Disaster Recovery

- Preparation for and recovery from a disaster
  - whether natural or man made

- In general, an incident is a **disaster** when:
  - organization is unable to contain or control the impact of an incident, or
  - level of damage or destruction from incident is so severe, the organization is unable to quickly recover

- Key role of DRP: defining how to reestablish operations at location where organization is usually located

Planning for Disaster

- Scenario development and impact analysis are used to categorize the level of threat of each potential disaster
- DRP must be tested regularly
- Key points in the DRP:
  - Clear delegation of roles and responsibilities
  - Execution of alert roster and notification of key personnel
  - Clear establishment of priorities
  - Documentation of the disaster
  - Action steps to mitigate the impact
  - Alternative implementations for various systems components

Crisis Management

- Crisis management is a set of focused steps taken during and after a disaster that deal primarily with people involved
- Crisis management team manages event:
  - Supporting personnel and their loved ones during crisis
  - Determining event's impact on normal business operations
  - When necessary, making a disaster declaration
  - Keeping public informed about event
  - Communicating with outside parties
- Two key tasks of crisis management team:
  - Verifying personnel status
  - Activating alert roster

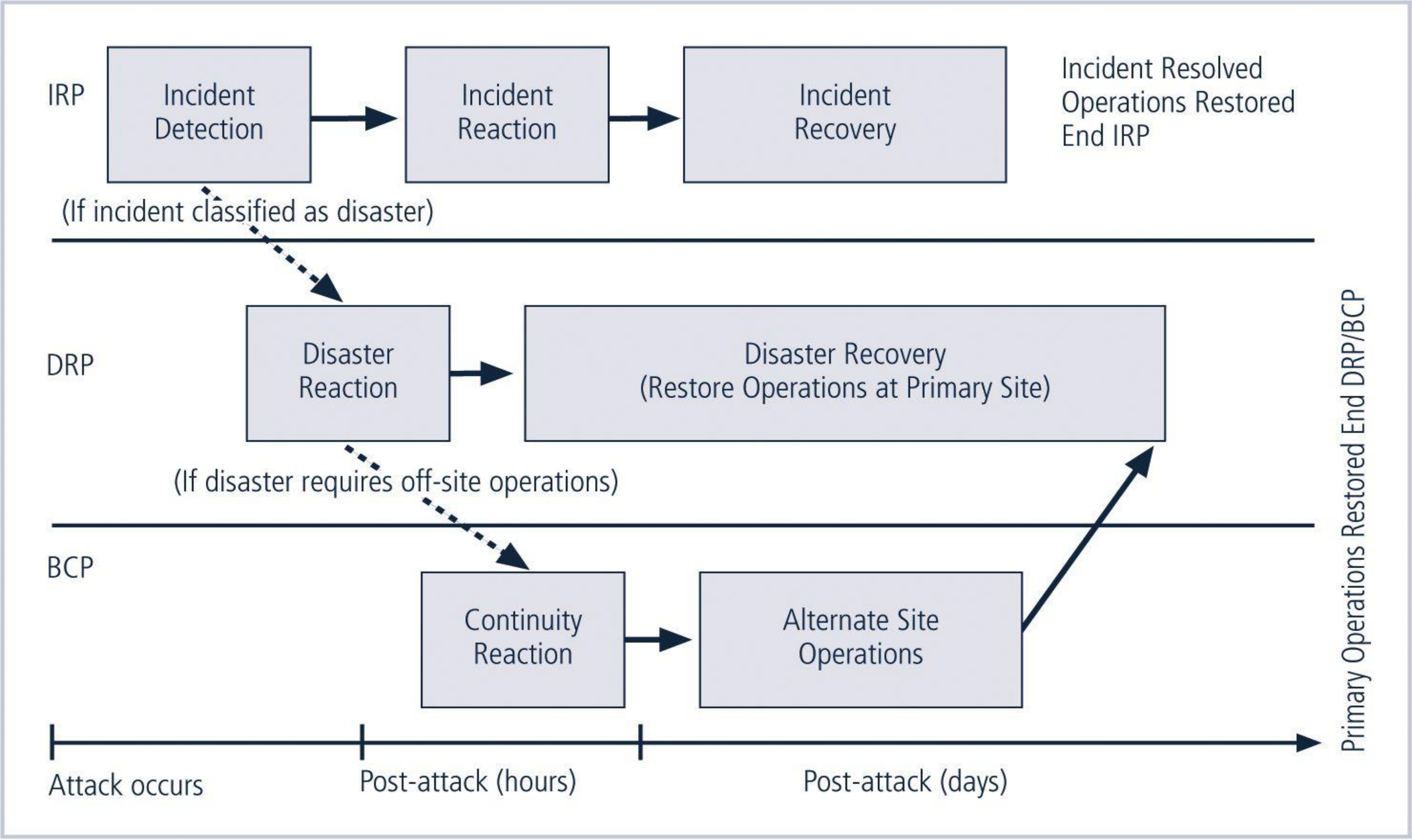
Sample Disaster Recovery Plan

- Name of agency
- Date of completion or update of the plan and test date
- 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

