Chapter 12
Contingency Planning
Learning Objectives

- Recognize the need for contingency planning
- Describe the major components of contingency planning
- Create a simple set of contingency plans, using business impact analysis
- Prepare and execute a test of contingency plans
- Explain the unified contingency plan approach
- Discuss the reasons for sound backup and recovery practices and know the elements that comprise backup and recovery techniques
An organization’s ability to weather losses caused by unexpected events depends on proper planning and execution of such plans.

Without a workable plan, unexpected events can cause severe damage to information resources and assets.

According to The Hartford insurance company: “On average, over 40% of businesses that don’t have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm.”
What Is Contingency Planning?

- Contingency planning (CP): overall process of preparing for unexpected events
- Main goal: restore normal modes of operation with minimal cost and disruption to normal business activities after unexpected event
- Ideally, should ensure continuous information systems availability despite unexpected events
What Is Contingency Planning?
(continued)

- Consists of four major components:
  - Business impact analysis (BIA)
  - Incident response plan (IR plan)
  - Disaster recovery plan (DR plan)
  - Business continuity plan (BC plan)

- Components can be created/developed:
  - As one unified plan or
  - Separately in conjunction with set of interlocking procedures that assure continuity
Contingency planning and operations teams:

- **CP team**: collects data about information systems and threats, conducts business impact analysis, creates contingency plans for incident response, disaster recovery, business continuity
- **IR team**: manages/executes IR plan by detecting, evaluating, responding to incidents
- **DR team**: manages/executes DR plan by detecting, evaluating, responding to disasters; reestablishes primary site operations
- **BC team**: manages/executes BC plan by establishing off-site operations
Contingency Planning Implementation Timeline

IRP: Incident Detection → Incident Reaction → Incident Recovery → Incident Resolved Operations Restored End IRP

(If incident classified as disaster)

DRP: Disaster Reaction → Disaster Recovery (Restore Operations at Primary Site)

(If disaster requires off-site operations)

BCP: Continuity Reaction → Alternate Site Operations

Primary Operations Restored End DRP/BCP

Attack occurs → Post-attack (hours) → Post-attack (days)
Components of Contingency Planning

- Business impact analysis (BIA):
  - First phase in CP process
  - Provides data about systems and threats faced
  - Provides detailed scenarios/effects of attacks

- CP team conducts BIA in the following stages:
  - Threat attack identification and prioritization
  - Business unit analysis
  - Attack success scenario development
  - Potential damage assessment
  - Subordinate plan classification
Major Tasks in Contingency Planning

- Business Impact Analysis (BIA)
  - Threat Attack Identification and Prioritization
  - Business Unit Analysis
  - Attack Success Scenario Development
  - Potential Damage Assessment
  - Subordinate Plan Classification

- Incident Response Planning
  - Incident Planning
  - Incident Detection
  - Incident Reaction
  - Incident Recovery

- Disaster Recovery Planning
  - Plan for Disaster Recovery
  - Crisis Management
  - Recovery Operations

- Business Continuity Planning
  - Establish Continuity Strategies
  - Plan for Continuity of Operation
  - Continuity Management
Incident Response Plan

- Document specifying actions an organization can and perhaps should take while incident is in progress
- Deals with identification, classification, response, and recovery from an incident
- Incident: any clearly identified attack on information assets that threaten the assets’ confidentiality, integrity, or availability
Absence of well-defined procedures can lead to:

- Extensive damage to data, systems, and networks, resulting in increased costs, loss of productivity, and loss of business
- Possibility of intrusion affecting multiple systems both inside and outside the organization
- Negative media exposure that can damage the organization’s stature and reputation
- Possible legal liability/prosecution for failure to exercise adequate standard of due care when systems are inadvertently or intentionally used to attack others
Disaster Recovery Plan

- Entails preparation for and recovery from disaster, whether natural or human-made
- Key role: defining how to reestablish operations at location where organization is usually located
- Some incidents are immediately classified as disasters (extensive fire, flood, earthquake, etc.)
- In general, disaster has occurred when either:
  - Organization is unable to contain or control the impact of an incident or
  - Level of damage/destruction from an incident is so severe organization cannot quickly recover
Business Continuity Plan

- Ensures that critical business functions can continue if a disaster occurs
- Activated/executed concurrently with DR plan when disaster is major or long term and requires fuller and complex restoration of IT resources
- Reestablishes critical business functions at an alternate site while DR plan team focuses on reestablishment of primary site
- Not every business needs such a plan or such facilities
Incident response (IR): set of procedures that commence when an incident is detected.

