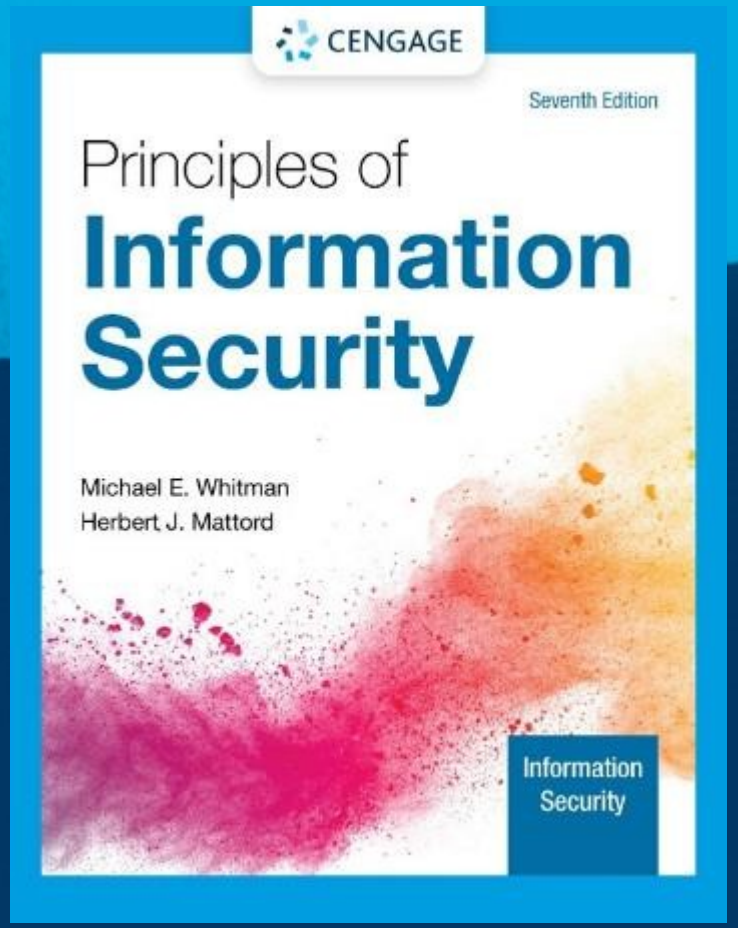

Module 5

Incident Response and Contingency Planning

Learning Objectives

Upon completion of this material, you should be able to:

5.1 Discuss the need for contingency planning

5.2 Describe the major components of incident response, disaster recovery, and business continuity

5.3 Define the components of crisis management

5.4 Discuss how the organization would prepare and execute a test of contingency plans

Introduction to Incident Response and Contingency Planning

- This module focuses on another type of planning—plans that are made for unexpected adverse events—when the use of technology is disrupted, and business operations can come to a standstill.
- An organization's ability to weather losses caused by an adverse event depends on proper planning and execution of such a plan, without which an adverse event can cause severe damage to an organization's information resources and assets from which it may never recover.
- According to the Hartford insurance company, over 40 percent of businesses that don't have a disaster plan go out of business after a major loss.

Fundamentals of Contingency Planning (1 of 2)

- The overall planning for unexpected **adverse events** is called **contingency planning (CP).**
- It is how communities of interest position their organizational units to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets.
- The main goal of CP is to restore normal modes of operation with minimum cost and disruption to normal business activities after an unexpected adverse event.

Fundamentals of Contingency Planning (2 of 2)

- CP consists of four major components:
  - Business impact analysis (BIA)
  - Incident response plan (IR plan)
  - Disaster recovery plan (DR plan)
  - Business continuity plan (BC plan)
- Depending on the organization's size and business philosophy, IT and InfoSec managers can either
  - Create and develop these four CP components as one unified plan or
  - Create the four separately in conjunction with a set of interlocking procedures that enable continuity

Knowledge Check Activity 1

Each of these is a major component of contingency planning EXCEPT _____.

a. incident response plan

b. business continuity plan

c. business loss analysis

d. disaster recovery plan

Knowledge Check Activity n: Answer

Each of these is a major component of contingency planning EXCEPT _____.

Answer: c. business loss analysis

Explanation.

The business impact analysis, or BIA, is much broader in its scope than a simple (potential) loss analysis would be. It includes impact to the organization and the relationships to other parts of the organization as well.

NIST CP Methodology

- Once formed, the **contingency planning management team (CPMT)** begins developing a CP document, for which NIST recommends using the following steps:
  1. Develop the CP policy statement.
  2. Conduct the BIA.
  3. Identify preventive controls.
  4. Create contingency strategies.
  5. Develop a contingency plan.
  6. Ensure plan testing, training, and exercises.
  7. Ensure plan maintenance.

CP Policy Components

- An introductory statement by senior management
- The scope and purpose of the CP operations
- A call for periodic risk assessment and BIA by the CPMT
- A description of the major components of the CP
- A call for, and guidance in, the selection of recovery options and business continuity strategies
- A requirement to test the various plans on a regular basis
- Identification of key regulations and standards that impact CP planning and a brief overview of their relevancy
- Identification of key individuals responsible for CP operations
- An appeal for support to the individual members of the organizations
- Additional administrative information

Individuals and Teams involved in CP

- The CPMT includes:
  - Champion
  - Project manager
  - Team members
    - Business managers
    - Information technology managers
    - Information security managers
    - Representatives of the supplemental planning teams (IR, DR, BC, CM)

