

Disaster Recovery, Business Continuity, and Organizational Policies



Chapter 19

Objectives

- Describe the various ways backups are conducted and stored.
- Explain different strategies for alternative site processing.
- Describe the various components of a business continuity plan.
- Explain how policies and procedures play a daily role in addressing the security needs of an organization.



Disaster Recovery

- Disasters:
 - Organizations face a variety of disaster scenarios.
 - Natural and human disasters can halt organizational operations for some length of time.
 - The events are not specifically aimed at an organization.
 - Disaster recovery plans consider all types of organizational disruption.
 - Different disruptions will require different recovery strategies.

3



Disaster Recovery

- How to prepare for a disaster and plans to mitigate the disaster dictate how long operations are disrupted.
 - These events do not happen often.
 - It is more likely that business operations will be interrupted due to employee error.
- A good disaster recovery plan prepares an organization for any type of disruption.

4



Plans/Process


- A disaster recovery plan (DRP)
 - Defines the data and resources necessary and the steps to take in order to restore critical processes.
 - Physical resources
 - Computer hardware and software.
 - Personnel
 - Organizations need somebody who knows how to run the systems that process critical data.

5



Disaster Recovery Plans (DRP) / Process


- DRPs intended to minimize disaster impact.
 - Defines the data, resources, and necessary steps to restore critical organizational processes.
- Planning process, initial phase:
 - Consider needed resources to perform the company's mission.
 - Identify critical functions.
- Initial phase yields the business impact assessment (BIA).
- Continued planning includes:
 - Outline of processes and procedures to restore an organizations critical operations
 - Prioritized according to criticality for restoral



Categories of Business Functions

- Categorize the various functions an organization performs to develop a Business Impact Assessment and a DRP.
 - Categorization based on how critical or important the function is to a business operation.
- Those functions that are the most critical should be restored first.
 - The DRP should reflect this.

7



Category	Level of the Function's Need	How Long Can the Organization Last Without the Function
Critical	Absolutely essential for operations. Without the function, the basic mission of the organization cannot occur.	The function is needed immediately. The organization cannot function without it.
Necessary for normal processing	Required for normal processing, but the organization can live without it for a short period of time.	Can live without it for at most 30 days before your organization is severely impacted.
Desirable	Not needed for normal processing but enhances the organization's ability to conduct its mission efficiently.	Can live without the function for more than 30 days, but it is a function that will eventually need to be accomplished when normal operations are restored.
Optional	Nice to have but does not affect the operation of the organization.	Not essential, and no subsequent processing will be required to restore this function.
Consider eliminating	No discernable purpose for the function.	No impact to the organization; the function is not needed for any organizational purpose.

Important



Business Continuity Plan (BCP)

- Focuses on continued operation of a business in extenuating circumstances.
- Stronger emphasis placed on critical systems.
- Will describe the functions that are most critical, based on a previously conducted BIA.
- Will describe the order in which functions should be returned to operation.
- Describes what is needed for the business to continue to operate.



Differences between a BCP and a DRP

- The focus of a BCP is the continued operation of the business or organization.
- The focus of a DRP is on the recovery and rebuilding of the organization after a disaster has occurred.
- The DRP is part of the larger BCP because business continuity is always an issue.
- In a BCP, you will see a more significant emphasis placed on the critical systems the organization needs to operate.
- The BCP will describe the functions that are most critical, based on a previously conducted BIA, and will describe the order in which functions should be returned to operation.
- The BCP describes what is needed in order for the business to continue to operate.
 - In this situation, the two documents can be considered companion documents.



Back Ups

- Backups
 - Data that an organization relies on to conduct its daily operations.
 - Application programs needed to process the data.
 - The operating system and utilities that the hardware platform requires to run the applications.

- The DRP should also address other items related to backups such as:
 - Personnel
 - Equipment
 - Electrical power

11



Types of Backups

- Full backup
 - All data files, application files and system files are copied onto the storage media.
 - Restoration is straightforward.
 - All the files are copied back onto the system.
 - While this is easy to understand, it may take a considerable amount of time.