Business Continuity Planning (BCP)

- Ensures critical business functions can continue in a disaster
- Most properly managed by CEO of organization
- Activated and executed concurrently with the DRP when needed
- Reestablishes critical functions at alternate site (DRP focuses on reestablishment at primary site)
- Relies on identification of critical business functions and the resources to support them

Contingency Plan Implementation Timeline



4. Security Policy

Why Policy?

- A quality information security program begins and ends with policy
- Policies are least expensive means of control and often the most difficult to implement
- Some basic rules must be followed when shaping a policy:
  - Never conflict with law
  - Stand up in court
  - Properly supported and administered
  - Contribute to the success of the organization
  - Involve end users of information systems

Policy

- To produce a complete information security policy, management must define three types of information security policy (NIST 800-14):
  - Enterprise information security program policy (EISP)
  - Issue-specific information security policies (ISSP)
  - Systems-specific information security policies (SysSP)

Enterprise Information Security Policy (EISP)

- Sets strategic direction, scope, and tone for organization’s security efforts
- Assigns responsibilities for various areas of information security
- Guides development, implementation, and management requirements of information security program

EISP Elements

- EISP documents should provide :
  - An overview of corporate philosophy on security
  - Information about information security organization and information security roles
  - Responsibilities for security shared by all members of the organization
  - Responsibilities for security unique to each role within the organization

Components of the EISP

- Statement of Purpose:
  - What the policy is for
- Information Technology Security Elements:
  - Defines information security
- Need for Information Technology Security:
  - justifies importance of information security in the organization
- Information Security Responsibilities and Roles:
  - Defines organizational structure
- References Information Technology standards and guidelines

EISP: Example

- Protection Of Information:
  - Information must be protected in a manner commensurate with its sensitivity, value, and criticality
- Use Of Information:
  - Company X information must be used only for business purposes expressly authorized by management
- Information Handling, Access, And Usage:
  - Information is a vital asset and all accesses to, uses of, and processing of Company X information must be consistent with policies and standards

EISP: Example

- Data And Program Damage Disclaimers:
- Legal Conflicts
- Exceptions To Policies
- Policy Non-Enforcement
- Violation Of Law
- Revocation Of Access Privileges
- Industry-Specific Information Security Standards
- Use Of Information Security Policies And Procedures
- Security Controls Enforceability

Issue-Specific Security Policy (ISSP)

- ISSP provides detailed, targeted guidance to instruct all members of the organization in the use of technology based systems.

- An effective ISSP:
  - Articulates the organization’s expectations about how the technology-based system in question should be used
  - Documents how the technology-based system is controlled and identifies the processes and authorities that provide this control
  - Serves to indemnify the organization against liability for an employee’s inappropriate or illegal system use

Issue-Specific Security Policy (ISSP)

- Every organization’s ISSP should:
  - Address specific technology-based systems
  - Require frequent updates
  - Contain an issue statement on the organization’s position on an issue
- ISSP topics could include:
  - E-mail use,
  - Internet and World Wide Web use,
  - Specific minimum configurations of computers to defend against worms and viruses,
  - Prohibitions against hacking or testing organization security controls,
  - Etc.

Typical ISSP Components

- Statement of Purpose
  - Scope and Applicability
  - Definition of Technology Addressed
  - Responsibilities
- Authorized Access and Usage of Equipment
  - User Access
  - Fair and Responsible Use
  - Protection of Privacy
- Prohibited Usage of Equipment
  - Disruptive Use or Misuse
  - Criminal Use
  - Offensive or Harassing Materials
  - Copyrighted, Licensed or other Intellectual Property
  - Other Restrictions

Components of the ISSP (Continued)

- Systems Management
  - Management of Stored Materials
  - Employer Monitoring
  - Virus Protection
  - Physical Security
  - Encryption
- Violations of Policy
  - Procedures for Reporting Violations
  - Penalties for Violations
- Policy Review and Modification
  - Scheduled Review of Policy and Procedures for Modification
- Limitations of Liability
  - Statements of Liability or Disclaimers

Systems-Specific Policy (SysSP)

- Systems-Specific Policies (SysSPs) frequently do not look like other types of policy

- They may often be created to function as
  - standards or procedures to be used when configuring or maintaining systems

- SysSPs can be separated into:
  - Management guidance
  - Technical specifications