Contingency Planning Hierarchies

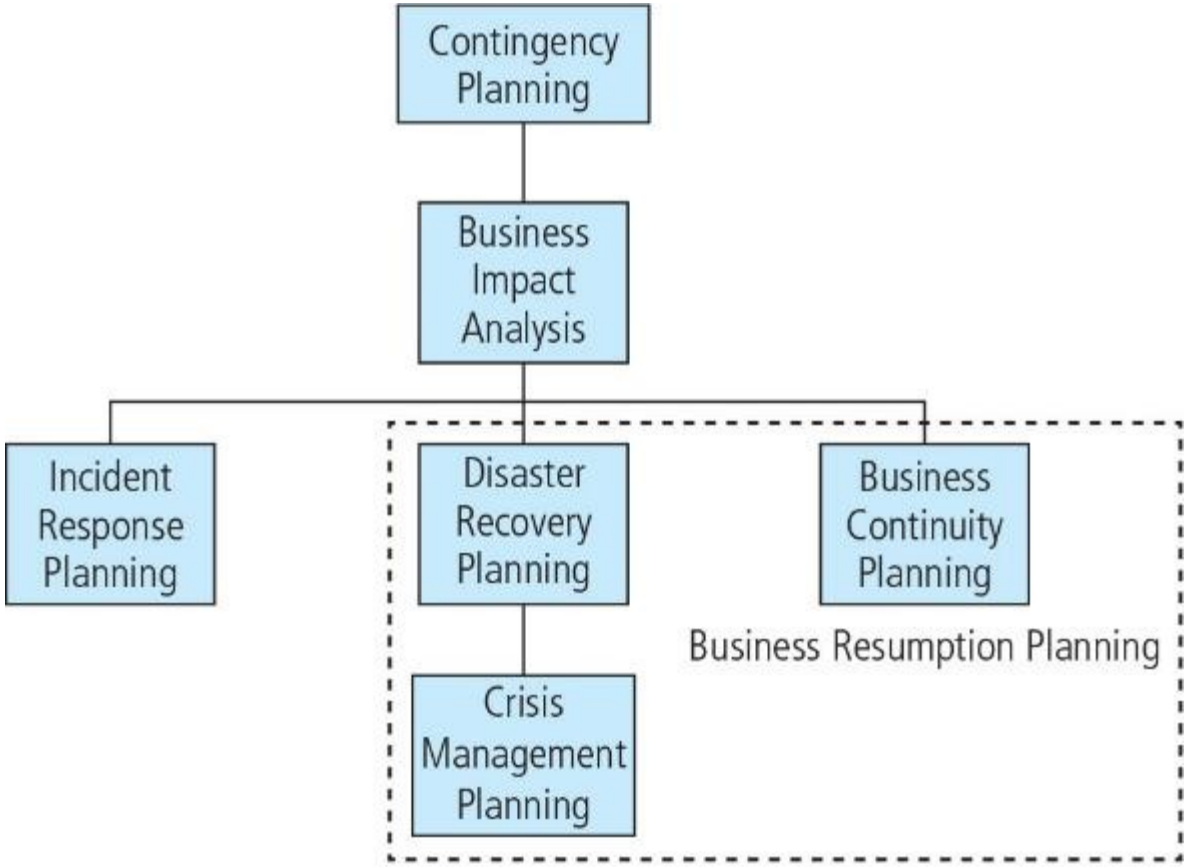

Figure 5-1 Contingency planning hierarchies

Contingency Planning Life Cycle

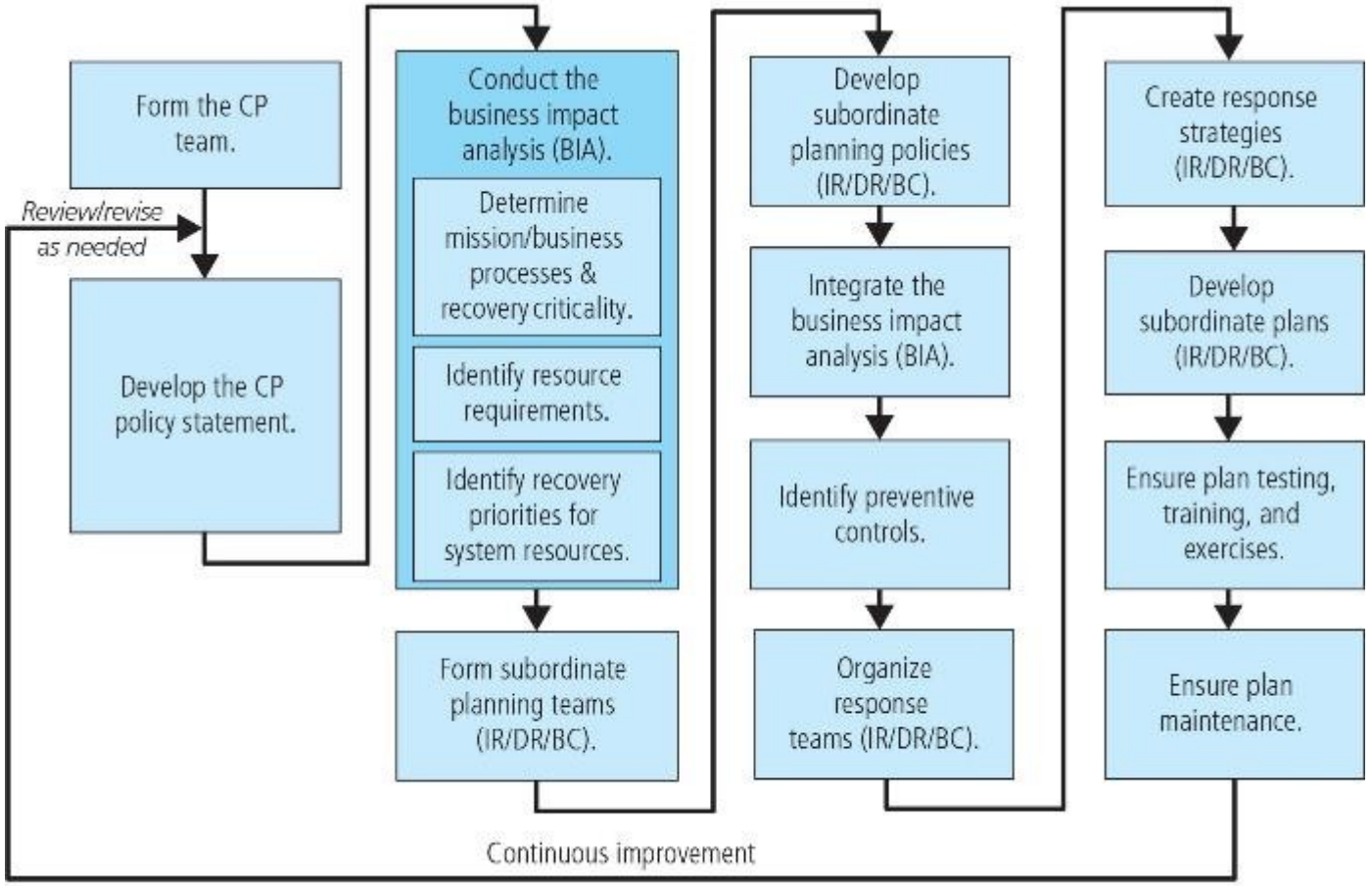

Figure 5-2 Contingency planning life cycle

Business Impact Analysis

- The **business impact analysis (BIA)** is the first phase of the CP process and serves as an investigation and assessment of the impact that various adverse events can have on the organization.
- One of the fundamental differences between a BIA and risk management is that risk management focuses on identifying the threats, vulnerabilities, and attacks to determine which controls can protect the information.
- The BIA assumes that these controls have been bypassed, have failed, or have otherwise proved ineffective, that the attack succeeded, and that the adversity that was being defended against has been successful.

Business Impact Analysis (BIA) (1 of 2)

- The BIA begins with the prioritized list of threats and vulnerabilities identified in the risk management process and enhances the list by adding the information needed to respond to the adversity.
- When undertaking the BIA, the organization should consider:
  - Scope
  - Plan
  - Balance
  - Objective
  - Follow-up

Business Impact Analysis (BIA) (2 of 2)

- According to NIST SP 800-34, Rev. 1, the CPMT conducts the BIA in three stages:
  - Determine mission/business processes and recovery criticality.
  - Identify resource requirements.
  - Identify recovery priorities for system resources.

Determine Business Process and Recovery Criticality (1 of 2)

- The first major BIA task is the analysis and prioritization of business processes within the organization, based on their relationship to the organization's mission.
- Each business department, unit, or division must be independently evaluated to determine how important its functions are to the organization as a whole.
- A weighted analysis table can be useful in evaluating business functions.
- The BIA questionnaire is useful in identifying and collecting information about business functions for analysis.

Example of Weighted Table Analysis of Business Processes (1 of 2)

	Criterion	*Impact on Revenue*	*Impact on Profitability*	*Impact on Product/Service Delivery*	*Impact on Market Share*	*Impact on Reputation*		
#	**Criterion Weight Business Process**	*0.25*	*0.3*	*0. 15*	*0.2*	*0.1*	**TOTAL**	**Importance (0–5; Not Important to Critically Important)**
1	Customer sales	*5*	*5*	*5*	*5*	*4*	4.9	Critically Important
2	Production	*5*	*5*	*5*	*3*	*3*	4.4	Critically Important
3	Information security services	*3*	*3*	*3*	*3*	*5*	3.2	Very Important

Example of Weighted Table Analysis of Business Processes (2 of 2)

	Criterion	*Impact on Revenue*	*Impact on Profitability*	*Impact on Product/Service Delivery*	*Impact on Market Share*	*Impact on Reputation*		
4	IT services	*4*	*3*	*4*	*2*	*2*	3.1	Very Important
5	Customer services	*2*	*3*	*2*	*1*	*4*	2.3	Important
6	Research & development	*1*	*1*	*2*	*3*	*3*	1.75	Somewhat Important
7	Employee support services	*1*	*1*	*2*	*1*	*2*	1.25	Somewhat Important

Determine Business Process and Recovery Criticality (2 of 2)

- When organizations consider recovery criticality, key recovery measures are usually described in terms of how much of the asset they must recover within a specified time frame.
- The terms most commonly used to describe this are:
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Maximum tolerable downtime (MTD)
  - Work recovery time (WRT)
- Plotting cost balance points will show an optimal point between disruption and recovery costs.

