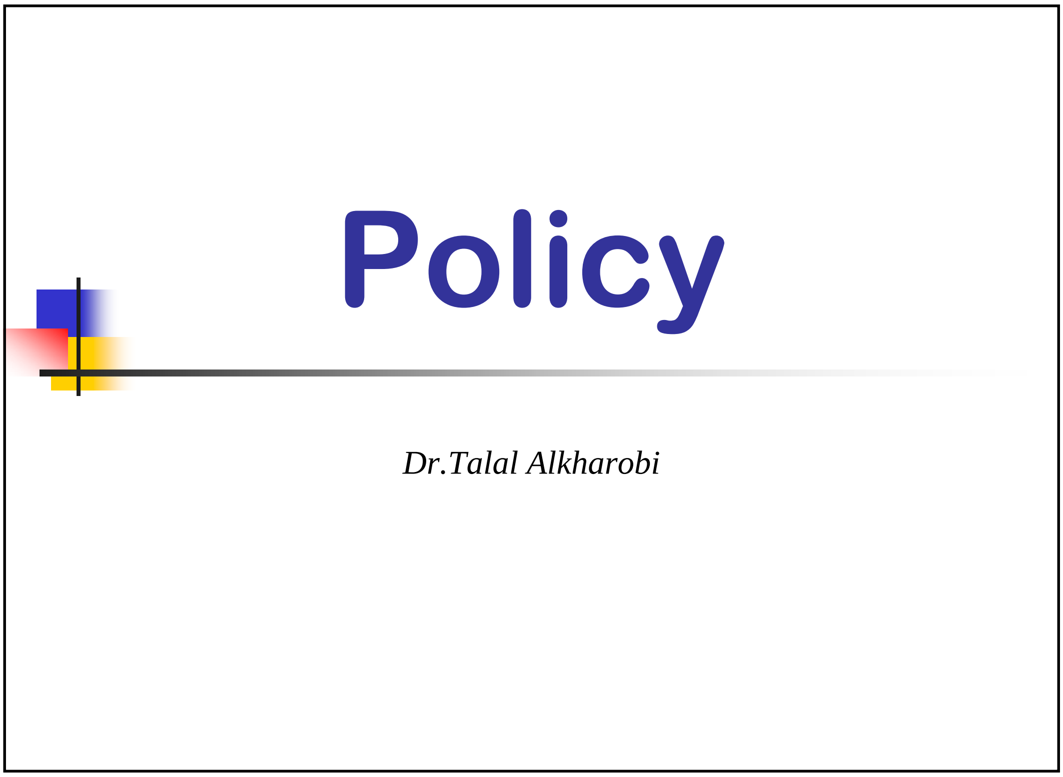
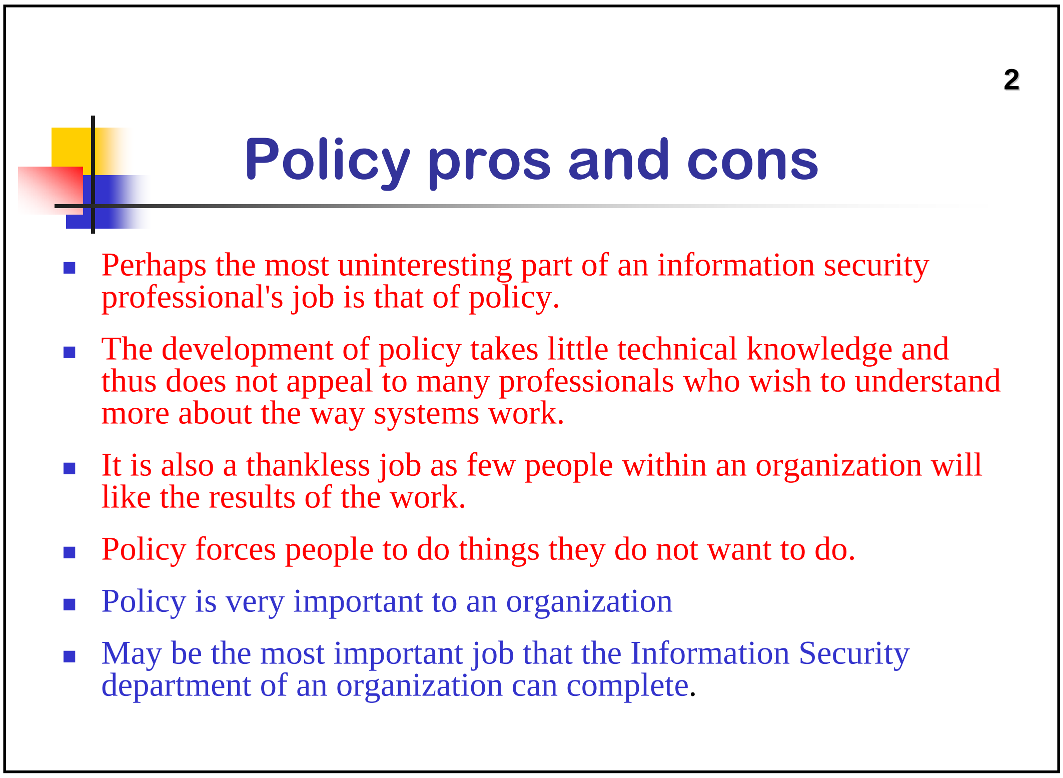


Policy

Dr.Talal Alkharobi



Policy pros and cons

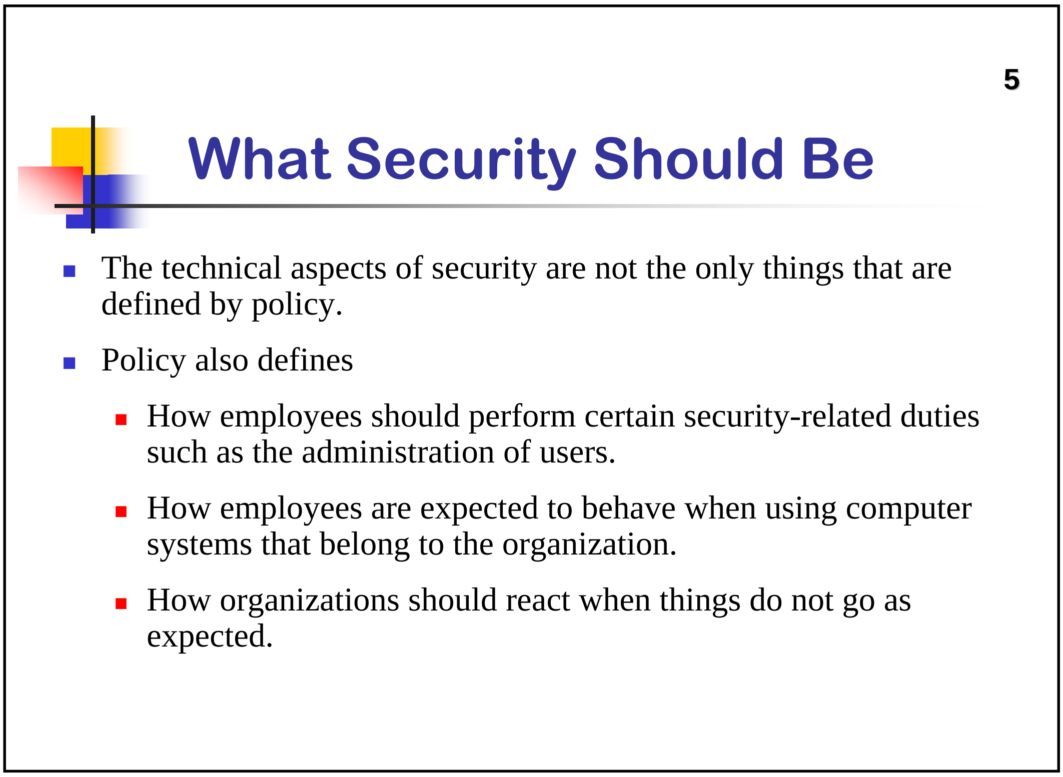
- Perhaps the most uninteresting part of an information security professional's job is that of policy.
- The development of policy takes little technical knowledge and thus does not appeal to many professionals who wish to understand more about the way systems work.
- It is also a thankless job as few people within an organization will like the results of the work.
- Policy forces people to do things they do not want to do.
- Policy is very important to an organization
- May be the most important job that the Information Security department of an organization can complete.

Why Policy Is Important

- Policy provides the rules that govern how systems should be configured and how employees of an organization should act in normal circumstances and react during unusual circumstances
- Policy performs two primary functions:
  - Defines what security should be within an organization.
  - Puts everyone on the same page so everyone understands what is expected

What Security Should Be

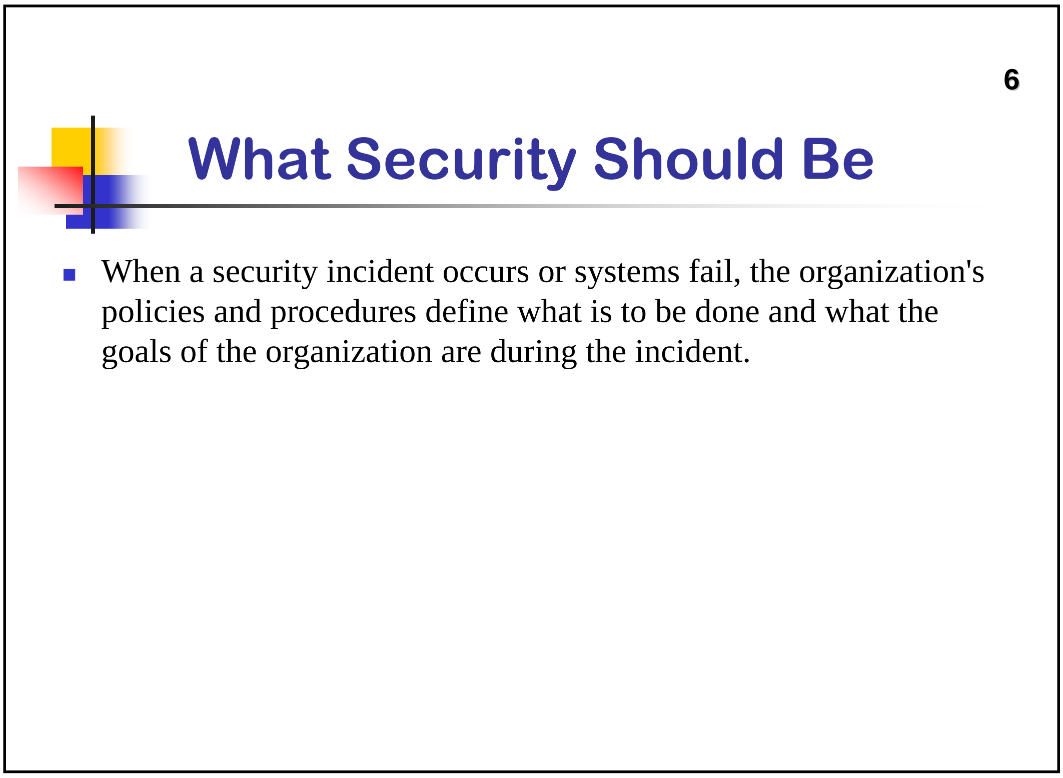
- Policy defines how security should be implemented.
- This includes the
  - proper configurations on computer systems
  - proper configurations on networks
  - physical security measures
  - proper mechanisms to use to protect information
  - proper mechanisms to use to protect systems



5

What Security Should Be

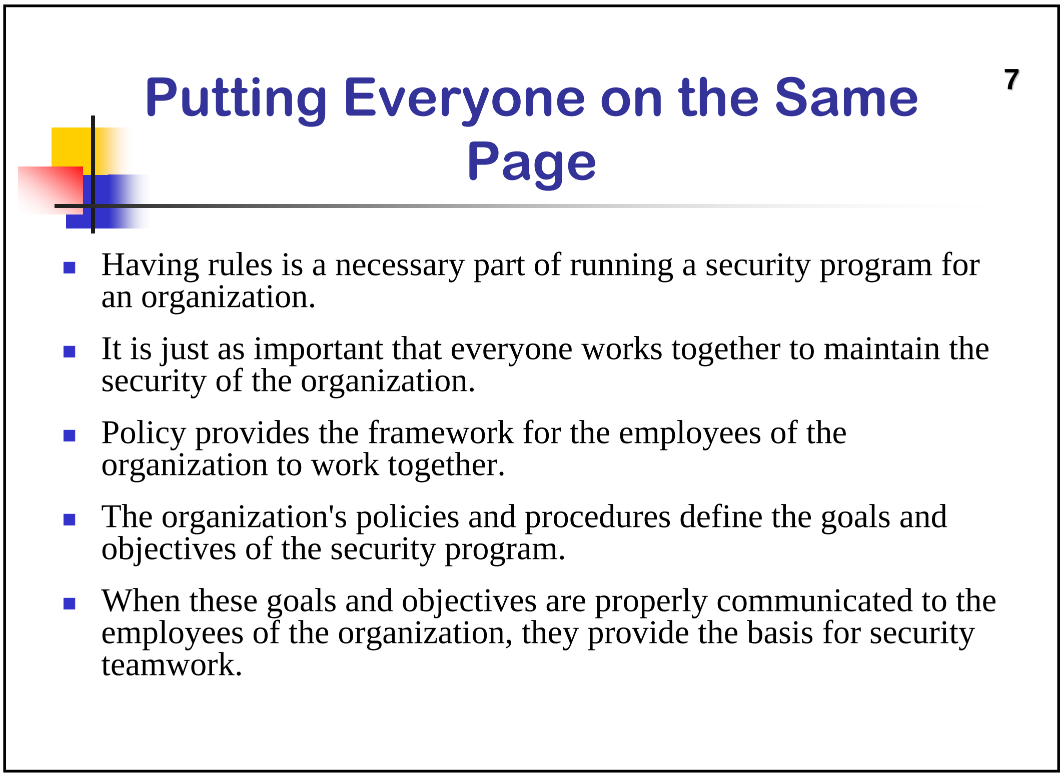
- The technical aspects of security are not the only things that are defined by policy.
- Policy also defines
  - How employees should perform certain security-related duties such as the administration of users.
  - How employees are expected to behave when using computer systems that belong to the organization.
  - How organizations should react when things do not go as expected.



6

What Security Should Be

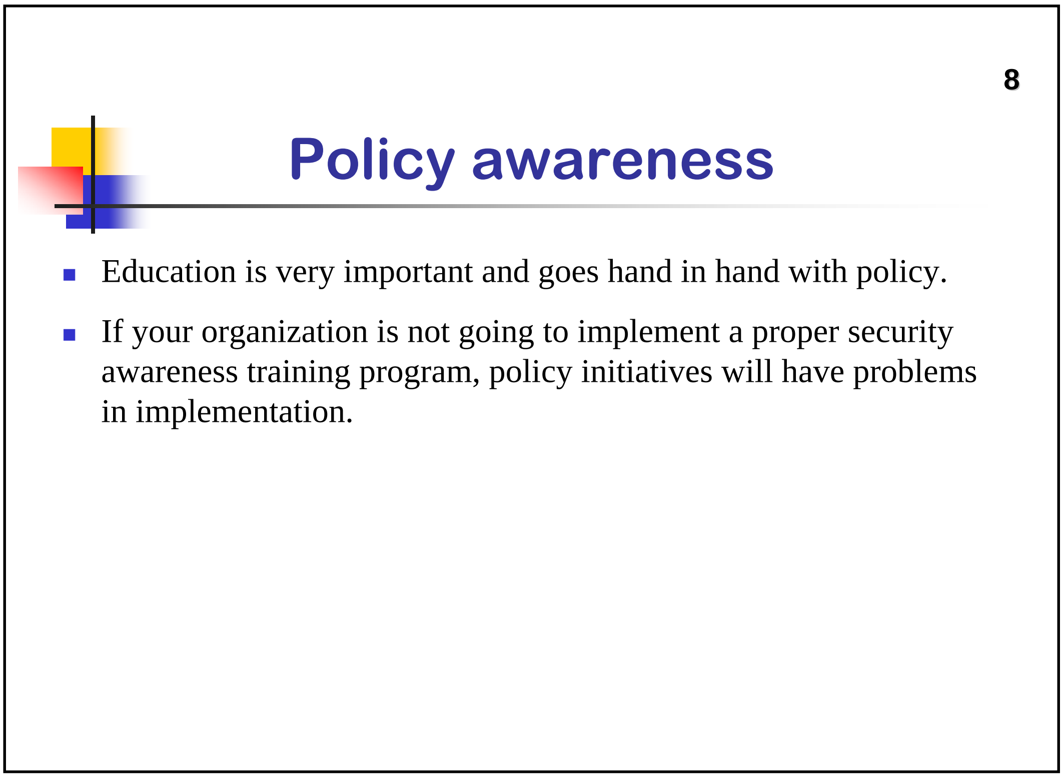
- When a security incident occurs or systems fail, the organization's policies and procedures define what is to be done and what the goals of the organization are during the incident.



7

Putting Everyone on the Same Page

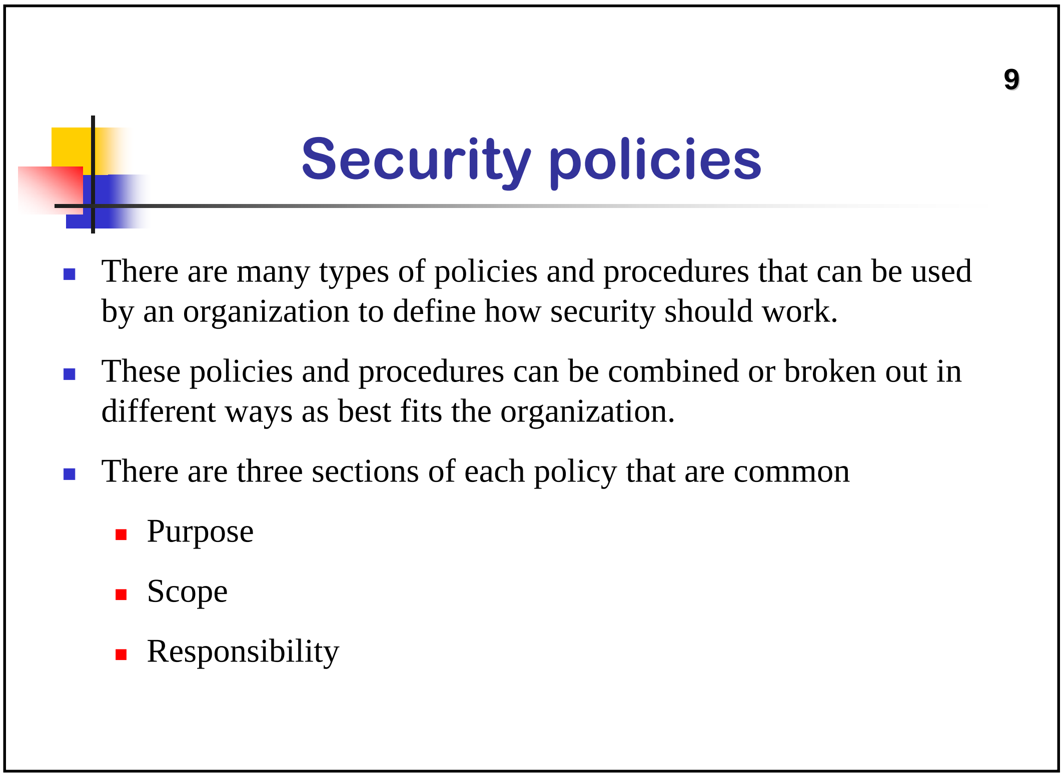
- Having rules is a necessary part of running a security program for an organization.
- It is just as important that everyone works together to maintain the security of the organization.
- Policy provides the framework for the employees of the organization to work together.
- The organization's policies and procedures define the goals and objectives of the security program.
- When these goals and objectives are properly communicated to the employees of the organization, they provide the basis for security teamwork.



8

Policy awareness

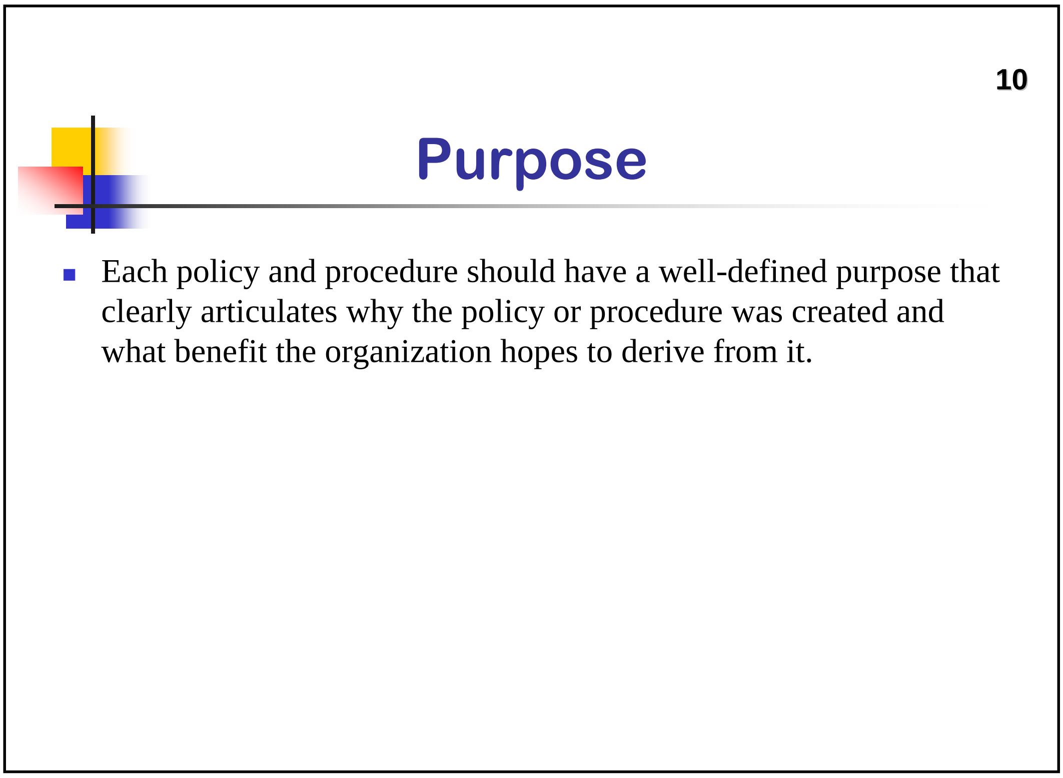
- Education is very important and goes hand in hand with policy.
- If your organization is not going to implement a proper security awareness training program, policy initiatives will have problems in implementation.



9

Security policies

- There are many types of policies and procedures that can be used by an organization to define how security should work.
- These policies and procedures can be combined or broken out in different ways as best fits the organization.
- There are three sections of each policy that are common
  - Purpose
  - Scope
  - Responsibility



10

Purpose

- Each policy and procedure should have a well-defined purpose that clearly articulates why the policy or procedure was created and what benefit the organization hopes to derive from it.

11

Scope

- Each policy and procedure should have a section defining its applicability.
- For example, a security policy might apply to all computer and network systems.

12

Responsibility

- The responsibility section of a policy or procedure defines who will be held accountable for the proper implementation of the document.
- Whoever is defined as having the responsibility for a policy or procedure must be properly trained and made aware of the requirements of the document.

13

Needed policies

1. **Information**
2. **Security**
3. **Computer use**
4. **Internet use**
5. **Email**
6. **Backup**
7. **User Management Procedure**
8. **System Administrator Procedure**
9. **Incident responding Procedure**
10. **Configuration Management Procedure**
11. **Design Methodology**
12. **Disaster Recovery**

14

[1] Information Policy

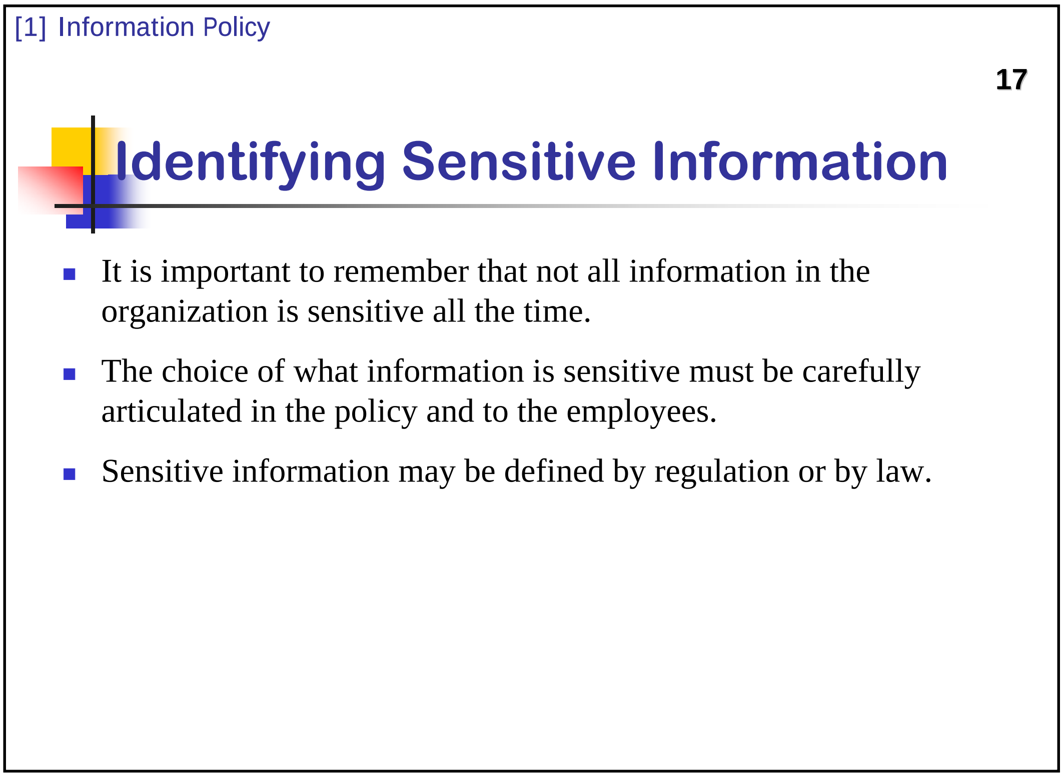
- Defines what sensitive information is within the organization and how that information should be protected.
- This policy should be constructed to cover all information within the organization.
- Each employee is responsible for protecting sensitive information that comes into the employee's possession.
- The policy must take into account information in paper records and electronic files.

Identifying Sensitive Information

- The information in an organization that is considered sensitive will differ depending on the business of the organization.
- Sensitive information may include
  - business records,
  - product designs,
  - patent information,
  - company phone books

Identifying Sensitive Information

- Some information that will be sensitive in all organizations:
  - payroll information,
  - home addresses and phone numbers for employees,
  - medical insurance information,
  - financial information before it is disclosed to the general public

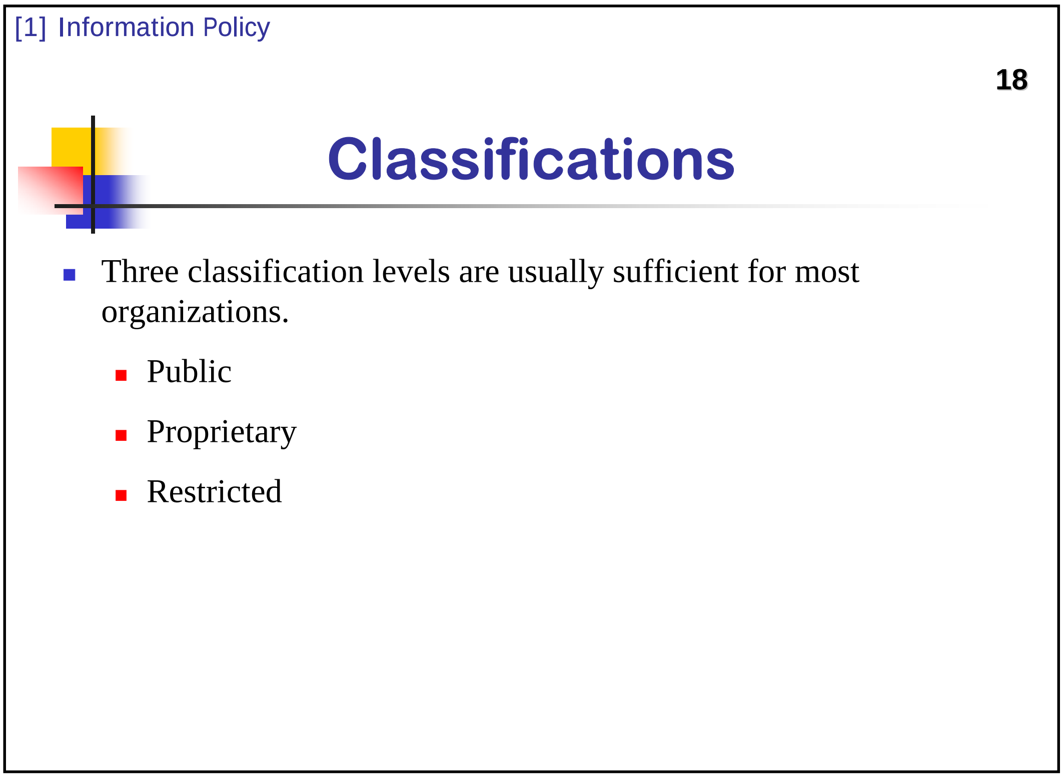


[1] Information Policy

17

Identifying Sensitive Information

- It is important to remember that not all information in the organization is sensitive all the time.
- The choice of what information is sensitive must be carefully articulated in the policy and to the employees.
- Sensitive information may be defined by regulation or by law.

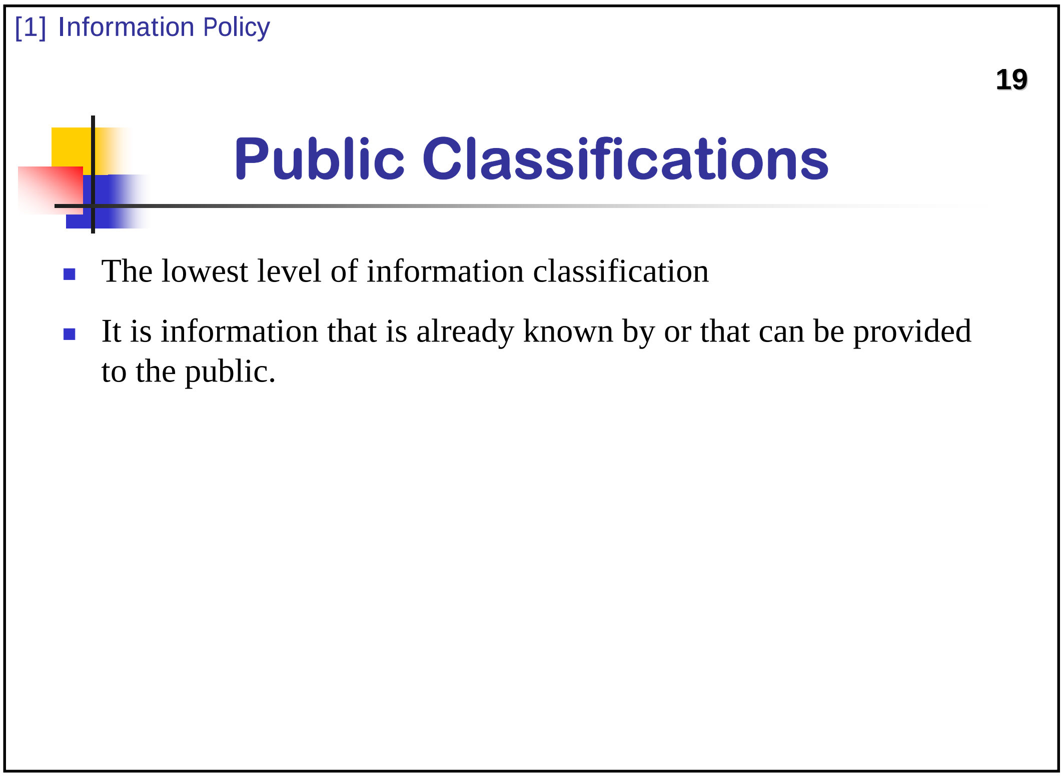


[1] Information Policy

18

Classifications

- Three classification levels are usually sufficient for most organizations.
  - Public
  - Proprietary
  - Restricted

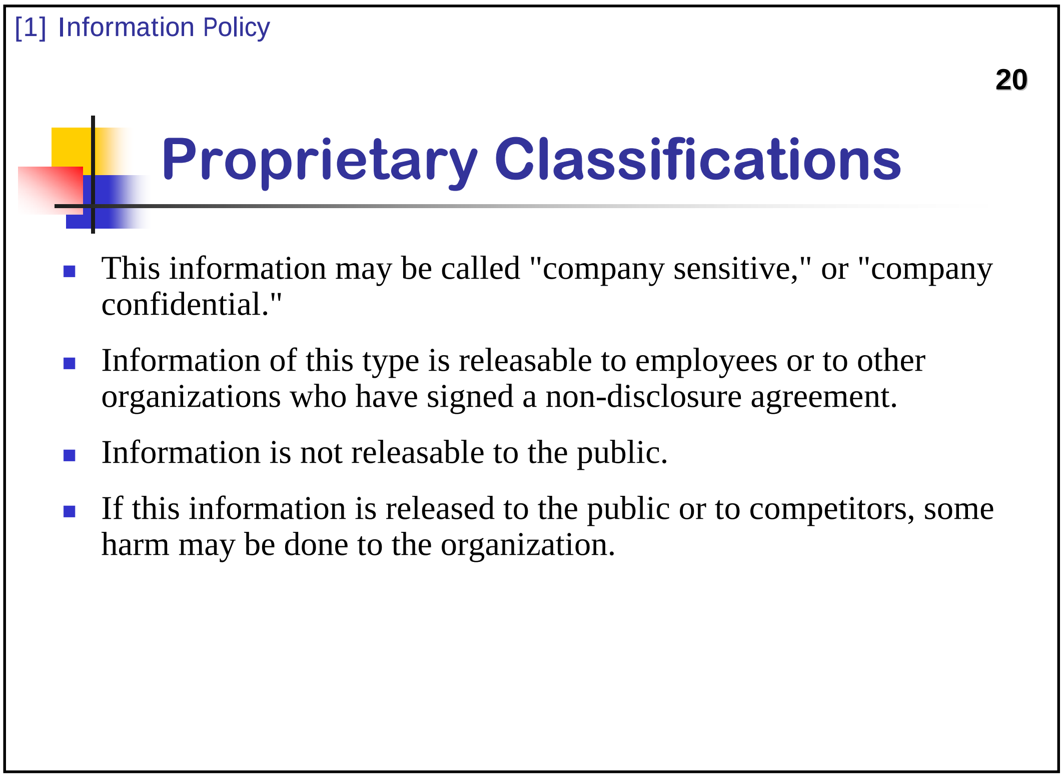


[1] Information Policy

19

Public Classifications

- The lowest level of information classification
- It is information that is already known by or that can be provided to the public.