- Differential backup
 - Only the files and software that have changed since the last full backup should be stored.
 - It implies that periodically a full backup will be done.
 - The frequency of the full backup versus the interim differential backups depends on the organization and is part of its defined strategy

12



Types of Backups

- Differential Backup Restoration
 - Restoration requires two steps:
 - The last full backup is loaded.
 - The differential backup can be applied to update the files that have been changed since the full backup was conducted.
 - The time to accomplish the periodic differential backup is less than a full backup.
 - If the period of time between differential backups is long, or if files change frequently, the differential backup is like a full backup.

13



Types of Backups

- Incremental backup
 - A variation on a differential backup.
 - Incremental backup relies on occasional full backups.
 - After that, only those files that have changed since the last backup need to be backed up.
- Incremental Backup Restoration
 - Requires more work.
 - Go back to the last full backup and reload the system with this data.
 - Then update the system with every incremental backup.
 - Advantage - requires less storage and time to accomplish.

14

Types of Backups

- Delta backup
 - Saves as little information as possible each time you conduct a backup.
 - An occasional full backup must be conducted.
 - Later, when a delta backup is conducted at specific intervals, only the portions of the files that have been changed will be stored.
 - Advantage
 - Only the information within files that has changed will be backed up.
 - Disadvantage
 - Restoration is a complex process since it requires more than just loading a file.
 - Requires that application software be run to update the records in the files that have been changed.

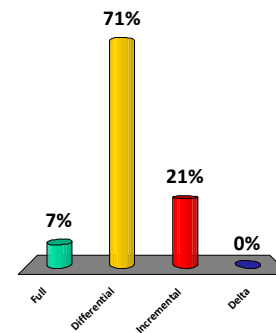
15

Characteristics of Different Backup Types

	Full	Differential	Incremental	Delta
Amount of Space	Large	Medium	Medium	Small
Restoration	Simple	Simple	Involved	Complex

In which backup strategy are only those portions of the files and software that have changed since the last backup backed up

1. Full
2. Differential
3. Incremental
- 😊 4. Delta



Backup Frequency and Retention

- The usefulness of a backup is related to the number of changes since the backup was created.
- How frequently should backups be performed?
 - How long an organization can survive without current data.
- Maintain Multiple backups
 - If the reason for restoring from the backup is the discovery of an intruder in the system – restore the system to its pre-intrusion state.
 - If multiple backups are maintained at intervals, it is easier to return to a point before the intrusion, security, or operational event occurred.



Backup Rule of Three

- There are several strategies or approaches to backup retention and a common and easy to remember is the “rule of three.”
 - This entails simply keeping the three most recent backups.

- When a new backup is created, the oldest copy is overwritten.
 - In certain environments, regulatory issues may prescribe a specific frequency and retention period.
 - It is important to know an organization and its requirements when determining how often a backup will be created and how long will it be kept.

19



Backups Storage

- Backups in separate locations.
 - The most recent copy could be stored locally, as it is the most likely to be needed.
 - Other copies can be kept at other locations.
- Online backup services.
 - A number of third-party companies offer high-speed connections for storing data on a frequent basis.
 - Using network connections reduces concerns with physical movement of more traditional storage media.

20



Alternate Sites

- Where should restoration services be conducted?
 - If an organization has suffered physical damage to a facility, having offsite storage of data is only part of the solution.
 - Data needs to be processed somewhere.
 - Computing facilities similar to those used in normal operations must be found.

21



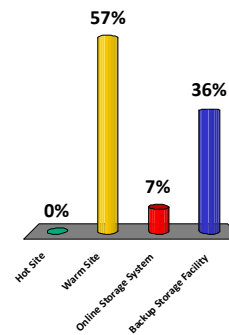
Alternate Sites

- Hot site
 - Fully configured environment similar to the normal operating environment.
- Warm
 - Partially configured, usually having the peripherals and software but perhaps not the more expensive main processing computer.
- Cold site
 - Basic environmental controls needed to operate. Has few computing components needed.
- Mobile backup
 - Trailers with the required computers and electrical power that can be driven to a location within hours of a disaster and set up to commence processing immediately.

22


Which of the following is the name for a partially configured environment that has the peripherals and software that the normal processing facility contains and that can be operational within a few days?

