MIS761
Cyber Security Strategies

Dept. of Information Systems & Business Analytics

Deakin Business School

Week 7 – Contingency Planning

AACSB ACCREDITED

DEAKIN BUSINESS SCHOOL

Contingency Plan	Primary Intentions	Main Characteristics	Benefits
Incident Response	• Detect and respond to security incidents. • Limit the effects of an information security event.	• Set of instructions for various potential scenarios (e.g., data breaches, DDoS attacks). • Provides clear guidelines for response.	• Reduces effects of security events. • Limits operational, financial, and reputational damage. • Faster incident response. Early threat mitigation.
Disaster Recovery	• Restore IT operations after a disaster. • Recover data and systems.	• IT-specific. • Focuses on the IT systems that support business functions.	• Quick restoration of IT services. • Minimized data loss.
Business Continuity	• Ensure continuous business operations during a disaster. • Maintain essential functions during and after a disaster.	• Focuses on business processes. • Ensures that essential functions can continue during and after a disaster.	• Minimized business operation interruptions. Ensures business survival.

Incident Response Life Cycle

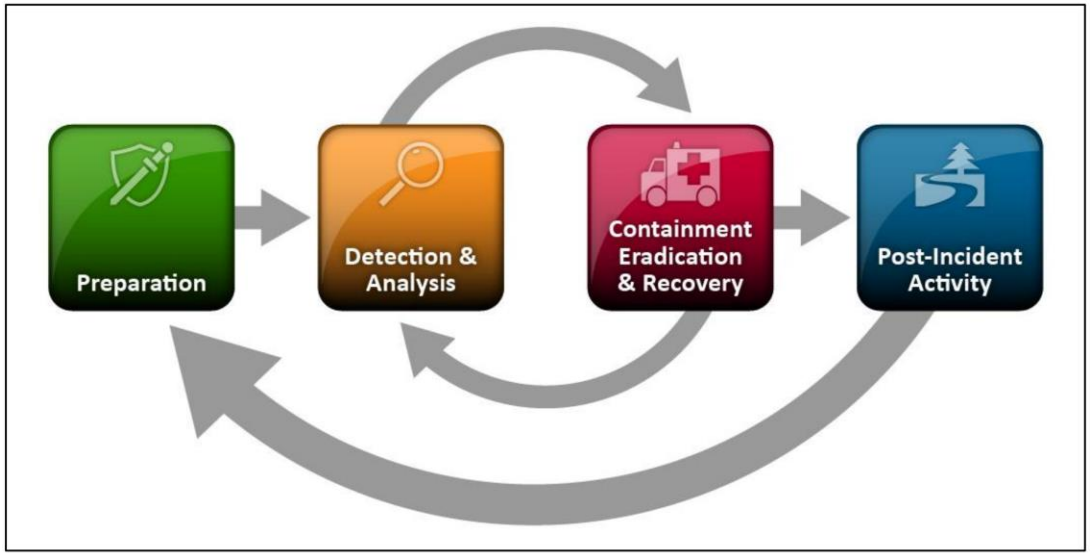


Figure 3-1. Incident Response Life Cycle

- **Preparation:** Establish and train teams, acquire tools, implement controls
  - Focus on risk assessment and minimizing incidents
- **Detection and Analysis:** Identify, categorize, and prioritize unusual activity
  - Analysts spend most working hours in this phase
- **Containment, Eradication, and Recovery:** Stop the spread, remove infection, restore operations
  - Develop a plan based on detection insights
- **Post-Incident Activity:** Review and document lessons learned, improve processes
  - Conduct after-action reports, update plans for future incidents

Preparation
-Elements of an Incident Response Plan

- **Purpose Statement**: Why and what types of incidents the plan covers
- **Clear Strategies**: Prioritize actions like containment or preservation
- **Roles & Responsibilities**: Who handles incidents and their authority
- **Communication**: Team, organization, and third-party coordination
- **Senior Management Approval**: Essential for executing unpopular actions