IR planning (IRP) follows these general stages:
- Form IR planning team
- Develop IR policy
- Organize security incident response team (SIRT)
- Develop IR plan
- Develop IR procedures

For each attack scenario end case, IR team creates procedures to be deployed during, after, and before the incident.
Planning for the Response During the Incident

- Most important phase of the IR plan is the reaction to the incident
- Each viable attack scenario end case is examined and discussed by the IR team:
  - Trigger (circumstances that cause IR team activation and IR plan initiation)
  - What must be done to react to the particular situation (source, extent of damage)
  - How to stop the incident if it is ongoing
  - Elimination of problem source
Planning for After the Incident

- During this phase, the goal is to return each system to its previous state.
- IR plan must describe stages necessary to recover from most likely events of the incident.
- It should also detail other events, like protection from follow-on incidents, forensic analysis, and the after-action review.
- After-action review (AAR): detailed examination of events that occurred from first detection to final recovery.
Planning for Before the Incident

- Consists of both preventative measures to manage risks associated with particular attack and activities to ensure IR team preparedness
- Process includes:
  - Training the SIRT
  - Testing the IR plan
  - Selecting and maintaining tools used by the SIRT
  - Training users of the systems and procedures controlled by the organization
Incident Classification and Detection

- Incident classification: process of evaluating organizational events, determining which events are incident candidates, and then determining whether it is an actual incident or a nonevent.
- IR design team creates process used to make this judgment; IR team actually classifies events.
- Incident candidates can be detected and tracked via reports from end users, intrusion detection systems, virus management software, and systems administrators.
Classifying Incidents

- D.L. Pipkin identified three broad categories of incident indicators: possible, probable, definite
- Four types of possible actual incidents are:
  - Presence of unfamiliar files
  - Presence or execution of unknown programs or processes
  - Unusual consumption of computing resources
  - Unusual system crashes
Classifying Incidents (continued)

- Four probable indicators of actual incidents:
  - Activities at unexpected times
  - Presence of new accounts
  - Reported attacks
  - Notification from IDS

- Five events are definite indicators of an incident:
  - Use of dormant accounts
  - Modified or missing logs
  - Presence of hacker tools
  - Notifications by partner or peer
  - Notification by hacker
Classifying Incidents (continued)

- In addition, the following events indicate that an incident is underway:
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality
  - Violation of policy
  - Violation of law
Data Collection

- Routine collection/analysis of data is required to properly detect/declare incidents
- Logs should be enabled, stored off entity that generates them, stored in hardened location
- Managing logs involves the following:
  - Be prepared for amount of data generated
  - Rotate logs on a schedule
  - Archive logs
  - Encrypt logs
  - Dispose of logs
Detecting Compromised Software

- If systems that monitor network, servers, or other components are compromised, then incident detection is compromised.
- Some organizations use separate Intrusion Detection System (IDS) sensor or agents monitor the IDS itself.
- If detection systems have been compromised, quarantine them and examine installation by comparing them to either original installation files or to insulated installation.
Challenges in Intrusion Detection

- Detection of intrusions can be tedious and technically demanding
- Only those with appropriate advanced technical skills can manually detect signs of intrusion through reviews of logs, system performance, user feedback, system processes and tasks
- Two key facets of incident detection:
  - Effective use of technology to assist in detection
  - Necessity of cooperation between incident response, information security professionals, and entire information technology department
Incident Reaction

- How and when to activate IR plans determined by IR strategy organization chooses to pursue
- In formulating incident response strategy, many factors influence an organization’s decision
- IR plan designed to stop incident, mitigate effects, provide data that facilitates recovery
- Two general categories of strategic approach for an organization as it responds to an incident:
  - Protect and forget
  - Apprehend and prosecute
Notification