RTO vs. RPO

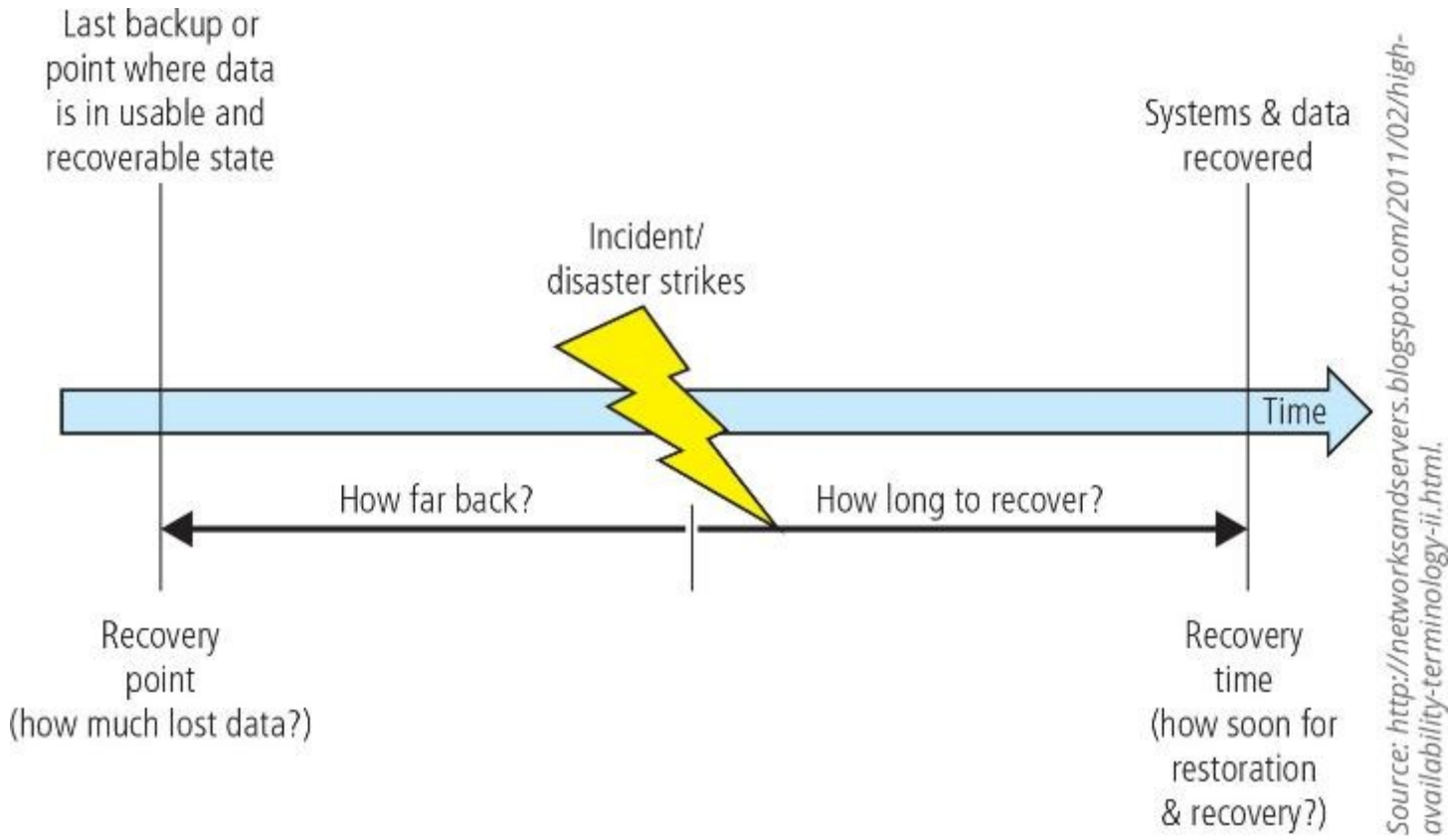

Figure 5-3 RTO vs. RPO

RTO, RPO, MTD, and WRT

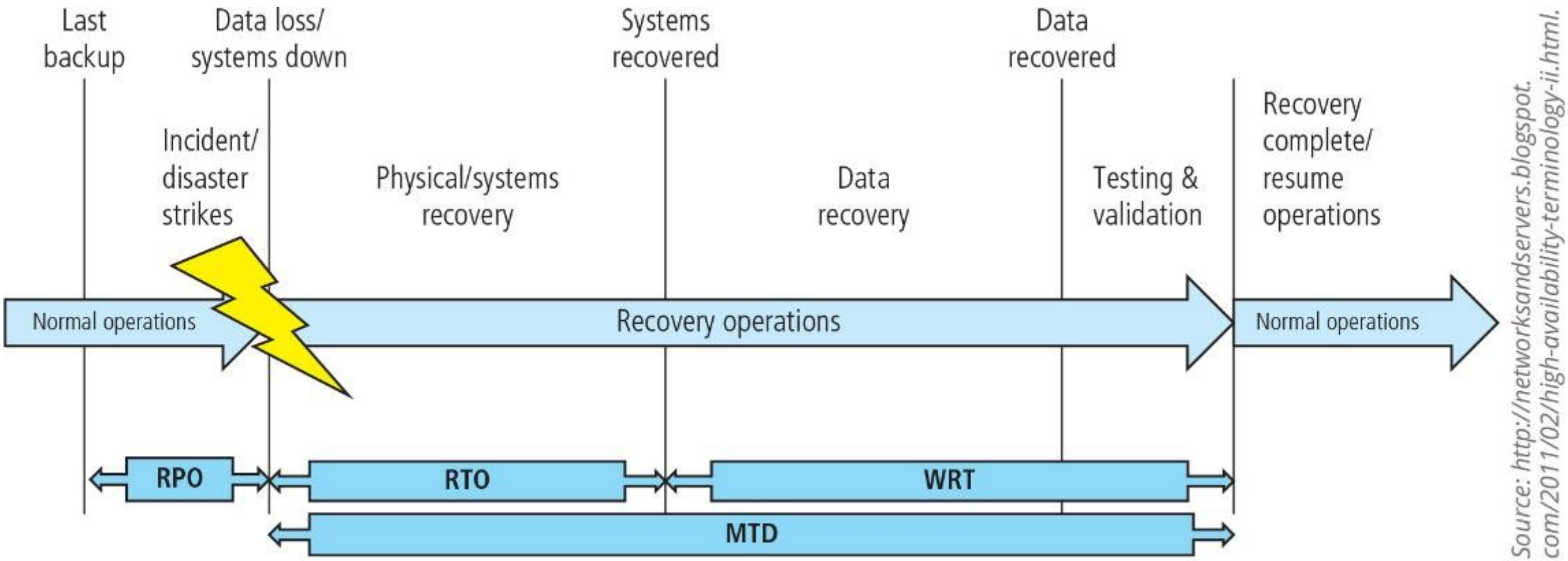

Figure 5-4 RTO, RPO, MTD, and WRT

Cost Balancing

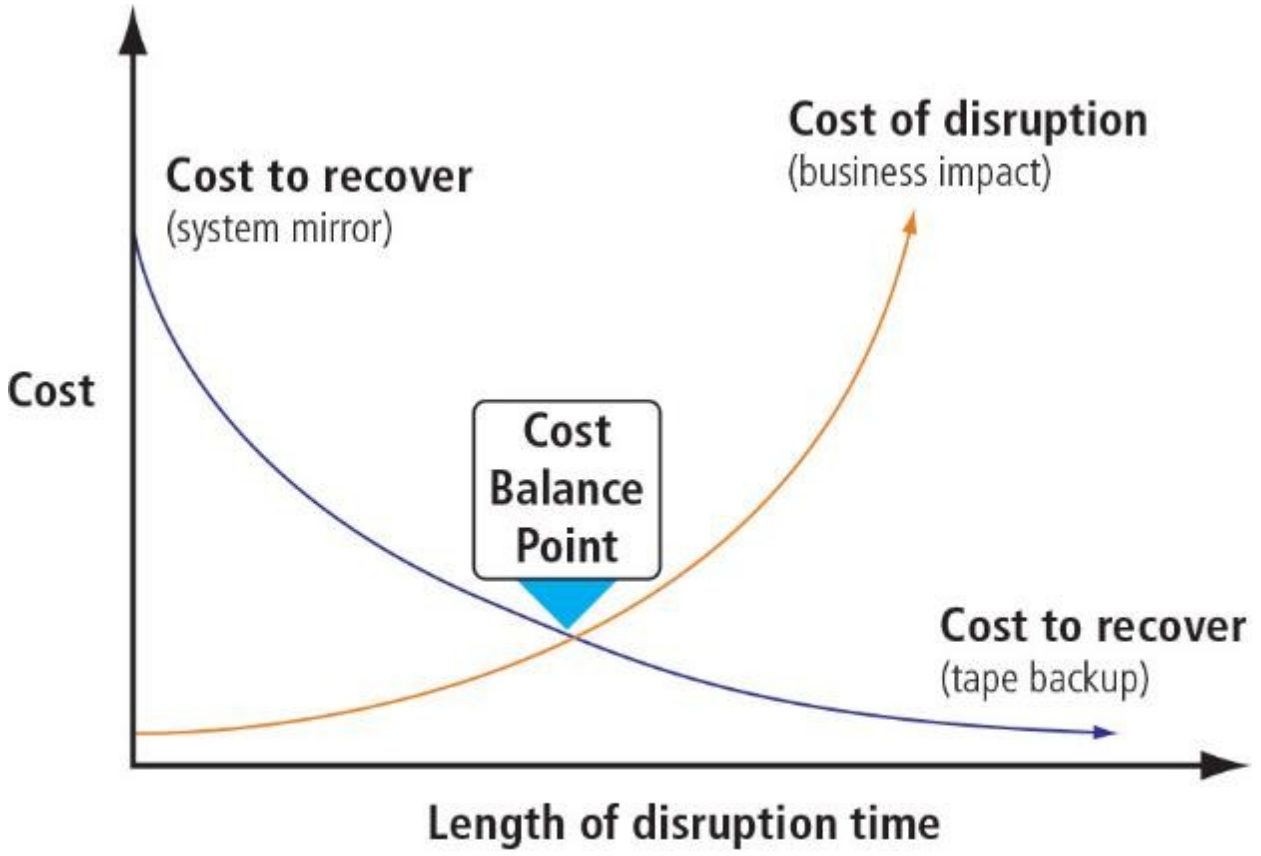

Figure 5-5 Cost balancing

Information Asset Prioritization

- As the CPMT conducts the BIA, it will be assessing priorities and relative values on mission/business processes.
- To do so, it needs to understand the information assets used by those processes, as the presence of high-value information assets may influence the valuation of a particular business process.
- Normally, this task would be performed as part of the risk assessment function within the risk management process.

Identify Recovery Resource Requirements

- Once the organization has created a prioritized list of its mission/business processes, it needs to determine what resources would be required in order to recover those processes and the assets associated with them.
- For each process (and information asset) identified in the previous BIA stage, the organization should identify and describe the relevant resources needed to provide or support that process.
- A simplified method for organizing this information is to put it into a resource/component table.

Example Resource/Component Table (1 of 2)

Mission/Business Process	Required Resource Components	Additional Resource Details	Description and Estimated Costs
Provide customer support (help-desk)	Trouble ticket and resolution application	Application server w/ LINUX OS, Apache server, and SQL database	Each help-desk technician requires access to the organization's trouble ticket and resolution software application, hosted on a dedicated server. See current cost recovery statement for valuation.
Provide customer support (help desk)	Help-desk network segment	25 Cat5e network drops, gigabit network hub	The help-desk applications are networked and require a network segment to access. See current cost recovery statement for valuation.