Preparation
- Developing Your Plan

- **Reference NIST SP 800-61:** Guides decision-making in planning
- **Resources/Templates:**
  - ACSC Emergency Response Guide (cyber.gov.au)
  - Cyber Security Incident Response Planning: Practitioner Guidance | Cyber.gov.au
  - https://www.vic.gov.au/sites/default/files/2019-07/VicGov-Cyber-Incident-Response-Plan-template.docx
- **Adapt to Your Needs:** Customize based on organizational requirements

Preparation
- Building IR team

- **Critical Asset:** A well-trained team is key to managing incidents
- **24/7 Availability:** Assign primary and backup personnel for coverage
- **Professional Development:** Opportunity to sharpen technical skills
- **Key Team Members:** Management, cybersecurity, technical experts, legal, PR, HR, physical security
- **Readiness Focus:** Design and train your team for effective response
  - **Regular Collaboration:** Meet regularly, not just during incidents
  - **Plan Testing:** Ensure the team works well together and is prepared

Preparation
- Enhancing Team Capabilities

- **Identify Gaps:** Assess team's capacity to handle incidents
- **External Support:** Consider retaining external incident response providers
- **Advance Planning:** Secure contracts before an incident occurs

Preparation
- Communications and Facilities for IR

- **Preparing Communication Needs:** Ensure effective internal and external communication
  - Prepare accurate contact lists and on-call schedules
  - Consider primary and backup communication methods
- **Facilities Planning:** Determine location and resources for response
  - Decide between central location or remote work
  - Ensure necessary equipment (computers, network access) is available
- **Information Tracking:** Plan for how to track incident details
  - Options: Electronic systems, spreadsheets, whiteboards
- **Contingency Plans:** Develop backup plans for communication and facilities
  - Address potential roadblocks (e.g., no cell service, equipment failures)
- **Training and Preparation:** Train staff on tools and procedures in advance
  - Test communication and facility plans through exercises

Preparation
- External Information Sharing

- **Media Interaction:** Establish a single point of contact
  - Limit details shared; avoid technical specifics
  - Prepare responses for common media questions
- **Law Enforcement:** Involve early if prosecution is desired
  - Coordinate with a designated contact, often from legal
  - Balance business needs with evidence preservation
- **Training and Preparation:** Ensure staff know what can be shared
  - Use standard phrases to redirect media inquiries
- **Communication Strategy:** Keep messages clear and concise
  - Avoid statements that could aid attackers

Detection & Analysis
- Continuous Monitoring for Incident Detection

- **Perpetual Monitoring:** Always watch for signs of incidents
- **Incident Identification:** Requires a robust security monitoring infrastructure
- **Data Responsibility:** Collect, analyze, and retain security information
- **Information Sources:** IDS/IPS, firewalls, authentication systems, logs, etc.

Detection & Analysis
- Utilizing SIEM Technology

- **Security Information and Event Management (SIEM):** Centralized log repositories and analysis tools
- **Data Correlation:** SIEMs handle massive amounts of log data
- **Incident Detection:** Rules and algorithms flag potential incidents
- **Centralized Investigation:** Provides a unified information source for investigators

Detection & Analysis
- Handling External Reports of Incidents

- **Detection Gaps:** Sometimes, monitoring systems fail to detect incidents
- **External Alerts:** Reports from employees, customers, external entities
- **Consistent Methods:** Receive, record, evaluate external incident reports
- **Quick Response:** First responders must act quickly to contain damage

Detection & Analysis
- Escalation and Notification Process

- **Evaluate Severity:** Assess incident based on organizational impact
- **Appropriate Response Level:** Escalate incident to suitable response team
- **Notify Stakeholders:** Inform management and stakeholders about the incident
- **Triaging Process:** Identify potential impact after containing an incident
- **Severity Rating:** Use scale - low, moderate, high impact

Detection & Analysis
- Incident Impact Levels and Response

- **Low-Impact Incidents:** Minimal effect; handled by first responders
- **Moderate-Impact Incidents:** Significant effect; triggers team activation and management notification
- **High-Impact Incidents:** Critical damage; immediate full response and executive notification
  - **Standby Status:** Non-critical members on alert during high-impact incidents
- **Clear Process:** Must have tools and contacts ready for escalation
- **Automated Solutions:** Consider tech to automate team response