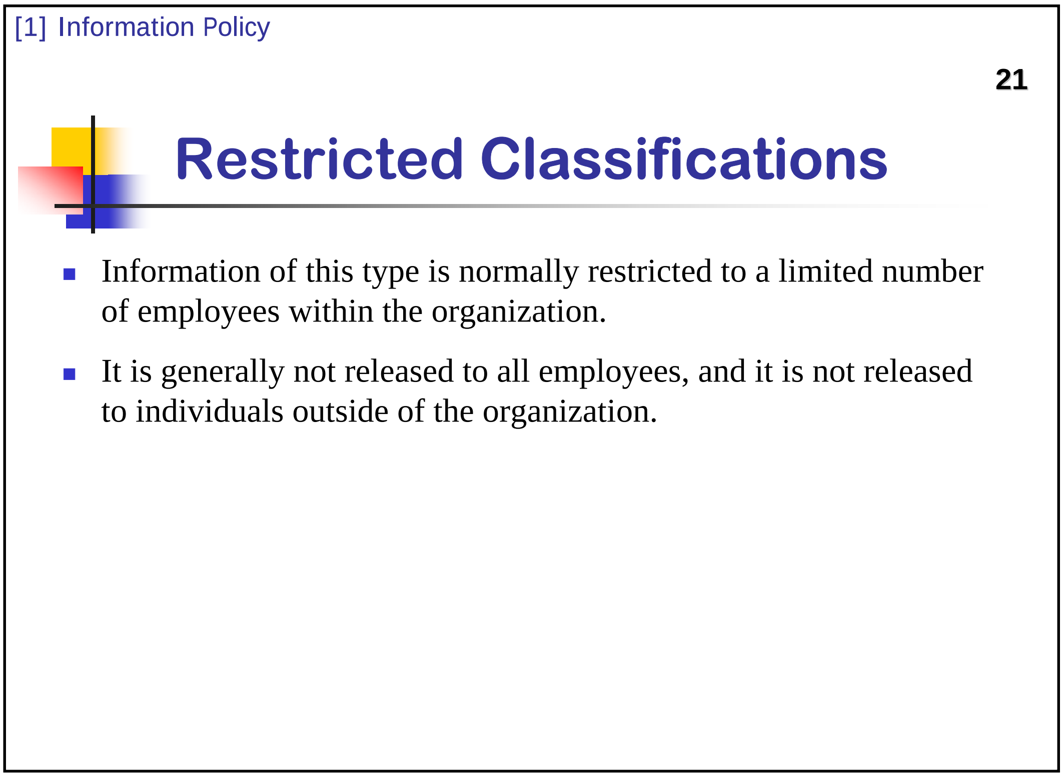


[1] Information Policy

20

Proprietary Classifications

- This information may be called "company sensitive," or "company confidential."
- Information of this type is releasable to employees or to other organizations who have signed a non-disclosure agreement.
- Information is not releasable to the public.
- If this information is released to the public or to competitors, some harm may be done to the organization.

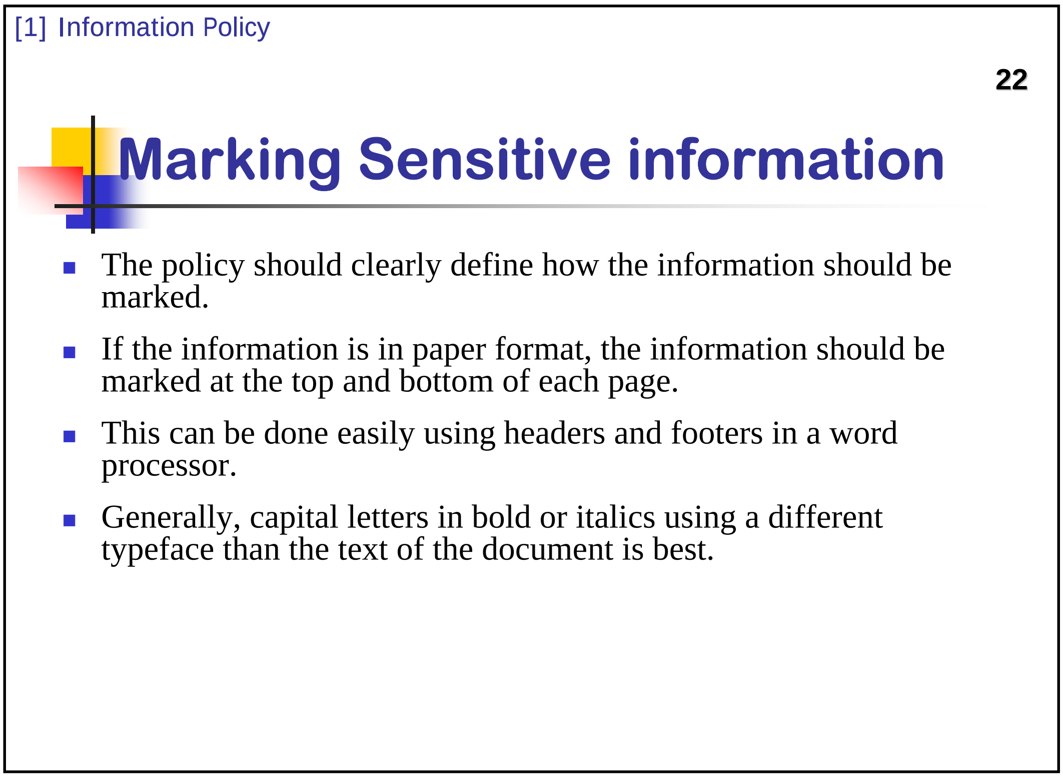


[1] Information Policy

21

Restricted Classifications

- Information of this type is normally restricted to a limited number of employees within the organization.
- It is generally not released to all employees, and it is not released to individuals outside of the organization.

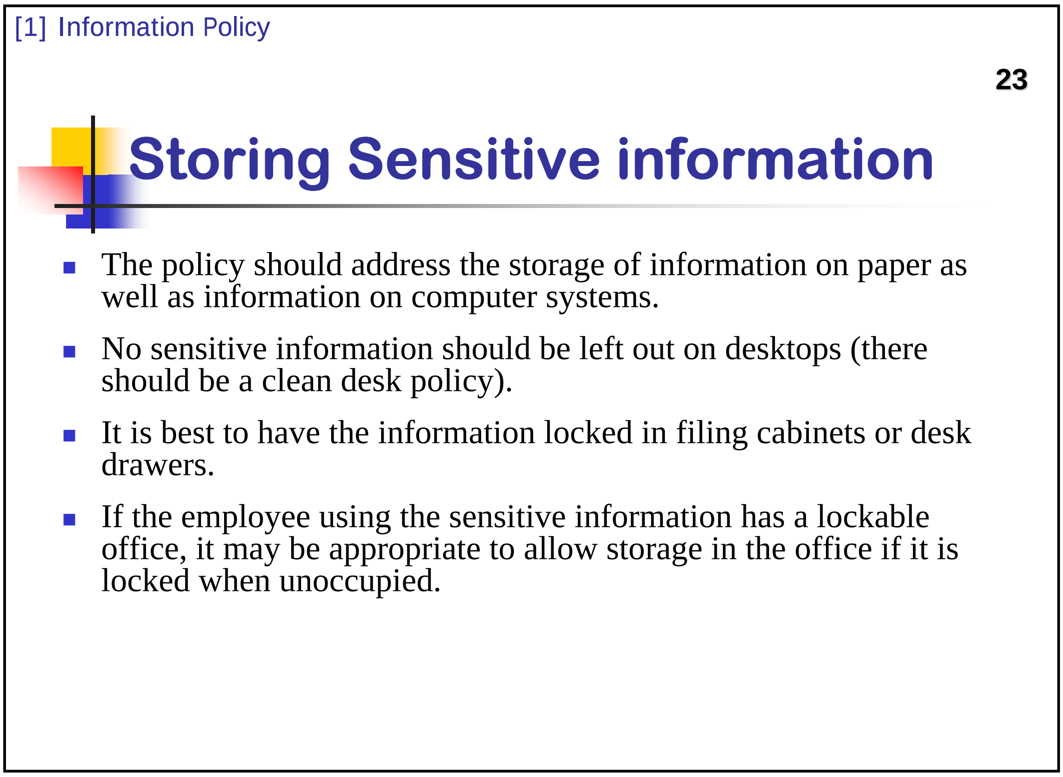


[1] Information Policy

22

Marking Sensitive information

- The policy should clearly define how the information should be marked.
- If the information is in paper format, the information should be marked at the top and bottom of each page.
- This can be done easily using headers and footers in a word processor.
- Generally, capital letters in bold or italics using a different typeface than the text of the document is best.

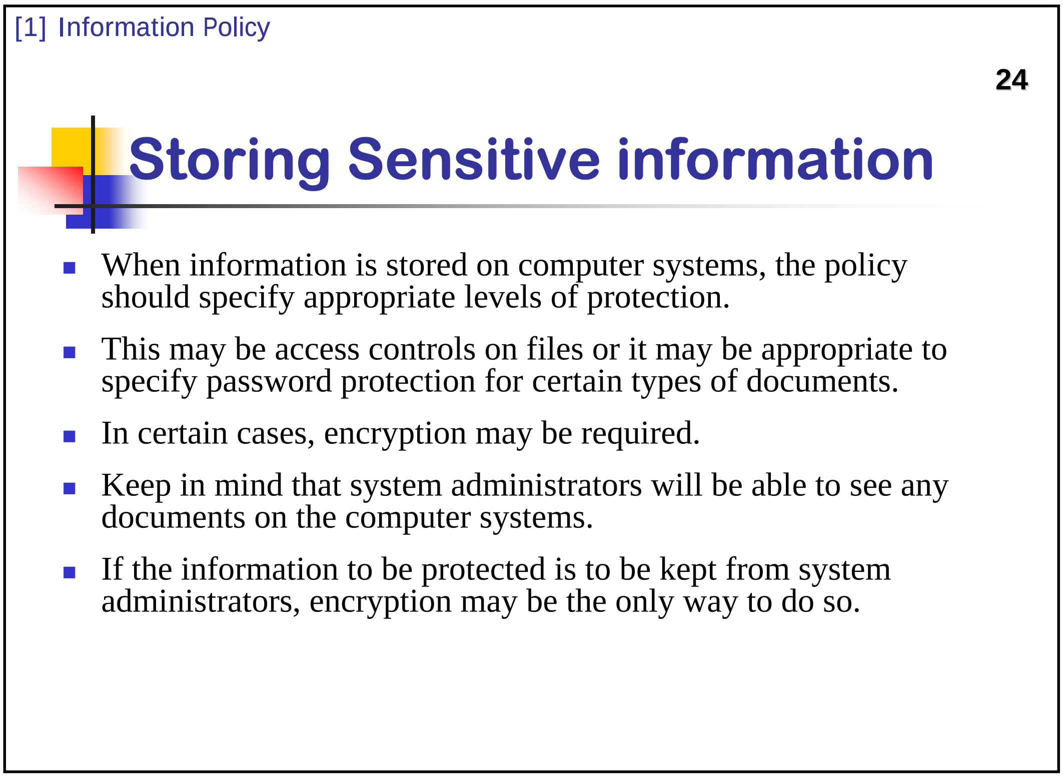


[1] Information Policy

23

Storing Sensitive information

- The policy should address the storage of information on paper as well as information on computer systems.
- No sensitive information should be left out on desktops (there should be a clean desk policy).
- It is best to have the information locked in filing cabinets or desk drawers.
- If the employee using the sensitive information has a lockable office, it may be appropriate to allow storage in the office if it is locked when unoccupied.



[1] Information Policy

24

Storing Sensitive information

- When information is stored on computer systems, the policy should specify appropriate levels of protection.
- This may be access controls on files or it may be appropriate to specify password protection for certain types of documents.
- In certain cases, encryption may be required.
- Keep in mind that system administrators will be able to see any documents on the computer systems.
- If the information to be protected is to be kept from system administrators, encryption may be the only way to do so.

[1] Information Policy

25

Transmission of Sensitive information

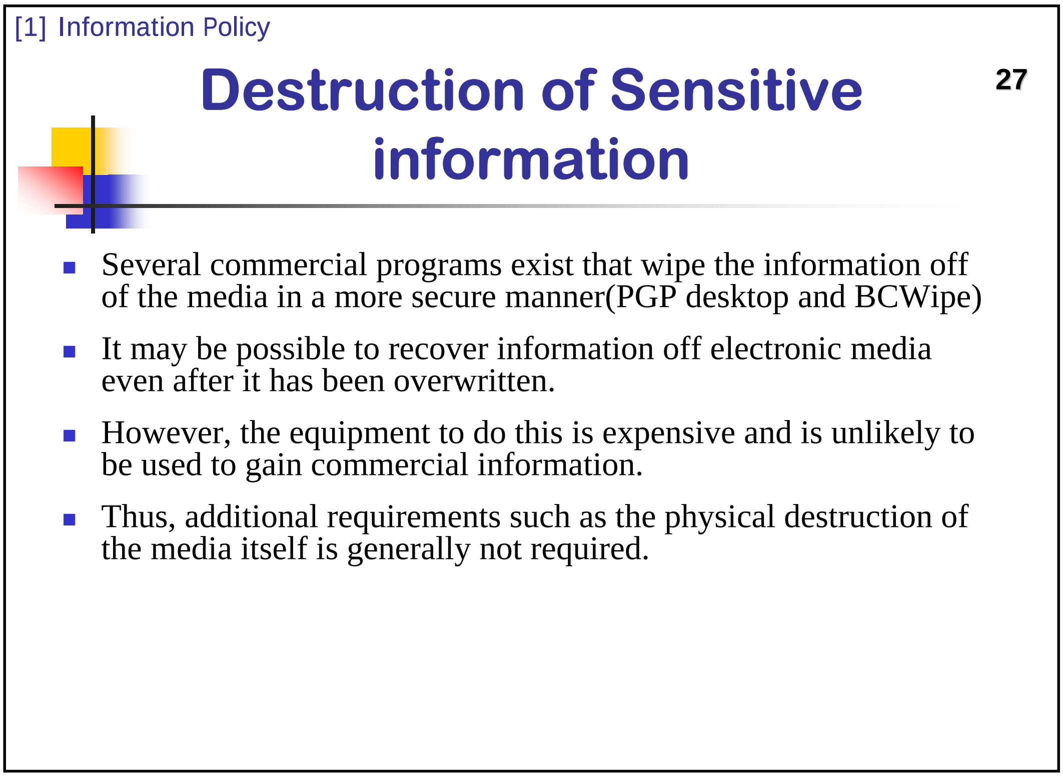
- The policy should address various way of transmitting information by e-mail, regular mail, or Fax
- For sensitive information sent through email, the policy should specify encryption of the attachments and/or the message body
- If hardcopies of the information are to be sent, some method that requires a signed receipt is appropriate (certified mail).
- When a document is to be faxed, it is appropriate to require a phone call to the receiving party and for the sender to request the receiver to wait by the fax machine for the document.
- This will prevent the document from sitting on the receiving fax machine for an extended period of time.

[1] Information Policy

26

Destruction of Sensitive information

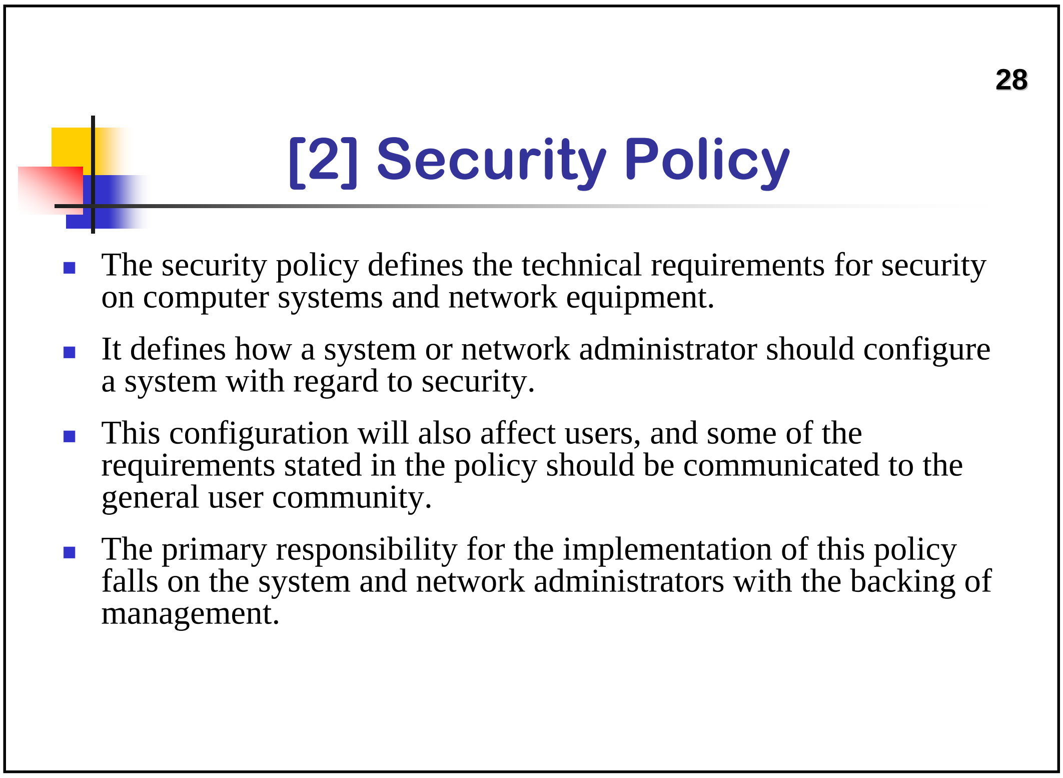
- Sensitive information that is thrown in the trash or in the recycling bin may be accessible by unauthorized individuals.
- Sensitive information on paper should be shredded.
- Cross-cut shredders provide an added level of protection by cutting paper both horizontally and vertically.
- This makes it very unlikely that the information could be reconstructed.
- Information that is stored on computer can be recovered after deletion if it is not deleted properly.



[1] Information Policy

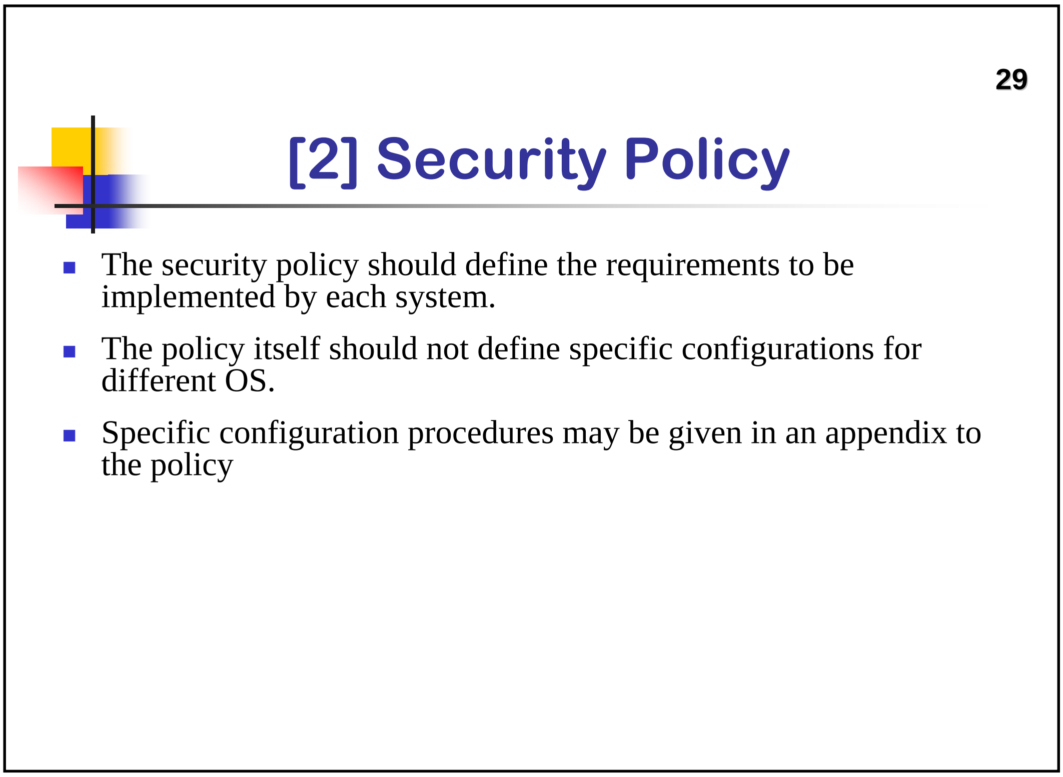
Destruction of Sensitive information

- Several commercial programs exist that wipe the information off of the media in a more secure manner(PGP desktop and BCWipe)
- It may be possible to recover information off electronic media even after it has been overwritten.
- However, the equipment to do this is expensive and is unlikely to be used to gain commercial information.
- Thus, additional requirements such as the physical destruction of the media itself is generally not required.



[2] Security Policy

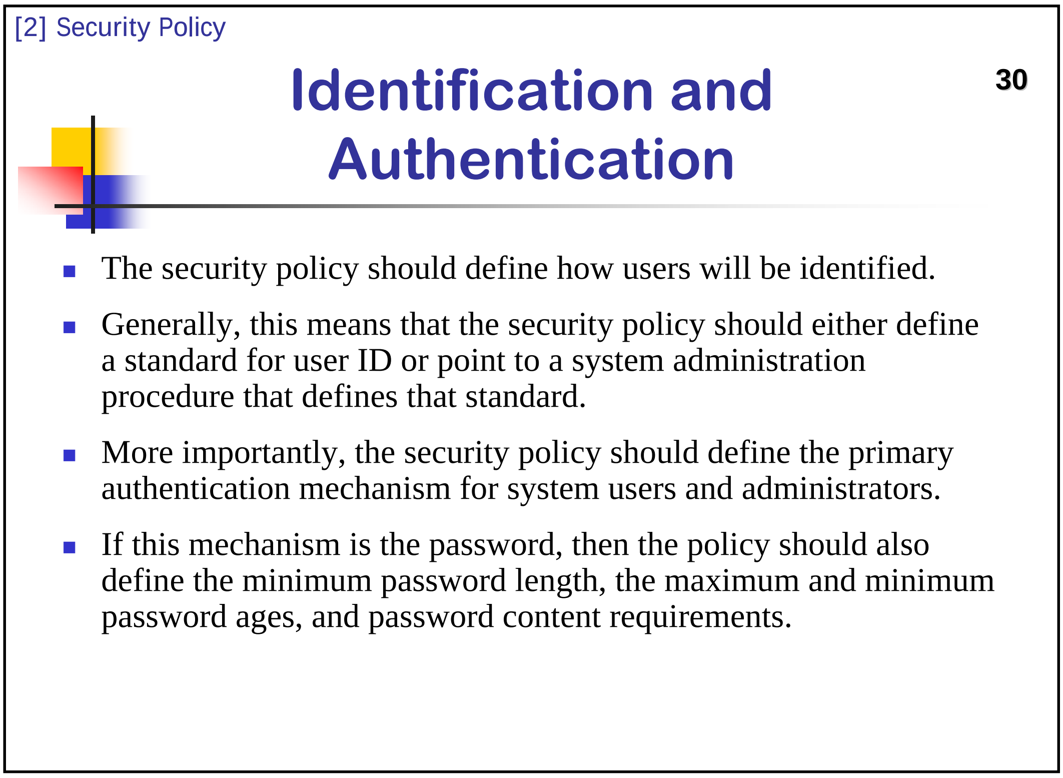
- The security policy defines the technical requirements for security on computer systems and network equipment.
- It defines how a system or network administrator should configure a system with regard to security.
- This configuration will also affect users, and some of the requirements stated in the policy should be communicated to the general user community.
- The primary responsibility for the implementation of this policy falls on the system and network administrators with the backing of management.



29

[2] Security Policy

- The security policy should define the requirements to be implemented by each system.
- The policy itself should not define specific configurations for different OS.
- Specific configuration procedures may be given in an appendix to the policy



[2] Security Policy

30

Identification and Authentication

- The security policy should define how users will be identified.
- Generally, this means that the security policy should either define a standard for user ID or point to a system administration procedure that defines that standard.
- More importantly, the security policy should define the primary authentication mechanism for system users and administrators.
- If this mechanism is the password, then the policy should also define the minimum password length, the maximum and minimum password ages, and password content requirements.

[2] Security Policy

31

Identification and Authentication

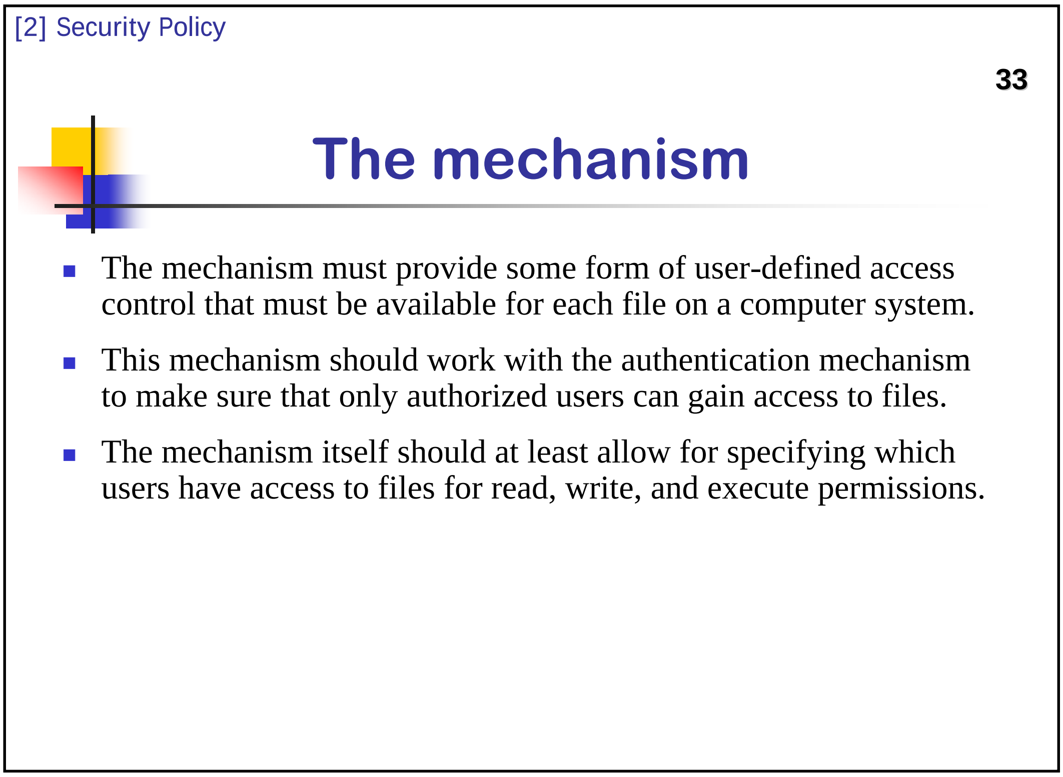
- Each organization, while developing its security policy, should decide whether administrative accounts should use the same authentication mechanism or a stronger one.
- If a stronger mechanism is to be required, this section of the policy should define the appropriate security requirements.
- This stronger mechanism may also be appropriate for remote access such as VPN or dial-in access.
- In almost all cases, administrative accounts should use stronger authentication methods such as smart cords.

[2] Security Policy

32

Files Access Control

- The security policy should define the standard requirement for access controls to be placed on electronic files.
- Two requirements should be defined:
  - the mechanism The default requirement for new files.

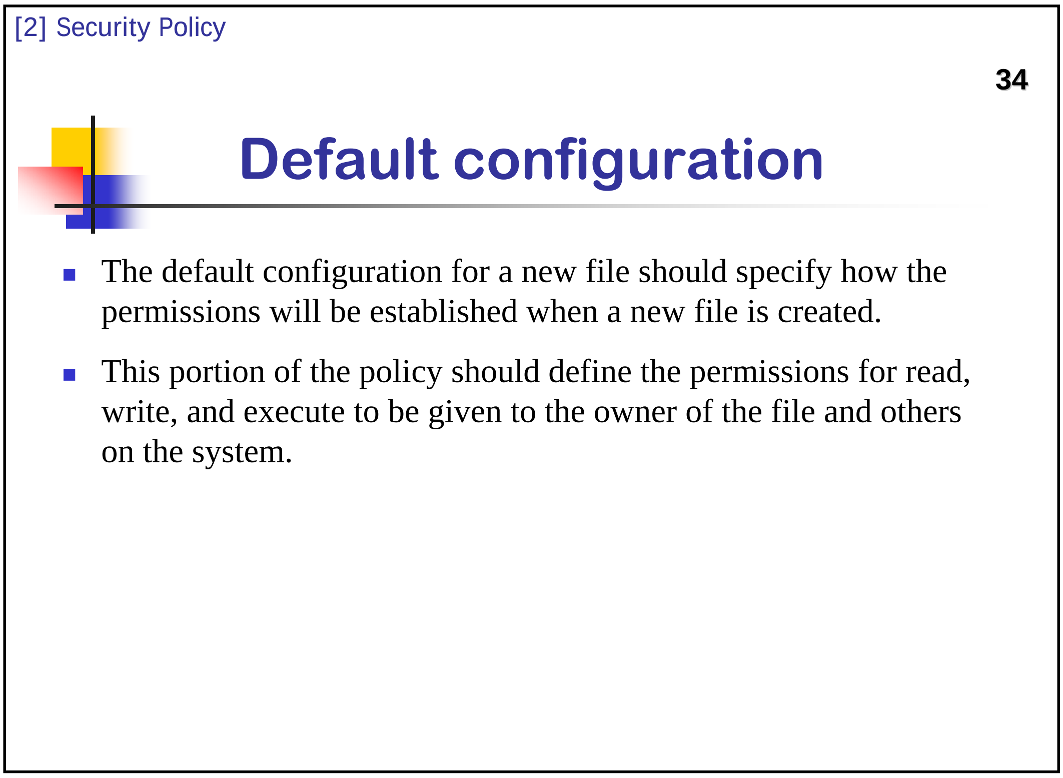


[2] Security Policy

33

The mechanism

- The mechanism must provide some form of user-defined access control that must be available for each file on a computer system.
- This mechanism should work with the authentication mechanism to make sure that only authorized users can gain access to files.
- The mechanism itself should at least allow for specifying which users have access to files for read, write, and execute permissions.