Example Resource/Component Table (2 of 2)

Mission/Business Process	Required Resource Components	Additional Resource Details	Description and Estimated Costs
Provide customer support (help desk)	Help-desk access terminals	1 laptop/PC per technician, with Web-browsing software	The help-desk applications require a Web interface on a laptop/PC to access. See current cost recovery statement for valuation.
Provide customer billing	Customized accounts receivable application	Application server with Linux OS, Apache server, and SQL database	Accounts Receivable requires access to its customized AR software and customer database to process customer billing. See current cost recovery statement for valuation.

System Resource Recovery Priorities

- The last stage of the BIA is prioritizing the resources associated with the mission/business processes, which provides a better understanding of what must be recovered first, even within the most critical processes.
- With the information from previous steps in hand, the organization can create additional weighted tables of the resources needed to support the individual processes.
- In addition to the weighted tables described earlier, a simple valuation and classification scale, such as Primary/Secondary/Tertiary, or Critical/Very Important/Important/Routine, can be used to provide a quicker method of valuating the supporting resources.

Contingency Planning Policies

- Prior to the development of each of the types of CP documents outlined in this module, the CP team should work to develop the policy environment that will enable the BIA process and should provide specific policy guidance toward authorizing the creation of each of the planning components (IR, DR, and BC).
- These policies provide guidance on the structure of the subordinate teams and the philosophy of the organization, and they assist in the structuring of the plan.
- Just as the enterprise InfoSec policy defines the InfoSec roles and responsibilities for the entire enterprise, each of the CP documents is based on a specific policy that defines the related roles and responsibilities for that element of the overall CP environment within the organization.

Incident Response (1 of 2)

- Most organizations have experience detecting, reacting to, and recovering from attacks, employee errors, service outages, and small-scale natural disasters, and are thus performing **incident response (IR)**.
- IR must be carefully planned and coordinated because organizations heavily depend on the quick and efficient containment and resolution of incidents.
- **Incident response planning (IRP)**, therefore, is the preparation for such an effort and is performed by the IRP team (IRPT).

Incident Response (2 of 2)

- When those events represent the potential for loss, they are referred to as **adverse events** or **incident candidates**.
- When an adverse event begins to manifest as a real threat to information, it becomes an **incident**.
- The **incident response plan (IR plan)** is usually activated when the organization detects an incident that affects it, regardless of how minor the effect is.

Getting Started

- An early task for the CPMT is to form the IRPT, which will begin work by developing policy to define the team's operations, articulate a response to various types of incidents, and advise users how to contribute to the organization's effective response, rather than contributing to the problem at hand.
- The IRPT then forms the **computer security incident response team (CSIRT).**
- As part of an increased focus on cybersecurity infrastructure protection, NIST has developed a Framework for Improving Critical Infrastructure Cybersecurity, also referred to as the NIST Cybersecurity Framework (CSF).

NIST Incident Response Life Cycle

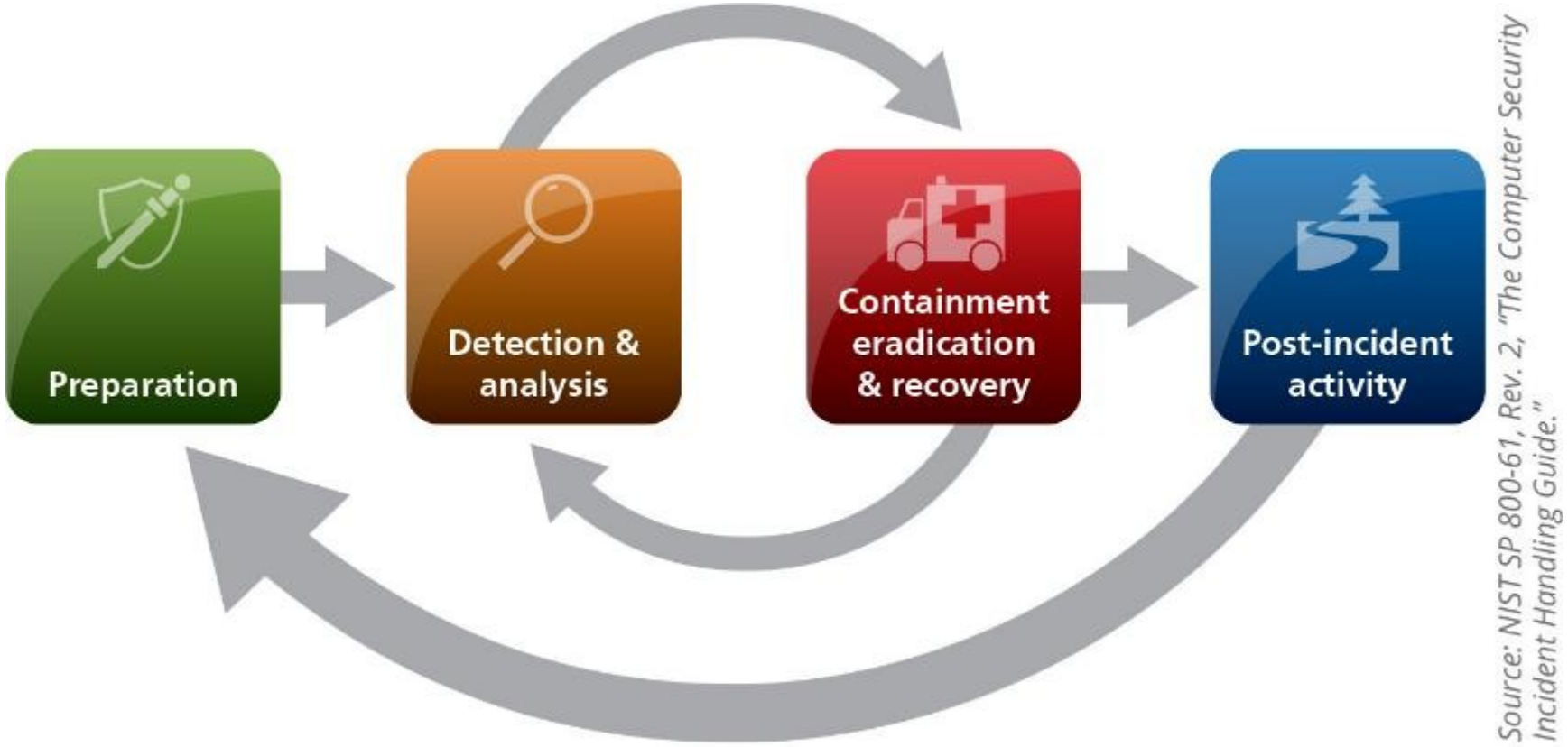

Figure 5-6 NIST incident response life cycle

NIST Cybersecurity Framework

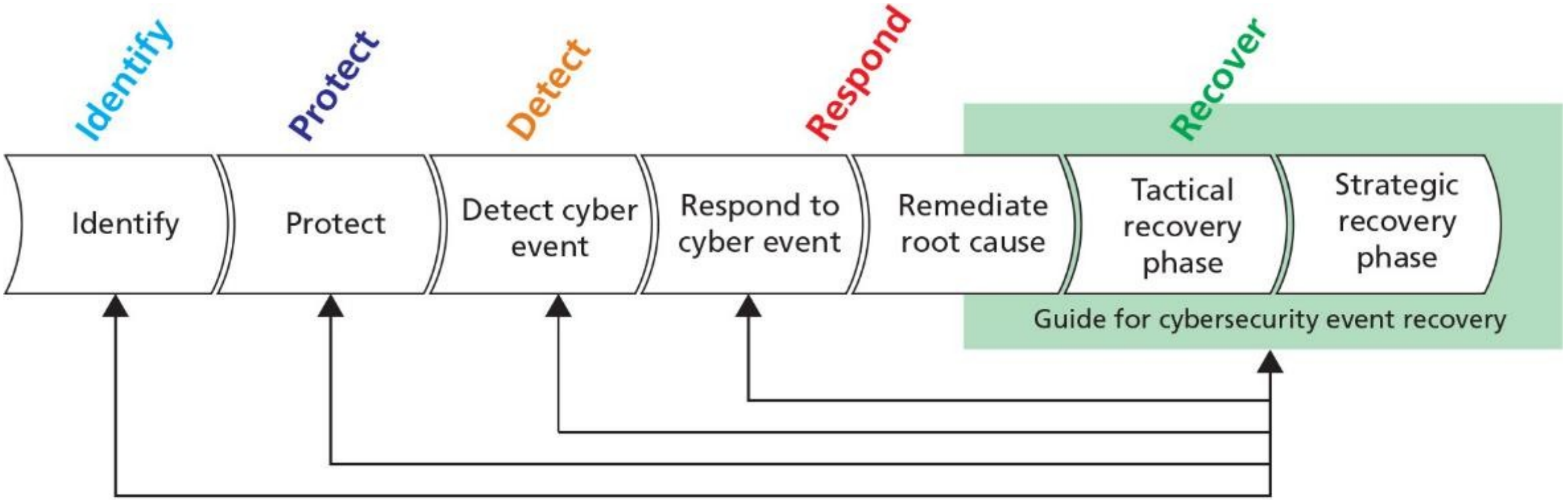

Figure 5-7 NIST Cybersecurity Framework

Incident Response Policy

- NIST SP 800-61, Rev. 2: The Computer Security Incident Handling Guide identifies the following key components of a typical IR policy:
  - Statement of management commitment
  - Purpose and objectives of the policy
  - Scope of the policy (to whom and what it applies and under what circumstances)
  - Definition of InfoSec incidents and related terms
  - Organizational structure and definition of roles, responsibilities, and levels of authority
  - Prioritization or severity ratings of incidents
  - Performance measures
  - Reporting and contact forms

Incident Response Planning

- When a threat becomes a valid adverse event, it is classified as an InfoSec incident if:
  - It is directed against information assets.
  - It has a realistic chance of success.
  - It threatens the confidentiality, integrity, or availability of information resources and assets.
- It is important to understand that IR is a reactive measure, not a preventive one, although most IR plans include preventive recommendations.