Detection & Analysis
- Immediate response: First Responder Actions

- **First Responder Priority:** Contain damage by isolating affected systems
- **System Isolation:** Quarantine to cut off compromised systems
- **Integrate Intelligence:** Combine incident response with threat intelligence
- **Counterintelligence:** Thwart adversaries' efforts to gather information

Containment, Eradication, and Recovery - Incident Mitigation and Containment

- **Containment Goals:** Prevent spread, minimize damage, control recovery costs
- **Containment Activities:** Focus on controlling scope and impact
- **Six NIST Criteria:**
  - 1. **Potential for Damage/Theft**: Evaluate risk of further damage or theft
  - 2. **Evidence Preservation**: Consider need to preserve evidence
  - 3. **Service Availability**: Assess impact on service availability requirements
  - 4. **Time and Resources**: Evaluate resources needed to implement strategy
  - 5. **Effectiveness**: Determine if strategy fully or partially contains incident
  - 6. **Duration**: Consider how long the containment solution will last

Containment, Eradication, and Recovery - Considerations During Containment

- **Balancing Act**: Align business needs with security objectives
- **Responder Judgment**: Use best judgment; consult management and stakeholders
- **Attacker Awareness**: Containment may alert attackers; expect rapid response
- **Semi-Stable State**: Aim for limited business operations with temporary solutions
- **Prepare for Recovery**: Ensure organization is ready for recovery and reconstitution

Containment, Eradication, and Recovery - Containment strategies—Segmentation

- **Segmentation Purpose:** Limit attack spread without alerting the attacker
- **Network Segmentation:** Divide networks into logical segments by user or system
- **Quarantine VLAN:** Move compromised systems to a separate VLAN
- **Access Controls:** Restrict communication to prevent further spread

Containment, Eradication, and Recovery - Containment strategies—Isolation

- **Isolation Strategy:** Disconnect compromised systems from the main network
- **Separated Network:** Systems remain connected but isolated from the organization
- **Controlled Communication:** Systems may still communicate externally, including with attackers
- **Advanced Containment:** Higher level of security than segmentation

Containment, Eradication, and Recovery - Containment strategies—Removal

- **Removal Strategy:** Fully disconnect compromised systems from all networks
- **No Communication:** Systems can't connect with others or the internet
- **Alerting the Attacker:** Attacker knows detection, but prevents further damage
- **Decision Making:** Balance investigation, damage prevention, and business impact

Containment, Eradication, and Recovery - Eradication and Recovery

- **Eradication Objective**: Remove all traces of the security incident
- **Securing Accounts**: Protect compromised user and administrator accounts
- **System Reconstruction**: Rebuild or reimage compromised systems and devices
- **Prevent Backdoors**: Ensure attackers can't regain access post-recovery
- **Recovery Objective**: Restore normal business operations securely
- **Linked Activities**: Eradication and recovery often occur simultaneously
- **System Rebuild**: Avoid using pre-attack images; address vulnerabilities
- **Access Control**: Strengthen controls to prevent future incidents

Containment, Eradication, and Recovery - Identifying and Mitigating Vulnerabilities

- **Prevent Reoccurrence**: Avoid restoring systems to pre-incident state
- **Vulnerability Remediation**: Identify and fix exploited vulnerabilities
- **Endpoint Security**: Use whitelisting, blacklisting, and quarantine technology
- **Compensating Controls**: Deploy controls for uncorrected vulnerabilities

Containment, Eradication, and Recovery - Improving Cybersecurity Measures

- **Tool Enhancements**: Update firewall rules and security configurations
- **Device Management**: Reconfigure or deploy mobile device management solutions
- **Data Protection**: Use data loss prevention and URL filtering tools
- **Digital Certificates**: Update or revoke compromised certificates

Containment, Eradication, and Recovery - Media Sanitization Techniques

- **Clearing**: Overwrite data to prevent casual analysis
- **Purging**: Use advanced techniques like degaussing or cryptographic functions
- **Destroying**: Shred, pulverize, or melt media for total data destruction
- Decision Flow Chart: Use NIST guidelines to choose sanitization method