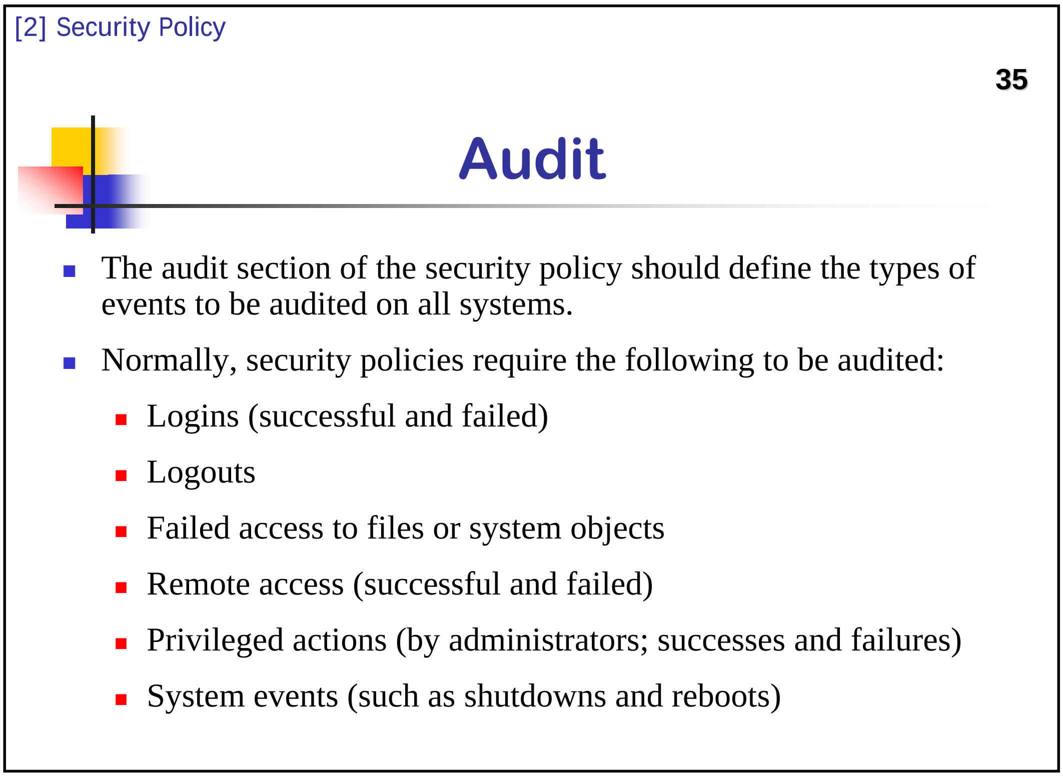


[2] Security Policy

34

Default configuration

- The default configuration for a new file should specify how the permissions will be established when a new file is created.
- This portion of the policy should define the permissions for read, write, and execute to be given to the owner of the file and others on the system.

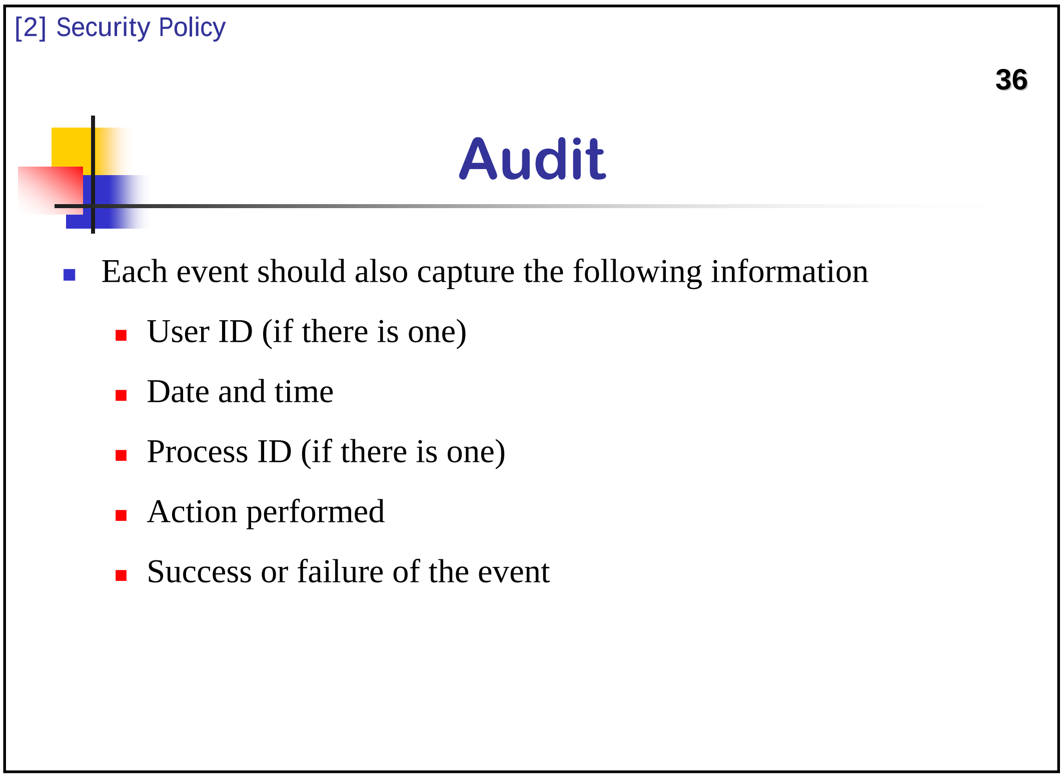


[2] Security Policy

35

Audit

- The audit section of the security policy should define the types of events to be audited on all systems.
- Normally, security policies require the following to be audited:
  - Logins (successful and failed)
  - Logouts
  - Failed access to files or system objects
  - Remote access (successful and failed)
  - Privileged actions (by administrators; successes and failures)
  - System events (such as shutdowns and reboots)

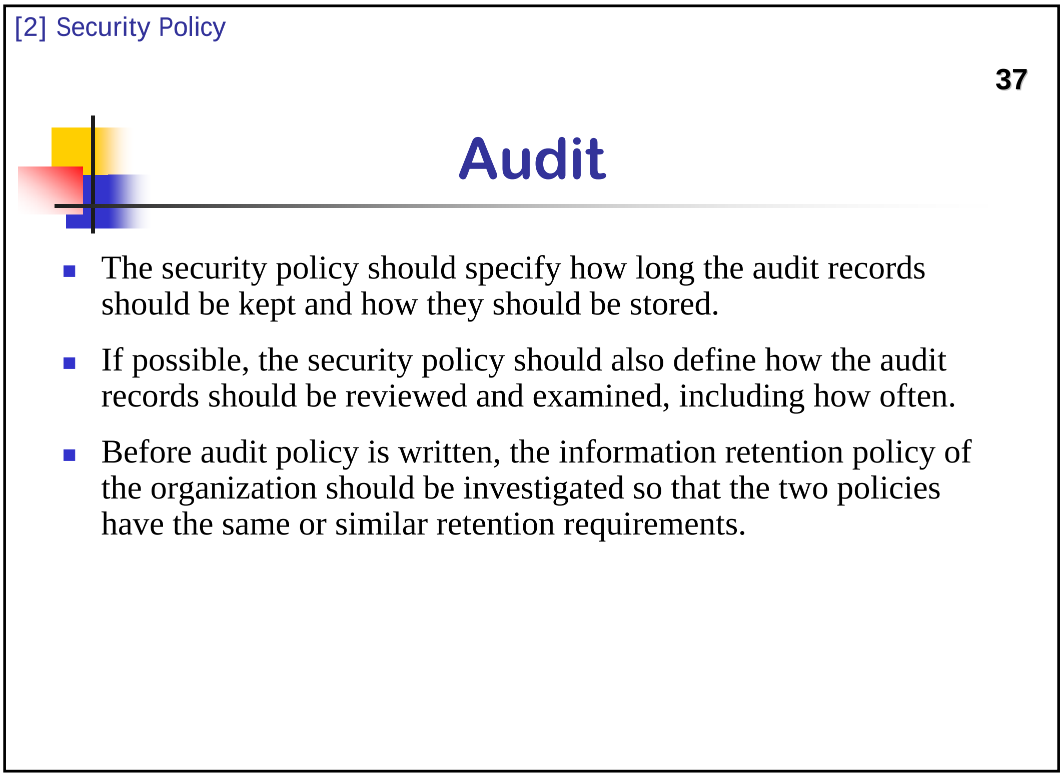


[2] Security Policy

36

Audit

- Each event should also capture the following information
  - User ID (if there is one)
  - Date and time
  - Process ID (if there is one)
  - Action performed
  - Success or failure of the event

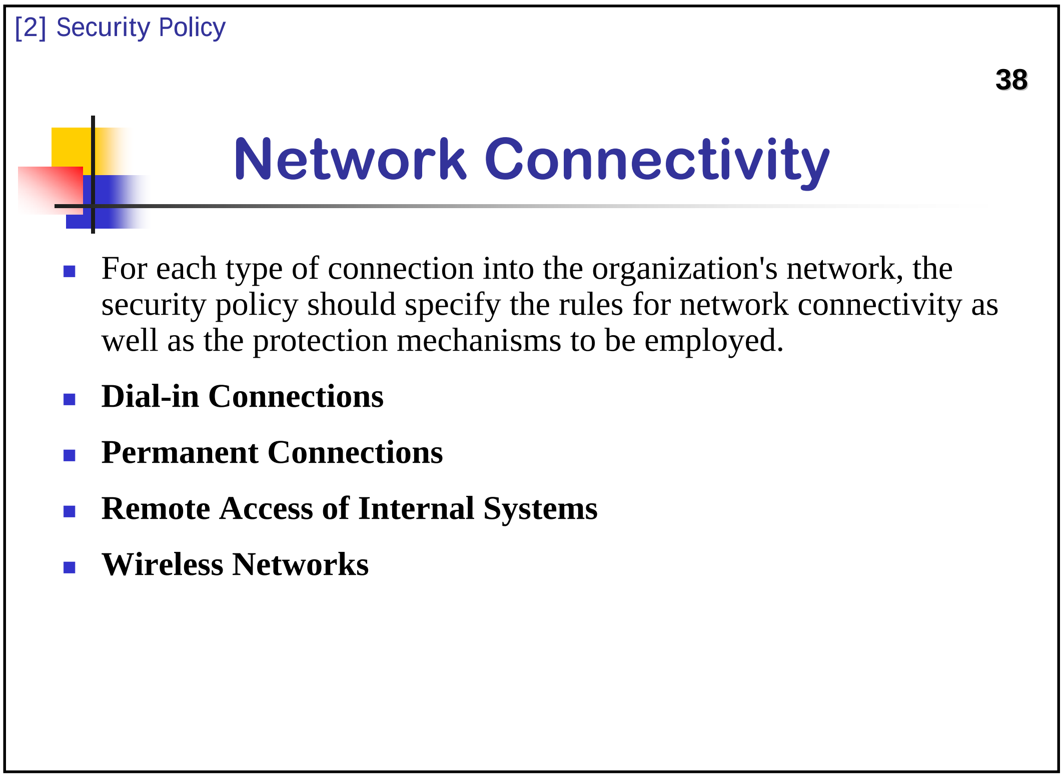


[2] Security Policy

37

Audit

- The security policy should specify how long the audit records should be kept and how they should be stored.
- If possible, the security policy should also define how the audit records should be reviewed and examined, including how often.
- Before audit policy is written, the information retention policy of the organization should be investigated so that the two policies have the same or similar retention requirements.

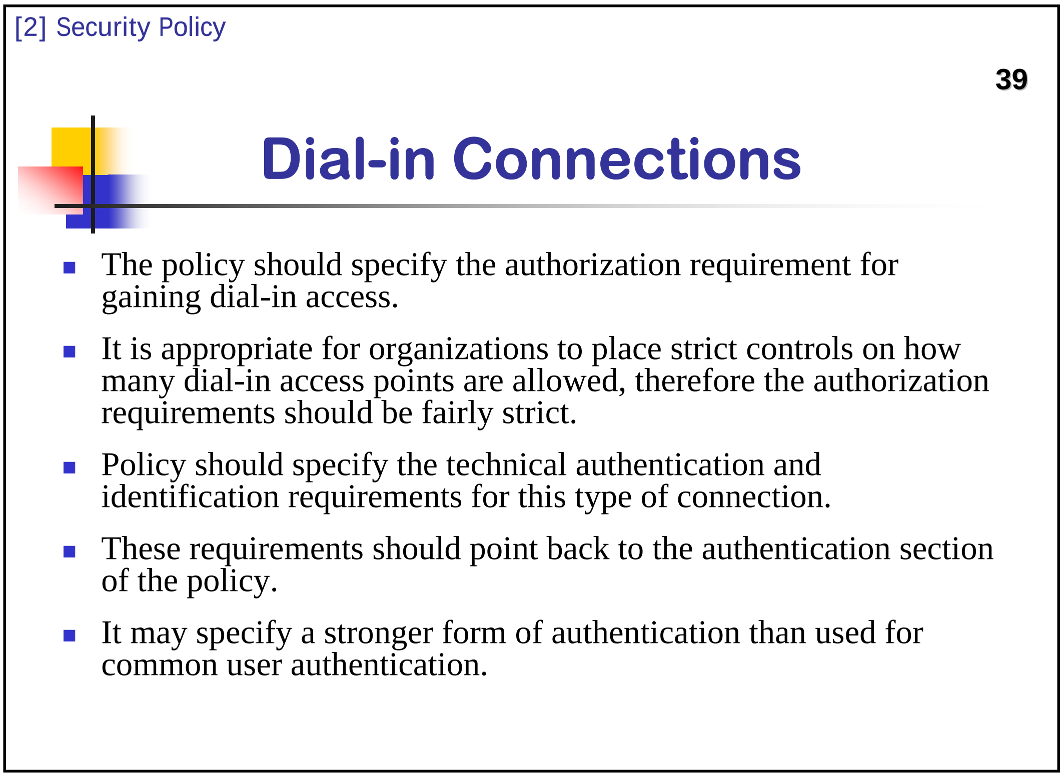


[2] Security Policy

38

Network Connectivity

- For each type of connection into the organization's network, the security policy should specify the rules for network connectivity as well as the protection mechanisms to be employed.
- **Dial-in Connections**
- **Permanent Connections**
- **Remote Access of Internal Systems**
- **Wireless Networks**

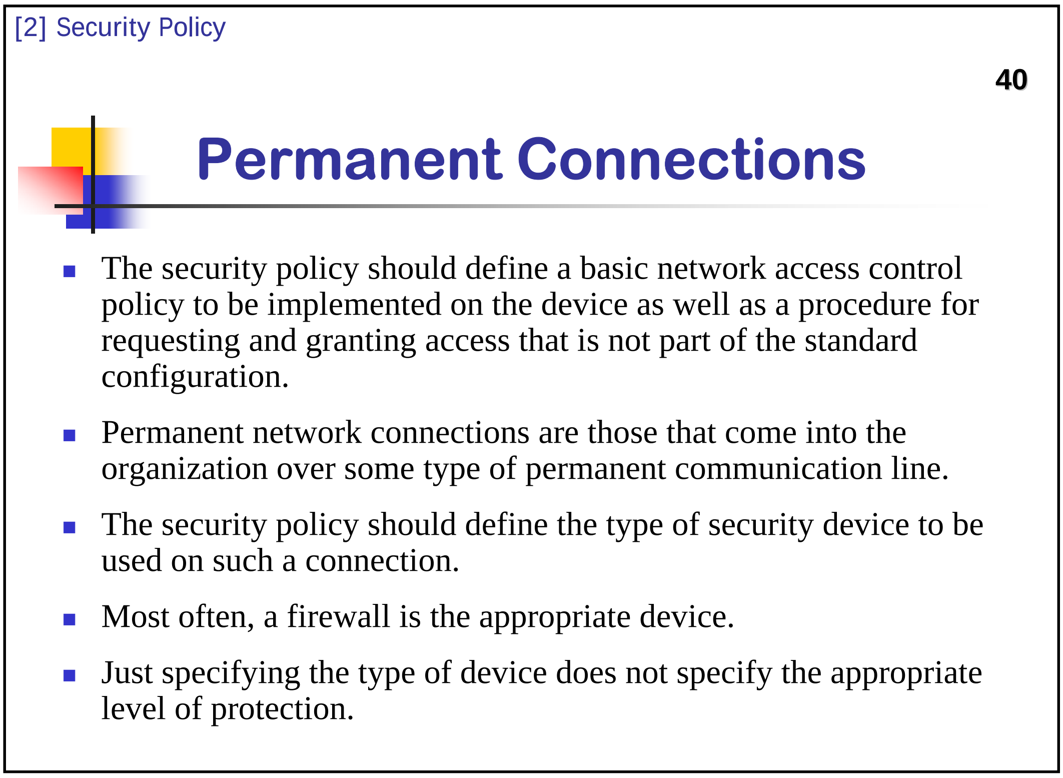


[2] Security Policy

39

Dial-in Connections

- The policy should specify the authorization requirement for gaining dial-in access.
- It is appropriate for organizations to place strict controls on how many dial-in access points are allowed, therefore the authorization requirements should be fairly strict.
- Policy should specify the technical authentication and identification requirements for this type of connection.
- These requirements should point back to the authentication section of the policy.
- It may specify a stronger form of authentication than used for common user authentication.

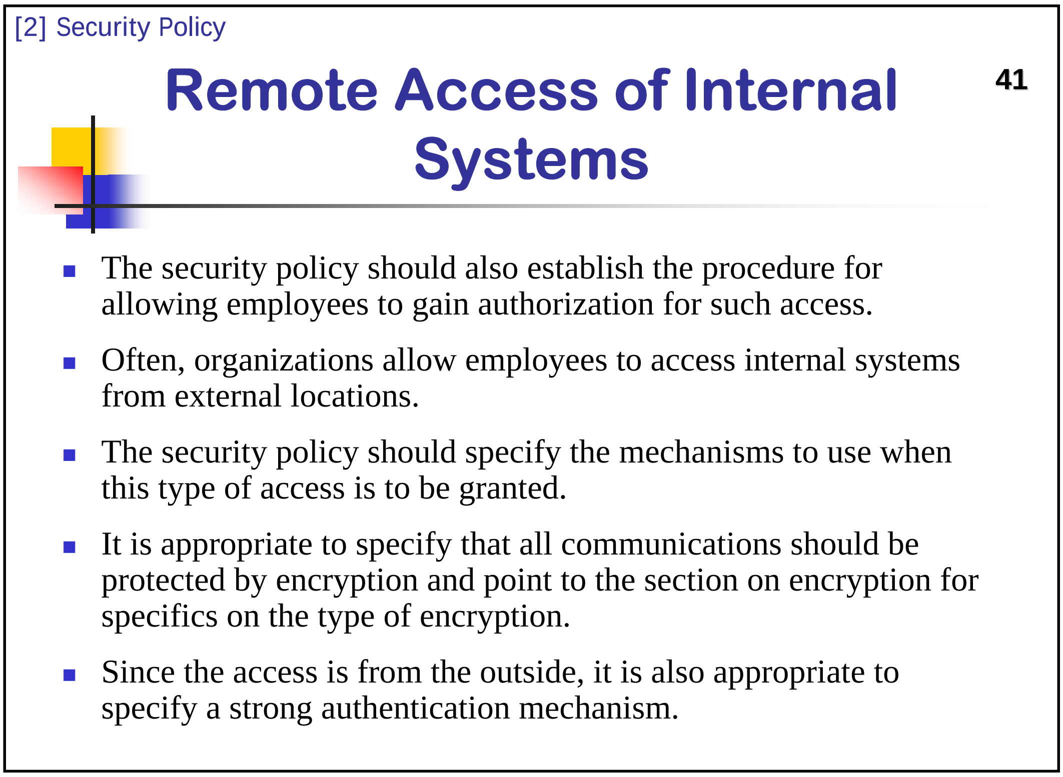


[2] Security Policy

40

Permanent Connections

- The security policy should define a basic network access control policy to be implemented on the device as well as a procedure for requesting and granting access that is not part of the standard configuration.
- Permanent network connections are those that come into the organization over some type of permanent communication line.
- The security policy should define the type of security device to be used on such a connection.
- Most often, a firewall is the appropriate device.
- Just specifying the type of device does not specify the appropriate level of protection.

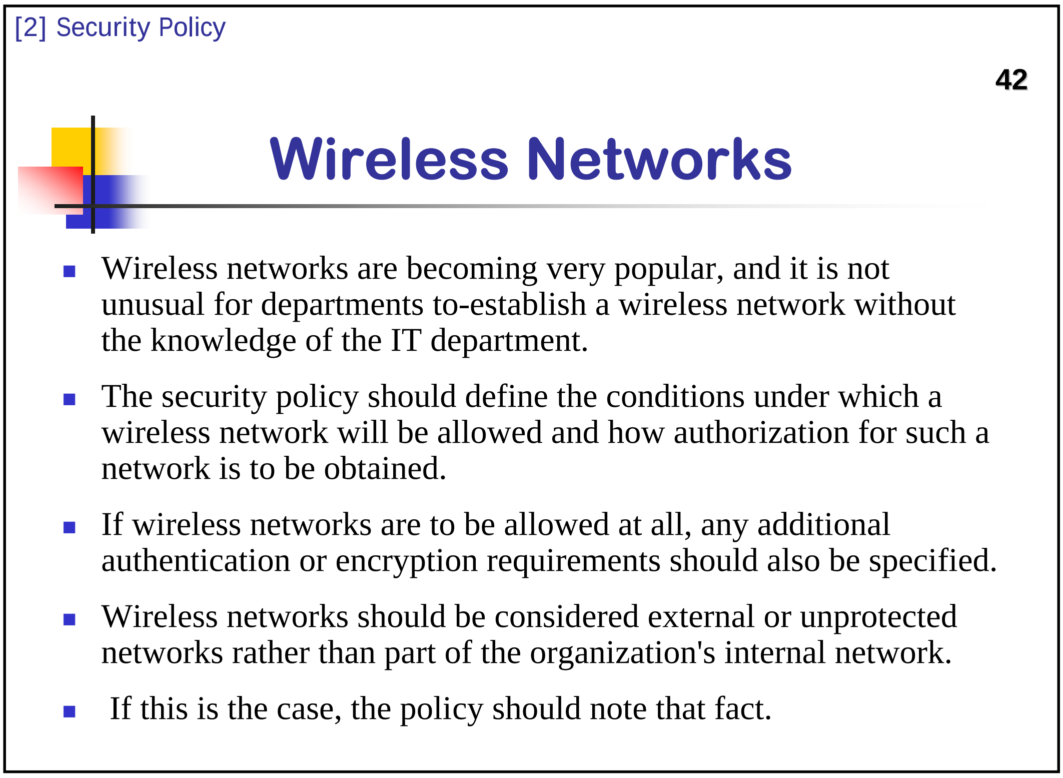


[2] Security Policy

41

Remote Access of Internal Systems

- The security policy should also establish the procedure for allowing employees to gain authorization for such access.
- Often, organizations allow employees to access internal systems from external locations.
- The security policy should specify the mechanisms to use when this type of access is to be granted.
- It is appropriate to specify that all communications should be protected by encryption and point to the section on encryption for specifics on the type of encryption.
- Since the access is from the outside, it is also appropriate to specify a strong authentication mechanism.

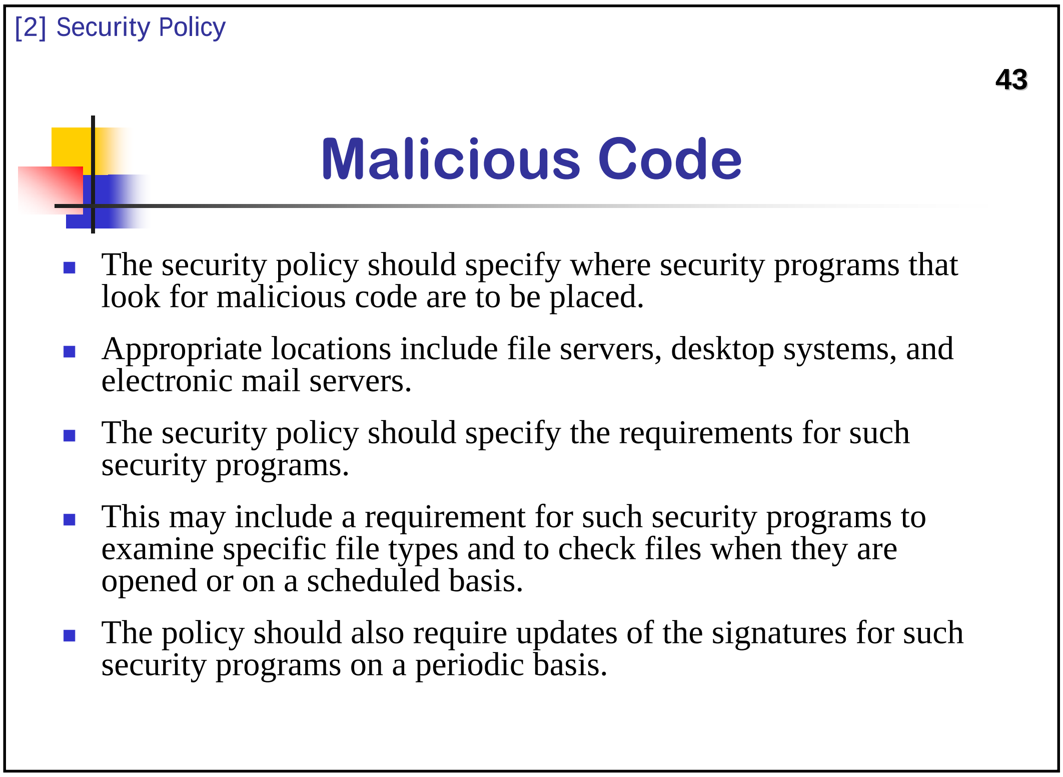


[2] Security Policy

42

Wireless Networks

- Wireless networks are becoming very popular, and it is not unusual for departments to-establish a wireless network without the knowledge of the IT department.
- The security policy should define the conditions under which a wireless network will be allowed and how authorization for such a network is to be obtained.
- If wireless networks are to be allowed at all, any additional authentication or encryption requirements should also be specified.
- Wireless networks should be considered external or unprotected networks rather than part of the organization's internal network.
- If this is the case, the policy should note that fact.

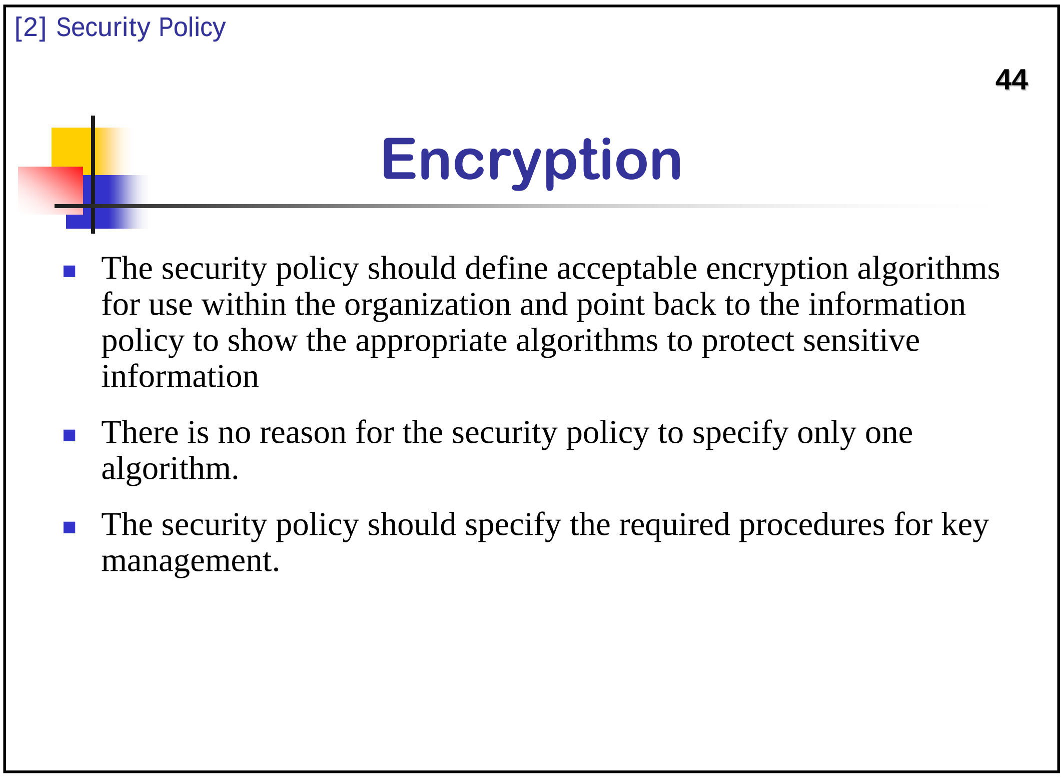


[2] Security Policy

43

Malicious Code

- The security policy should specify where security programs that look for malicious code are to be placed.
- Appropriate locations include file servers, desktop systems, and electronic mail servers.
- The security policy should specify the requirements for such security programs.
- This may include a requirement for such security programs to examine specific file types and to check files when they are opened or on a scheduled basis.
- The policy should also require updates of the signatures for such security programs on a periodic basis.

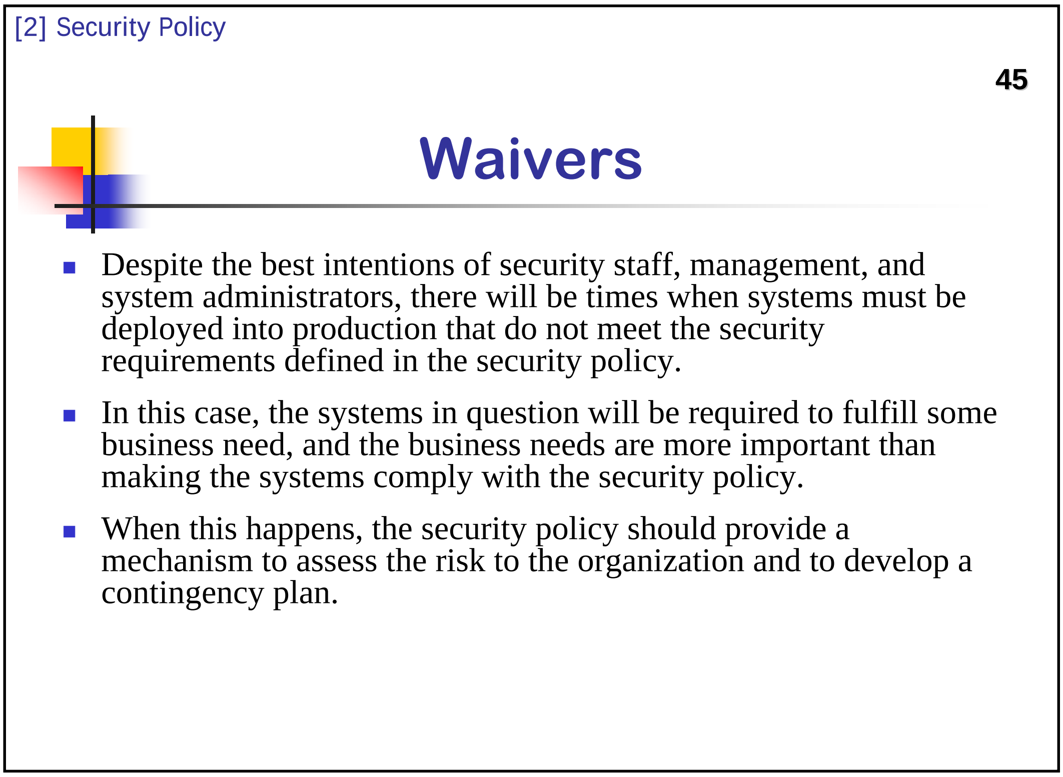


[2] Security Policy

44

Encryption

- The security policy should define acceptable encryption algorithms for use within the organization and point back to the information policy to show the appropriate algorithms to protect sensitive information
- There is no reason for the security policy to specify only one algorithm.
- The security policy should specify the required procedures for key management.