IR Planning (1 of 3)

- The responsibility for creating an organization's IR plan usually falls to the CISO, or an IT manager with security responsibilities.
- According to NIST SP 800-61, Rev. 2, the IR plan includes:
  - Mission
  - Strategies and goals
  - Senior management approval
  - Organizational approach to incident response
  - How the incident response team will communicate
  - Metrics for measuring incident response capability and effectiveness
  - Roadmap for maturing incident response capability
  - How the program fits into the overall organization

IR Planning (2 of 3)

- For every incident scenario, the CP team creates three sets of incident handling procedures:
  - During the incident
  - After the incident
  - Before the incident
- Once these sets of procedures are clearly documented, the IR portion of the IR plan is assembled, and the critical information outlined in these planning sections is recorded.

IR Planning (3 of 3)

- The execution of the IR plan typically falls to the computer security incident response team (CSIRT).
- The CSIRT is a separate group from the IRPT, although some overlap may occur, and is composed of technical and managerial IT and InfoSec professionals prepared to diagnose and respond to an incident.
- In some organizations, the CSIRT may simply be a loose or informal association of IT and InfoSec staffers who would be called up if an attack were detected.
- In other, more formal implementations, the CSIRT is a set of policies, procedures, technologies, people, and data put in place to prevent, detect, react to, and recover from an incident.

IR Actions

- Incident response actions can be organized into three basic phases:
  - Detection
  - Reaction
  - Recovery

Incident Handling Checklist from NIST SP 800-61, Rev. 2 (1 of 3)

		Action	Completed
		Detection and Analysis	
1.		Determine whether an incident has occurred	
	1.1	Analyze the precursors and indicators	
	1.2	Look for correlating information	
	1.3	Perform research (e.g., search engines, knowledge base)	
	1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.		Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.		Report the incident to the appropriate internal personnel and external organizations	

Incident Handling Checklist from NIST SP 800-61, Rev. 2 (2 of 3)

		Action	Completed
		Containment, Eradication, and Recovery	
4.		Acquire, preserve, secure, and document evidence	
5.		Contain the incident	
6.		Eradicate the incident	
	6.1	Identify and mitigate all vulnerabilities that were exploited	
	6.2	Remove malware, inappropriate materials, and other components	
	6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	

Incident Handling Checklist from NIST SP 800-61, Rev. 2 (3 of 3)

		Action	Completed
7.		Recover from the incident	
	7.1	Return affected systems to an operationally ready state	
	7.2	Confirm that the affected systems are functioning normally	
	7.3	If necessary, implement additional monitoring to look for future related activity	
		Post-Incident Activity	
8.		Create a follow-up report	
9.		Hold a lessons learned meeting (mandatory for major incidents, optional otherwise). While not explicitly noted in the NIST document, most organizations will document the findings from this activity and use it to update relevant plans, policies, and procedures.	

Data Protection in Preparation for Incidents

- An organization has several options for protecting its information and getting operations up and running quickly after an incident:
  - Traditional data backups
  - Electronic vaulting
  - Remote journaling
  - Database shadowing
- Industry recommendations for data backups include:
  - "3-2-1 backup rule,"—three copies of important data on at least two different media, with at least one copy stored off-site
  - Daily on-site backups
  - Weekly off-site backups

Detecting Incidents

- The challenge is determining whether an event is the product of routine systems use or an actual incident.
- Incident classification is the process of examining an adverse event or incident candidate and determining whether it constitutes an actual incident.
- Initial reports from end users, intrusion detection systems, virus detection software, and systems administrators are all ways to track and detect incident candidates.
- Once an actual incident is properly identified and classified, members of the IR team can effectively execute the corresponding procedures from the IR plan.

Incident Indicators (1 of 2)

- Possible indicators
  - Presence of unfamiliar files
  - Presence or execution of unknown programs or processes
  - Unusual consumption of computing resources
  - Unusual system crashes
- Probable indicators
  - Activities at unexpected times
  - Presence of new accounts
  - Reported attacks
  - Notification from IDS

Incident Indicators (2 of 2)

- Definite indicators
  - Use of dormant accounts
  - Changes to logs
  - Presence of hacker tools
  - Notifications by partner or peer
  - Notification by hacker
- Potential incident results
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality
  - Violation of policy
  - Violation of law

Knowledge Check Activity 2

Which of these is not a definite indicator that an event is an incident?

a. Use of dormant accounts

b. Unusual system crashes

c. Changes to logs

d. Presence of hacker tools

Knowledge Check Activity 2: Answer

Which of these is not a definite indicator that an event is an incident?

Answer: b. Unusual system crashes

Explanation.

Unusual system crashes may be a possible indicator, and should be carefully investigated, but they do not rise to the level of a definite indicator.

Reacting to Incidents

- Once an actual incident has been confirmed and properly classified, the IR plan moves from the detection phase to the reaction phase.
- The steps in IR are designed to stop the incident, mitigate its effects, and provide information for the recovery from the incident.
- In the incident response phase, a number of action steps taken by the CSIRT and others must occur quickly and may occur concurrently.

Notification of Key Personnel

- As soon as an incident is declared, the right people must be immediately notified in the right order.
- An alert roster is a document containing contact information on the individuals to be notified in the event of an actual incident, either sequentially or hierarchically.
- The alert message is a scripted description of the incident.
- Other key personnel must also be notified of the incident only after the incident has been confirmed, but before media or other external sources learn of it.

Documenting an Incident

- As soon as an incident has been confirmed and the notification process is underway, the team should begin to document it.
- The documentation should record the who, what, when, where, why, and how of each action taken while the incident is occurring.
- It serves as a case study after the fact to determine if the right actions were taken, and if they were effective.
- It can also prove the organization did everything possible to deter the spread of the incident.

Incident Containment Strategies

- The essential task of IR is to stop the incident and contain its scope or impact.
- Incident containment strategies focus on two tasks:
  - Stopping the incident
  - Recovering control of the affected systems
- Typical containment strategies include:
  - Disabling compromised user accounts
  - Reconfiguring a firewall to block the problem traffic
  - Temporarily disabling the compromised process or service
  - Taking down the conduit application or server
  - Disconnecting the affected network or network segment
  - Stopping all computers and network devices

Incident Escalation

- An incident may increase in scope or severity to the point that the IRP cannot adequately contain the incident.
- Each organization will have to determine, during the business impact analysis, the point at which the incident becomes a disaster.
- The organization must also document when to involve outside responders.

Recovering from Incidents (1 of 2)

- Once the incident has been contained, and system control regained, incident recovery can begin.
- As in the incident reaction phase, the first task is to inform the appropriate human resources.
- Almost simultaneously, the CSIRT must assess the full extent of the damage to determine what must be done to restore the systems.
- The immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets is called incident damage assessment.
- Those who document the damage must be trained to collect and preserve evidence in case the incident is part of a crime or results in a civil action.

Recovering from Incidents (2 of 2)

- The incident recovery process includes:
  - Identify the vulnerabilities that allowed the incident to occur and spread and resolve them.
  - Address the safeguards that failed to stop or limit the incident or were missing from the system in the first place. Install, replace, or upgrade them.
  - Evaluate monitoring capabilities (if present).
  - Restore the data from backups as needed.
  - Restore the services and processes in use.
  - Continuously monitor the system.
  - Restore the confidence of the communities of interest.

Common Mistakes CSIRTs make

- According to McAfee, CSIRTS commonly fail to:
  - Appoint a clear chain of command with a specified individual in charge
  - Establish a central operations center
  - “Know their enemy”
  - Develop a comprehensive IR plan with containment strategies
  - Record IR activities at all phases
  - Document the events as they occur in a timeline
  - Distinguish incident containment from incident remediation (as part of reaction)
  - Secure and monitor networks and network devices
  - Establish and manage system and network logging
  - Establish and support effective antivirus and antimalware solutions

NIST Recommendations for Incident Handling (1 of 2)

- Acquire tools and resources.
- Prevent incidents from occurring.
- Identify precursors and indicators through alerts generated by security software.
- Establish mechanisms for outside parties to report incidents.
- Require a baseline level of logging and auditing on all systems.
- Profile networks and systems.
- Understand the normal behaviors of networks, systems, and applications.
- Create a log retention policy.
- Perform event correlation.
- Keep all host clocks synchronized.