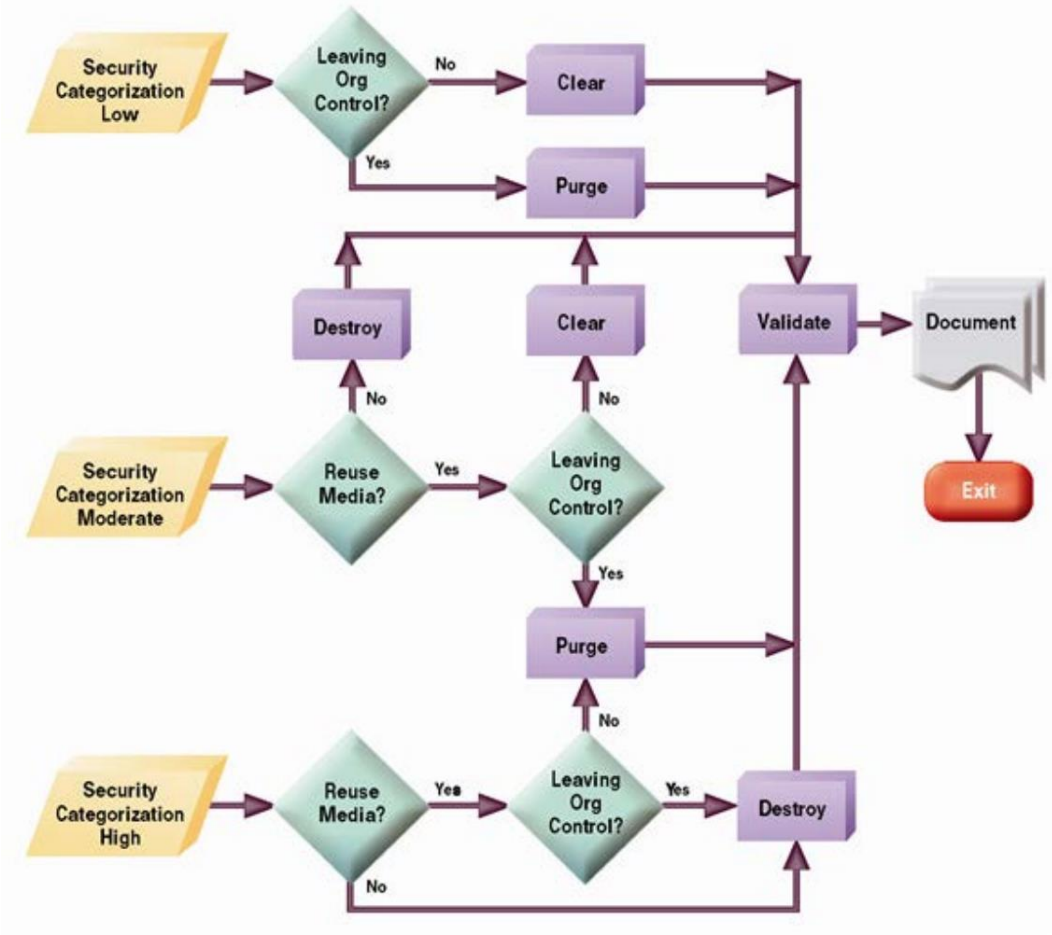


Figure 4-1: Sanitization and Disposition Decision Flow

Containment, Eradication, and Recovery - Validation: System and Network Checks

- **Validate Security:** Check all systems, especially compromised ones
- **Automated Tools:** Use configuration management tools to automate checks
- **Patch Updates:** Ensure all systems have current security updates
- **Vulnerability Scanning:** Use scanners to find any exposed vulnerabilities
- **Account Review:** Verify only authorized accounts exist, no backdoors

Containment, Eradication, and Recovery - Validation: Logging and Restoration Checks

- **Logging Verification:** Ensure systems are logging all security information
- **SIEM Integration:** Confirm all logs are sent to SIEM solutions
- **Service Restoration:** Verify full restoration of capabilities and services
- **Ready for Operations:** Ensure readiness for normal business operations
- **Incident Resolution:** Complete validation before moving to post-incident activities