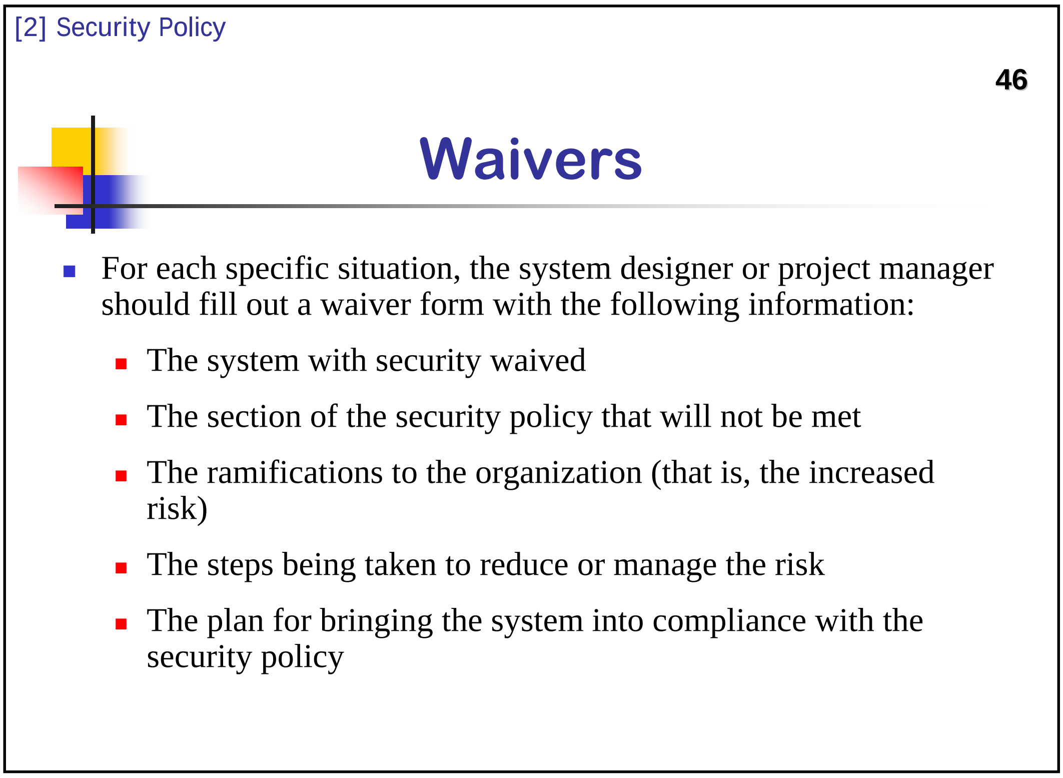


[2] Security Policy

45

Waivers

- Despite the best intentions of security staff, management, and system administrators, there will be times when systems must be deployed into production that do not meet the security requirements defined in the security policy.
- In this case, the systems in question will be required to fulfill some business need, and the business needs are more important than making the systems comply with the security policy.
- When this happens, the security policy should provide a mechanism to assess the risk to the organization and to develop a contingency plan.

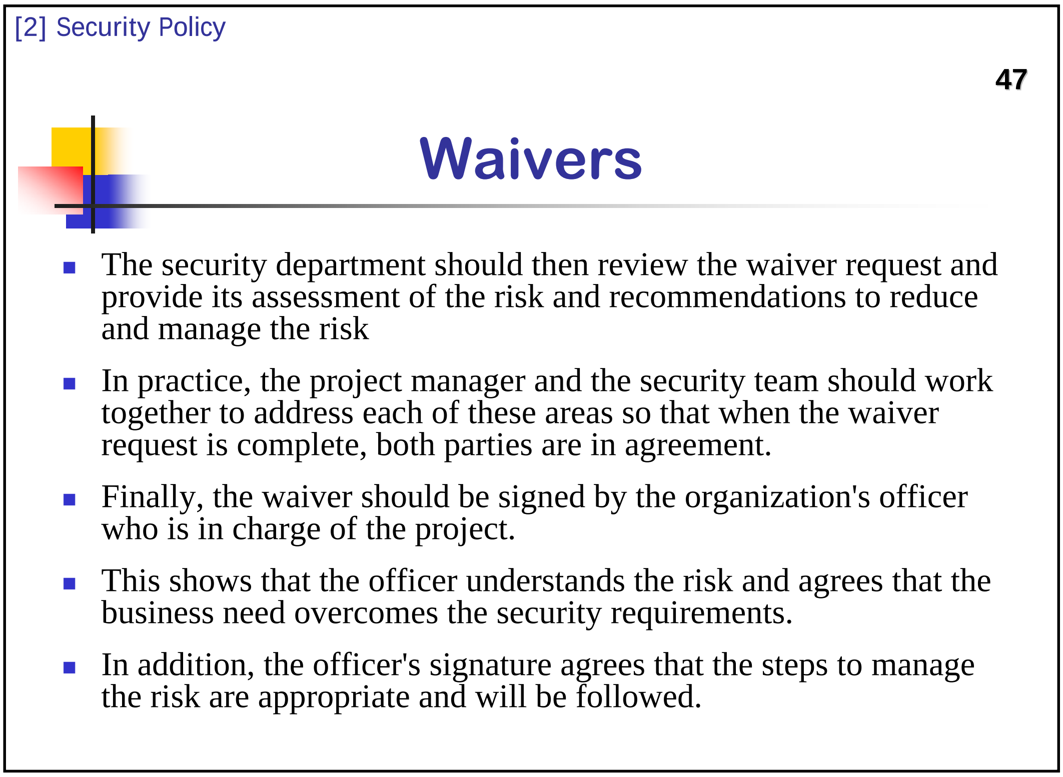


[2] Security Policy

46

Waivers

- For each specific situation, the system designer or project manager should fill out a waiver form with the following information:
  - The system with security waived
  - The section of the security policy that will not be met
  - The ramifications to the organization (that is, the increased risk)
  - The steps being taken to reduce or manage the risk
  - The plan for bringing the system into compliance with the security policy

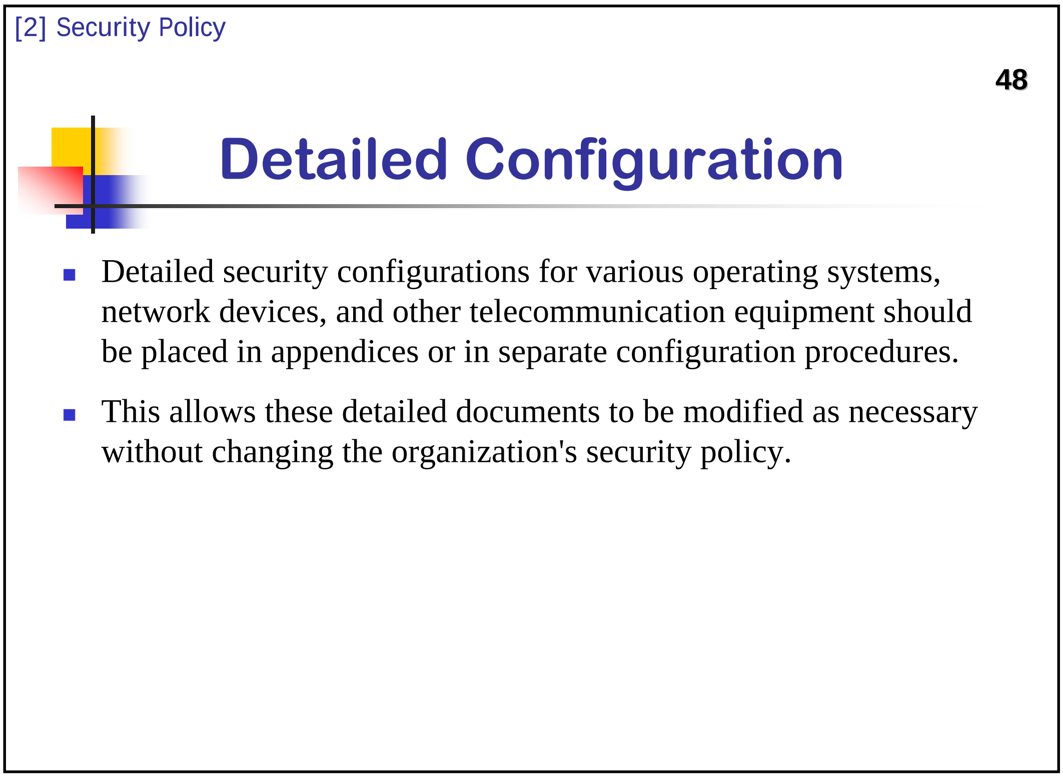


[2] Security Policy

47

Waivers

- The security department should then review the waiver request and provide its assessment of the risk and recommendations to reduce and manage the risk
- In practice, the project manager and the security team should work together to address each of these areas so that when the waiver request is complete, both parties are in agreement.
- Finally, the waiver should be signed by the organization's officer who is in charge of the project.
- This shows that the officer understands the risk and agrees that the business need overcomes the security requirements.
- In addition, the officer's signature agrees that the steps to manage the risk are appropriate and will be followed.



[2] Security Policy

48

Detailed Configuration

- Detailed security configurations for various operating systems, network devices, and other telecommunication equipment should be placed in appendices or in separate configuration procedures.
- This allows these detailed documents to be modified as necessary without changing the organization's security policy.

49

[3] Computer Use Policy

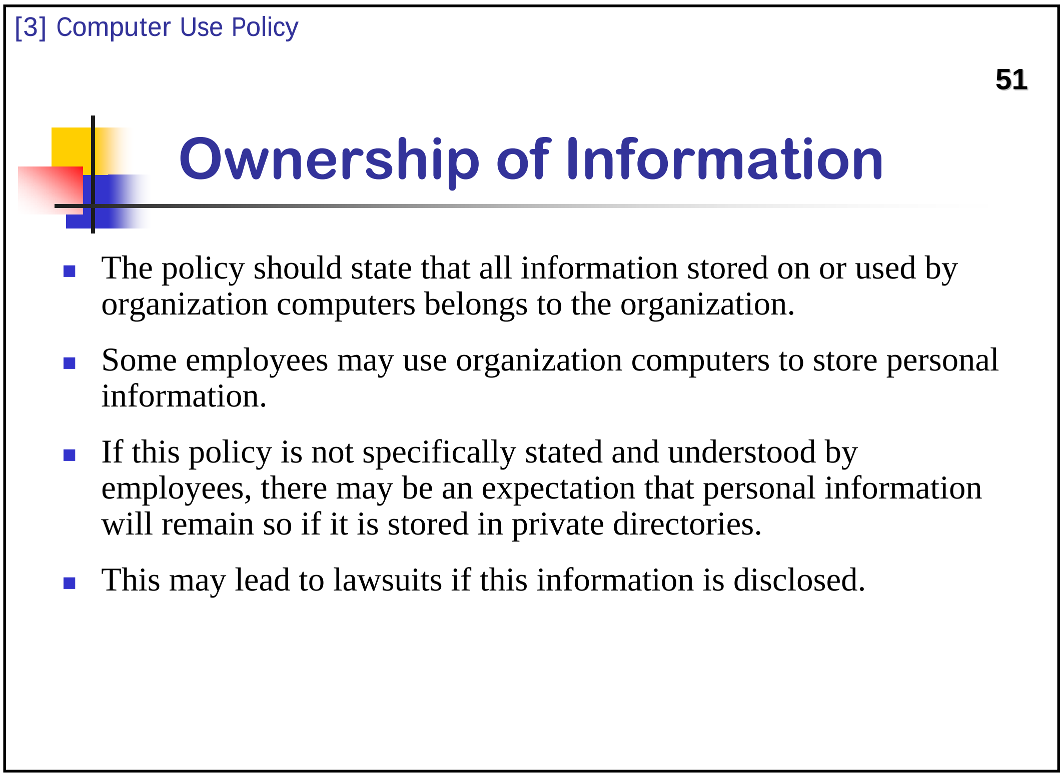
- The computer use policy lays out the law when it comes to who may use computer systems and how they may be used.
- Much of the information in this policy seems like common sense but if the organization does not specifically define a policy of computer ownership and use, the organization leaves itself open to lawsuits from employees.

[3] Computer Use Policy

50

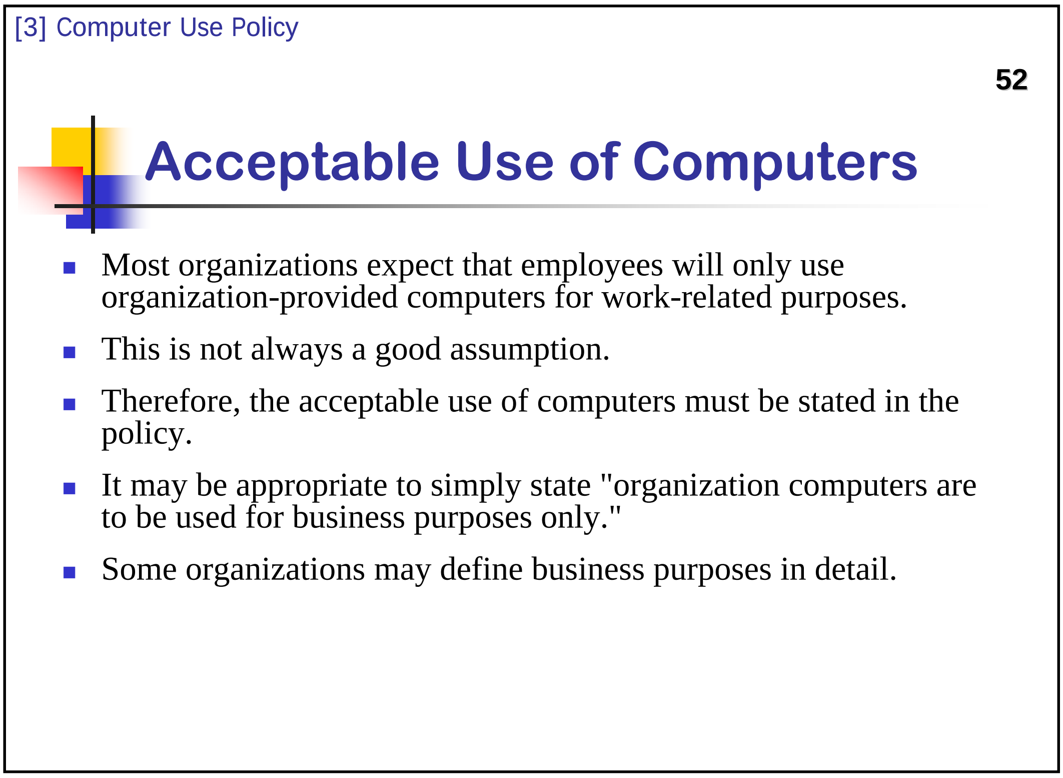
Ownership of Computers

- The policy should clearly state that all computers are owned by the organization and that they are provided to employees for use in accordance with their jobs within the organization.
- The policy may also prohibit the use of non-organization computers for organization business.
- For example, if employees are expected to perform some work at home, the organization will provide a suitable computer.
- It may also be appropriate to state that only organization-provided computers can be used to connect to the organization's internal computer systems via a remote access system



Ownership of Information

- The policy should state that all information stored on or used by organization computers belongs to the organization.
- Some employees may use organization computers to store personal information.
- If this policy is not specifically stated and understood by employees, there may be an expectation that personal information will remain so if it is stored in private directories.
- This may lead to lawsuits if this information is disclosed.



Acceptable Use of Computers

- Most organizations expect that employees will only use organization-provided computers for work-related purposes.
- This is not always a good assumption.
- Therefore, the acceptable use of computers must be stated in the policy.
- It may be appropriate to simply state "organization computers are to be used for business purposes only."
- Some organizations may define business purposes in detail.

[3] Computer Use Policy

53

Acceptable Use of Computers

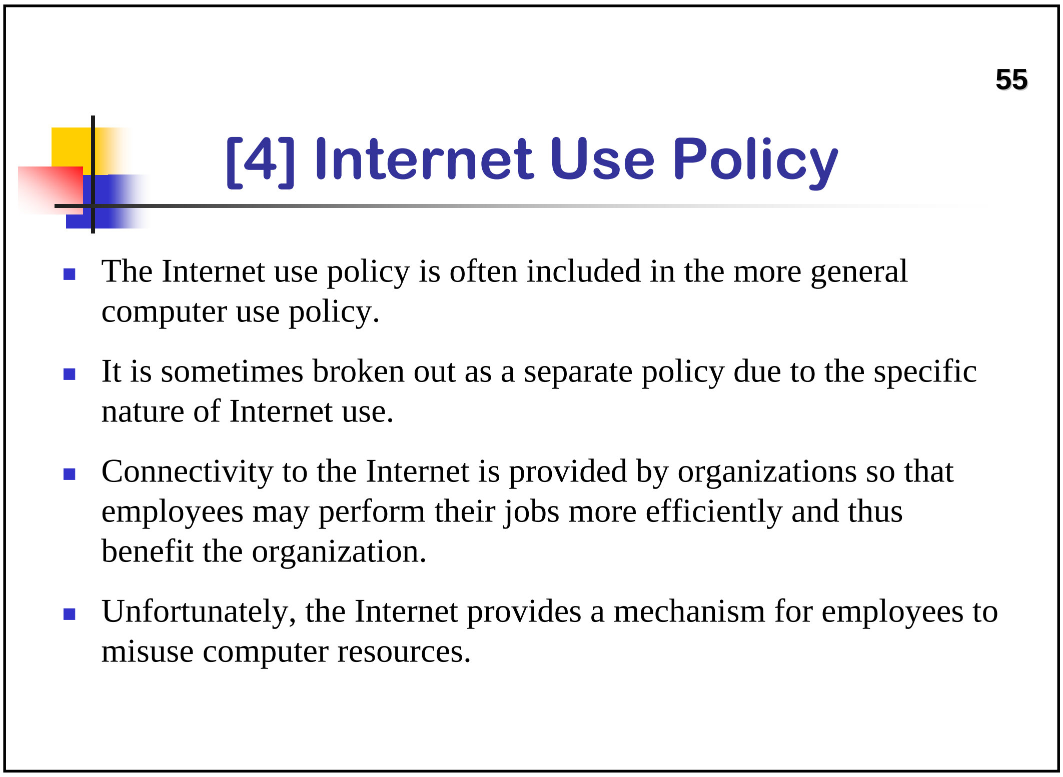
- Occasionally, organizations allow employees to use organization computers for other purposes.
- For example, an organization may allow employees to play games across the internal network at night. If this is to be allowed, it should be stated clearly in the policy.
- The use of the computers provided by the organization will also impact what software is loaded on the systems.
- It may be appropriate for the organization to state that no unauthorized software may be loaded on the computer systems.
- The policy should then define how software becomes authorized and who may load authorized software.

[3] Computer Use Policy

54

No Expectation of Privacy

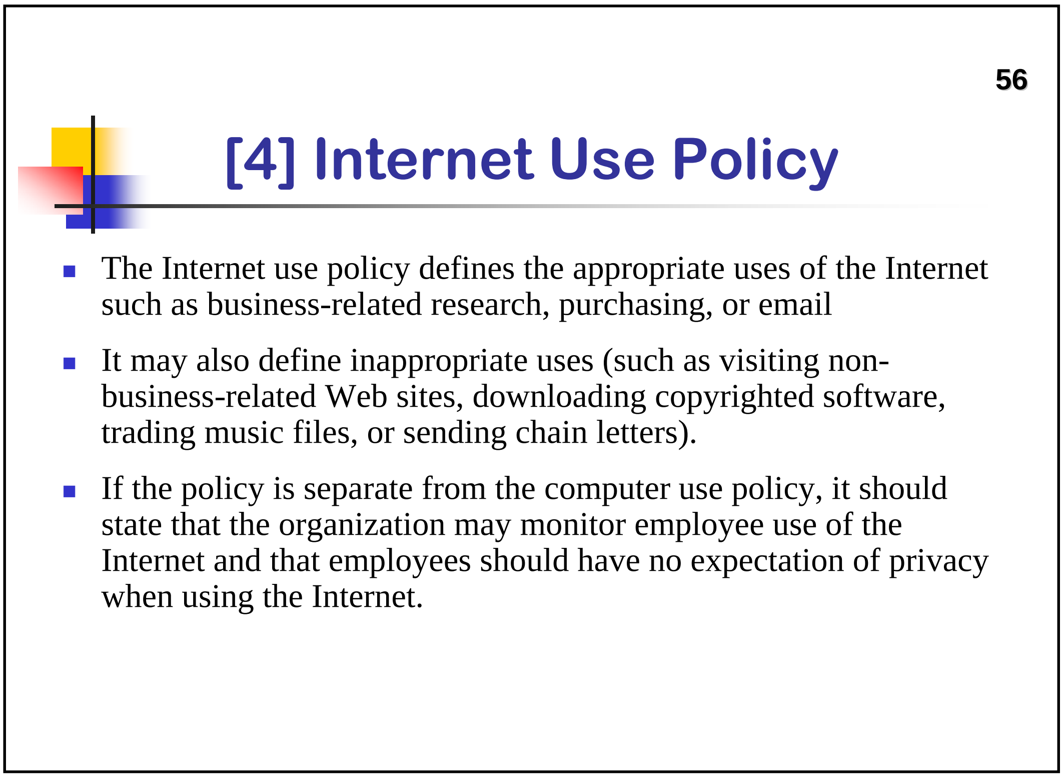
- Perhaps the most important part of the computer use policy is the statement that the employee should have no expectation of privacy for any information stored, sent, or received on any organization computers.
- It is very important for the employee to understand that any information, including electronic mail, may be examined by administrators.
- Also, the employee should understand that administrators or security staff may monitor all computer-related activities, including the visiting of Web sites.



55

[4] Internet Use Policy

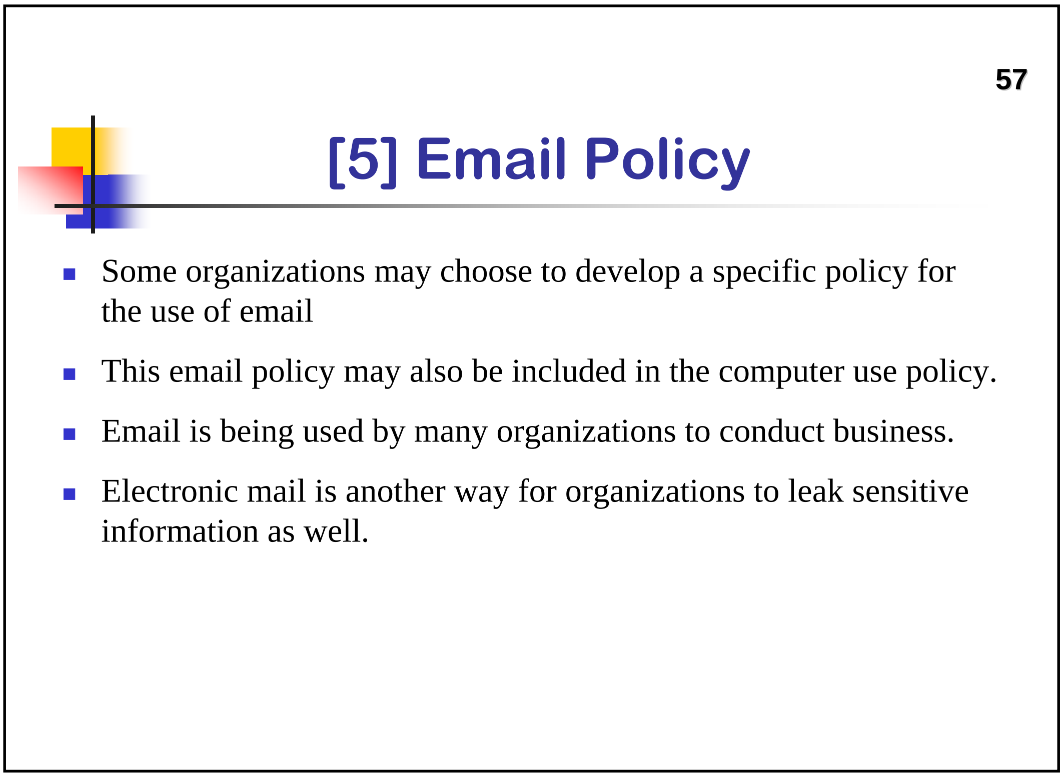
- The Internet use policy is often included in the more general computer use policy.
- It is sometimes broken out as a separate policy due to the specific nature of Internet use.
- Connectivity to the Internet is provided by organizations so that employees may perform their jobs more efficiently and thus benefit the organization.
- Unfortunately, the Internet provides a mechanism for employees to misuse computer resources.



56

[4] Internet Use Policy

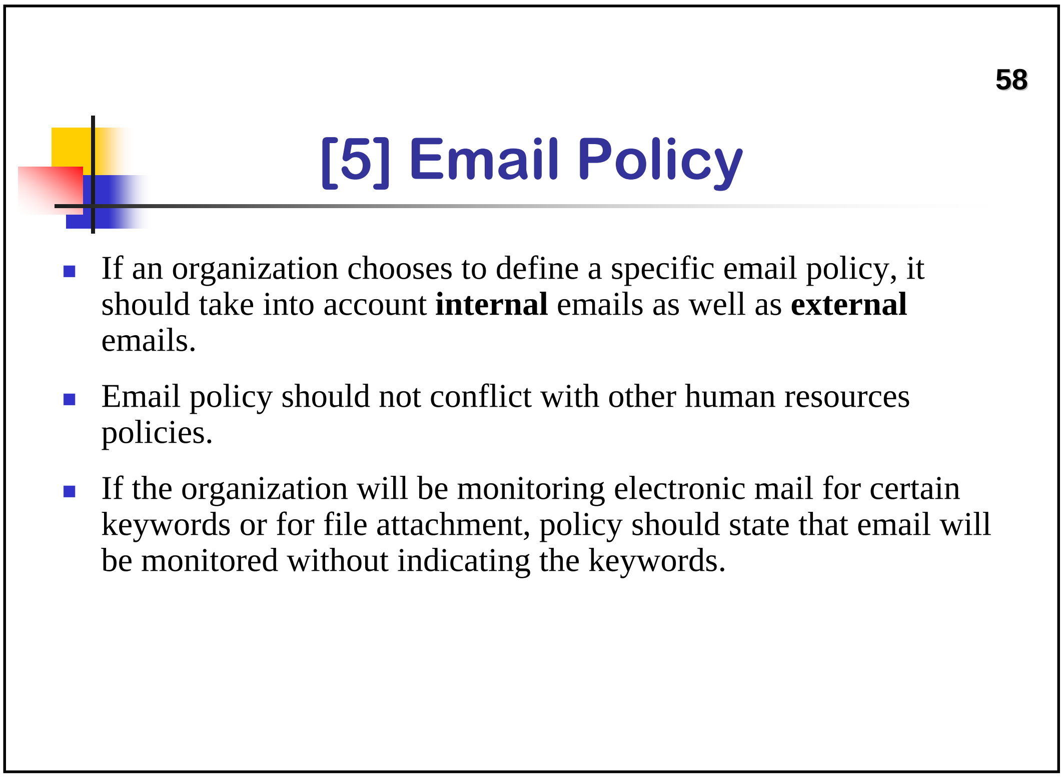
- The Internet use policy defines the appropriate uses of the Internet such as business-related research, purchasing, or email
- It may also define inappropriate uses (such as visiting non-business-related Web sites, downloading copyrighted software, trading music files, or sending chain letters).
- If the policy is separate from the computer use policy, it should state that the organization may monitor employee use of the Internet and that employees should have no expectation of privacy when using the Internet.



57

[5] Email Policy

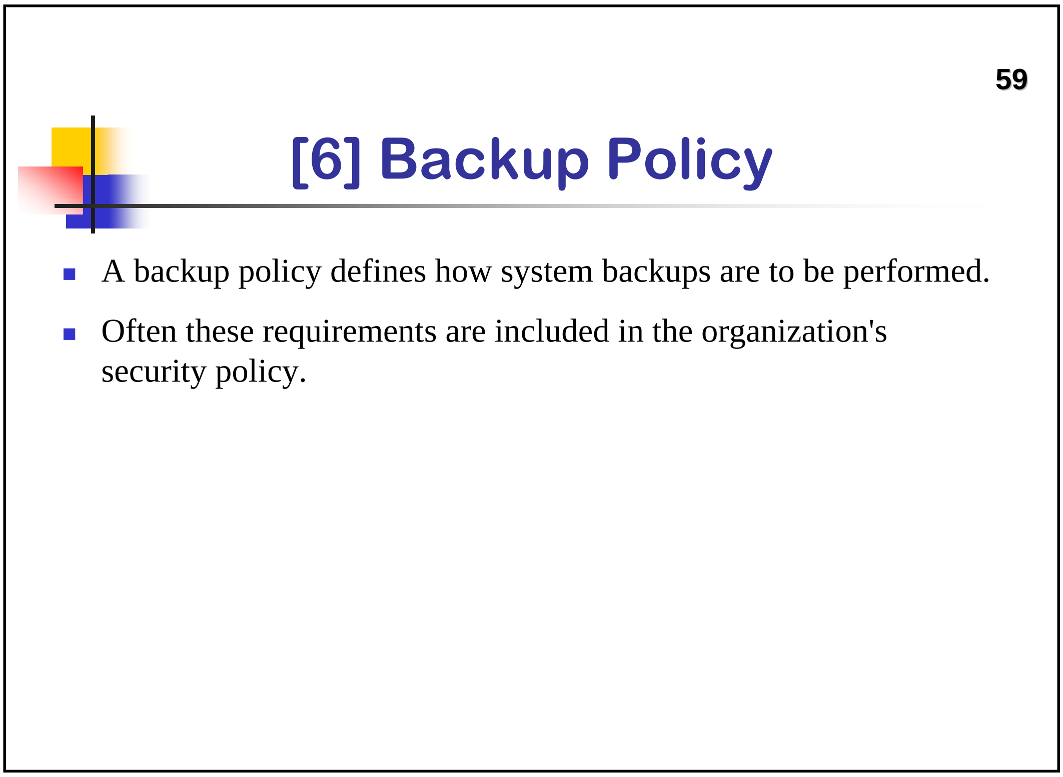
- Some organizations may choose to develop a specific policy for the use of email
- This email policy may also be included in the computer use policy.
- Email is being used by many organizations to conduct business.
- Electronic mail is another way for organizations to leak sensitive information as well.



58

[5] Email Policy

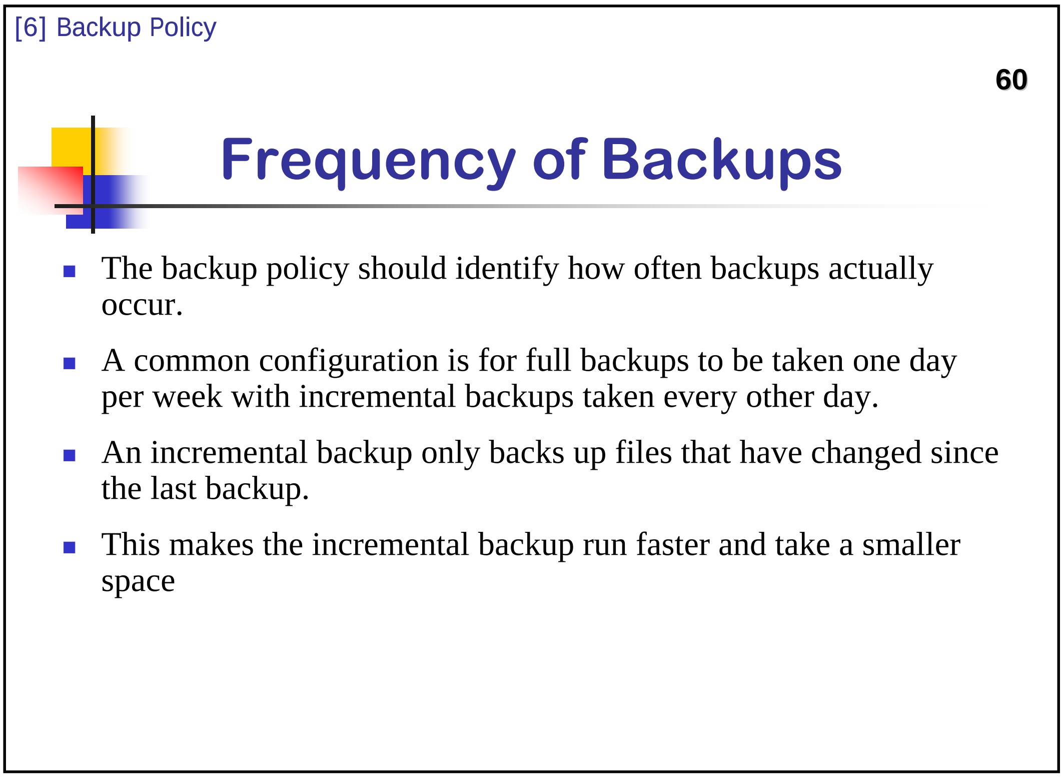
- If an organization chooses to define a specific email policy, it should take into account **internal** emails as well as **external** emails.
- Email policy should not conflict with other human resources policies.
- If the organization will be monitoring electronic mail for certain keywords or for file attachment, policy should state that email will be monitored without indicating the keywords.



