

IT 4823

Information Security Administration

Contingency Planning and Business Continuity



Notice: This session is
being recorded.

Three Kinds of Contingency Plans

- Incident Response Plan (during)
- Disaster Recovery Plan (immediately after)
- Business Continuity Plan (longer-term)

Incident Response Plan

- IRP focuses on immediate response; what to do during a security incident.
 - Notifications
 - Actions
 - Limitations
- If incident escalates or is disastrous, the process changes to disaster recovery and business continuity.

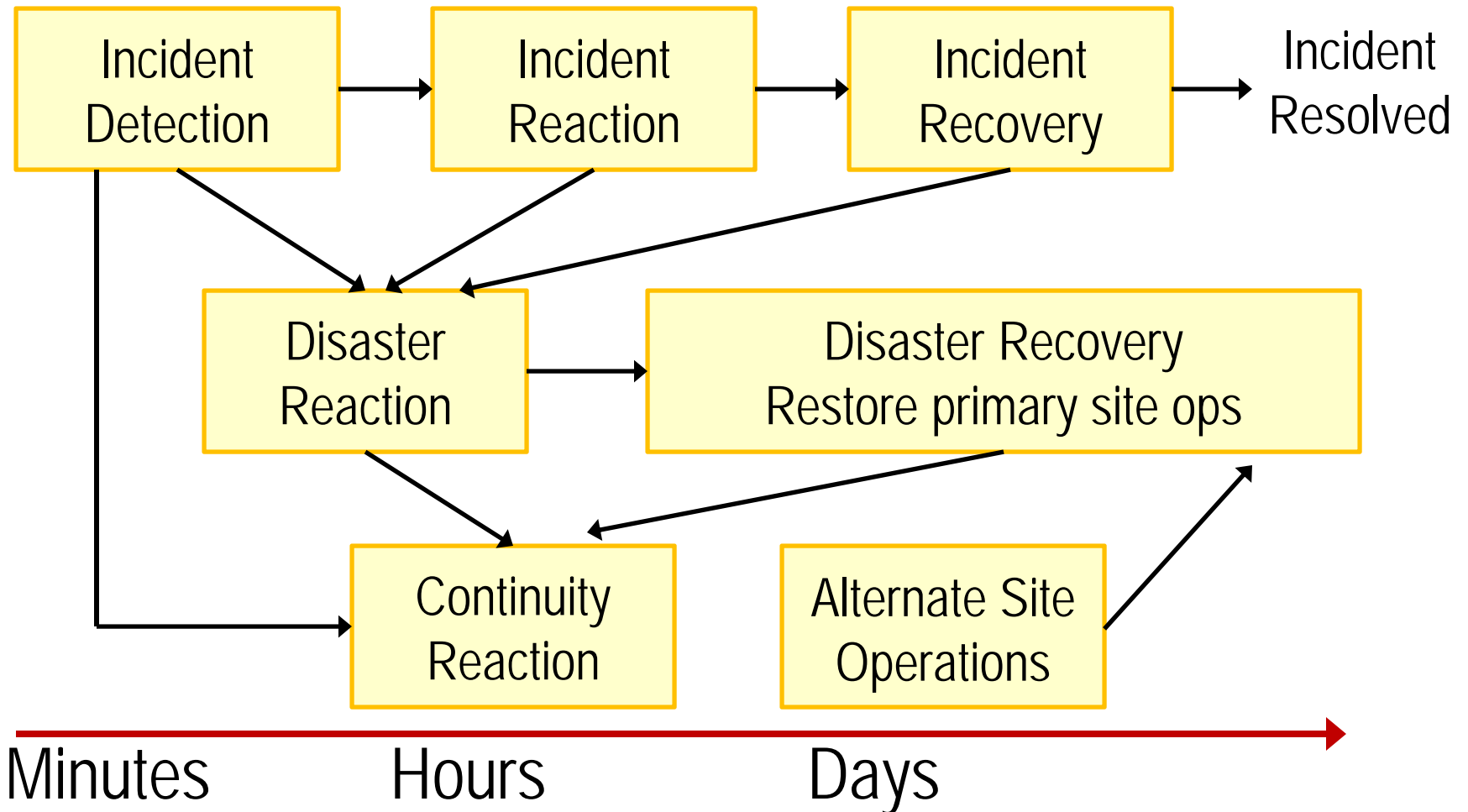
Disaster Recovery Plan

- Focuses on restoring systems after disasters occur;
- Outcomes:
 - Continued operation *or*
 - Implementation of BCP