Importance of Post-Incident Activities

Post-incident activities often overlooked after recovery

- **Four Key Activities:**
  - Lessons Learned
  - Root Cause Analysis
  - Evidence Retention
  - Indicators of Compromise
- **Purpose:** Enhance future incident response efforts and security posture
- **Timing:** Conduct activities soon after returning to normal operations

Post-Incident Activities
- Lessons Learned Process

- **Purpose:** Reflect on roles and overall response effectiveness
- **Method:** Conduct sessions led by a neutral facilitator
  - Facilitator should not have been involved in the incident
  - Encourage open and honest feedback
- **Timeliness:** Hold sessions promptly to capture accurate details
- **Outcome:** Identify improvements for processes and technologies

Post-Incident Activities
- Suggested Questions for Lessons Learned

- **Incident Review:** What happened and when?
- **Performance Evaluation:** How well did staff and management respond?
- **Procedural Adequacy:** Were documented procedures followed and effective?
- **Future Improvements:** What should be done differently next time?
- **Information Sharing:** How could it be improved with other organizations?
- **Preventive Actions:** What corrective actions can prevent future incidents?
- **Detection Tools:** What additional tools or resources are needed?

Post-Incident Activities
- Root Cause Analysis

- **Purpose:** Identify what allowed the incident to occur
- **Focus Areas:** Technical, operational, and managerial causes
- **Goal:** Improve security program and prevent future incidents
- **Approach:** Analyze the underlying issues beyond immediate symptoms

Post-Incident Activities - Evidence Retention

- **Decision Making:** Based on data retention policy and legal considerations
- **Retention Guidelines:** Determine if evidence should be kept securely
- **Chain of Custody:** Document and maintain evidence securely
- **Legal Relevance:** Assess if evidence might be needed for future actions

Post-Incident Activities
- Indicators of Compromise (IoCs)

- **Review Incident Details:** Identify new indicators that could detect incidents
- **Update Monitoring:** Add new indicators to the security monitoring program
- **Future Detection:** Improve detection capabilities for similar incidents
- **Continuous Improvement:** Enhance security tools and processes

Post-Incident Activities

Post-incident activities often overlooked after recovery

- **Four Key Activities:**
  - Lessons Learned
  - Root Cause Analysis
  - Evidence Retention
  - Indicators of Compromise
- **Purpose:** Enhance future incident response efforts and security posture

Key Metrics for Incident Response Effectiveness

- **Mean Time to Detect (MTTD):** Measures time from incident occurrence to detection
  - **Goal:** Shorter MTTD for early detection and minimal damage
- **Mean Time to Respond (MTTR):** Measures time from detection to response action
  - **Goal:** Quick mobilization to mitigate issues promptly
- **Mean Time to Remediate (MTTRM):** Time from detection to restoration of normal operations
  - **Goal:** Minimize MTTRM to reduce impact and recover quickly

Analysing Metrics and Alert Volume

- **Alert Volume:** Number of alerts from security tools and systems
  - **Challenge:** Excess alerts may indicate false positives or overwhelm teams
  - **Solution:** Optimize tools and processes to focus on critical events
- **Using Metrics to Improve:** Track trends and identify areas for improvement
  - **Example:** High MTTD suggests need for better detection tools
  - **Example:** High MTTR indicates need for improved team coordination
- **Continuous Improvement:** Metrics guide enhancements to incident response capabilities

Business Continuity Planning Overview

- **Core Responsibility:** Ensures business operations continue amid adversity
  - Adversity ranges from minor incidents to major disasters
- **Focus of BCP:** Maintain operations, also known as COOP (Continuity of Operations Planning)
- **Security Objective:** Supports the availability aspect of cybersecurity
  - One of the "CIA Triad": Confidentiality, Integrity, Availability
- **Common Misconception:** Often seen as an operational task, but crucial for security

