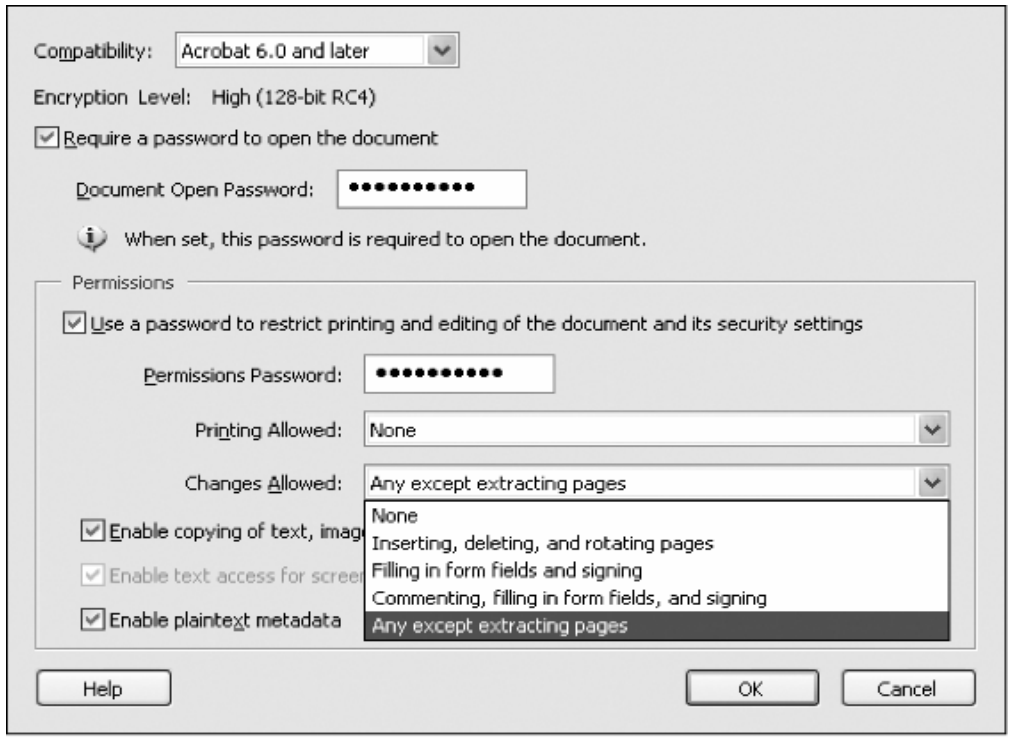


Fig.3 Restrictions to document

Acquiring Effective Training and Education

- Organizations should provide education and training at set times and on an ad hoc basis
- Opportunities for security education and training:
  - New employee is hired
  - Employee is promoted or given new responsibilities
  - New user software is installed
  - User hardware is upgraded
  - Aftermath of an infection by a worm or virus
  - Annual department retreats

How Learners Learn

- Learning involves communication: a person or material developed by a person is communicated to a receiver
- In the United States, generation traits influence how people learn
- Also understand that the way you were taught may not be the best way to teach others

Available Resources

- Seminars and workshops are a good means of learning the latest technologies and networking with other security professionals in the area
- Print media is another resource for learning content
- The Internet contains a wealth of information that can be used on a daily basis to keep informed about new attacks and trends