Business Continuity Plan

- The BCP is implemented concurrently with DRP
 - when damage is major ...
 - or long term, requiring more than simple restoration of information and information resources

Contingency Planning Timeline



The Planning Team

- Champion: high-level manager to support, promote, and endorse findings of project
- Project manager: leads project and makes sure sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed
- Team members: should be managers or their representatives from various communities of interest: business, IT, and information security

Major Steps in Contingency Planning

Business Impact Analysis

Identification of threats and attacks

Business unit analysis

Scenarios of successful attacks

Assessment of Potential Damage

Classification of subordinate plans

IR Planning

Incident planning

Incident detection

Incident reaction

Incident Recovery

DR Planning

Plan for disaster recovery

Crisis management

Recovery Operations

BC Planning

Establish continuity strategy

Plan for continuity of operations

Continuity management

Incident Response Planning

- Incident response planning covers
 - identification of,
 - classification of, and
 - response to an incident

Attacks, Events, and Incidents

- “Attack” implies both purposefulness and malice.
- Most security compromises are not the result of attacks!
 - Employee error
 - Hardware, software, or utility failure
 - Natural or accidental events, *e.g.* flood or fire
- Think about security “events”

Think in Broad Terms

- Often the result of an event is more important than the cause.
- Example: the corporate data center becomes inaccessible
 - Fire in the data center
 - Fire elsewhere in the building
 - Flood
 - Toxic substance
- The *result* is the same, or close to it.

Incident Response Planning

- Events are classified as incidents if they
 - Threaten confidentiality, integrity, or availability of information resources
 - With a reasonable probability of damage
- Incident response (IR) is more reactive than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

Predefined Responses

- Pre-defined responses enable organization to react quickly and effectively to incidents if:
 - An incident (result) was foreseeable
 - Organization has IR team
 - Organization can detect the incident
 - IR team consists of individuals needed to handle systems as incident takes place
- Planners should develop guidelines for reacting to and recovering from foreseeable incidents

Incident Detection

- Most common indication is a complaint about technology support, often delivered to help desk
- Careful training is needed to quickly identify and classify an incident
- Once an incident is properly identified and classified, the organization can respond

Incident Reaction

- Consists of actions that guide organization to stop incident, mitigate impact of incident, and provide information for recovery from incident
- In reacting to an incident there are actions that must occur quickly:
 - Notification of key personnel
 - Containment of damage
 - Documentation of incident

Incident Containment Strategies

- Before incident can be contained, scope must be determined
- Actions:
 - stop or contain the incident
 - regain control of systems and physical spaces
 - attempt to recover
 - consider “external relations”

Incident Recovery

- Assess damage
- Identify human resources needed
- Implement recovery measures
- Repair vulnerabilities, address any shortcomings in safeguards, and restore data and services of the systems

Damage Assessment

- Sources of information on damage:
 - system logs;
 - intrusion detection logs;
 - configuration logs and documents;
 - documentation from incident response;
 - results of detailed assessment of systems and data storage

Damage Assessment

- Computer evidence must be carefully collected, documented, and maintained to be acceptable in formal proceedings
- Individuals who assess damage may need special training

Recovery

- Once extent of damage determined, recovery process can begin
- Process involves much more than simple restoration of stolen, damaged, or destroyed data files
- Example: How do you know whether a particular file has been read? Written? Are you sure?

Automated Response

- Some systems can respond to incident threat autonomously
- Downsides of current automated response systems may outweigh benefits
- Entrapment is luring an individual into committing a crime to get a conviction
- Enticement is legal and (may be) ethical, while entrapment is not

Disaster Recovery Planning

- Disaster recovery planning (DRP) is planning the preparation for and recovery from a disaster
- The contingency planning team must decide which circumstances constitute disasters and which constitute incidents.
- This is a policy decision as much as a technical decision.

Disaster Recovery Planning

- When situations are classified as disasters, plans change as to how to respond; take action to secure most valuable assets to preserve value for the longer term
- DRP strives to reestablish operations at the primary site

Disaster Recovery Functions

- Restore access to critical physical spaces (if applicable)
- If a recurrence is likely (*e.g.* cracking, malicious code) implement safeguards
- Repair/restore equipment
- Repair/restore software
- Repair/restore data

Business Continuity Planning

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the critical facilities unusable for continued operations, there must be a plan to allow business to continue functioning

Business Continuity Planning

- Select a continuity strategy
- Integrate off-site data storage and recovery functions into this strategy
- Conduct business impact assessment (BIA)

Business Impact Assessment

- For each IT function, determine
 - Its relationship to the function of the organization
 - Time period required for recovery
 - Fallback position, if possible
- This can produce a matrix, not just a linear list.
- Example: The criticality of the payroll system rises as payday approaches.