59

[6] Backup Policy

- A backup policy defines how system backups are to be performed.
- Often these requirements are included in the organization's security policy.

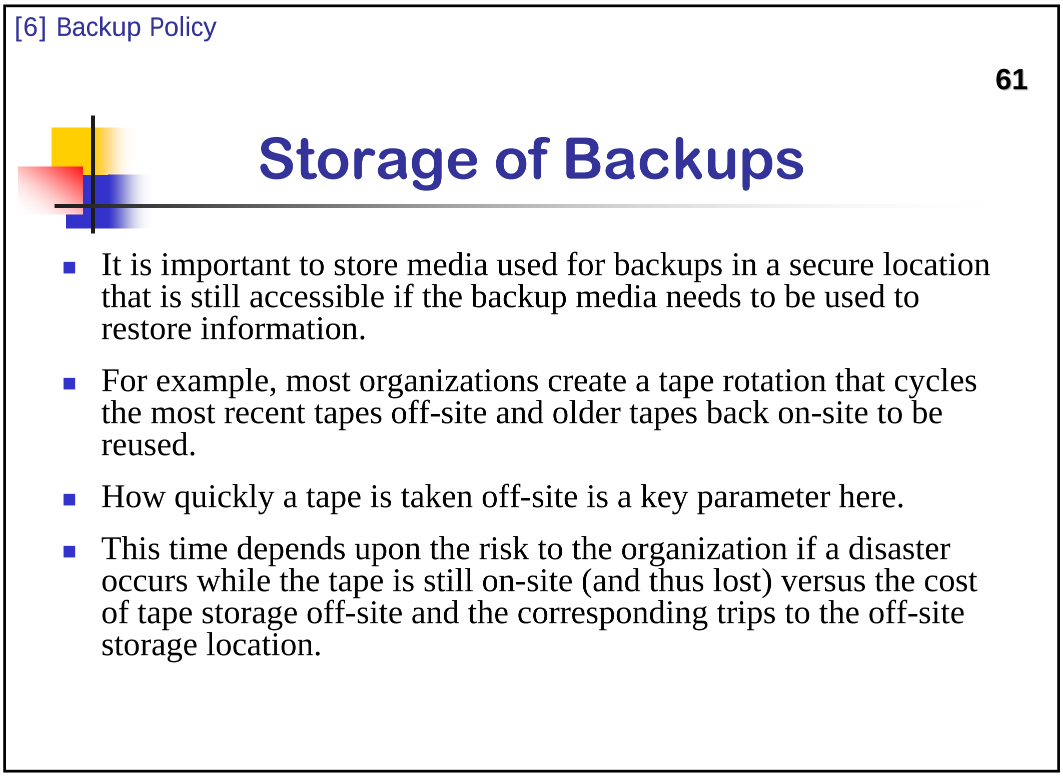


[6] Backup Policy

60

Frequency of Backups

- The backup policy should identify how often backups actually occur.
- A common configuration is for full backups to be taken one day per week with incremental backups taken every other day.
- An incremental backup only backs up files that have changed since the last backup.
- This makes the incremental backup run faster and take a smaller space

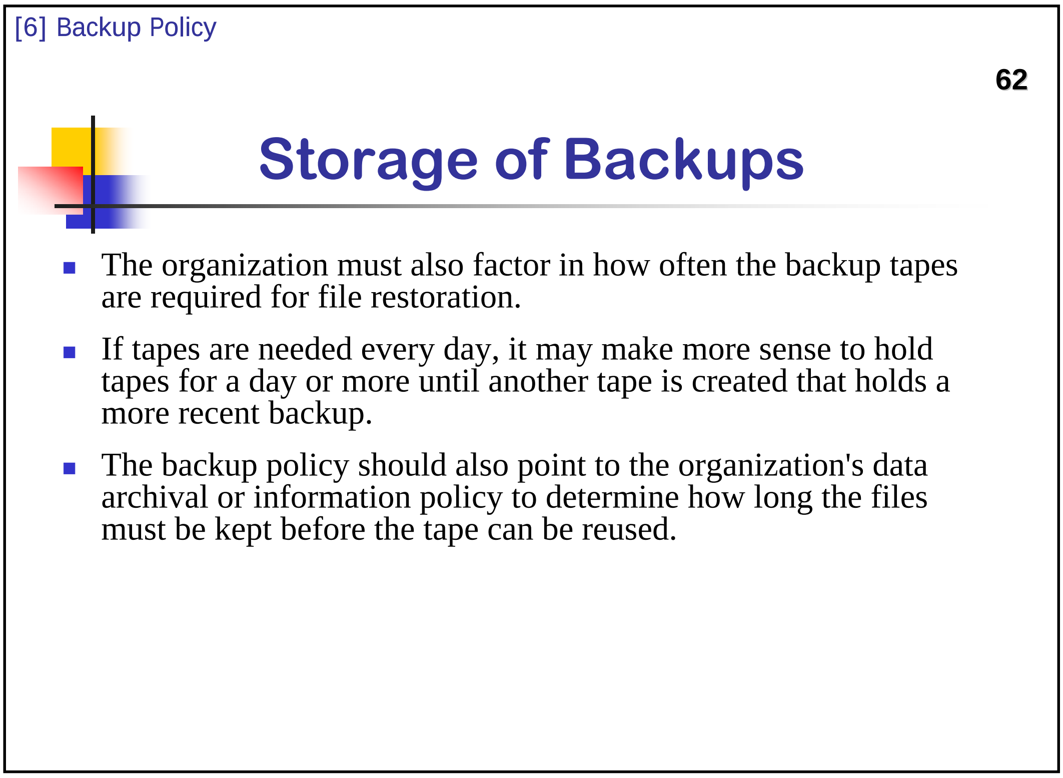


[6] Backup Policy

61

Storage of Backups

- It is important to store media used for backups in a secure location that is still accessible if the backup media needs to be used to restore information.
- For example, most organizations create a tape rotation that cycles the most recent tapes off-site and older tapes back on-site to be reused.
- How quickly a tape is taken off-site is a key parameter here.
- This time depends upon the risk to the organization if a disaster occurs while the tape is still on-site (and thus lost) versus the cost of tape storage off-site and the corresponding trips to the off-site storage location.

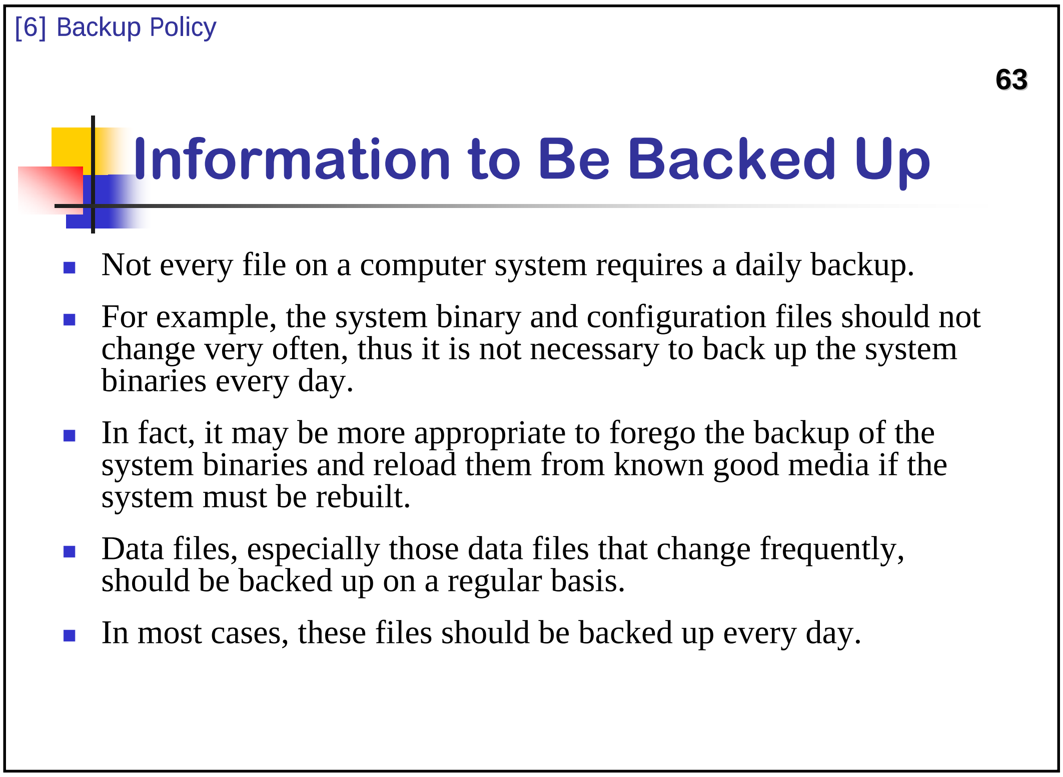


[6] Backup Policy

62

Storage of Backups

- The organization must also factor in how often the backup tapes are required for file restoration.
- If tapes are needed every day, it may make more sense to hold tapes for a day or more until another tape is created that holds a more recent backup.
- The backup policy should also point to the organization's data archival or information policy to determine how long the files must be kept before the tape can be reused.

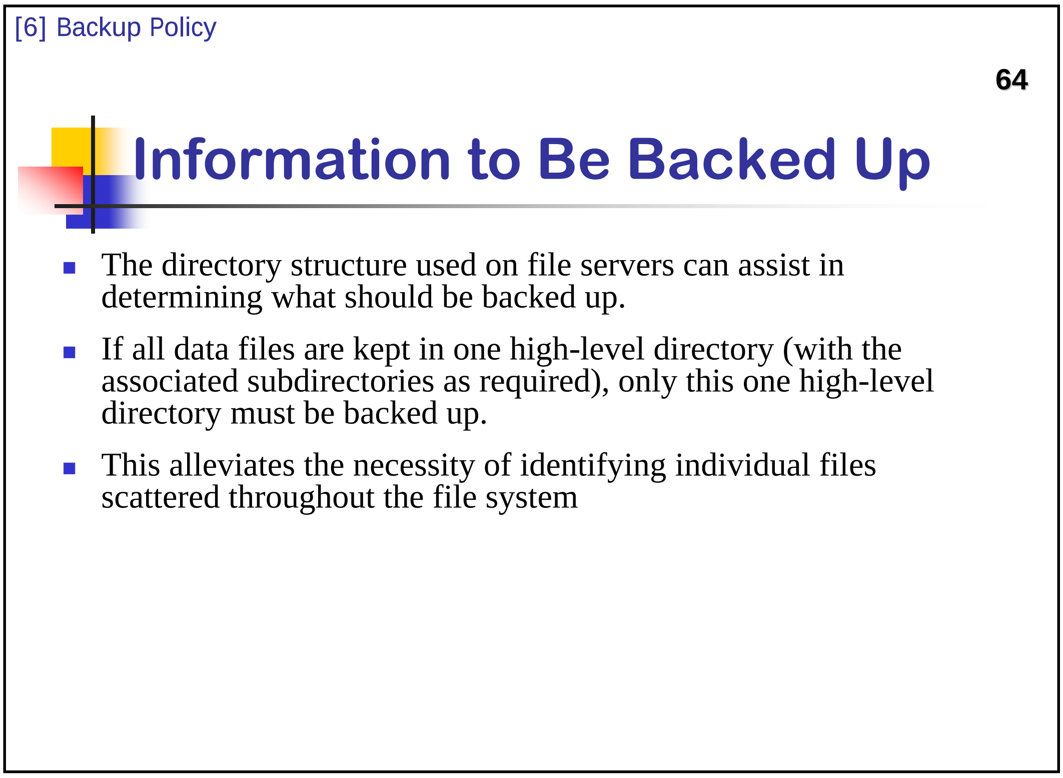


[6] Backup Policy

63

Information to Be Backed Up

- Not every file on a computer system requires a daily backup.
- For example, the system binary and configuration files should not change very often, thus it is not necessary to back up the system binaries every day.
- In fact, it may be more appropriate to forego the backup of the system binaries and reload them from known good media if the system must be rebuilt.
- Data files, especially those data files that change frequently, should be backed up on a regular basis.
- In most cases, these files should be backed up every day.



[6] Backup Policy

64

Information to Be Backed Up

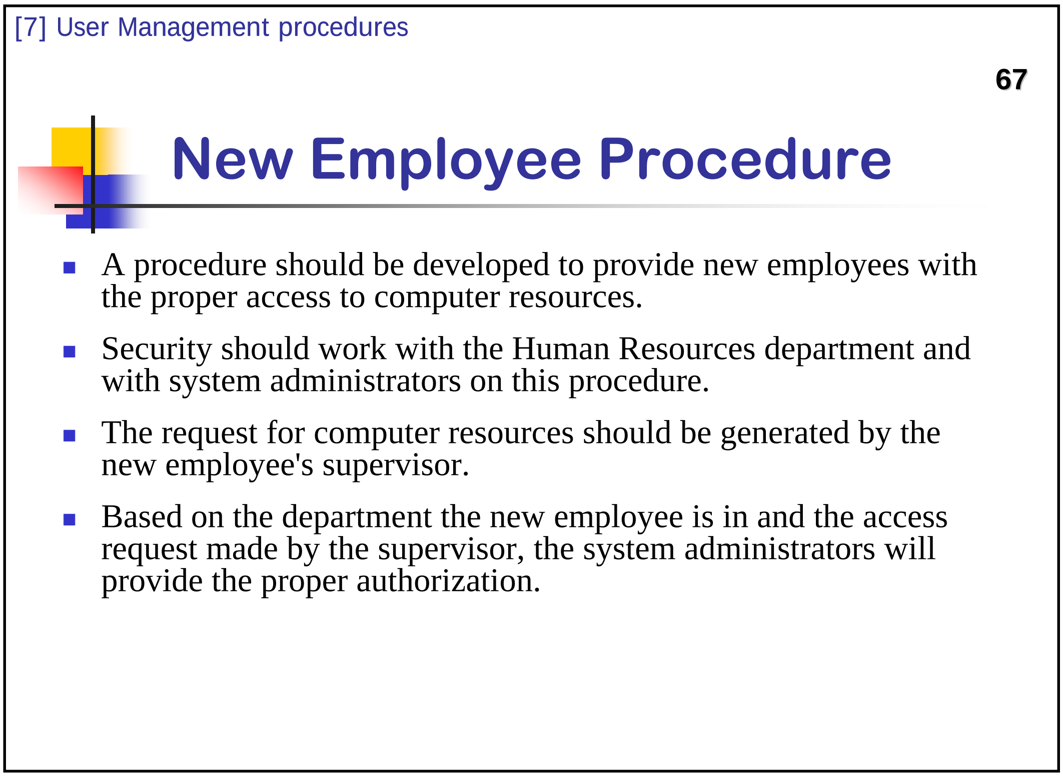
- The directory structure used on file servers can assist in determining what should be backed up.
- If all data files are kept in one high-level directory (with the associated subdirectories as required), only this one high-level directory must be backed up.
- This alleviates the necessity of identifying individual files scattered throughout the file system

Backup testing

- Periodic restore testing should be mentioned in the backup policy.
- Backups may run fine with no errors, but when a file needs to be restored, errors are found or the file is unreadable for some reason.
- If the backup media is periodically tested you will be more likely to find these types of problems before they affect your organization.

[7] User Management procedures

- User management procedures are the security procedures that are most overlooked by organizations and yet provide the potential for the greatest risk.
- Security mechanisms to protect systems from unauthorized individuals can be rendered completely useless if the users of computer systems are not properly managed.

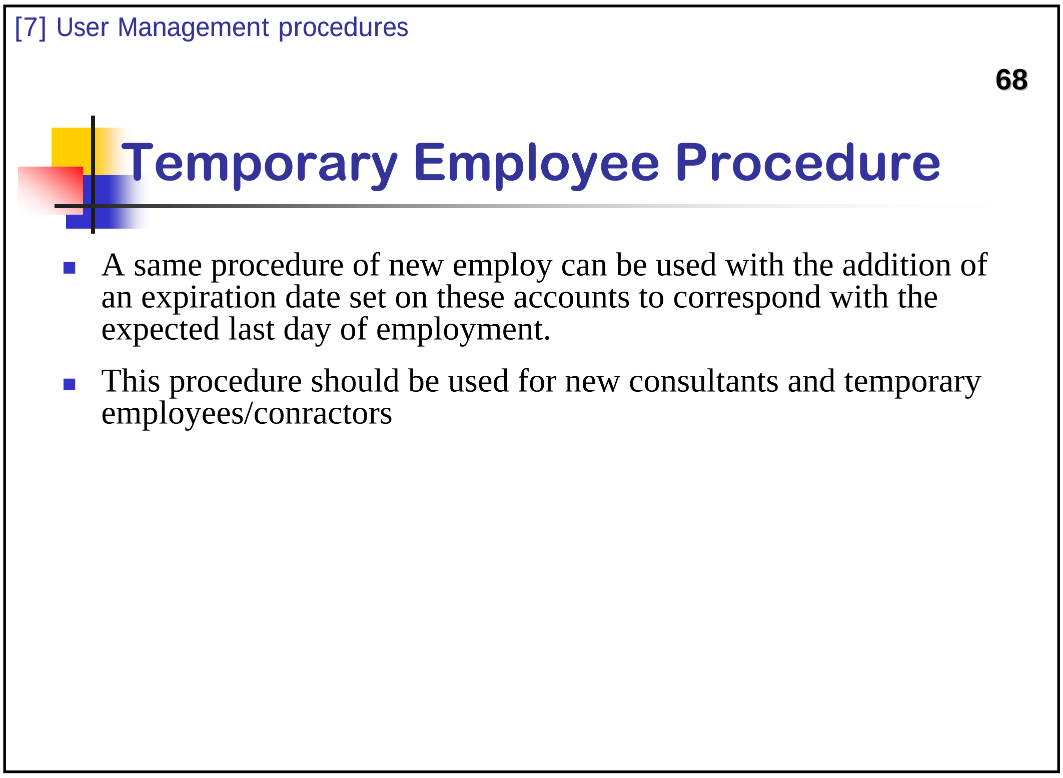


[7] User Management procedures

67

New Employee Procedure

- A procedure should be developed to provide new employees with the proper access to computer resources.
- Security should work with the Human Resources department and with system administrators on this procedure.
- The request for computer resources should be generated by the new employee's supervisor.
- Based on the department the new employee is in and the access request made by the supervisor, the system administrators will provide the proper authorization.

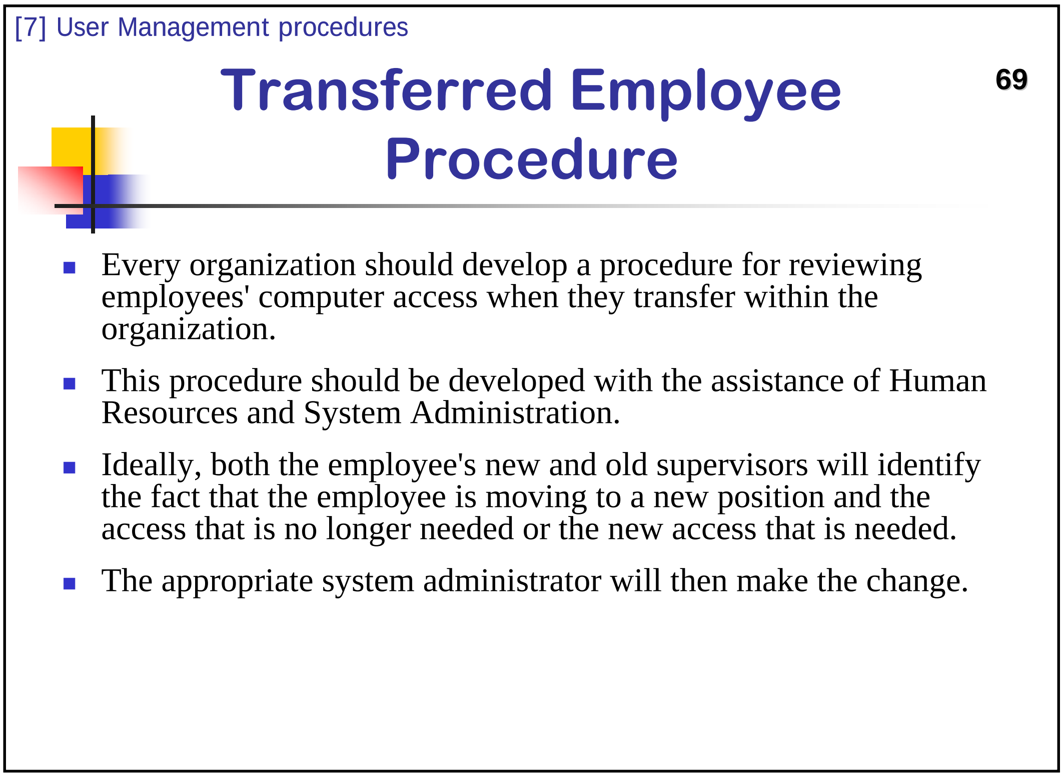


[7] User Management procedures

68

Temporary Employee Procedure

- A same procedure of new employ can be used with the addition of an expiration date set on these accounts to correspond with the expected last day of employment.
- This procedure should be used for new consultants and temporary employees/conractors

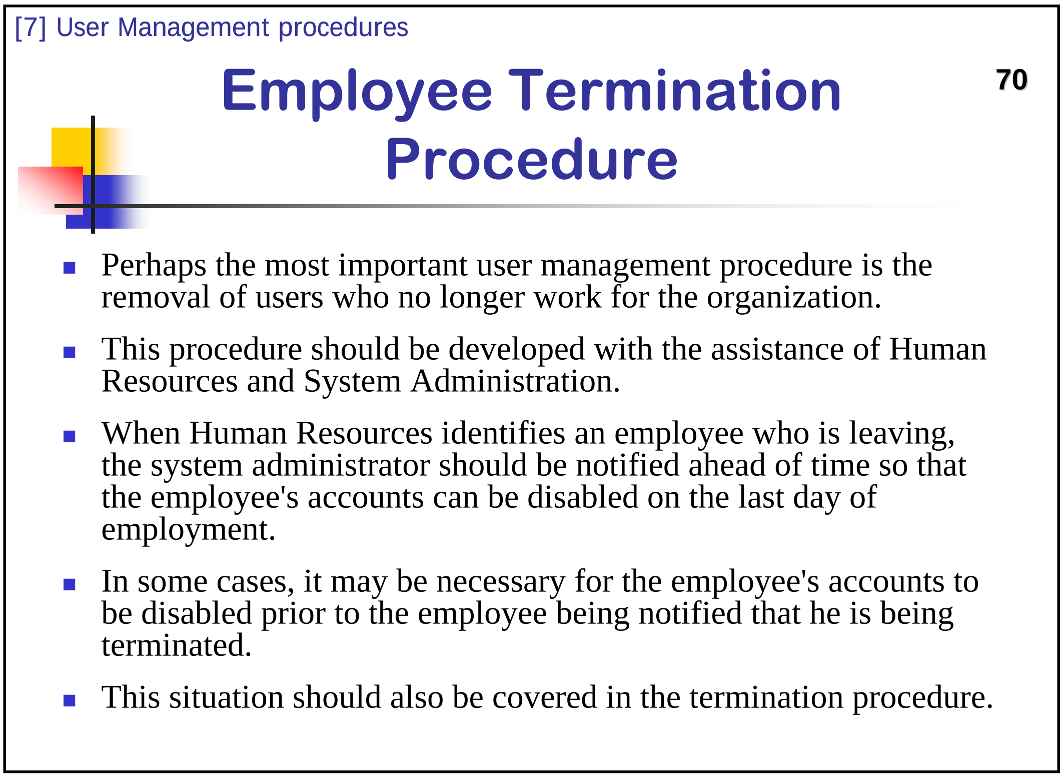


[7] User Management procedures

69

Transferred Employee Procedure

- Every organization should develop a procedure for reviewing employees' computer access when they transfer within the organization.
- This procedure should be developed with the assistance of Human Resources and System Administration.
- Ideally, both the employee's new and old supervisors will identify the fact that the employee is moving to a new position and the access that is no longer needed or the new access that is needed.
- The appropriate system administrator will then make the change.

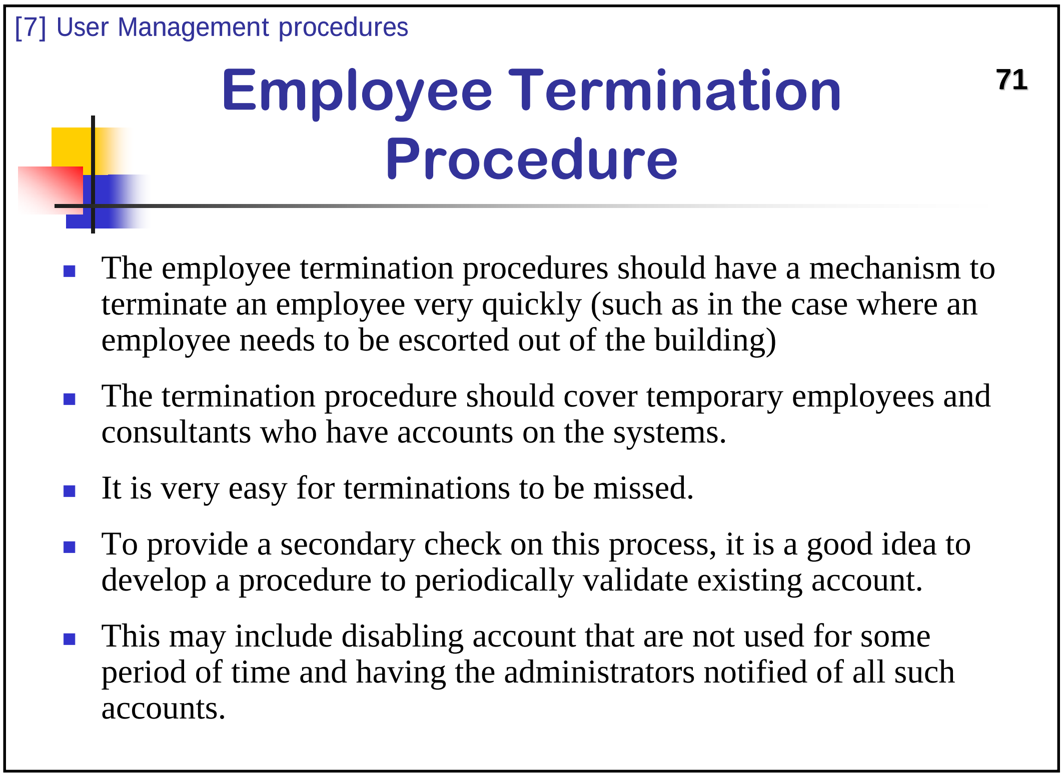


[7] User Management procedures

70

Employee Termination Procedure

- Perhaps the most important user management procedure is the removal of users who no longer work for the organization.
- This procedure should be developed with the assistance of Human Resources and System Administration.
- When Human Resources identifies an employee who is leaving, the system administrator should be notified ahead of time so that the employee's accounts can be disabled on the last day of employment.
- In some cases, it may be necessary for the employee's accounts to be disabled prior to the employee being notified that he is being terminated.
- This situation should also be covered in the termination procedure.

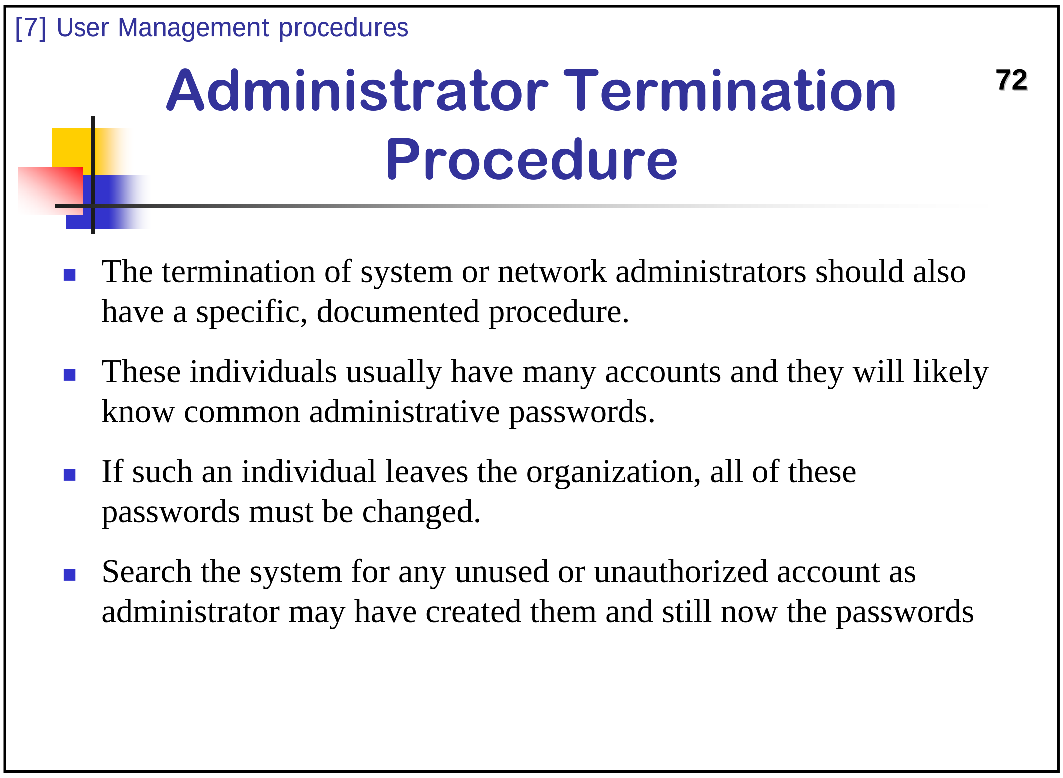


[7] User Management procedures

71

Employee Termination Procedure

- The employee termination procedures should have a mechanism to terminate an employee very quickly (such as in the case where an employee needs to be escorted out of the building)
- The termination procedure should cover temporary employees and consultants who have accounts on the systems.
- It is very easy for terminations to be missed.
- To provide a secondary check on this process, it is a good idea to develop a procedure to periodically validate existing account.
- This may include disabling account that are not used for some period of time and having the administrators notified of all such accounts.