Defining Scope and Conducting a BIA

- **Define Scope:** Clarify what the BCP will cover
  - Which business activities and systems are included?
  - What controls will be considered?
- **Business Impact Assessment (BIA):** Tool for assessing risks
  - Identifies mission-essential functions and supporting IT systems
  - Assesses risks to these systems, both quantitatively and qualitatively
- **Purpose of BIA:** Prioritize risks that could disrupt operations
  - Helps in making informed prioritization decisions

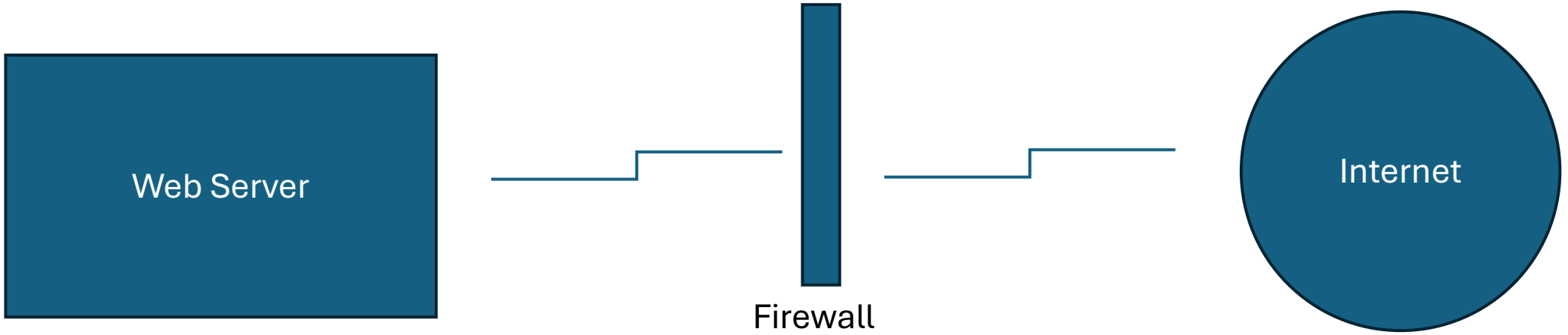
Prioritizing Risks and Cloud Considerations

- **Risk Prioritization:** Focus on risks with highest potential impact
  - Use a risk list ordered by expected loss
  - Prioritize based on risk and cost-effective controls
- **Cost-Benefit Example:** Justify investments with expected payback periods
  - E.g., flood prevention system to mitigate hurricane damage
- **Cloud-Centric BCP:** Collaboration between service providers and customers
  - Providers may build infrastructure, while customers replicate services
  - Consider multi-region replication to enhance continuity

Importance of Redundancy

- **Redundancy Purpose:** Ensure systems continue running despite component failures
  - Prevents entire system failure from a single issue
- **Single Point of Failure (SPOF):** Identifying and removing SPOFs is crucial
- **Redundant Design:** Key to maintaining business continuity
  - Allows operations to continue during predictable failures
- **Analysis Process:** Regular SPOF analysis helps enhance system reliability

Examples of Single Points of Failure (SPOF)



- **Web Server:** A single server failure stops web service
  - **Solution:** Implement a clustered server farm for redundancy
- **Firewall:** A single firewall failure blocks internet access
  - **Solution:** Use high availability firewall pairs for backup
- **Network Connections:** Single network connection failure disrupts service
  - **Solution:** Deploy dual network connections for redundancy
- **Continuous Improvement:** Ongoing SPOF analysis to identify and mitigate risks

Broader Business Continuity Considerations

- **IT Contingency Planning:** Consider risks beyond single points of failure
  - **Examples:** Vendor bankruptcy, capacity shortages, utility failures
- **Personnel Succession Planning:** Prepare for key staff departures
  - **Importance:** IT relies on skilled team members
  - **Action:** Identify successors and provide professional development
- **Continuous Assessment:** Regularly evaluate and update continuity plans
  - **Goal:** Mitigate all potential risks to business operations