- As soon as IR team determines an incident is in progress, appropriate people must be notified in the correct order
- Alert roster: document containing contact info for individuals to be notified during an incident
- Two ways to activate alert roster:
  - Sequentially
  - Hierarchically
- Alert message: scripted description of incident containing enough info for each responder to know what to do without impeding alert process
Documenting an Incident

- Should begin immediately after incident is confirmed and notification process is underway
- Record who, what, when, where, why, and how of each action taken while incident is occurring
- Afterward, serves as case study to determine whether right and effective actions were taken
- Helps prove the organization did everything possible to prevent spread of the incident
- Can also be used as simulation in future training sessions on future versions of IR plan
One of the most critical components of IR is stopping incident or containing its scope/impact.

Affected areas must be identified.

Incident containment strategies focus on two tasks:
- Stopping the incident
- Recovering control of the affected systems

IR team can attempt to stop incident and try to recover control by means of several strategies.
Interviewing Individuals Involved in the Incident

- Part of determining scale, scope, impact of an incident is collection of information from those reporting the incident and responsible for systems impacted by the incident.

- Interviews involve three groups of stakeholders:
  - End users
  - Help desk personnel
  - Systems administrators

- Each group provides a different perspective of the incident as well as clues to its origin, cause, and impact.
Recovering from Incidents

- Once incident is contained and system control regained, incident recovery can begin
- Incident damage assessment: immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets
- Steps to be taken in the recovery process:
  - Identify and resolve vulnerabilities
  - Restore data
  - Restore services and processes
  - Restore confidence across the organization
The After-Action Review

Ongoing IR plan maintenance includes procedures to:
- Conduct after-action reviews
- Plan review and maintenance
- Train staff involved in incident response
- Rehearse process that maintains readiness for all aspects of the incident plan

IR team must conduct after-action review, detailed examination of events during incident

AAR serves as review tool, historical record, case training tool, closure
IR Plan Review and Maintenance

- At periodic intervals, an assigned member of management should review the IR plan.
- When shortcomings are noted, the plan should be reviewed and revised to remediate deficiencies.
- Organization must undertake training programs to ensure a sufficient pool of qualified staff are available to execute the plan when activated.
- Ongoing and systematic approach to planning requires plans be rehearsed until responders are prepared to perform as expected.
Data and Application Resumption

- There are a number of data backup and management methods that aid in preparation for incident response
- Backup methods must be founded in an established policy that meets organizational needs
- In general, data files and critical system files should be backed up daily; nonessential files backed up weekly
- Equally important is determination of how long data should be stored
Disk-to-Disk-to-Tape

- With decrease in costs of storage media, more and more organizations are creating massive arrays of independent but large-capacity disk drives to store information.
- Libraries of these devices can be built to support massive data backup and recovery.
- Problem with this technology is lack of redundancy should both online and backup versions fail.
- Secondary data disks should be backed up to tape or other removable media periodically.
Backup Strategies

- Three basic types of backups:
  - Full: full and complete backup of entire system
  - Differential: storage of all files that have changed or been added since last full backup
  - Incremental: only archives data that have been modified that day
Backup Strategies (continued)

Backup strategy guidelines:

- All on-site and off-site storage must be secured.
- Common practice to use media-certified fireproof safes or filing cabinets to store backup media.
- Off-site storage in particular must be in a safe location (bank, backup and recovery service, etc.).
- Use conditioned environment for media (airtight, humidity-controlled, static-free storage container).
- Clearly label and write protect each media unit.
- Retire individual media units before they reach the end of their useful life.
Tape Backup and Recovery

- Most common backup schedule is daily on-site, incremental, or differential backup, with weekly off-site full backup
- Most backups are conducted during twilight hours, when systems activity is lowest and probability of user interruption limited
- Classic methods for selecting files to back up:
  - Six-tape rotation
  - Grandfather-Father-Son
  - Towers of Hanoi
Redundancy-Based Backup and Recovery Using RAID