NIST Recommendations for Incident Handling (2 of 2)

- Maintain and use a knowledge base of information.
- Start recording all information as soon as the team suspects that an incident has occurred.
- Safeguard incident data.
- Prioritize handling of the incidents based on the relevant factors.
- Include provisions for incident reporting in the organization's incident response policy.
- Establish strategies and procedures for containing incidents.
- Follow established procedures for evidence gathering and handling.
- Capture volatile data from systems as evidence.
- Obtain system snapshots through full forensic disk images, not file system backups.
- Hold lessons-learned meetings after major incidents.

Organizational Philosophy on Incident and Disaster Handling

- Eventually, the organization will encounter incidents and disasters that stem from an intentional attack on its information assets by an individual or group, as opposed to one from an unintentional source.
- At that point, the organization must choose one of two philosophies that will affect its approach to IR and DR as well as subsequent involvement of digital forensics and law enforcement
  - Protect and forget, also known as “patch and proceed”
  - Apprehend and prosecute, also known as “pursue and prosecute”

Digital Forensics (1 of 2)

- Used to determine what happened and how an incident occurred
- Based on the field of traditional **forensics**
- Involves preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary and/or root-cause analysis
- **Evidentiary material (EM):** any item or information that applies to an organization's legal or policy-based case

Digital Forensics (2 of 2)

- Used for two key purposes:
  - To investigate allegations of digital malfeasance
  - To perform root cause analysis
- Organization chooses one of two approaches:
  - Protect and forget (patch and proceed)
  - Apprehend and prosecute (pursue and prosecute)

The Digital Forensics Team

- Most organizations:
  - Cannot sustain a permanent digital forensics team
  - Collect data and outsource analysis
- Information security group personnel should be trained to understand and manage the forensics process to avoid contamination of potential EM.
- Expertise can be obtained by training.

Affidavits and Search Warrants

- Affidavit
  - Sworn testimony that certain facts are in the possession of the investigating officer; can be used to request a search warrant
  - The facts, the items, and the place must be specified.
- When an approving authority signs the affidavit, it becomes a search warrant, giving permission to:
  - Search for EM at a specified location
  - Seize specific items for official examination

Digital Forensics Methodology

- All investigations follow the same basic methodology.
  1. Identify relevant EM.
  2. Acquire (seize) the evidence without alteration or damage.
  3. Take steps to ensure that the evidence is at every step verifiably authentic and is unchanged from the time it was seized.
  4. Analyze the data without risking modification or unauthorized access.
  5. Report the findings to the proper authority.

The Digital Forensics Process

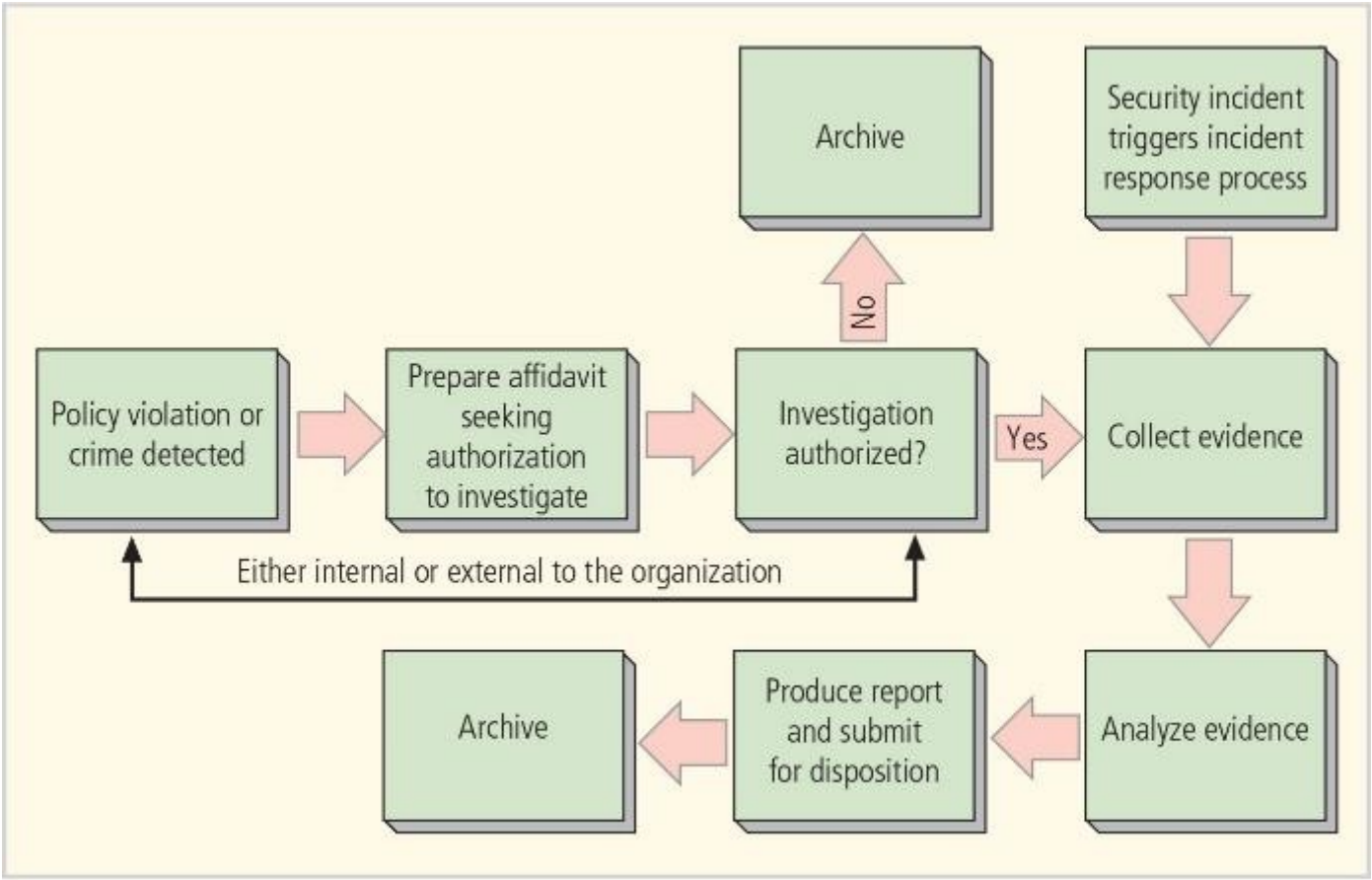

Figure 5-9 The digital forensics process

Evidentiary Procedures

- Strong procedures for handling potential evidentiary material can minimize the probability of an organization losing a legal challenge.
- Organizations should develop specific procedures, along with guidance for effective use.
- Should be supported by a procedures manual

Summary of Methods Employed to Acquire Forensic Data (1 of 3)

Method	Advantages	Disadvantages
Use a dedicated forensic workstation to examine a write-protected hard drive or image of the suspect hard drive.	No concern about the validity of software or hardware on the suspect host. Produces evidence most easily defended in court.	Inconvenient, time-consuming. May result in loss of volatile information.
Boot the system using a verified, write-protected CD or other media with kernel and tools.	Convenient, quick. Evidence is defensible if suspect drives are mounted as read-only.	Assumes that hardware has not been compromised because it is much less likely than compromised software. May result in loss of volatile information.
Build a new system that contains an image of the suspect system and examine it.	Completely replicates operating environment of suspect computer without running the risk of changing its information.	Requires availability of hardware that is identical to that on the suspect computer. May result in las of volatile information.

Summary of Methods Employed to Acquire Forensic Data (2 of 3)

Method	Advantages	Disadvantages
Examine the system using external media with verified software.	Convenient, quick. Allows examination of volatile information.	If a kernel is compromised, results may be misleading. External media may not contain every necessary utility.
Verify the software on the suspect system, and then use the verified local software to conduct the examination.	Requires minimal preparation. Allows examination of volatile information. Can be performed remotely.	Lack of write protection for suspect drives makes evidence difficult to defend in court. Finding sources for hash values and verifying the local software requires at least several hours, unless Tripwire was used ahead of time.

Summary of Methods Employed to Acquire Forensic Data (3 of 3)

Method	Advantages	Disadvantages
Examine the suspect system using the software on it, without verifying the software.	Requires least amount of preparation. Allows examination of volatile information. Can be performed remotely.	Least reliable method. This is exactly what cyberattackers are hoping you will do. Often a complete waste of time.

Disaster Recovery (1 of 2)

- **Disaster recovery planning (DRP)** entails preparation for and recovery from a disaster, whether natural or human-made.
- In general, an incident is a disaster when:
  - The organization is unable to contain or control the impact of an incident, or
  - The level of damage or destruction from an incident is so severe that the organization is unable to quickly recover.
- The key role of a **DR plan** is defining how to reestablish operations at the location where the organization is usually located (primary site).