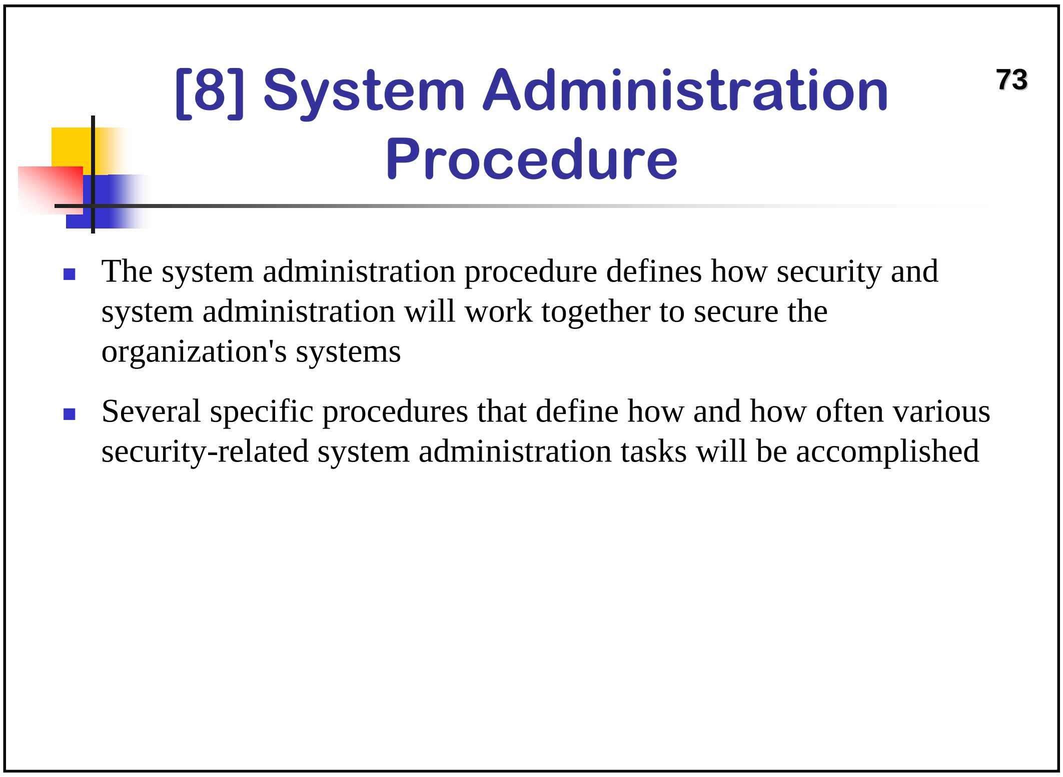


[7] User Management procedures

72

Administrator Termination Procedure

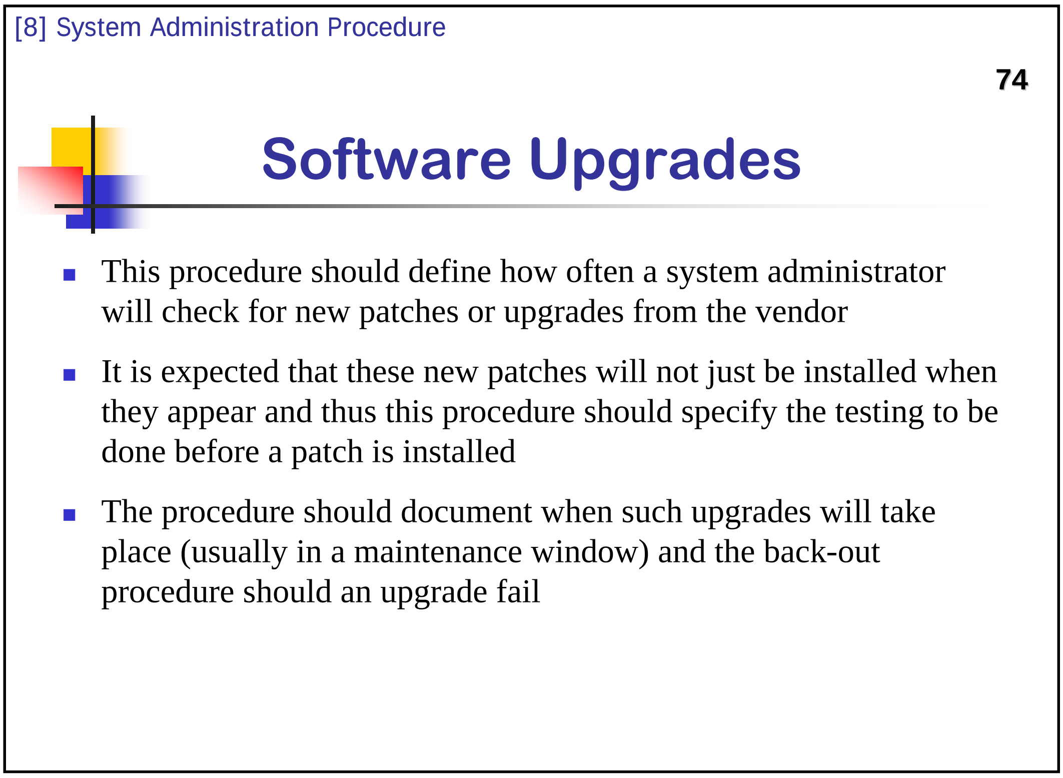
- The termination of system or network administrators should also have a specific, documented procedure.
- These individuals usually have many accounts and they will likely know common administrative passwords.
- If such an individual leaves the organization, all of these passwords must be changed.
- Search the system for any unused or unauthorized account as administrator may have created them and still now the passwords



73

[8] System Administration Procedure

- The system administration procedure defines how security and system administration will work together to secure the organization's systems
- Several specific procedures that define how and how often various security-related system administration tasks will be accomplished

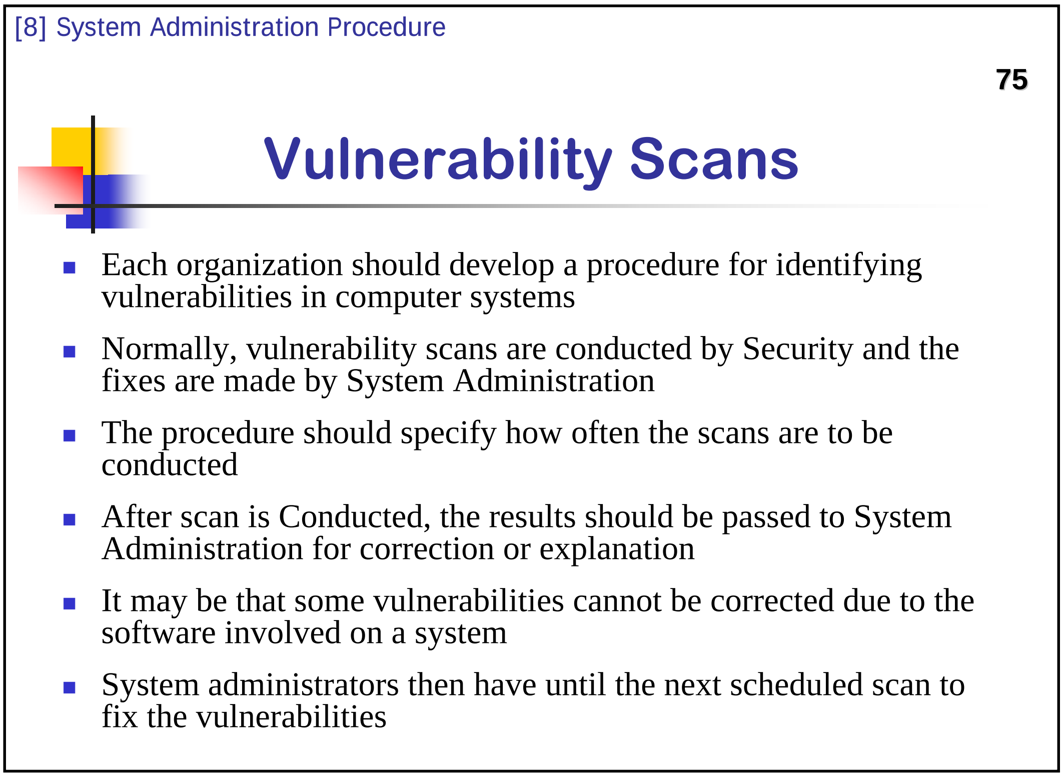


[8] System Administration Procedure

74

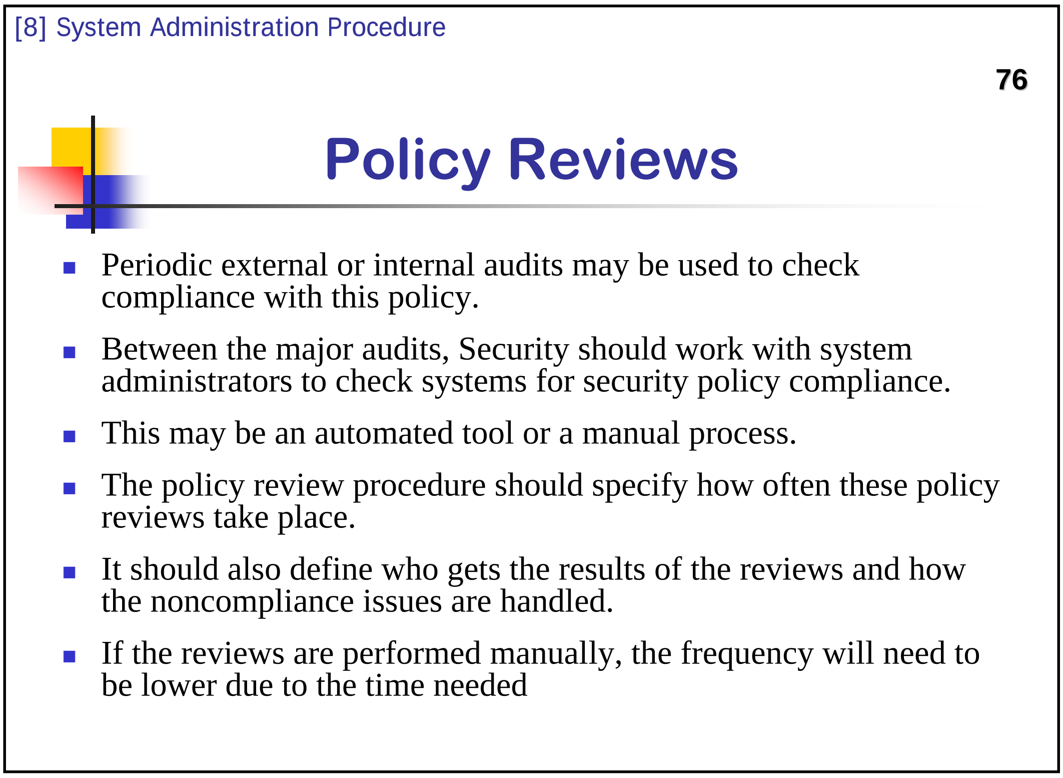
Software Upgrades

- This procedure should define how often a system administrator will check for new patches or upgrades from the vendor
- It is expected that these new patches will not just be installed when they appear and thus this procedure should specify the testing to be done before a patch is installed
- The procedure should document when such upgrades will take place (usually in a maintenance window) and the back-out procedure should an upgrade fail



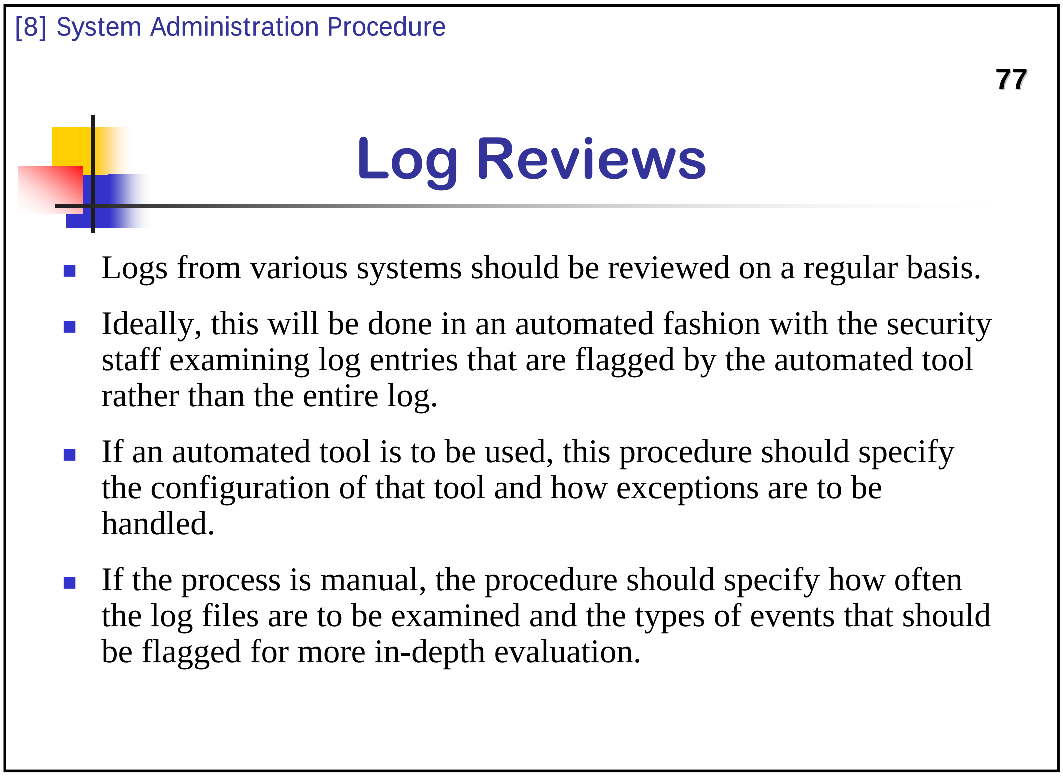
Vulnerability Scans

- Each organization should develop a procedure for identifying vulnerabilities in computer systems
- Normally, vulnerability scans are conducted by Security and the fixes are made by System Administration
- The procedure should specify how often the scans are to be conducted
- After scan is Conducted, the results should be passed to System Administration for correction or explanation
- It may be that some vulnerabilities cannot be corrected due to the software involved on a system
- System administrators then have until the next scheduled scan to fix the vulnerabilities



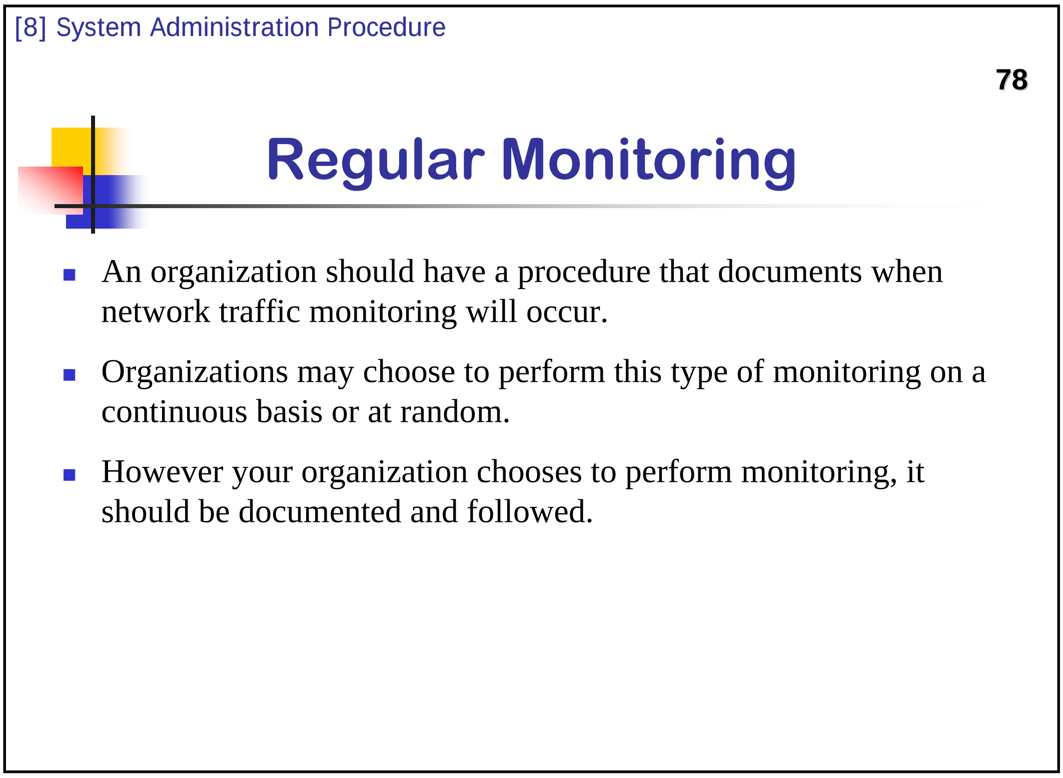
Policy Reviews

- Periodic external or internal audits may be used to check compliance with this policy.
- Between the major audits, Security should work with system administrators to check systems for security policy compliance.
- This may be an automated tool or a manual process.
- The policy review procedure should specify how often these policy reviews take place.
- It should also define who gets the results of the reviews and how the noncompliance issues are handled.
- If the reviews are performed manually, the frequency will need to be lower due to the time needed



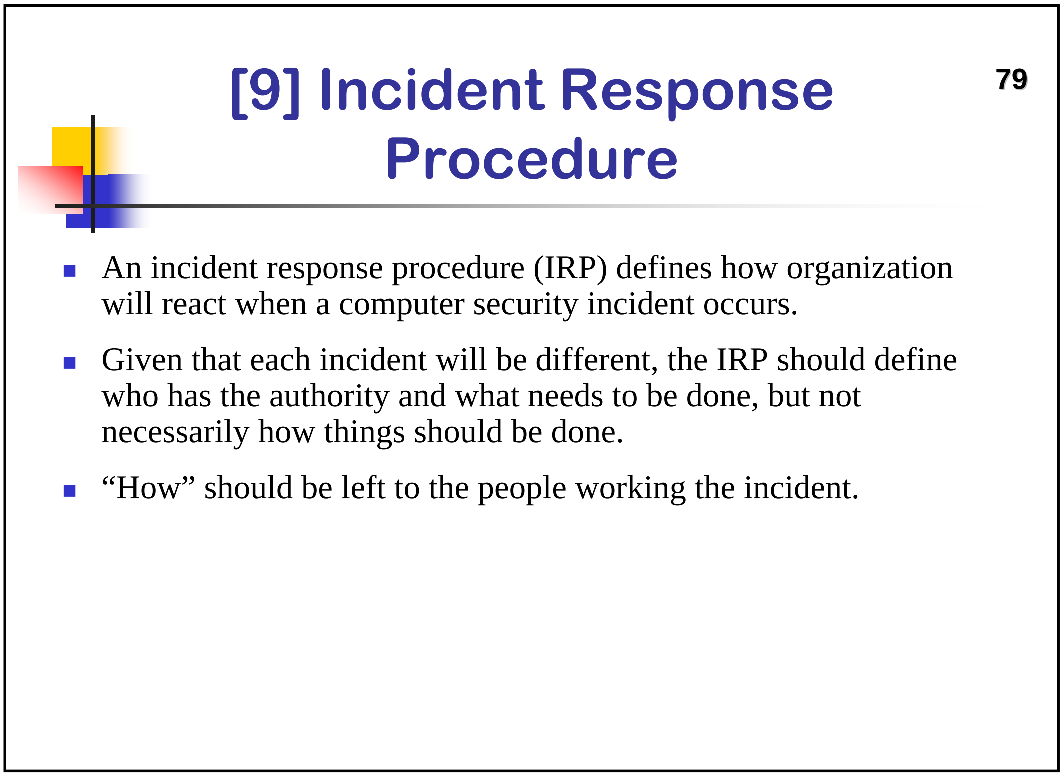
Log Reviews

- Logs from various systems should be reviewed on a regular basis.
- Ideally, this will be done in an automated fashion with the security staff examining log entries that are flagged by the automated tool rather than the entire log.
- If an automated tool is to be used, this procedure should specify the configuration of that tool and how exceptions are to be handled.
- If the process is manual, the procedure should specify how often the log files are to be examined and the types of events that should be flagged for more in-depth evaluation.



Regular Monitoring

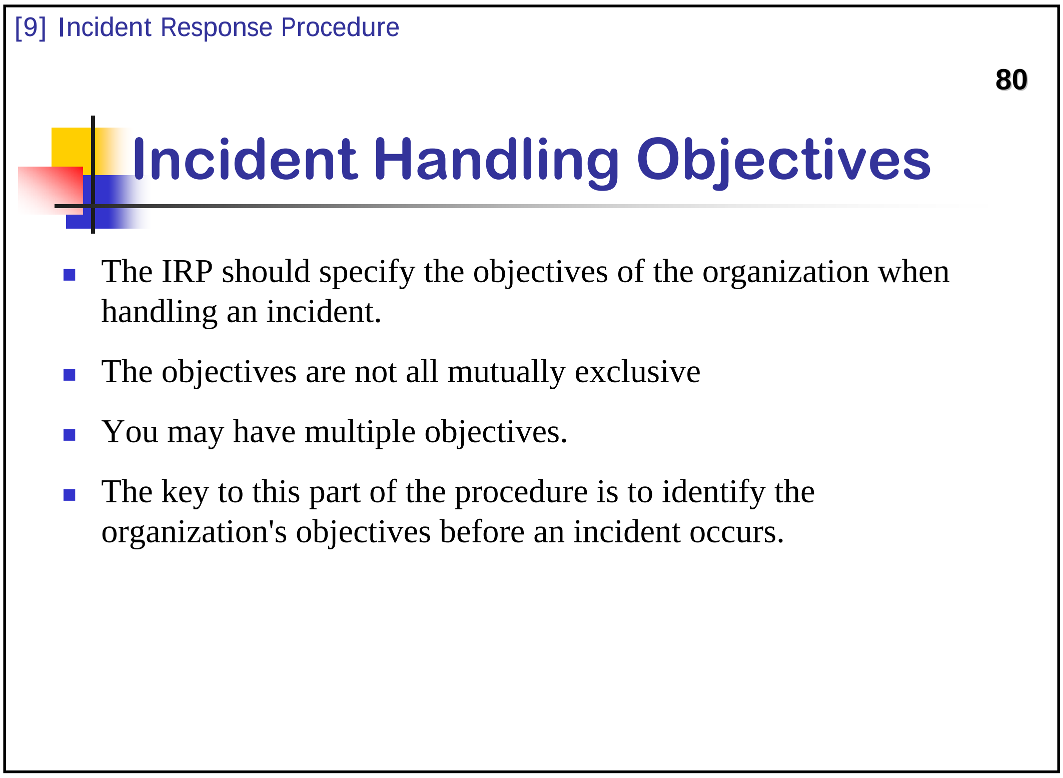
- An organization should have a procedure that documents when network traffic monitoring will occur.
- Organizations may choose to perform this type of monitoring on a continuous basis or at random.
- However your organization chooses to perform monitoring, it should be documented and followed.



79

[9] Incident Response Procedure

- An incident response procedure (IRP) defines how organization will react when a computer security incident occurs.
- Given that each incident will be different, the IRP should define who has the authority and what needs to be done, but not necessarily how things should be done.
- “How” should be left to the people working the incident.

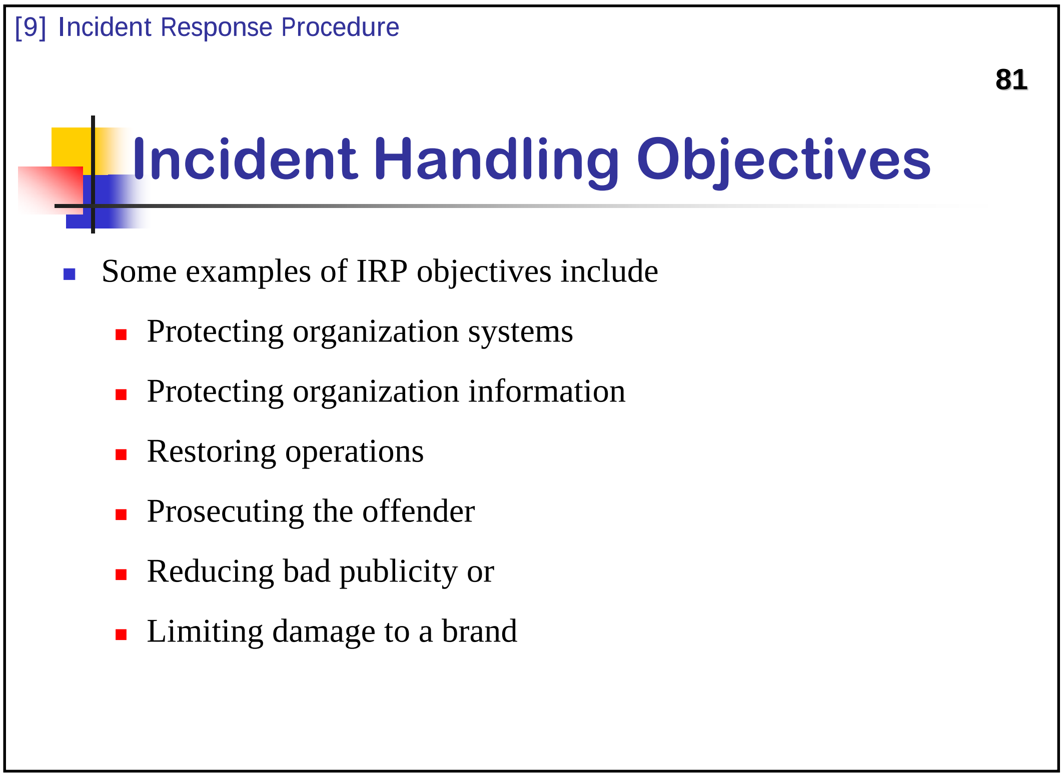


[9] Incident Response Procedure

80

Incident Handling Objectives

- The IRP should specify the objectives of the organization when handling an incident.
- The objectives are not all mutually exclusive
- You may have multiple objectives.
- The key to this part of the procedure is to identify the organization's objectives before an incident occurs.

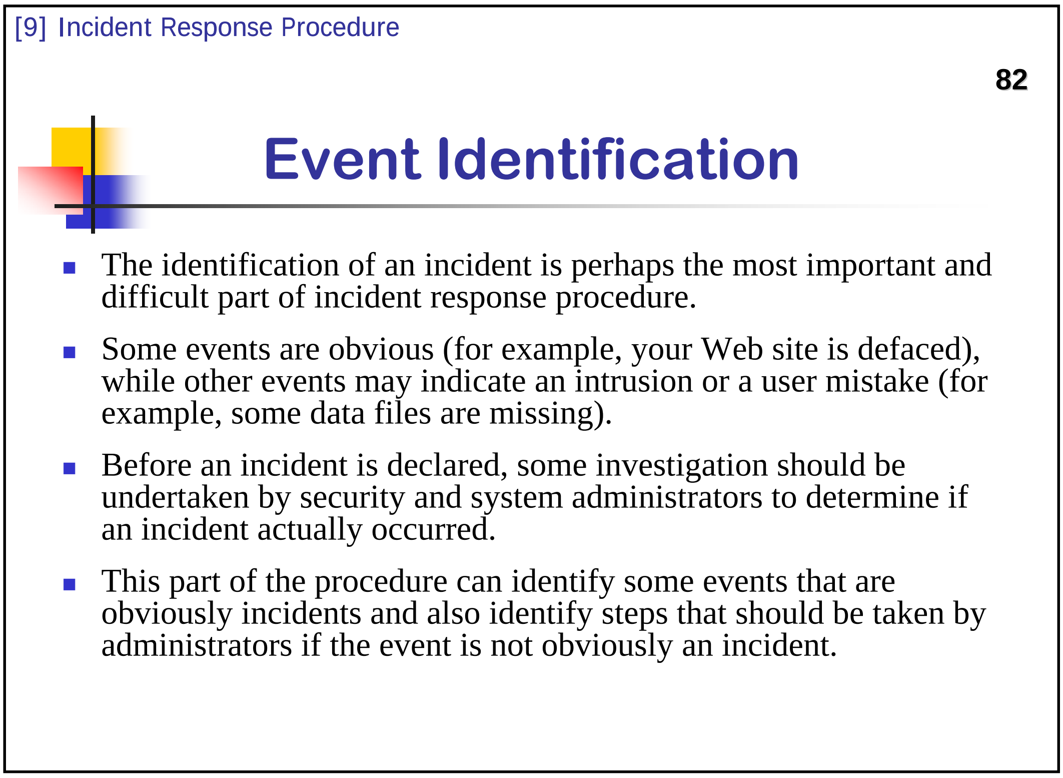


[9] Incident Response Procedure

81

Incident Handling Objectives

- Some examples of IRP objectives include
  - Protecting organization systems
  - Protecting organization information
  - Restoring operations
  - Prosecuting the offender
  - Reducing bad publicity or
  - Limiting damage to a brand

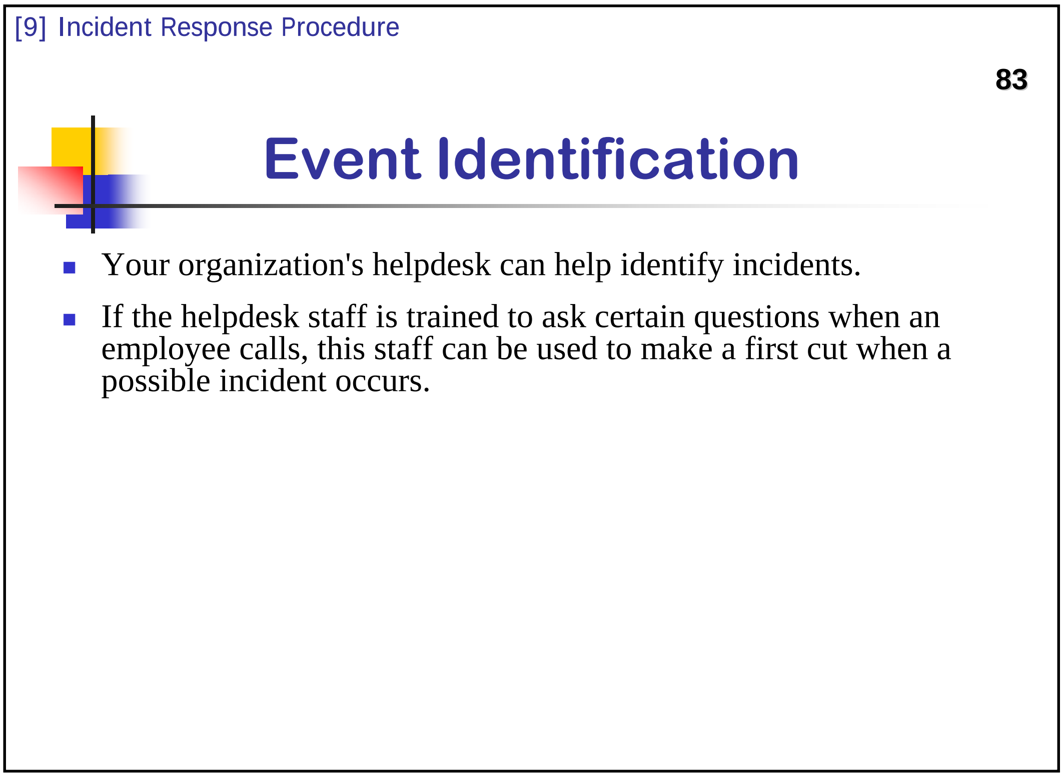


[9] Incident Response Procedure

82

Event Identification

- The identification of an incident is perhaps the most important and difficult part of incident response procedure.
- Some events are obvious (for example, your Web site is defaced), while other events may indicate an intrusion or a user mistake (for example, some data files are missing).
- Before an incident is declared, some investigation should be undertaken by security and system administrators to determine if an incident actually occurred.
- This part of the procedure can identify some events that are obviously incidents and also identify steps that should be taken by administrators if the event is not obviously an incident.

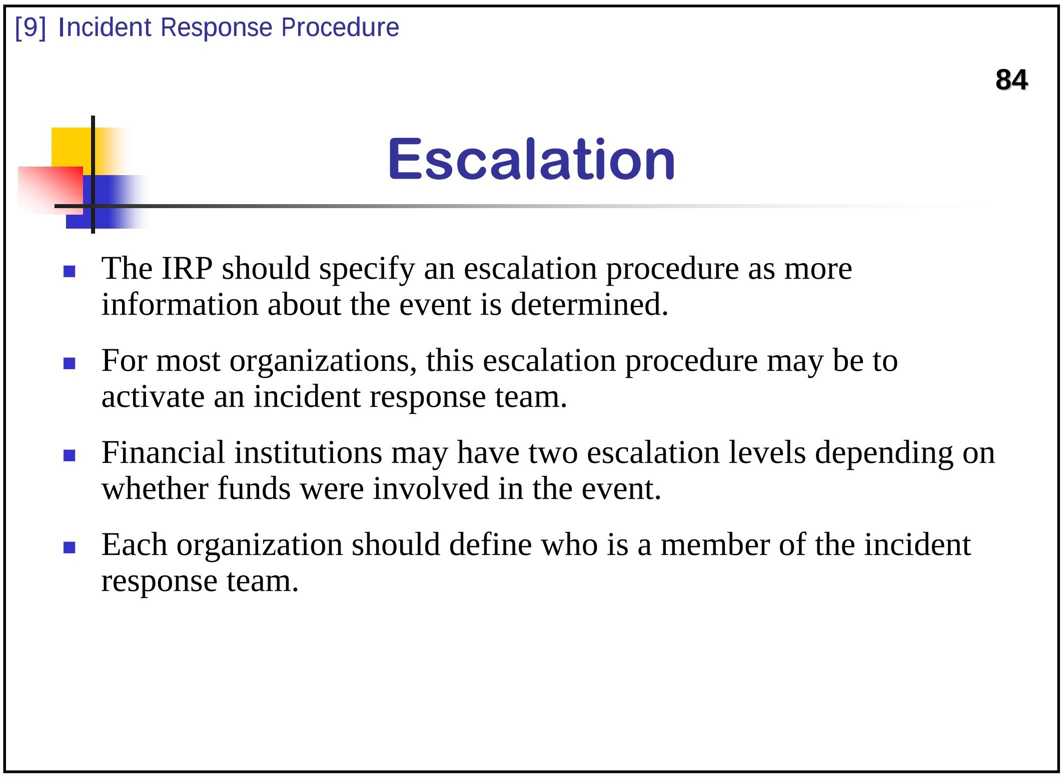


[9] Incident Response Procedure

83

Event Identification

- Your organization's helpdesk can help identify incidents.
- If the helpdesk staff is trained to ask certain questions when an employee calls, this staff can be used to make a first cut when a possible incident occurs.