- Redundant array of independent disks (RAID)
- Uses number of hard drives to store information across multiple drive units
- For operational redundancy, can spread out data and, when coupled with checksums, can eliminate or reduce impact of hard drive failure
- Many RAID configurations (called levels)
Database and Application Backups

- Systems that use databases, regardless of type, require special backup and recovery procedures

Database backup considerations include:
- May not be able to back up database with utilities provided with server operating systems
- Can system backup procedures be used without interrupting use of the database
- Is database using special journal file systems that enable database concurrency functions

Some applications use file systems in ways that invalidate customary backup and recovery
Real-Time Protection, Server Recovery, and Application Recovery

- Some strategies seek to improve robustness of servers or systems in addition to or instead of performing data backups
- Mirroring provides real-time protection and data backup via duplication of server data storage using multiple hard drive volumes (RAID 1)
- One method of server recovery and redundancy uses hot, warm, and cold servers
- Another option for online backup and application availability is server clustering
Electronic Vaulting

- Bulk transfer of data in batches to off-site facility
- Transfer usually conducted via dedicated network links or data communications services provided for a fee
- Can be more expensive than tape backup and slower than data mirroring, so should be used only for data that warrants additional expense
- Can be performed over public infrastructure, but data must be encrypted while in transit, which can slow data transfer rate
Remote Journaling

- Transfer of live transactions to an off-site facility
- Differs from electronic vaulting:
  - Only transaction data is transferred, not archived data
  - Transfer is performed online and much closer to real time
Database Shadowing

- The propagation of transactions to a remote copy of the database
- Combines electronic vaulting with remote journaling, applying transactions to database simultaneously in two separate locations
- Shadowing techniques generally used by organizations needing immediate data recovery
- "Shadowed" database available for reading and writing, thus serving as dynamic off-site backup
- Database shadowing works well for read-only functions
Network-Attached Storage and Storage Area Networks

- NAS usually implemented via a device attached to a network; uses common communications methods to provide online storage
- NAS/SANs similar but implemented differently
- NAS uses TCP/IP-based protocols; SANs use fibre-channel or iSCSI connections between systems and storage devices themselves
- For general file sharing or data backup, NAS provides less expensive solution
- For high-speed and higher-security solutions, SANs may be preferable
Service Agreements

- Contractual documents guaranteeing certain minimum levels of service provided by vendors
- Effective service agreement should contain the following sections:
  - Definition of applicable parties
  - Services to be provided by the vendor
  - Fees and payments for these services
  - Statements of indemnification
  - Nondisclosure agreements and intellectual property assurances
  - Noncompetitive agreements
Chapter Summary

- Contingency planning: process of positioning an organization to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets.
- Goal of CP is to restore normal operations after an unexpected event.
- Business impact analysis (BIA), first phase in the CP process, provides CP team with information about systems and threats they face.
Chapter Summary (continued)

- Actions an organization should take while incident is in progress should be defined in incident response plan (IR plan)
- Disaster recovery planning (DRP) entails preparations for and recovery from disaster, whether natural or human-made
- Business continuity planning (BCP) ensures critical business functions can continue if disaster occurs
Incident classification: process of determining which events are possible incidents

Three broad categories of incident indicators established: possible, probable, definite

Routine collection and analysis of data required to properly detect and declare incidents

How and when to activate IR plans determined by IR strategy organization chooses to pursue

Two general strategies govern how organization responds to an incident: protect and forget or apprehend and prosecute
One of the most critical components of IR is stopping incident or containing its scope/impact.

Incident containment strategies vary depending on incident and amount of damage caused.

Once incident has been contained and system control has been regained, incident recovery can begin.

IR team must assess full extent of damage to determine what is needed to restore systems.
Ongoing maintenance of IR plan includes:
- Effective after-action reviews
- Planned review and maintenance
- Training staff involved in incident response
- Rehearsing process that maintains IR readiness

Number of data backup/management methods that aid in preparation for incident response

Most commonly used varieties are disk backup and tape backup

Backup method must be founded in established policy that meets organizational needs