Disaster Recovery (2 of 2)

- As you learned earlier, the CP team creates the **DR planning team (DRPT).**
- The DRPT in turn organizes and prepares the **DR response teams (DRRTs)** to actually implement the DR plan in the event of a disaster.
- These teams may have multiple responsibilities in the recovery of the primary site and the reestablishment of operations:
  - Recover information assets that are salvageable from the primary facility after the disaster.
  - Purchase or otherwise acquire replacement information assets from appropriate sources.
  - Reestablish functional information assets at the primary site if possible or at a new primary site, if necessary.

Disaster Recovery Response Teams

Some common DRRTs include:

- DR management
- Communications
- Computer recovery (hardware)
- Systems recovery (OS)
- Network recovery
- Storage recovery
- Applications recovery
- Data management
- Vendor contact
- Damage assessment and salvage
- Business interface
- Logistics
- Others as needed

Disaster Recovery Process

- The NIST methodology can be adapted for DRP:
  - Organize the DR team.
  - Develop the DR planning policy statement.
  - Review the BIA.
  - Identify preventive controls.
  - Create DR strategies.
  - Develop the DR plan document.
  - Ensure DR plan testing, training, and exercises.
  - Ensure DR plan maintenance.

Disaster Recovery Policy

- The DR team, led by the manager designated as the DR team leader, begins with the development of the DR policy soon after the team is formed.
- The DR policy contains the following key elements:
  - Purpose
  - Scope
  - Roles and responsibilities
  - Resource requirements
  - Training requirements
  - Exercise and testing schedules
  - Plan maintenance schedule
  - Special considerations

Disaster Classifications

- A DR plan can classify disasters in a number of ways:
  - Natural disasters
  - Human-made disasters
- Disasters may be classified by their rate of occurrence:
  - Rapid-onset disasters
  - Slow-onset disasters

Natural Disasters

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or mudslide
- Tornado or severe windstorm
- Hurricane or typhoon
- Tsunami
- Electrostatic discharge (ESD)
- Dust contamination

Planning to Recover

- Scenario development and impact analysis are used to categorize the level of threat of each potential disaster.
- When generating a DR scenario, start with the most important asset: people.
- Key points in the DR plan:
  1. Clear delegation of roles and responsibilities
  2. Execution of the alert roster and notification of key personnel
  3. Clear establishment of priorities
  4. Documentation of the disaster
  5. Action steps to mitigate the impact
  6. Alternative implementations for the various systems components

Simple DR Plan Elements

- Name of agency
- Date of completion or update of the plan and the date of the most recent test
- Agency staff to be called in the event of a disaster
- Emergency services to be called (if needed) in event of a disaster
- Locations of in-house emergency equipment and supplies
- Sources of off-site equipment and supplies
- Salvage priority list
- Agency disaster recovery procedures
- Follow-up assessment

Knowledge Check Activity 3

When generating a disaster scenario for planning or rehearsal, start with the most important asset: _____.

a. networks

b. threats

c. data

d. people

Knowledge Check Activity 3: Answer

When generating a disaster scenario for planning or rehearsal, start with the most important asset: _____.

Answer: d. people

Explanation.

Human resources are central to all planning and response actions and should form the core of scenarios used to develop plans or to rehearse the use of the plans.

Business Continuity (1 of 2)

- Sometimes disasters have such a profound effect on the organization that it cannot continue operations at its primary site until it fully completes all DR efforts, which requires **business continuity (BC)** strategies.
- **BC planning (BCP)** ensures critical business functions can continue in a disaster and is most likely managed by the CEO or COO of the organization.
- BCP is activated and executed concurrently with the DRP when needed.
- While BCP reestablishes critical functions at an alternate site, DRP focuses on reestablishment at the primary site.

Business Continuity (2 of 2)

- The NIST methodology can also be adapted to BC:
  1. Form the BC team.
  2. Develop the BC planning policy statement.
  3. Review the BIA.
  4. Identify preventive controls.
  5. Create relocation strategies.
  6. Develop the BC plan.
  7. Ensure BC plan testing, training, and exercises.
  8. Ensure BC plan maintenance.

Business Continuity Policy

- Purpose
- Scope
- Roles and responsibilities
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Special considerations

Continuity Strategies (1 of 2)

- Several possible strategies for business continuity; the determining factor is usually cost.
- Three exclusive-use options:
  - Hot sites
  - Warm sites
  - Cold sites
- Three shared-use options:
  - Timeshare
  - Service bureaus
  - Mutual agreements

Continuity Strategies (2 of 2)

- Specialized options:
  - Rolling mobile site
  - Externally stored resources
  - Temporary facilities
  - Cloud-based provisioning

Incident Response and Disaster Recovery

Incident: Ransomware attack on a single system/user

Disaster: Ransomware attack on all organizational systems/users

Attack occurs: Depending on scope, may be classified as an incident or a disaster

Source: This figure has multiple sources. Top left: PR Image Factory/Shutterstock.com. Top right: Zephyr_p/ Shutterstock.com. Bottom center: poylock19/Shutterstock.com.