Comprehensive Redundancy Strategy

- Combine **High Availability (HA)**, **Fault Tolerance (FT)**, and diversity for robust protection
  - **Ensures resilience against a variety of failure scenarios**
- **High Availability (HA):** Ensures systems remain operational despite failures
  - Examples: Clusters of web servers, redundant firewalls
  - Geographic Dispersal: Protects against facility damage
- **Technology Diversity:** Avoid reliance on a single vendor or technology
  - Prevents simultaneous failure of redundant elements
- **Cryptography Diversity:** Use different cryptographic controls to reduce risk

Comprehensive Redundancy Strategy

Fault Tolerance (FT): Makes systems resilient to technical failures

- **Power Supply Redundancy:** Protects servers from power supply failure
  - Uninterruptible Power Supplies (UPS): Battery backup for short disruptions
  - Managed Power Distribution Units (PDUs): Condition and clean power within server racks
- Storage Protection with RAID
  - RAID Technology: Provides redundancy against single storage device failure
  - RAID is not a backup strategy
  - Regular backups still necessary for catastrophic failures
- **Network Redundancy:** Prevents network single points of failure
  - Multiple ISPs: Diverse entry points for internet service
  - NIC Teaming: Use of dual network interface cards

Understanding Disaster Recovery

- **Disaster Recovery (DR):** Restores business operations after disruptions
  - Subset of business continuity activities
  - Aims to restore normal operations quickly
- **Triggers for DR Plan:**
  - Environmental or man-made disasters, like hurricanes, ransomware attacks
  - Internal or external sources, like data center failures or power outages
- **Activation of DR Plan:** Recognize circumstances and initiate recovery

Initial Response and Staffing in DR

- **Initial Response:** Contain damage and restore immediate capacity
  - Activate alternate processing facilities
  - Contain physical damage or call emergency contractors
- **Staffing Flexibility:** Employees may assume temporary roles
  - Shift focus from normal duties to recovery tasks
  - Training is key for disaster readiness
  - Predefine roles and provide disaster training

Communication and Assessment in DR

- **Communication:** Secure, reliable methods are crucial
  - Includes activation of the disaster plan after hours
  - Regular status updates for field teams and leadership
  - Ad hoc communications for tactical needs
- **Assessment Phase:** Shifts from response to damage assessment
  - Triage damage and implement recovery plans
  - Intermediate steps may temporarily restore operations

Disaster Recovery Metrics and Final Steps

- **Key Metrics:**
  - **RTO (Recovery Time Objective):** Targeted time to restore service
  - **RPO (Recovery Point Objective):** Maximum allowable data loss period
  - **RSL (Recovery Service Level):** Required service availability percentage
- **Plan Execution:** Restore operations in an orderly manner
  - Disaster recovery concludes when normal operations resume
- **Training and Awareness:** Regular training on roles and responsibilities
  - Periodic training and awareness programs for preparedness

Importance of Backups in Disaster Recovery

- **Critical Role:** Backups are essential for disaster recovery
  - Data is central to business operations
  - Loss of data could be catastrophic
- **Purpose:** Recover data after technology failure, human error, or disaster
- **Safety Net:** Ensures data can be restored in emergencies
- **Backup Methods:** Vary from simple file copying to sophisticated strategies
  - Manual backups are error-prone; automated solutions are preferred

Types of Backup Strategies

- **Traditional Tape Backups:** Still common but hard to manage
- **Disk-to-Disk Backups:** Backup to dedicated disks, often in separate locations
  - Ensures physical disaster won't affect both primary and backup sites
- **Cloud Backups:** Use storage from providers like AWS, Azure
  - Geographic diversity and provider backups add extra protection
- **Backup Location:** Choose based on disaster recovery needs

Primary Backup Types

- **Full Backups:** Complete copy of all data
  - Provides a full recovery base
- **Differential Backups:** Copies data changed since the last full backup
  - Restores quicker with fewer files
- **Incremental Backups:** Copies data changed since the last full or incremental backup
  - Saves space but takes longer to restore
- **Restoration Example:**
  - Differential: Restore full backup + last differential
  - Incremental: Restore full backup + all incremental backups in sequence