1. Hot Site
2. Warm Site
3. Online Storage System
4. Backup Storage Facility




Strategies for Backups

- Considerations for backup strategies include:
 - Size of the backup
 - The cost of the backup media
 - Time required to conduct the backup
 - Who will be responsible for conducting the backup?
 - What software and hardware are needed?
 - Where the backups will be stored?
 - When will the backups be performed?
 - The frequency with which backups are created
 - How long will the backups be maintained?



- Optimal backup frequency Criteria:
 - The cost of the backup strategy chosen.
 - The cost of recovery if the backup strategy is not implemented (meaning if there were no backups created).

25

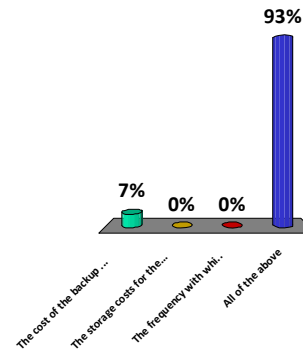


- Cost of the backup strategy:
 - The cost of the backup media required for a single backup
 - The storage costs
 - The labor costs
 - The frequency with which backups are created

26

Which of the following is a consideration in calculating the cost of a backup strategy?

1. The cost of the backup media
2. The storage costs for the backup media
3. The frequency with which backups are created
4. All of the above



Utilities

- Computers and networks require power to operate
 - Emergency power must be planned for in case of disruption.
- UPS
 - For short-term power interruptions
 - Enough to keep a system running should power only be lost for a few minutes.
 - Enough to allow administrators to halt the system or network.
- Back up Generators:
 - Long term interruptions, Back up power
 - Ensure the reserve capacity is beyond the anticipated load
 - Needs testing on regular basis
 - Expensive, require fuel



Utilities

- Communication
 - Telephone and Internet communication may be lost.
 - Wireless services may also not be available.
 - Planning redundant communication can help with most outages.
 - Backup plans should include the option to continue operations from a different location while waiting for communications to be restored.

29



Secure Recovery

- Provide power, communications, and technical support.
- Offer a secure operating environment.
- Provide restoration of critical files and data.



Cloud Computing

- Allows for the contracting of functions like e-mail and file storage to third parties
- Can be more cost effective but also comes with inherent risks

- Pushing computing into the cloud may make good business sense from a cost perspective,
- but doing so does not change the fact that your organization is still responsible for ensuring that all the appropriate security measures are properly in place.
 - How are backups being performed?
 - What plan is in place for disaster recovery?
 - How frequently are systems patched? What is the service-level agreement (SLA) associated with the systems?



High Availability and Fault Tolerance

- High availability
 - The ability to maintain data and operational processing despite any disruption.
 - Requires redundant systems for both power and processing.
 - If one system fails, the other can take over operations without a break in service.

- Fault tolerance
 - Refers to availability and is accomplished by the mirroring of data and systems.
 - Should a “fault” occur that disrupts a device such as a disk controller, the mirrored system provides the requested data with no interruption in service.



Increasing Reliability

- Redundant Array of Independent Disks (RAID).
 - RAID can mitigate availability problems caused by disk failures.
 - Redundant systems and spare parts also serve to decrease availability issues.
- Varieties of RAIDs
 - RAID 0
 - Spread data out to speed access but with no redundancy to improve reliability
 - RAID 1
 - Implement exact copies of disks so that all data is mirrored on another drive providing complete redundancy.
 - extremely expensive .
 - RAID 5
 - Spreads data across disks and adds parity in a manner such that the loss of any single disk in the array will not result in the loss of any data



Spare Parts and Redundancy

- Common applications of redundancy
 - Redundant servers
 - Redundant connections
 - Redundant ISPs
 - Spare parts



Computer Incident Response Teams (CIRT)

- Investigate incidents, advise on how to proceed.
- CIRTs should consist of permanent and ad hoc team members.
- Details of CIRT team should be finalized before an incident occurs.
- Includes individuals with technical and non-technical individuals who provide guidance on ways to handle media attention, legal issues, management issues.
- Conducts investigations of the incident and makes recommendations about how to proceed.
 - Policies and procedures for investigation should also be worked out in advance.
 - It is also advisable to have the team periodically meet to review these procedures.