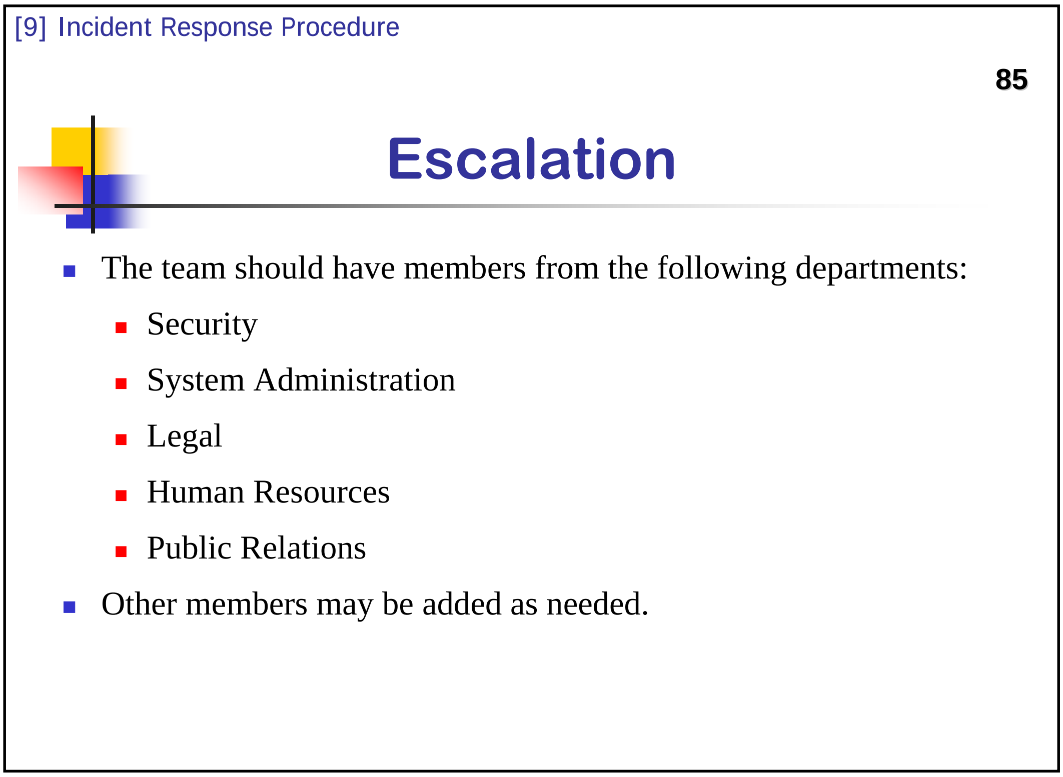


[9] Incident Response Procedure

84

Escalation

- The IRP should specify an escalation procedure as more information about the event is determined.
- For most organizations, this escalation procedure may be to activate an incident response team.
- Financial institutions may have two escalation levels depending on whether funds were involved in the event.
- Each organization should define who is a member of the incident response team.

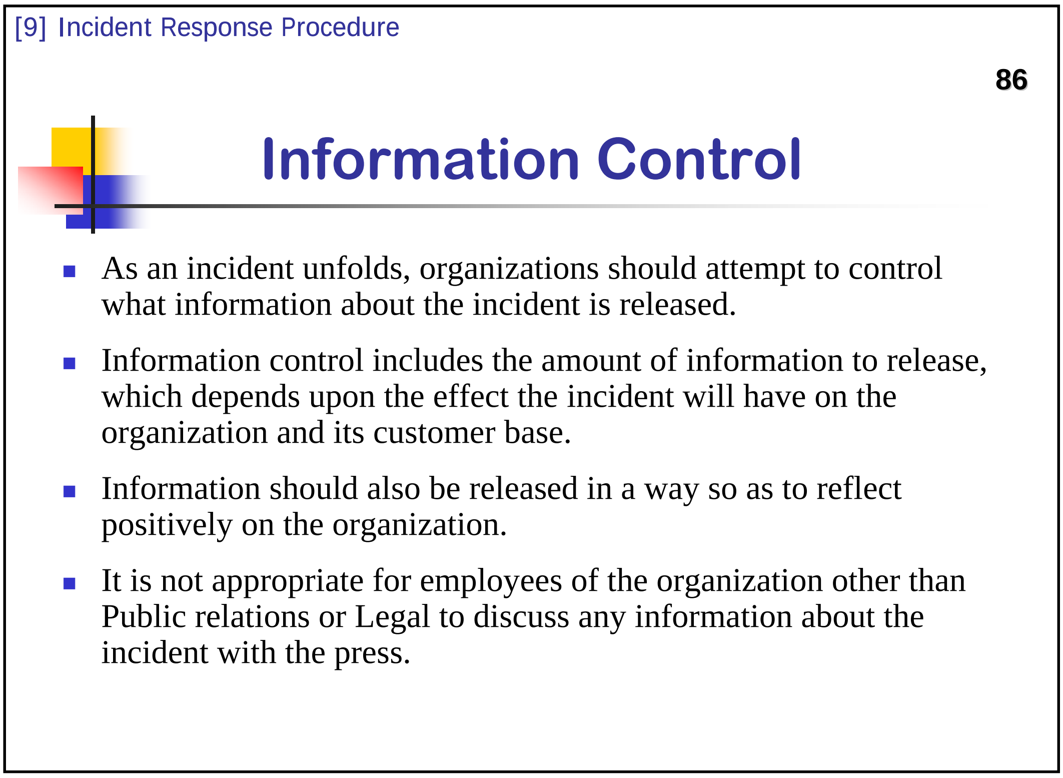


[9] Incident Response Procedure

85

Escalation

- The team should have members from the following departments:
  - Security
  - System Administration
  - Legal
  - Human Resources
  - Public Relations
- Other members may be added as needed.

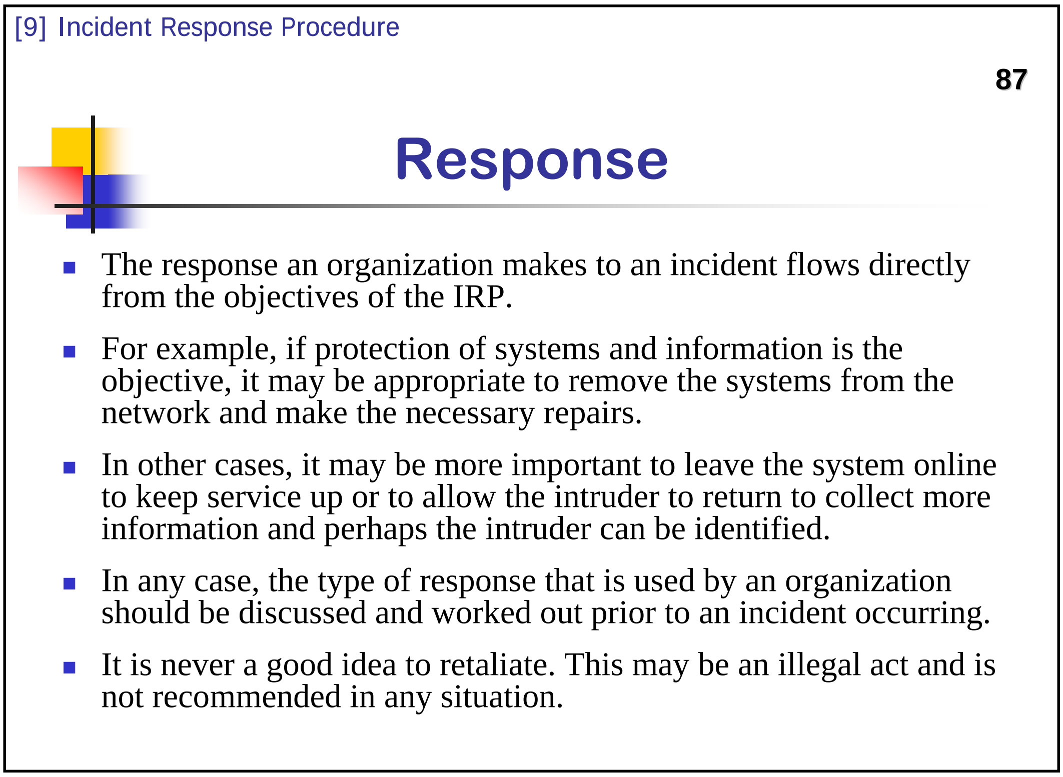


[9] Incident Response Procedure

86

Information Control

- As an incident unfolds, organizations should attempt to control what information about the incident is released.
- Information control includes the amount of information to release, which depends upon the effect the incident will have on the organization and its customer base.
- Information should also be released in a way so as to reflect positively on the organization.
- It is not appropriate for employees of the organization other than Public relations or Legal to discuss any information about the incident with the press.

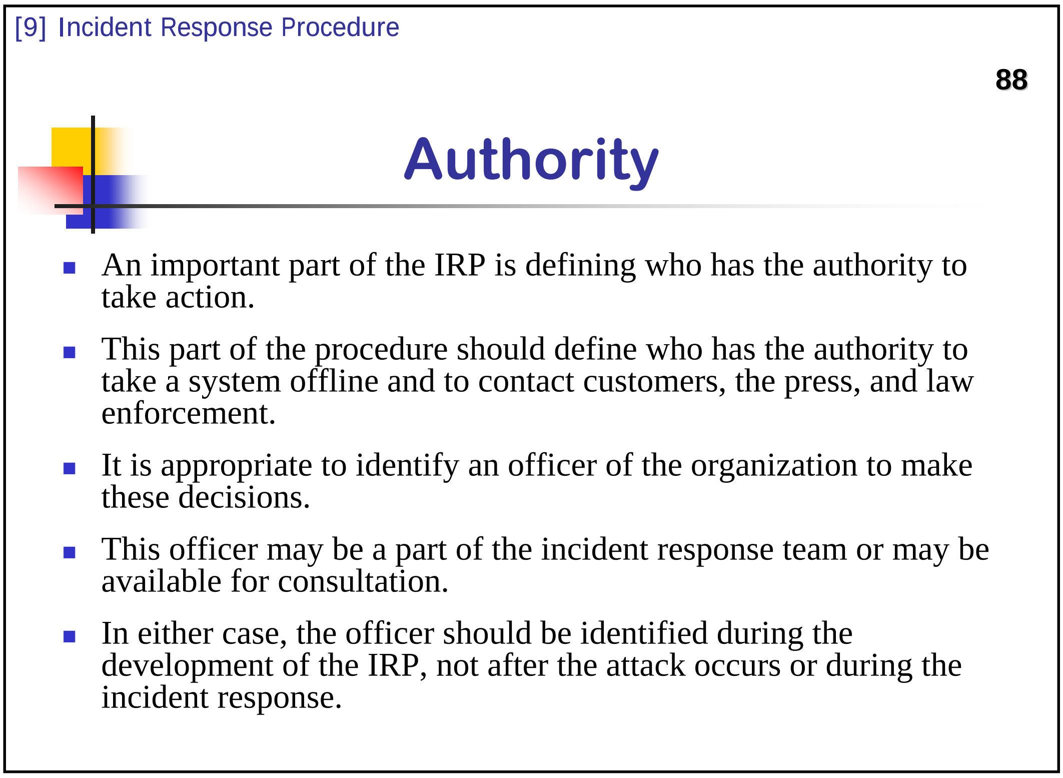


[9] Incident Response Procedure

87

Response

- The response an organization makes to an incident flows directly from the objectives of the IRP.
- For example, if protection of systems and information is the objective, it may be appropriate to remove the systems from the network and make the necessary repairs.
- In other cases, it may be more important to leave the system online to keep service up or to allow the intruder to return to collect more information and perhaps the intruder can be identified.
- In any case, the type of response that is used by an organization should be discussed and worked out prior to an incident occurring.
- It is never a good idea to retaliate. This may be an illegal act and is not recommended in any situation.

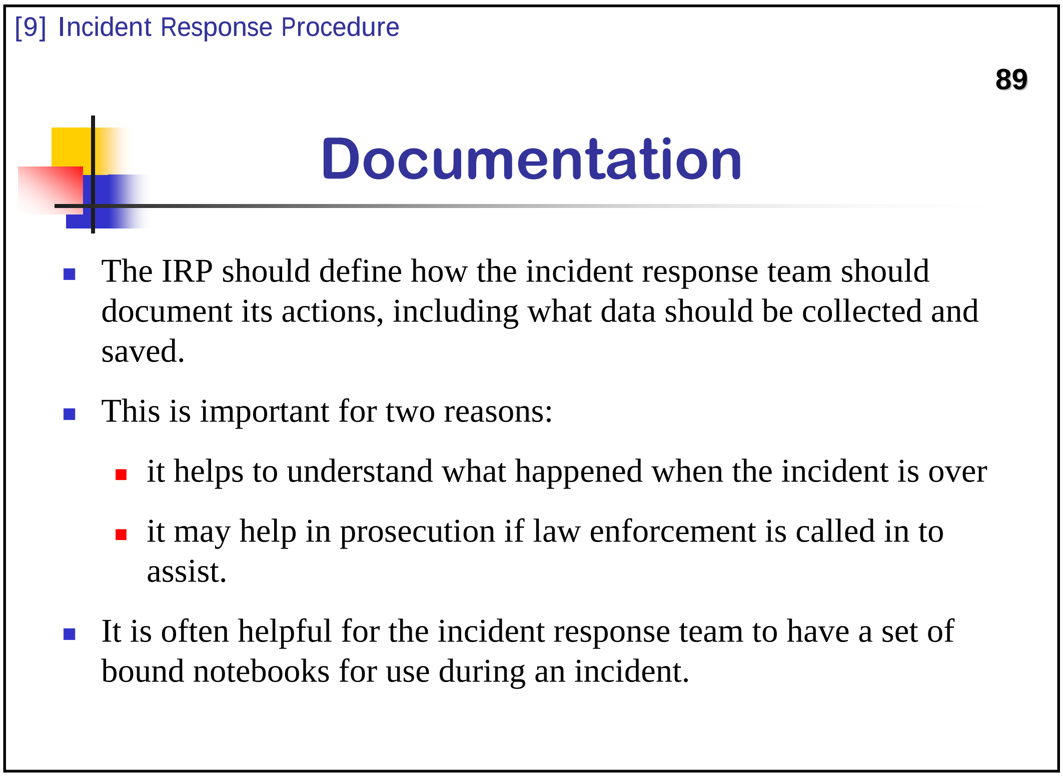


[9] Incident Response Procedure

88

Authority

- An important part of the IRP is defining who has the authority to take action.
- This part of the procedure should define who has the authority to take a system offline and to contact customers, the press, and law enforcement.
- It is appropriate to identify an officer of the organization to make these decisions.
- This officer may be a part of the incident response team or may be available for consultation.
- In either case, the officer should be identified during the development of the IRP, not after the attack occurs or during the incident response.

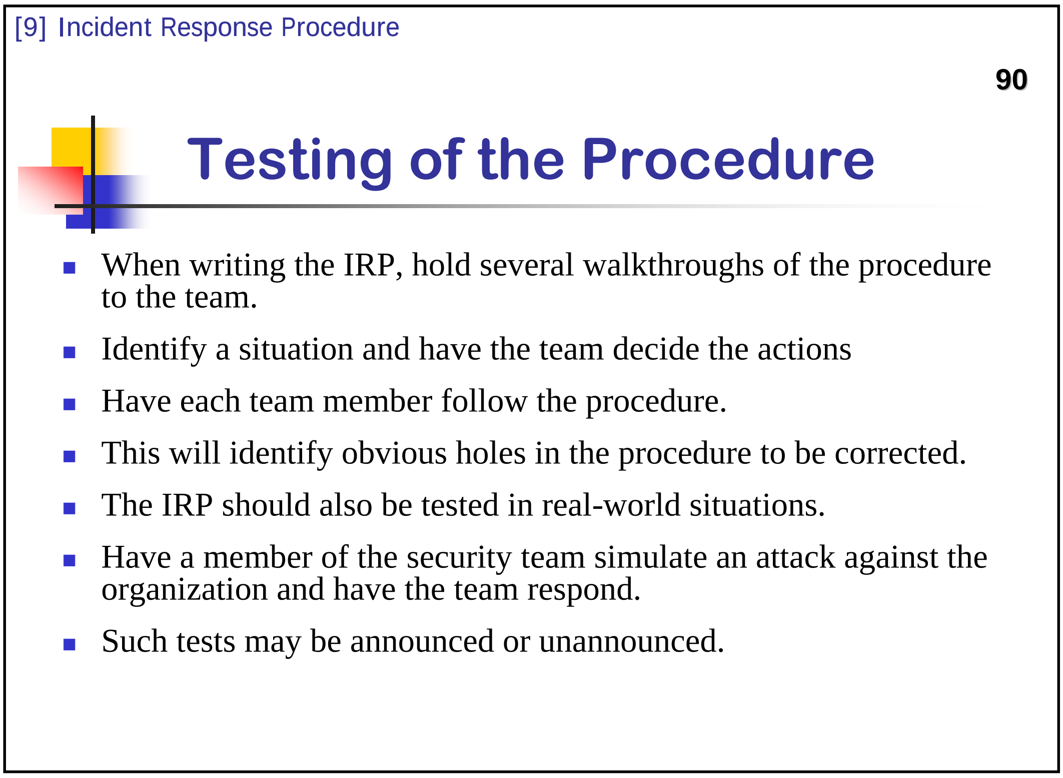


[9] Incident Response Procedure

89

Documentation

- The IRP should define how the incident response team should document its actions, including what data should be collected and saved.
- This is important for two reasons:
  - it helps to understand what happened when the incident is over
  - it may help in prosecution if law enforcement is called in to assist.
- It is often helpful for the incident response team to have a set of bound notebooks for use during an incident.

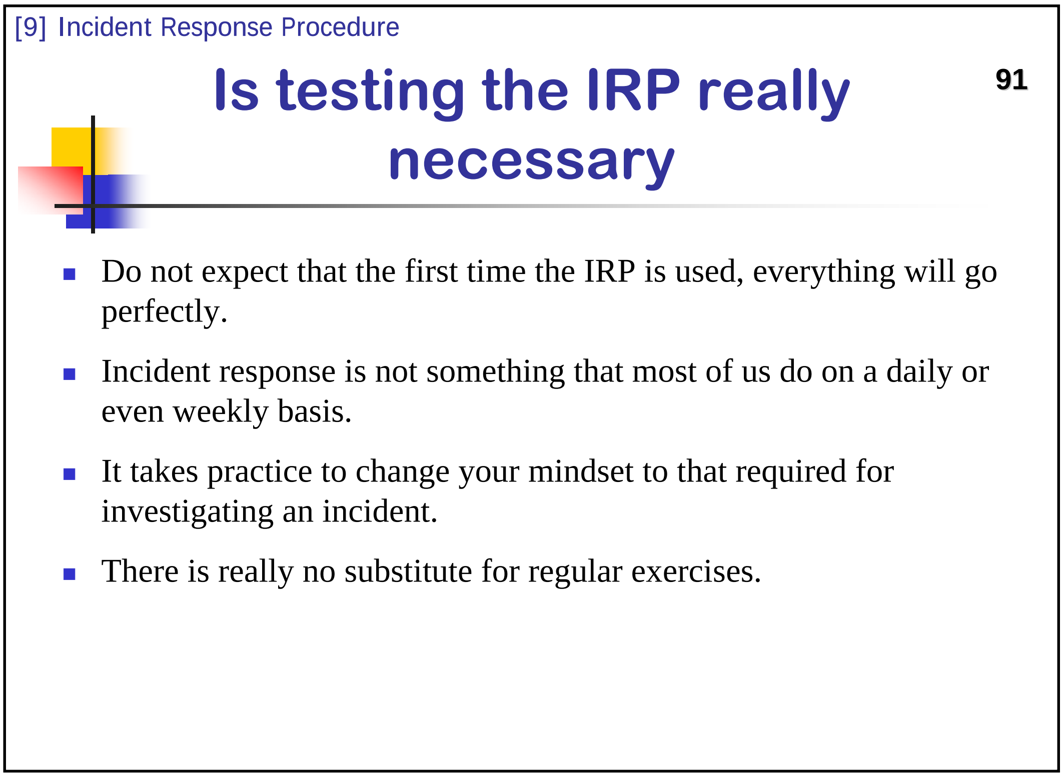


[9] Incident Response Procedure

90

Testing of the Procedure

- When writing the IRP, hold several walkthroughs of the procedure to the team.
- Identify a situation and have the team decide the actions
- Have each team member follow the procedure.
- This will identify obvious holes in the procedure to be corrected.
- The IRP should also be tested in real-world situations.
- Have a member of the security team simulate an attack against the organization and have the team respond.
- Such tests may be announced or unannounced.

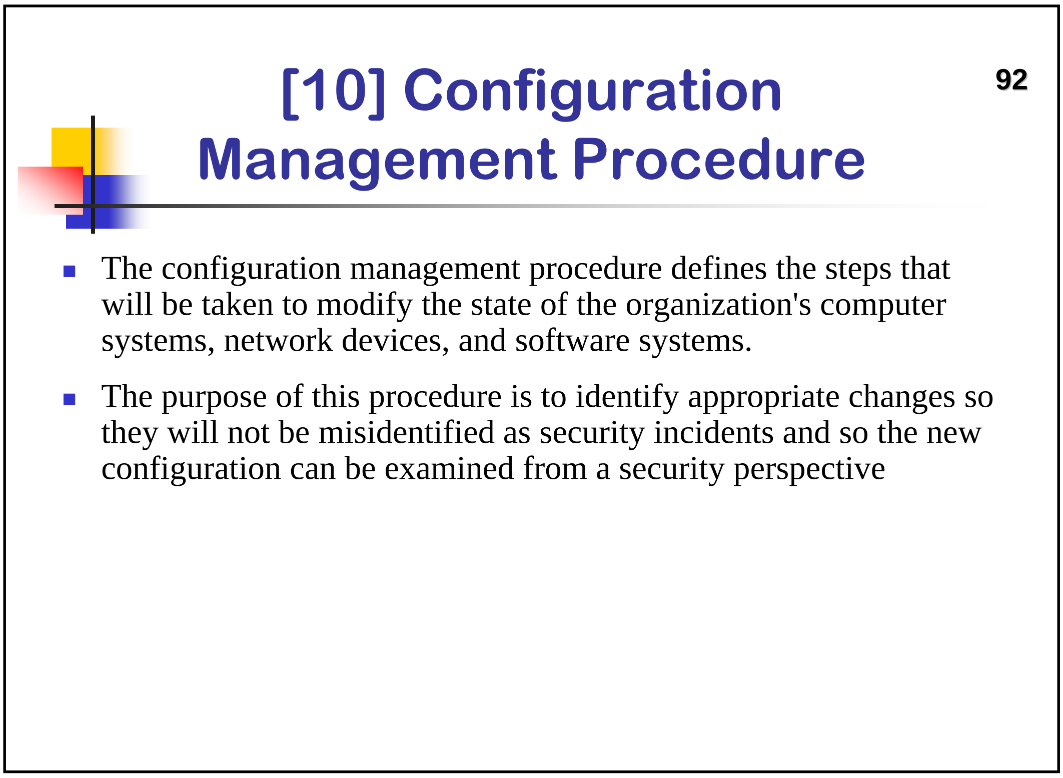


[9] Incident Response Procedure

91

Is testing the IRP really necessary

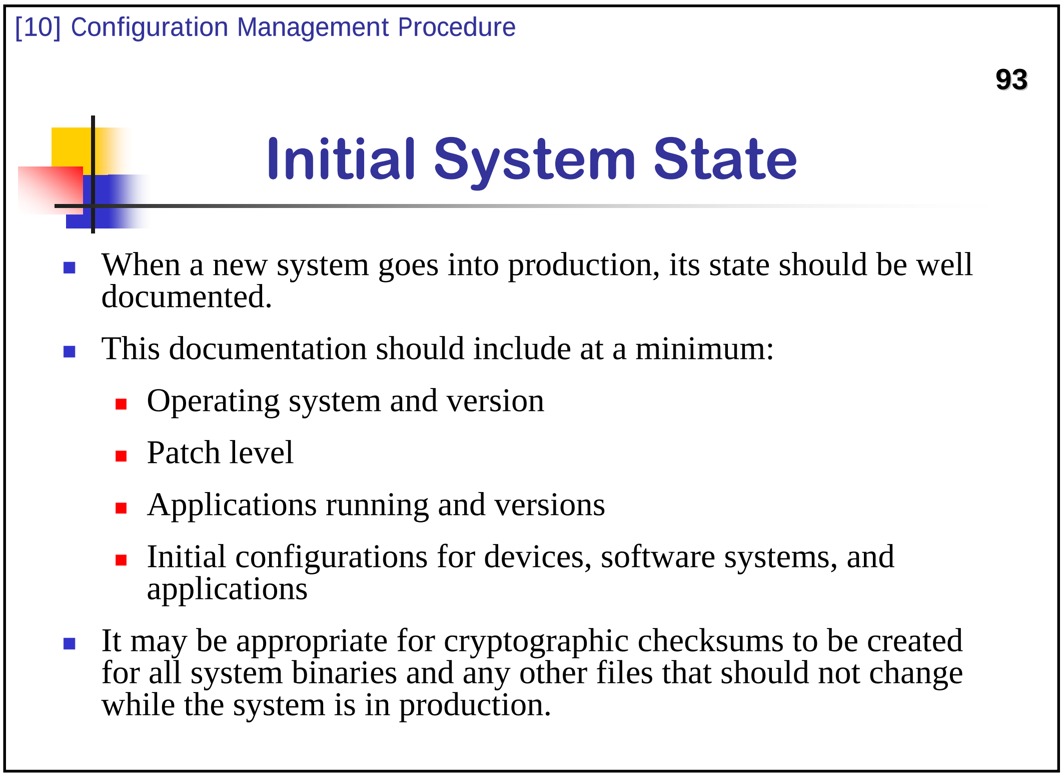
- Do not expect that the first time the IRP is used, everything will go perfectly.
- Incident response is not something that most of us do on a daily or even weekly basis.
- It takes practice to change your mindset to that required for investigating an incident.
- There is really no substitute for regular exercises.



92

[10] Configuration Management Procedure

- The configuration management procedure defines the steps that will be taken to modify the state of the organization's computer systems, network devices, and software systems.
- The purpose of this procedure is to identify appropriate changes so they will not be misidentified as security incidents and so the new configuration can be examined from a security perspective

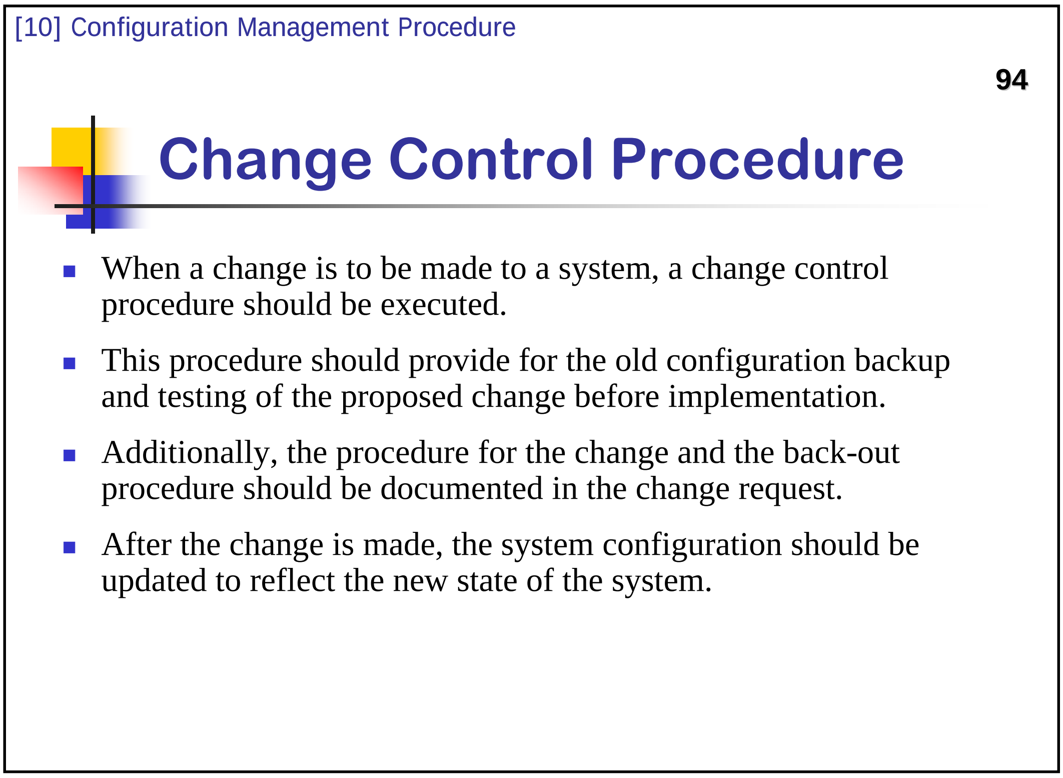


[10] Configuration Management Procedure

93

Initial System State

- When a new system goes into production, its state should be well documented.
- This documentation should include at a minimum:
  - Operating system and version
  - Patch level
  - Applications running and versions
  - Initial configurations for devices, software systems, and applications
- It may be appropriate for cryptographic checksums to be created for all system binaries and any other files that should not change while the system is in production.

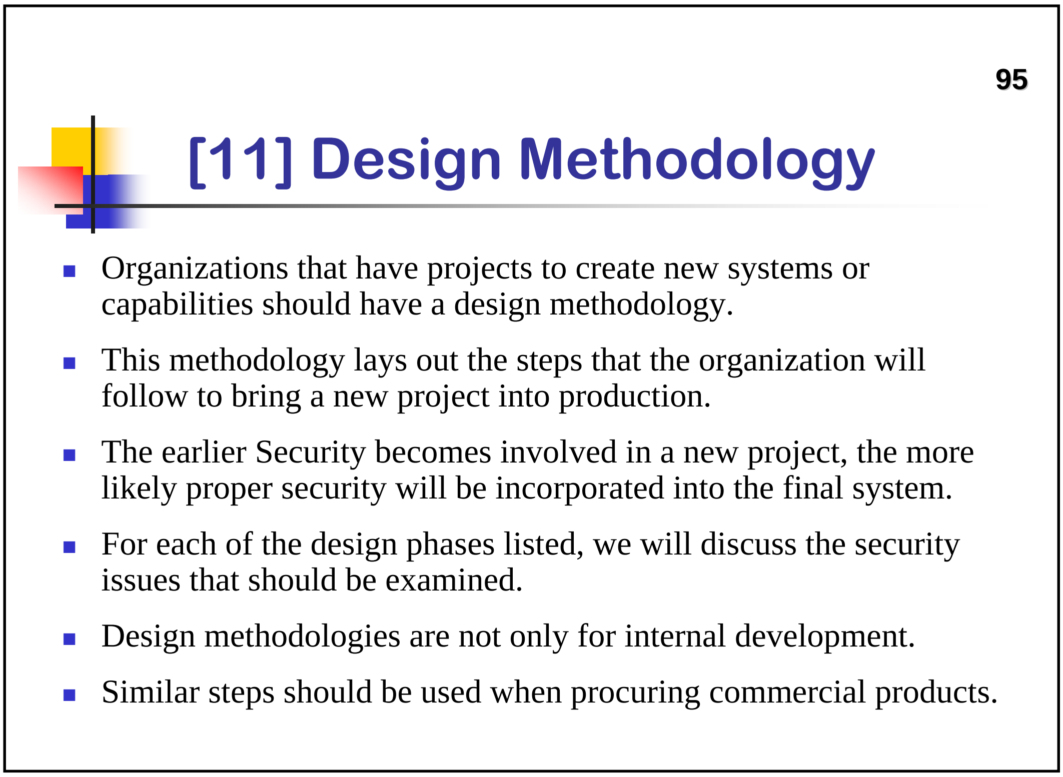


[10] Configuration Management Procedure

94

Change Control Procedure

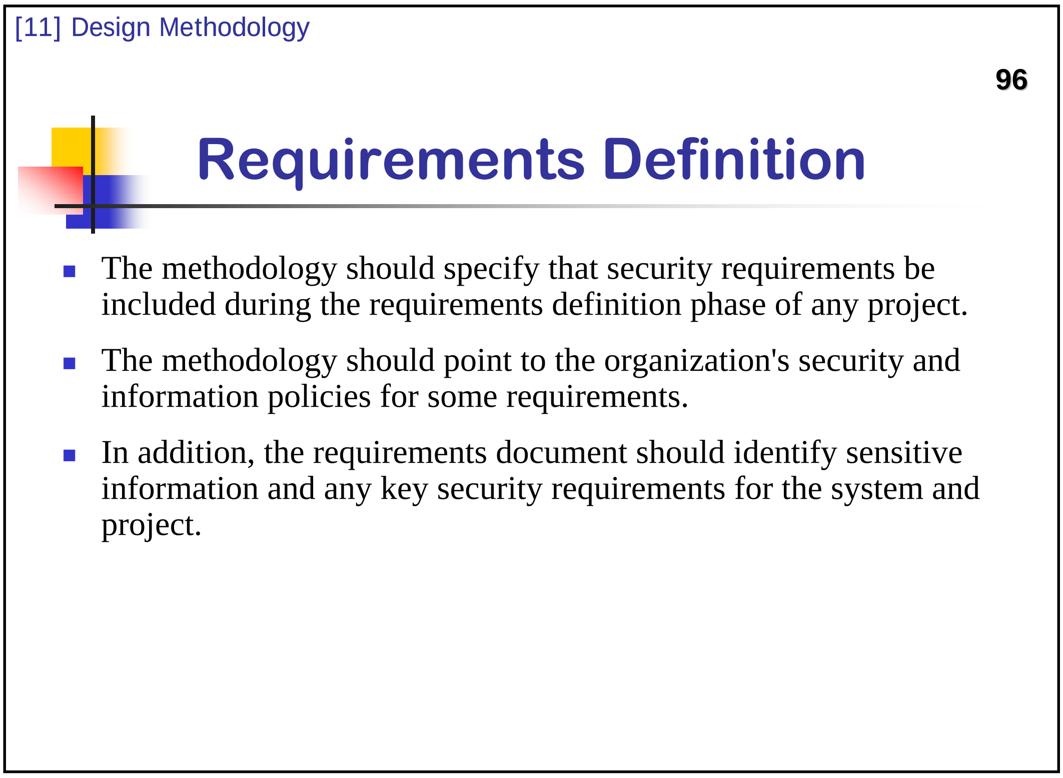
- When a change is to be made to a system, a change control procedure should be executed.
- This procedure should provide for the old configuration backup and testing of the proposed change before implementation.
- Additionally, the procedure for the change and the back-out procedure should be documented in the change request.
- After the change is made, the system configuration should be updated to reflect the new state of the system.