BIA Categories

- Critical – Required for the basic functioning of the organization
- Necessary – Required for normal operations; absence of this function impairs operation.
- Improves efficiency – Not needed for normal operation, but operation is more efficient when available.
- Optional – Does not affect the primary mission of the organization.
- Must also consider time frames!

Continuity Strategies

- In general there are three exclusive options:
 - hot sites;
 - warm sites;
 - cold sites
- The determining factor in selecting between options is usually cost-effectiveness
- Three shared functions: time-share; service bureaus; and mutual aid agreements

Backup Strategies

- Full backup
- Differential backup (full + 1 needed)
- Incremental backup (full + all needed)
- Delta backup (full + all, and complex restore)
- Database journals
- Understand your data!

Backup Frequency/Retention

- Frequency: how much can you afford to lose (Brown's laptop; about one day)
- Retention: how far back might you need to go. (Pretty far!)
- Cost and storage considerations
- Off-site storage: Why are backups needed?
 - To recover from errors
 - Disaster recovery
 - Reconstruction of historical data
- These have different storage requirements.

Archival (Long-Term) Retention

- Backup media degrade
(Generally, periods measured in years.)
- So, how long might you need to recover old data?
(Health care: 28 or more years!)
- Backup media become obsolete
(We have the data, but it's on 7-track magnetic tape!)

Off-Site Disaster Data Storage

- To get sites up and running quickly, organization must have ability to port data into new site's systems
- Options for getting operations up and running include:
 - Electronic vaulting (batch process)
 - Remote journaling (journal records only)
 - Database shadowing (duplicate database)
 - Remote storage attachment networks

Consolidated Contingency Plan

- Single document set approach supports concise planning and encourages smaller organizations to develop, test, and use IR, DR and BC plans
- This model is based on analyses of disaster recovery and incident response plans of dozens of organizations

The Planning Document

Six steps in contingency planning process:

- Identifying mission- or business-critical functions
- Identifying resources that support critical functions
- Anticipating potential contingencies or disasters
- Selecting contingency planning strategies
- Implementing contingency strategies
- Testing and revising strategy

Identifying Critical Functions

- What information processing functions are critical (to survival of the business) in the next 24 hours?
- What functions are critical in the next seven days?
- What functions are critical in the next 30 days?
- Example: Payroll is critical at the next pay date. (Strategy: pay the same as previous.)

Location of the Plan

- Copies in several locations:
 - Data center
 - Corporate headquarters
 - Key employees' homes
- An off-site electronic copy, *e.g.* at a Web hosting company, or maybe on employees' iPads.

Keeping The Plan Up to Date

- Regular reviews
 - Annually
 - When major systems are commissioned or decommissioned.
- Revise electronic copy as necessary
- Print new paper copies
 - Require exchanges
 - Account for out-of-date copies

Law Enforcement Involvement

- When an incident constitutes a violation of law, the organization may determine involving law enforcement is necessary
- Policy questions: (Decide these *in advance!*)
 - When should organization get law enforcement involved?
 - What level of law enforcement agency should be involved (local, state, federal)?
 - What happens when law enforcement agency is involved?

Law Enforcement Involvement

- Some questions are best answered by organization's legal department or law firm.
- If organization detects a criminal act, it may be legally obligated to involve appropriate law enforcement officials
- It is helpful to have made contacts in advance, especially with local law enforcement.

Advantages of Law Enforcement Involvement

Involving law enforcement has advantages:

- Agencies may be better equipped to process evidence
- Law enforcement agencies are prepared to handle warrants and subpoenas needed
- Law enforcement officers are skilled at obtaining witness statements and other information collection

Disadvantages of Involvement

Involving law enforcement has disadvantages:

- Once a law enforcement agency takes over case, organization loses some control over chain of events
- Organization may not hear about case for weeks or months
- Equipment vital to the organization's business may be seized as evidence

Crisis Management

- Actions taken during and after a disaster that focus on people involved and address the viability of the business
- A *separate* crisis management team is responsible for managing event from an enterprise perspective.

Crisis Management Functions

- Supporting personnel and families during crisis
- Determining impact on normal business operations and, if necessary, making disaster declaration
- Keeping the public informed
- Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Questions