Test, Exercise, and Rehearse

- Test BCP, DRP, backup procedures, or method to address computer incidents and other plans.
 - This ensures that they are sufficient and that all key individuals know what their role is.
- Conduct Exercises
 - Ensure that the procedures and technology will work in case of a real life incident.
 - Care should be taken not to impact actual operations.
- Rehearse
 - Items that are disruptive to actual operations.

Policies and Procedures

- Policies
 - High-level statements made by the management laying out an organization's position on some issue.
 - Mandatory but are not specific in their details.
 - Focused on the result – not the methods for achieving that result.

- Procedures
 - Step-by-step instructions describing exactly how employees are expected to act in a given situation or to accomplish a specific task.

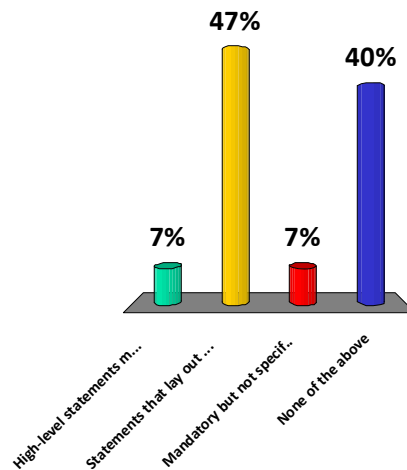
- Standards
 - Mandatory elements regarding the implementation of policy in detail.

Also see Chap. 2

37

Standards are:

1. High-level statements made by management
2. Statements that lay out the organization's position on some issue
3. Mandatory but not specific in their details
- 😊 4. None of the above





Security Policies

- Security policies define high-level goals for security for an organization.
- Other more specific policies include:
 - Acceptable use policy
 - Internet usage policy
 - Email usage policy
 - Due care and due diligence



Additional Security Policies

- Prudent person principle
- Separation of duties
- Need to know and least privilege
- Password management
- Disposal and destruction
- Change management policy
- Classification of information



Security Policies

- Security policy
 - High-level statement produced by senior management that outlines what security means to the organization.
 - States the organization's goals are for security.
 - Describe how security is handled from an organizational point of view.
 - It describes which office and corporate officer or manager oversees the organization's security program.
 - Should be reviewed regularly and updated as needed.
 - Should be updated less frequently than the procedures that implement them.
 - High-level goals do not change as often as the environment in which they must be implemented.
 - All policies should also be reviewed by a legal counsel.

41



Acceptable Use

- Acceptable use policy (AUP)
 - Outlines the appropriate use of company resources, computer systems, and networks.
 - Organizations should be concerned with the personal use of organizational assets which do not benefit the company.
- A good policy ensures employee productivity while limiting liability through inappropriate use of the assets. It should delineate what activities are not allowed

42



Internet Usage Policy

- Internet usage policy
 - Ensures employee productivity and limits liability from inappropriate use of the Internet in a workplace.
 - Addresses which sites employees are allowed to visit.
 - If the company allows employees to surf the Web during non-work hours, the policy should spell out acceptable parameters including times and prohibited sites.


43



E-Mail Usage Policy

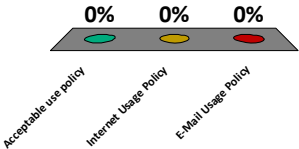
- The e-mail usage policy like the Internet usage policy.
 - States what the company will allow employees to send in terms of e-mail.
 - The policy should spell out if non-work e-mail traffic is allowed or is restricted.
 - should cover the type of message that would be considered inappropriate to send to other employees.
 - Should specify any disclaimers that must be attached to an employee's message sent outside the company.