Common Scenarios for Restoring Backups

- **Human or Technical Error:** Most common reason for restoring backups
  - Accidental file deletion or system crashes
  - Other unintentional mishaps requiring data recovery
- **Disaster Recovery Efforts:** Critical for comprehensive recovery after major events
  - Prioritize restoration of essential services first
  - Plan order of restoration based on business needs
- **Non-Persistence Goal:** Back up critical data, not entire systems
  - Use Infrastructure as Code to rebuild systems
  - Restore only unique data from backups

Alternative Restoration Methods and Tools

- **Selective Restoration:** Revert to last known good configuration
  - Useful for correcting configuration errors
  - Quick resolution without full rebuild
- **Live Boot Media:** Enables recovery without original operating system
  - Found on USB drives or similar media
  - Boot system from USB to access storage for data recovery
- **Backup Strategy Planning:** Essential for effective data and system restoration
  - Prepare for both minor errors and catastrophic events
  - Ensure diverse backup methods and tools are available

Types of Disaster Recovery Sites

- **Hot Sites:** Fully operational data centers ready to run
  - Can activate immediately or automatically when primary fails
  - Provides high redundancy but is costly
- **Cold Sites:** Basic facilities without servers or data
  - Have racks, cabling, network, and environmental controls
  - Low cost but slow to activate (weeks to months)
- **Warm Sites:** Compromise between hot and cold sites
  - Equipped with necessary hardware and software, not fully active
  - Activation time ranges from hours to days

Offsite Backup and Storage

- **Disaster Recovery Sites:** Serve as offsite data storage locations
  - Secure, geographically distant from the primary site
  - Ensures the same disaster doesn't affect both sites
- **Site Risk Assessment:** Evaluates location risks for site resiliency
- **Backup Transportation:** Physical or digital transfer methods
  - Physical: Periodic transportation of backups
  - Digital: Site replication using storage area network (SAN) or virtual machine (VM) platforms
- **Backup Format Choice:** Online vs. Offline backups
  - Online: Immediate availability, higher cost
  - Offline: Requires manual intervention, lower cost

Alternate Business Processes

- **Definition:** Alternate methods to maintain operations during disasters
- **Example:** Paper-based ordering if electronic systems are down
- **Purpose:** Provides flexibility and continuity during extended outages
- **Integration:** Part of comprehensive disaster recovery planning
  - Helps ensure business operations continue smoothly
  - Supports rapid adaptation to disaster scenarios

Types of IR/BC/DR Testing

- **Read-Throughs:** Simple review of the plan by team members
  - Also known as checklist reviews
  - Provides feedback for updates to keep the plan current
- **Walk-Throughs:** Group review, also called tabletop exercises
  - Allows discussion and collective understanding of the plan
  - More effective than read-throughs
- **Simulations:** Discuss response to specific scenarios
  - Involves detailed role-playing exercises
  - May evolve into full-scale, hands-on exercises

Advanced Testing Types

- **Parallel Tests:** Activates DR plan without full switch
  - Runs DR environment parallel to the primary site
  - Tests actual technology and procedures
- **Full-Interruption Tests:** Simulates disaster by shutting down primary environment
  - Tests the organization's ability to operate from DR site
  - Highly effective but potentially disruptive

Benefits and Strategy of Combined Testing

- **Validation of Plans:** Ensures incident response and DR plans work as expected
  - Confirms technology functionality and readiness
- **Identify Updates:** Adjust plans based on technology or business changes
  - Regular feedback loops keep plans current
- **Combined Approach:** Use multiple test types for comprehensive preparedness
  - Regular read-throughs and walk-throughs supplemented by simulations
  - Periodic parallel and full-interruption tests enhance readiness

After-action Reports

- **Executive Summary:** Concise overview of the event and key findings
- **Background Information:** Context for the event and contributing factors
  - State of environment, external influences, relevant data
- **Event Summary:** Detailed facts covering who, what, when, where, why
  - Key questions answered to provide a complete picture
- **Lessons Learned:** Evaluate performance and identify areas for improvement
  - Outline successful processes and areas needing correction
- **Next Steps:** Clear action plan with responsibilities and timelines
  - Assign accountability for implementing changes