Figure 5-12 Incident response and disaster recovery

Disaster Recovery and Business Continuity Planning

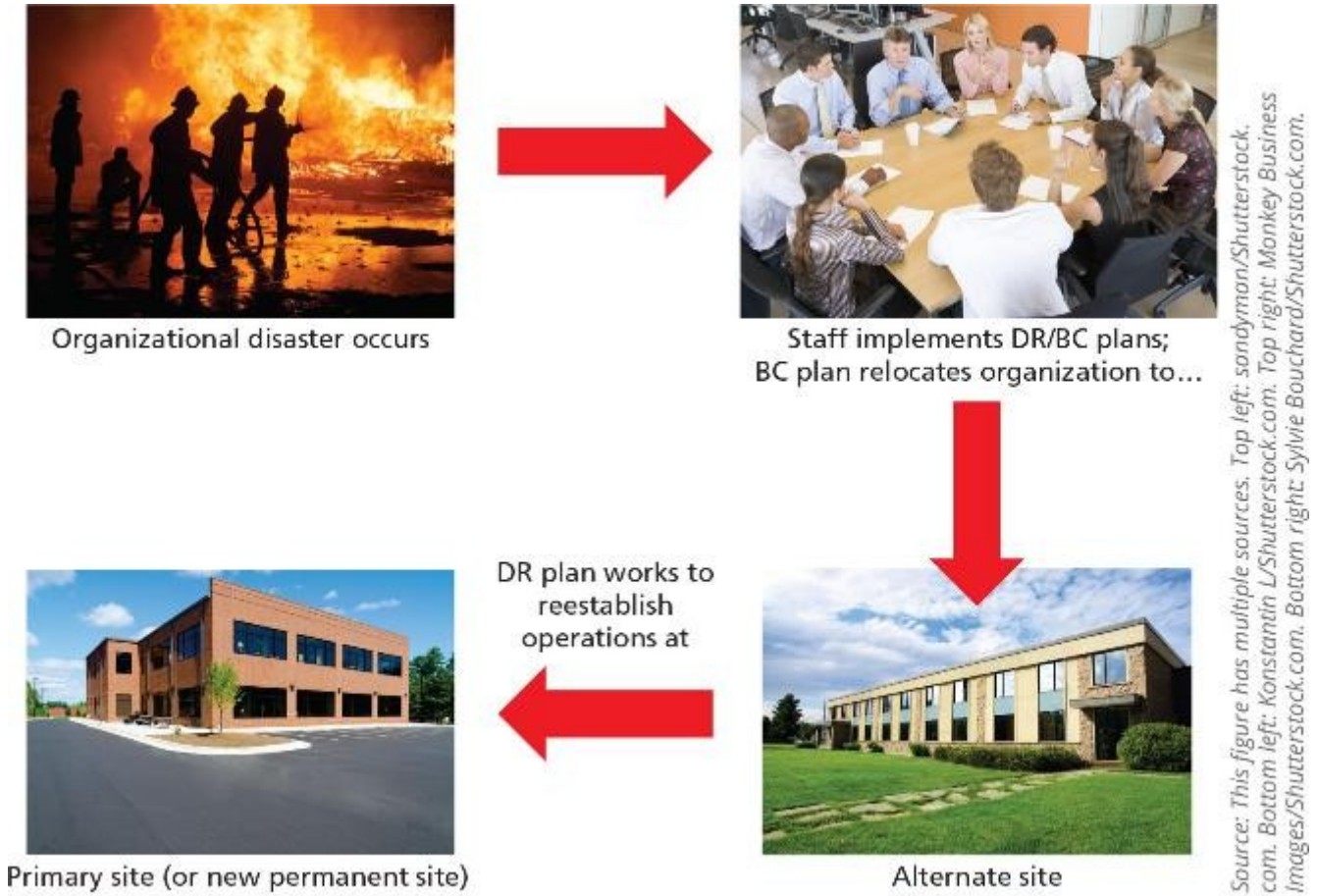

Figure 5-13 Disaster recovery and business continuity planning

Contingency Planning Implementation Timeline

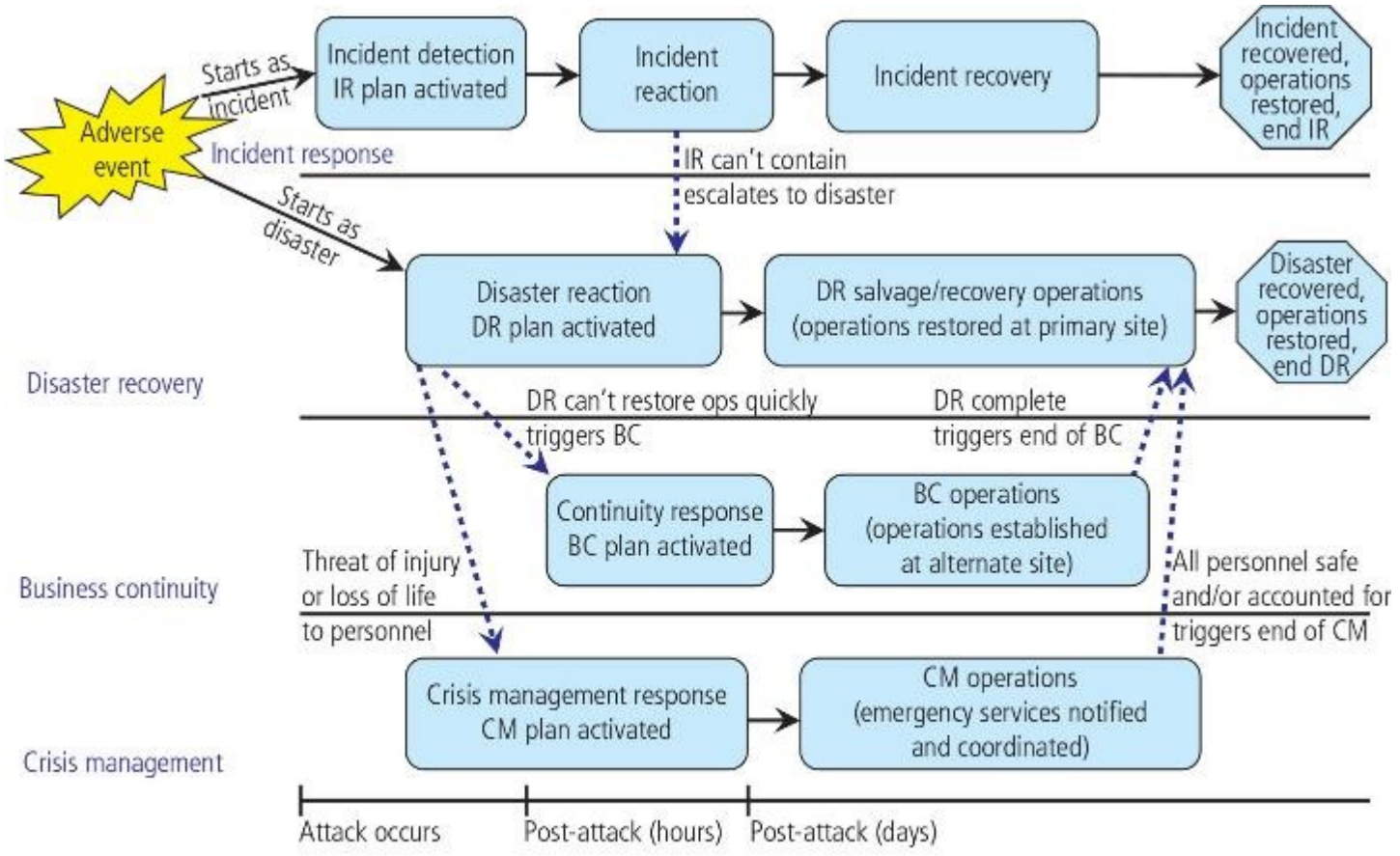

Figure 5-14 Contingency planning implementation timeline

Crisis Management (1 of 3)

- Another process that many organizations plan for separately is **crisis management (CM),** which focuses more on the effects that a disaster has on people than its effects on information assets.
- While some organizations include crisis management as a subset of the DR plan, the protection of human life and the organization's image is such a high priority that it may deserve its own committee, policy, and plan.

Crisis Management (2 of 3)

- According to Gartner Research, the crisis management team is responsible for managing the event from an enterprise perspective and performs the following roles:
  - Supporting personnel and their loved ones during the crisis
  - Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise
  - Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Crisis Management (3 of 3)

- The crisis management planning team (CMPT) should establish a base of operations or command center near the site of the disaster as soon as possible.
- The CMPT should include individuals from all functional areas of the organization in order to facilitate communications and cooperation.
- The CMPT is charged with three primary responsibilities:
  - Verifying personnel status
  - Activating the alert roster
  - Coordinating with emergency services

Knowledge Check Activity 4

The key initial focus of a crisis management response should be on _____.

a. safety of staff, visitors, and the public

b. the image of the organization

c. returning the organization to production

d. communicating to the stockholders/owners

Knowledge Check Activity 4: Answer

The key initial focus of a crisis management response should be on _____.

Answer: a. safety of staff, visitors, and the public

Explanation.

While each of these is important, the earliest and most urgent efforts should be to locate the people involved in the crisis and undertake whatever can be done to support the personnel and their families.

Business Resumption Planning

- Because the DR and BC plans are closely related, most organizations merge the two functions into a single function called **business resumption planning (BRP).**
- Such a comprehensive plan must be able to support the reestablishment of operations at two different locations—one immediately at an alternate site and one eventually back at the primary site.

Testing Contingency Plans

- Very few plans are executable as initially written; instead, they must be tested to identify vulnerabilities, faults, and inefficient processes.
- There are four testing strategies that can be used to test contingency plans:
  - Desk check
  - Structured walk-through
  - Simulation
  - Full interruption

Final Thoughts on CP

- Iteration results in improvement.
- A formal implementation of this methodology is a process known as **continuous process improvement (CPI)**.
- Each time the plan is rehearsed, it should be improved.
- Constant evaluation and improvement leads to an improved outcome.

Summary (1 of 6)

- Planning for unexpected events is usually the responsibility of managers from both the information technology and the information security communities of interest.
- For a plan to be seen as valid by all members of the organization, it must be sanctioned and actively supported by the general business community of interest.
- Some organizations are required by law or other mandate to have contingency planning procedures in place at all times, but all business organizations should prepare for the unexpected.
- Contingency planning (CP) is the process by which the information technology and information security communities of interest position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, both human and artificial.

Summary (2 of 6)

- CP is made up of four major components: the data collection and documentation process known as the business impact analysis (BIA), the incident response (IR) plan, the disaster recovery (DR) plan, and the business continuity (BC) plan.
- Organizations can either create and develop the three planning elements of the CP process (the IR, DR, and BC plans) as one unified plan, or they can create the three elements separately in conjunction with a set of interlocking procedures that enable continuity.

Summary (3 of 6)

- To ensure continuity during the creation of the CP components, a seven-step CP process is used:
  1. Develop the contingency planning policy statement.
  2. Conduct the BIA.
  3. Identify preventive controls.
  4. Create contingency strategies.
  5. Develop a contingency plan.
  6. Ensure plan testing, training, and exercises.
  7. Ensure plan maintenance.

Summary (4 of 6)

- Four teams of individuals are involved in contingency planning and contingency operations: the CP team, the IR team, the DR team, and the BC team. The IR team ensures the CSIRT is formed.
- The IR plan is a detailed set of processes and procedures that plan for, detect, and resolve the effects of an unexpected event on information resources and assets.
- For every scenario identified, the CP team creates three sets of procedures—for before, during, and after the incident—to detect, contain, and resolve the incident.
- Incident classification is the process by which the IR team examines an incident candidate and determines whether it constitutes an actual incident.
- Three categories of incident indicators are used: possible, probable, and definite.

Summary (5 of 6)

- When any one of the following happens, an actual incident is in progress: loss of availability of information, loss of integrity of information, loss of confidentiality of information, violation of policy, or violation of law.
- Digital forensics is the investigation of wrongdoing in the arena of information security. Digital forensics requires the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis.
- DR planning encompasses preparation for handling and recovering from a disaster, whether natural or human-made.
- BC planning ensures that critical business functions continue if a catastrophic incident or disaster occurs. BC plans can include provisions for hot sites, warm sites, cold sites, timeshares, service bureaus, and mutual agreements.

Summary (6 of 6)

- Because the DR and BC plans are closely related, most organizations prepare the two at the same time and may combine them into a single planning document called the business resumption (BR) plan.
- The DR plan should include crisis management, the action steps taken during and after a disaster. In some cases, the protection of human life and the organization's image are such high priorities that crisis management may deserve its own policy and plan.
- All plans must be tested to identify vulnerabilities, faults, and inefficient processes. Several testing strategies can be used to test contingency plans: desk check, structured walk-through, simulation, and full interruption.

Self-Assessment

- Contingency planning is about expecting to operate the business in non-normal circumstances.
- How planning for “normal operations” make more effective planning for “non-normal” operations?
- How about the opposite? Can you think of parts of contingency planning that might make more effective planning for “normal” operations?