44




_____ Outlines the appropriate use of company resources, computer systems, and networks.

1. Acceptable use policy
2. Internet Usage Policy
3. E-Mail Usage Policy



Policy Category	Completion Rate
Acceptable use policy	0%
Internet Usage Policy	0%
E-Mail Usage Policy	0%



Separation of Duties

- Separation of duties
 - Principle employed in many organizations to ensure that no single individual has the ability to conduct transactions alone.
 - Spreads responsibilities over an organization so no single individual becomes indispensable.
 - Each task should have a primary and backup person.
 - Trust in any one individual is lessened.
 - No one has the “keys to the kingdom” or unique knowledge about how the system works.
 - The risk of catastrophic damage to the organization is also decreased.
 - Good practice as a security tool

46



Privacy Policy

- Explains the guiding principles used to guard personal data they access.
 - Customers have a legal right to expect that their information is kept private.
 - Organizations violating this trust may be sued.
- Privacy policy should be completed detailing how information is safeguarded.
- Privacy is enforced by law for some organizations.
- Personally Identifiable Information (PII) is becoming increasingly important to safeguard.
 - In the field of health care, federal regulations have been created that prescribe stringent security controls on private information.

47



Human Resources Policies

- People are the weakest link in security.
- Specific policies should be developed regarding:
 - New hire screening processes
 - Periodic review process for current employees
 - Employee termination process
 - Mandatory vacation to uncover wrongdoing



Employee Retirement, Separation, or Termination

- Employees who retire by choice may announce their retirement weeks or even months in advance.
 - Limiting access to sensitive documents the moment they announce their intention is the safest thing to do.
 - It may not be necessary.
- Each situation should be evaluated individually.
 - When an employee decides to leave a company, for a new job, continued access to sensitive information should be carefully considered.
 - If the employee leaves with hard feelings, it is wise to revoke the access privileges as soon as possible.

49



Employee Retirement, Separation, or Termination

- If they leave for a better job, you may decide to allow them to gracefully transfer their projects to other employees.
 - The decision should be considered carefully if the new company is a competitor.

50



Employee Retirement, Separation, or Termination

- If the employee is terminated, they may become disgruntled.
 - Immediately revoke their access privileges to sensitive information and facilities.
 - Access cards, keys, and badges should be collected.
 - The employee should be escorted to their desk and watched as they pack their personal belongings.
 - They should be escorted from the building.
 - Combinations should be changed quickly once they have been informed of their termination.

51



Code of Ethics

- Describes expected behavior from a high-level standpoint
- Sets tone for employee conduct
- Encourages integrity and high ethical standards



Incident Response Policies and Procedures

- Several phases should be covered in an incident response policy:
 - Preparation
 - Detection
 - Containment and eradication
 - Recovery
 - Follow-up actions



Preparation

- Preparing for an incident is the first phase.
 - The steps to be taken when an incident is discovered or suspected should be established.
 - Determine the points of contact
 - Employees training.
 - Incident response Strategy
 - Additional training such as computer forensics

- Organization's legal counsel should be part of the team
- The public affairs office should be available on an as-needed basis.
 - It is their responsibility to formulate the public response should the event become public.



Detection

- Procedures should be established to describe the process that administrators will use to check for possible security events.
- The tools should be identified during the preparation phase described.
- Any required training to operate the equipment should also be acquired.

55



Detection

- A technique used by intruders to acquire information useful in gaining access to computer systems, networks, or physical facilities is social engineering.
 - Anyone in the organization may be the target of a social engineering attack.
 - All employees need to know what to look for when faced with this type of attack.
- Training is essential to thwart social engineering attacks.
 - The organization should have a policy on who will be required to receive this type of training and how frequently they should receive it.
- Whatever the type of security incident suspected, and whoever suspects it, a reporting procedure needs to be in place for the employees.

56



Containment and Eradication

- The team should quickly contain the problem.
- Decide whether to restore operations or prosecute.
- If the decision to prosecute is made, specific procedures need to be followed in handling potential evidence.
Another decision that should be made quickly is how to address containment.
- If an intruder is on the system, one response is to disconnect from the Internet until the system can be restored and vulnerabilities patched.

57



Recovery

- Recovery activities
 - Assess the situation to determine what actually occurred.
 - Begin recovery based on assessment.
 - May involve use of BCP to return business back to normal operation.

58



Follow-On Actions

- Once the operations have been restored to their pre-incident state, a few details need to be taken care of.
 - Senior-level management should be informed of what occurred.
 - Recommendations should be made to improve processes and policies so that a repeat will not occur.
 - If prosecution of the individual responsible is desired, then additional time will be spent in helping law enforcement agencies and in possible testimony.
 - Training material should be developed or modified as part of the new policies and procedures.