95

[11] Design Methodology

- Organizations that have projects to create new systems or capabilities should have a design methodology.
- This methodology lays out the steps that the organization will follow to bring a new project into production.
- The earlier Security becomes involved in a new project, the more likely proper security will be incorporated into the final system.
- For each of the design phases listed, we will discuss the security issues that should be examined.
- Design methodologies are not only for internal development.
- Similar steps should be used when procuring commercial products.

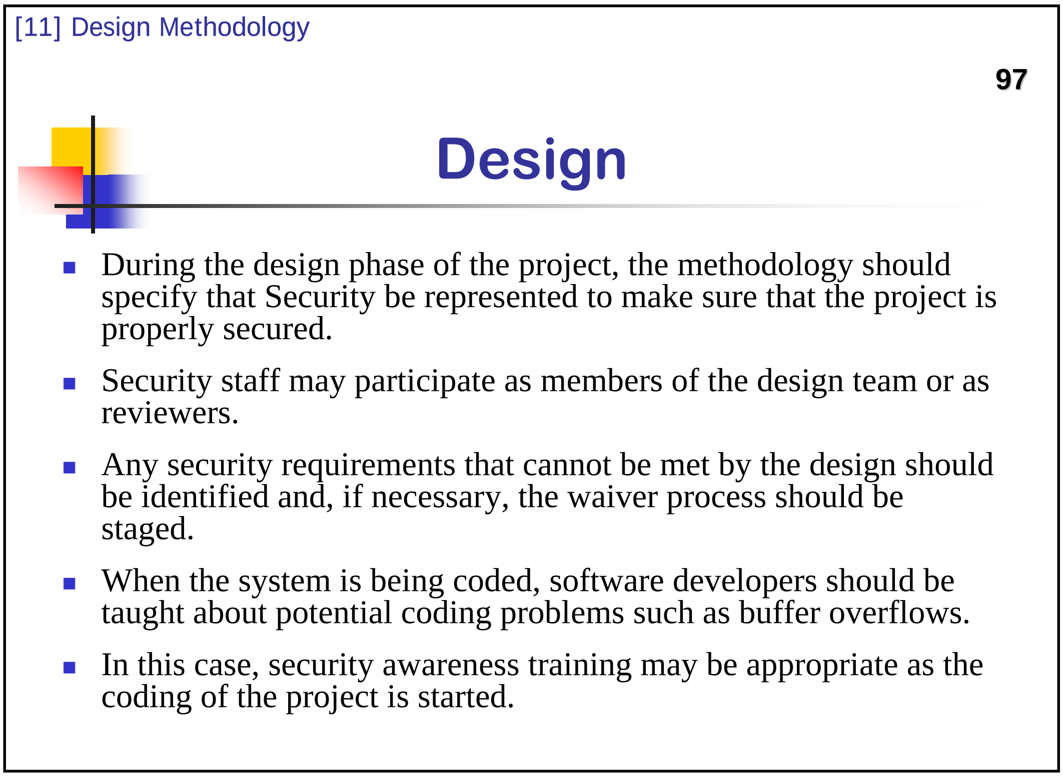


[11] Design Methodology

96

Requirements Definition

- The methodology should specify that security requirements be included during the requirements definition phase of any project.
- The methodology should point to the organization's security and information policies for some requirements.
- In addition, the requirements document should identify sensitive information and any key security requirements for the system and project.

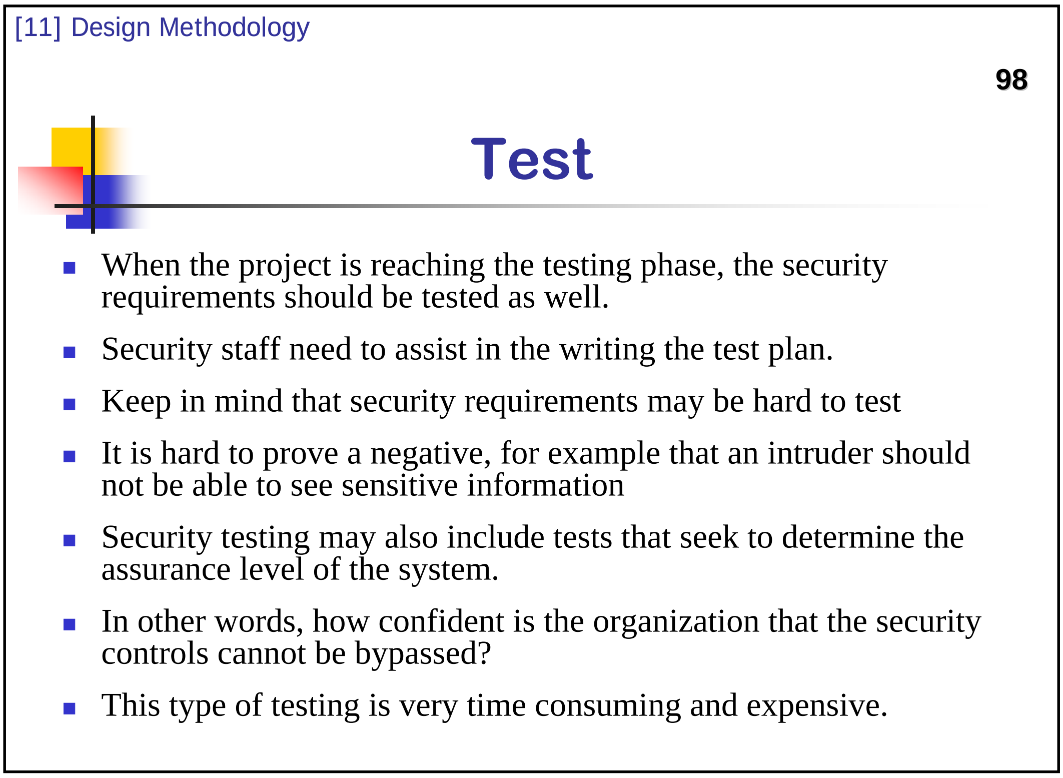


[11] Design Methodology

97

Design

- During the design phase of the project, the methodology should specify that Security be represented to make sure that the project is properly secured.
- Security staff may participate as members of the design team or as reviewers.
- Any security requirements that cannot be met by the design should be identified and, if necessary, the waiver process should be staged.
- When the system is being coded, software developers should be taught about potential coding problems such as buffer overflows.
- In this case, security awareness training may be appropriate as the coding of the project is started.



[11] Design Methodology

98

Test

- When the project is reaching the testing phase, the security requirements should be tested as well.
- Security staff need to assist in the writing the test plan.
- Keep in mind that security requirements may be hard to test
- It is hard to prove a negative, for example that an intruder should not be able to see sensitive information
- Security testing may also include tests that seek to determine the assurance level of the system.
- In other words, how confident is the organization that the security controls cannot be bypassed?
- This type of testing is very time consuming and expensive.

[11] Design Methodology

99

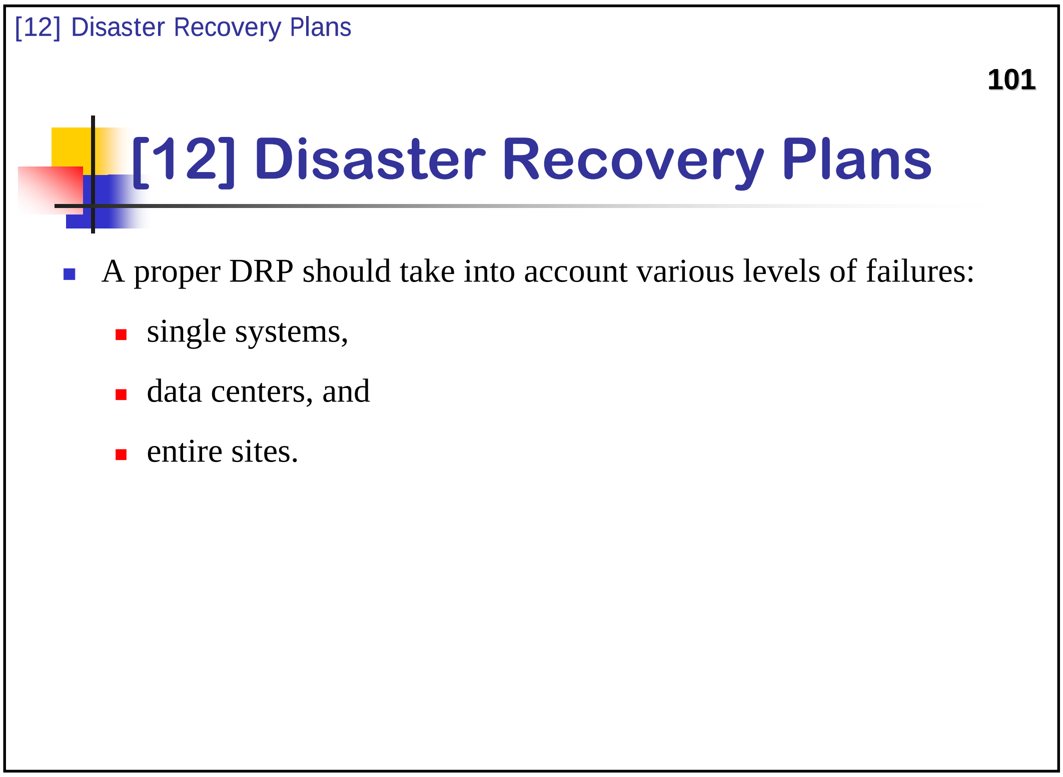
Implementation

- The implementation phase of the project also has security requirements.
- During this process, the implementation team should be using proper configuration management procedures.
- In addition, before a new system is deployed to production, the Security staff should examine the system for vulnerabilities and proper security policy compliance.

100

[12] Disaster Recovery Plans

- Every organization should have a disaster recovery plan (DRP) to handle fires, floods, and other site-destroying events.
- Many organizations do not have one because they see them as very expensive, and they do not feel that they can afford a hot site (an alternate location for operations that has all the necessary equipment configured and ready to go).
- DRPs do not necessarily require a hot site. Rather, a DRP is the plan that an organization will follow if the worst happens.
- It may be a very simple document that tells key staff to meet at a local restaurant if the building bums.
- Other documents may define how the organization will continue to operate if some or all of the computer systems are unavailable.

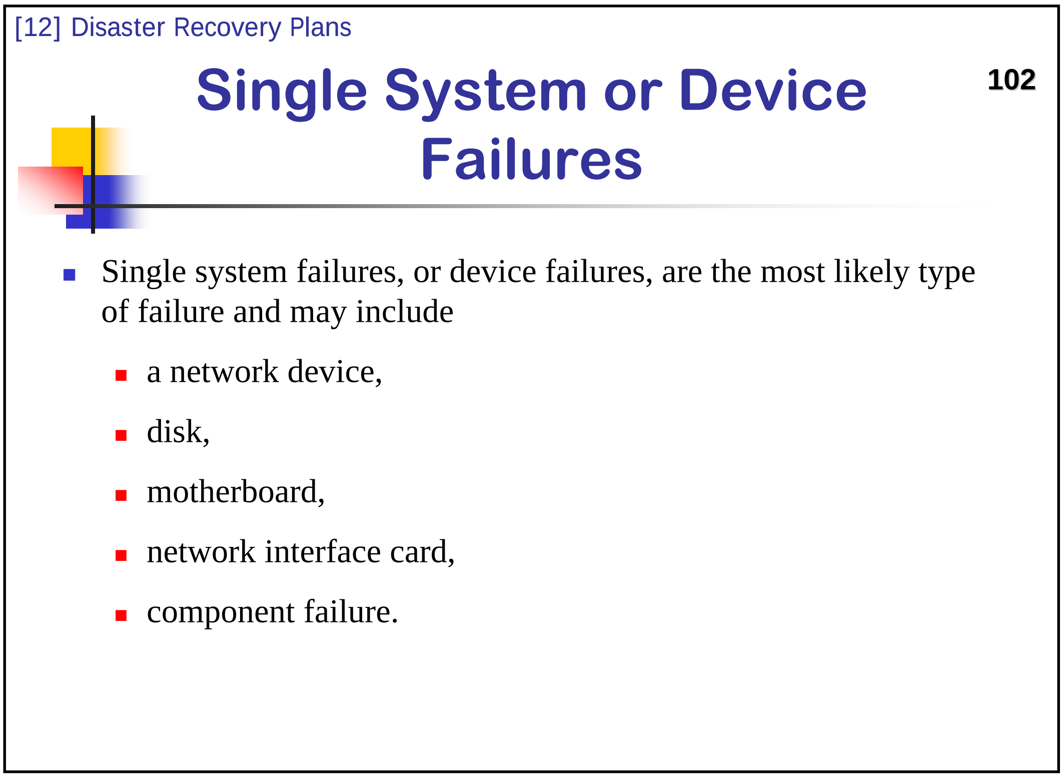


[12] Disaster Recovery Plans

101

[12] Disaster Recovery Plans

- A proper DRP should take into account various levels of failures:
  - single systems,
  - data centers, and
  - entire sites.

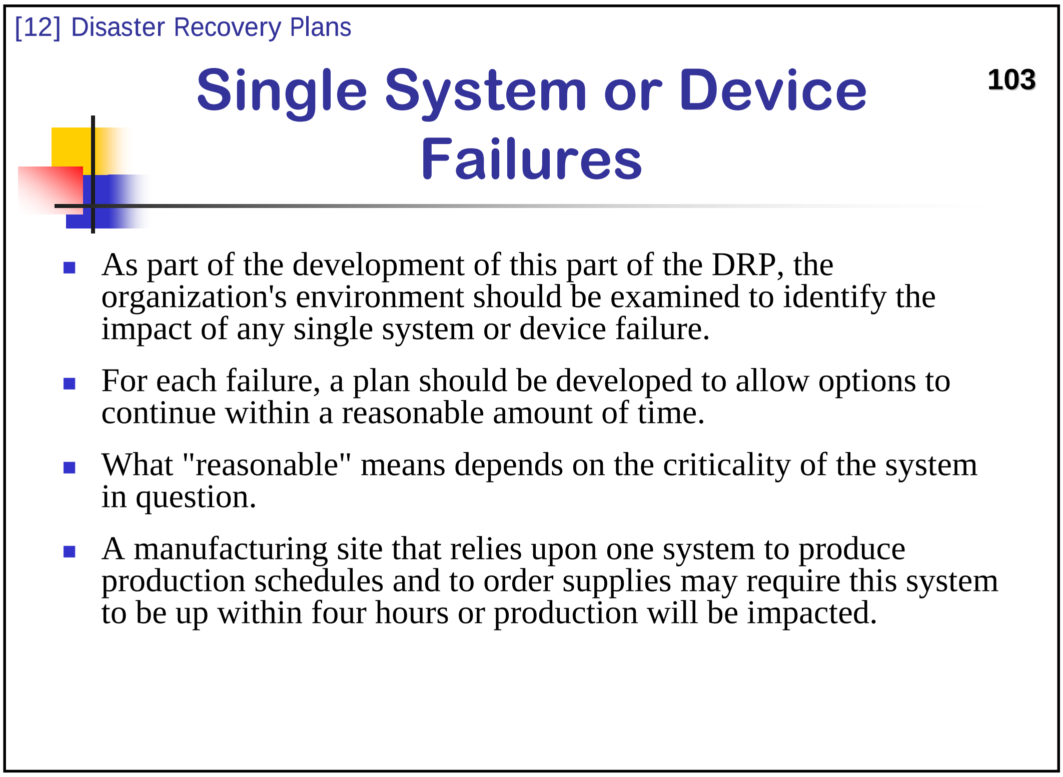


[12] Disaster Recovery Plans

102

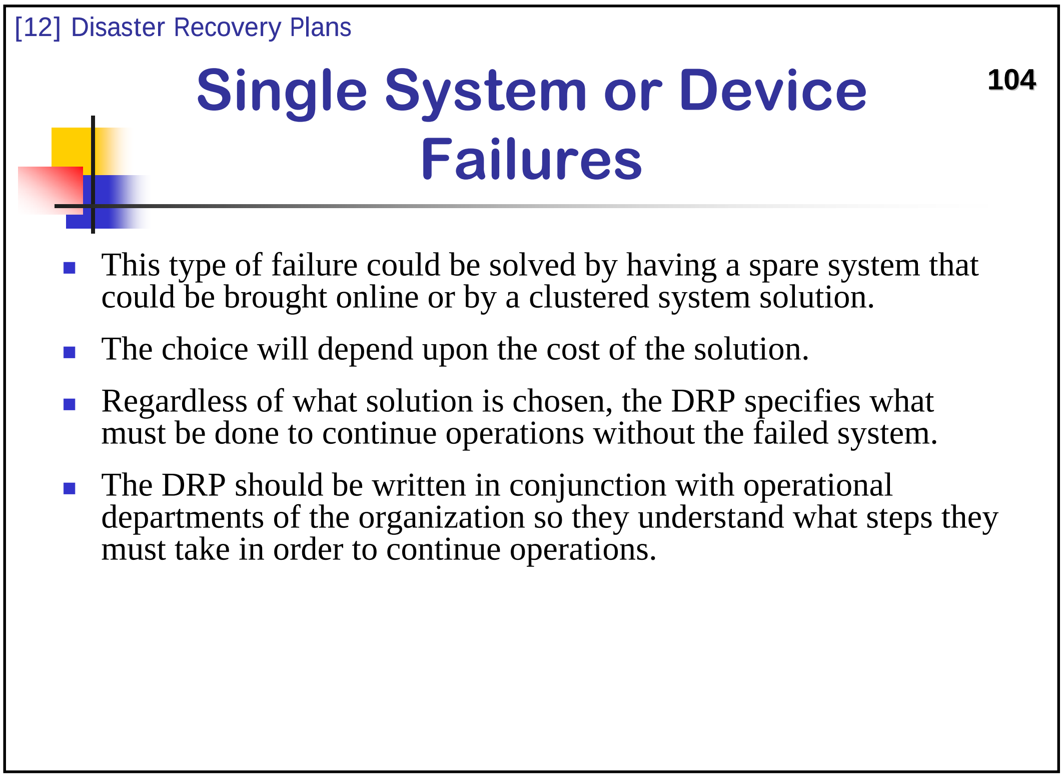
Single System or Device Failures

- Single system failures, or device failures, are the most likely type of failure and may include
  - a network device,
  - disk,
  - motherboard,
  - network interface card,
  - component failure.



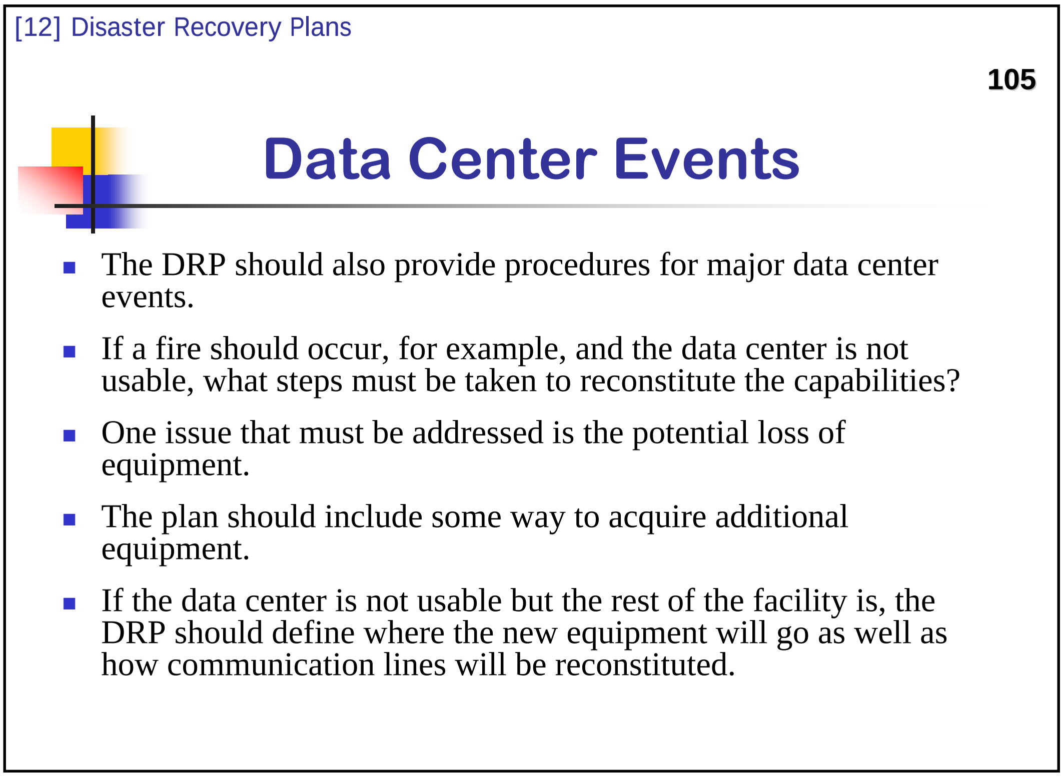
Single System or Device Failures

- As part of the development of this part of the DRP, the organization's environment should be examined to identify the impact of any single system or device failure.
- For each failure, a plan should be developed to allow options to continue within a reasonable amount of time.
- What "reasonable" means depends on the criticality of the system in question.
- A manufacturing site that relies upon one system to produce production schedules and to order supplies may require this system to be up within four hours or production will be impacted.



Single System or Device Failures

- This type of failure could be solved by having a spare system that could be brought online or by a clustered system solution.
- The choice will depend upon the cost of the solution.
- Regardless of what solution is chosen, the DRP specifies what must be done to continue operations without the failed system.
- The DRP should be written in conjunction with operational departments of the organization so they understand what steps they must take in order to continue operations.

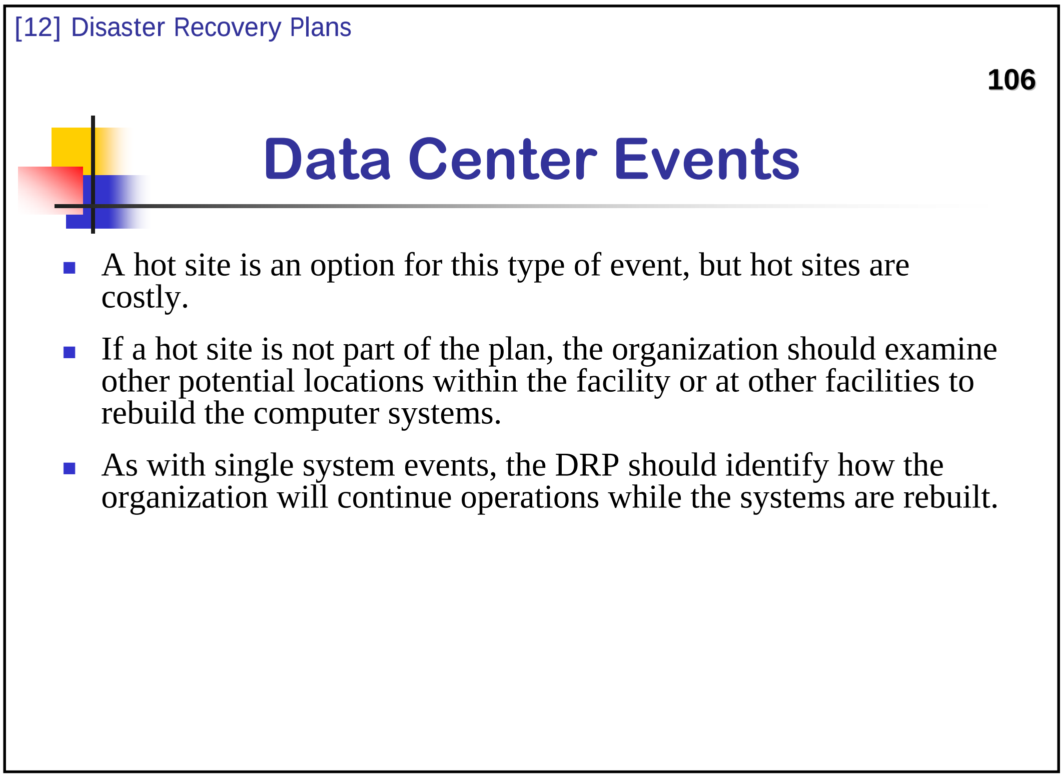


[12] Disaster Recovery Plans

105

Data Center Events

- The DRP should also provide procedures for major data center events.
- If a fire should occur, for example, and the data center is not usable, what steps must be taken to reconstitute the capabilities?
- One issue that must be addressed is the potential loss of equipment.
- The plan should include some way to acquire additional equipment.
- If the data center is not usable but the rest of the facility is, the DRP should define where the new equipment will go as well as how communication lines will be reconstituted.

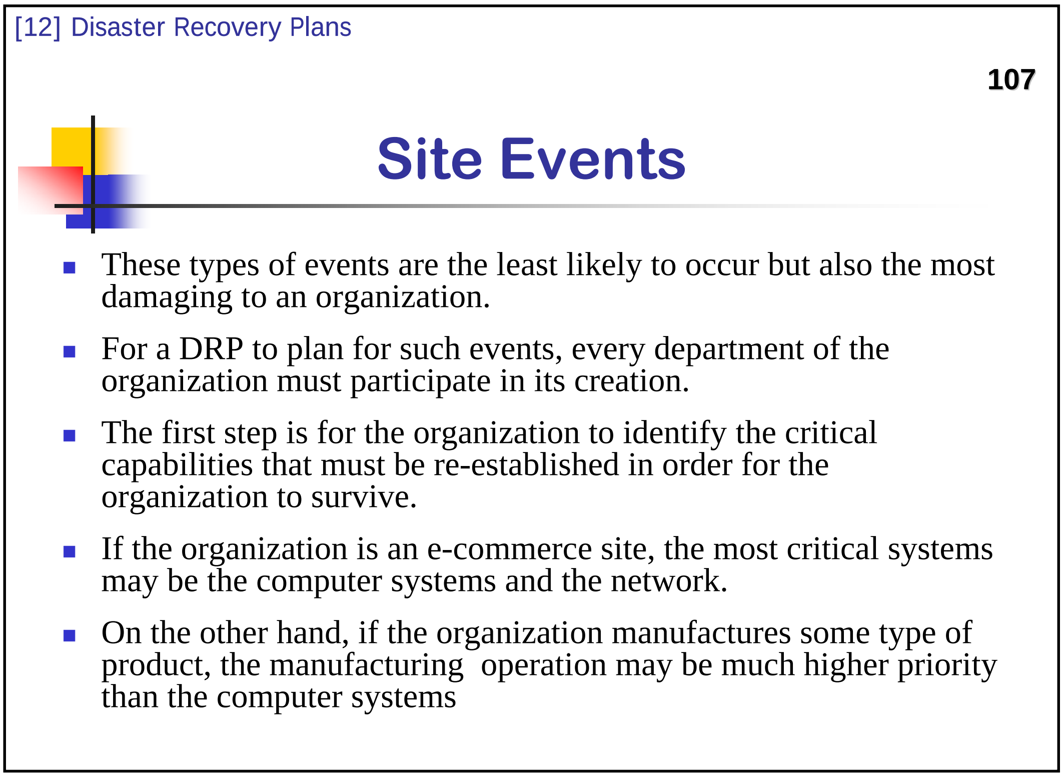


[12] Disaster Recovery Plans

106

Data Center Events

- A hot site is an option for this type of event, but hot sites are costly.
- If a hot site is not part of the plan, the organization should examine other potential locations within the facility or at other facilities to rebuild the computer systems.
- As with single system events, the DRP should identify how the organization will continue operations while the systems are rebuilt.

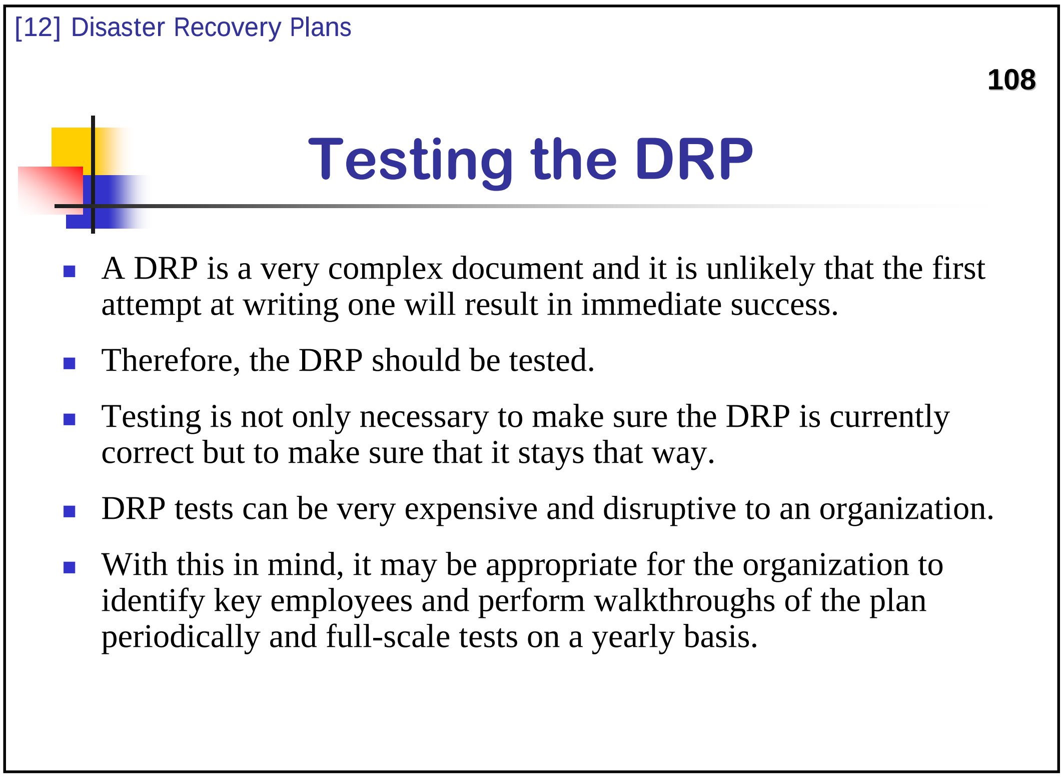


[12] Disaster Recovery Plans

107

Site Events

- These types of events are the least likely to occur but also the most damaging to an organization.
- For a DRP to plan for such events, every department of the organization must participate in its creation.
- The first step is for the organization to identify the critical capabilities that must be re-established in order for the organization to survive.
- If the organization is an e-commerce site, the most critical systems may be the computer systems and the network.
- On the other hand, if the organization manufactures some type of product, the manufacturing operation may be much higher priority than the computer systems



[12] Disaster Recovery Plans

108

Testing the DRP

- A DRP is a very complex document and it is unlikely that the first attempt at writing one will result in immediate success.
- Therefore, the DRP should be tested.
- Testing is not only necessary to make sure the DRP is currently correct but to make sure that it stays that way.
- DRP tests can be very expensive and disruptive to an organization.
- With this in mind, it may be appropriate for the organization to identify key employees and perform walkthroughs of the plan periodically and full-scale tests on a yearly basis.