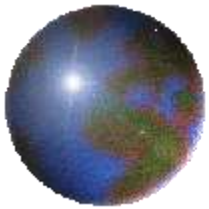


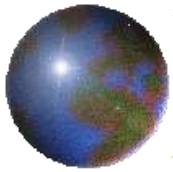
Chapter 5 Planning for Security

Begin with the end in mind.

STEPHEN COVEY, AUTHOR OF SERVEN HABITS OF HIGHLY EFFECTIVE PEOPLE

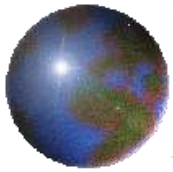
PRINCIPLES OF INFORMATION SECURITY

Second Edition



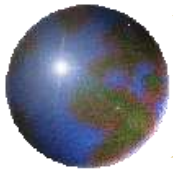
Introduction

- Creation of information security program includes:
  - Creation of *policies, standards, and practices*, selection or creation of information security architecture and the development
  - Use of a detailed information security *blueprint* creates plan for future success
  - Creation of *contingency planning* consisting of incident response planning, disaster recovery planning, and business continuity plans
- Without policy, blueprints, and planning, organization is unable to meet information security needs of various communities of interest



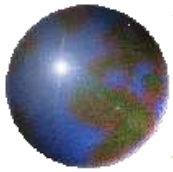
Information Security Policy, Standards and Practices

- Communities of interest must consider policies as basis for all information security efforts
- Policies direct how issues should be addressed and technologies used
- Security policies are least expensive controls to execute but most difficult to implement
- Shaping policy is difficult



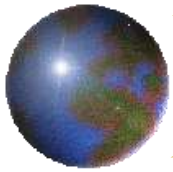
Shaping Policy Difficult

- Never conflict with laws
- Standup in court if challenged
- Be properly administered through dissemination and documented acceptance



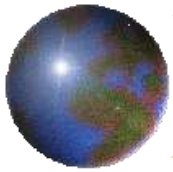
Policy

- Plan or course of action
- Convey instructions
- Organizational laws
- Dictate acceptable and unacceptable behavior



Policy

- Define
  - What is right
  - What is worn
  - The appeal process
  - What are the penalties for violating policy
- Written to support the mission, vision and strategic plan of organization
- For a policy to be effective, must be properly disseminated, read, understood and agreed to by all members of organization



Standards

- Detail statements of what must be done to comply with policy
- Types
  - Informal – de facto standards
  - Formal – de jure standards

Mission/Vision/Strategic Plan

- Mission – written statement of organization purpose
- Vision – written statement of organization goals
- Strategic Plan - written statement of moving the organization toward its mission

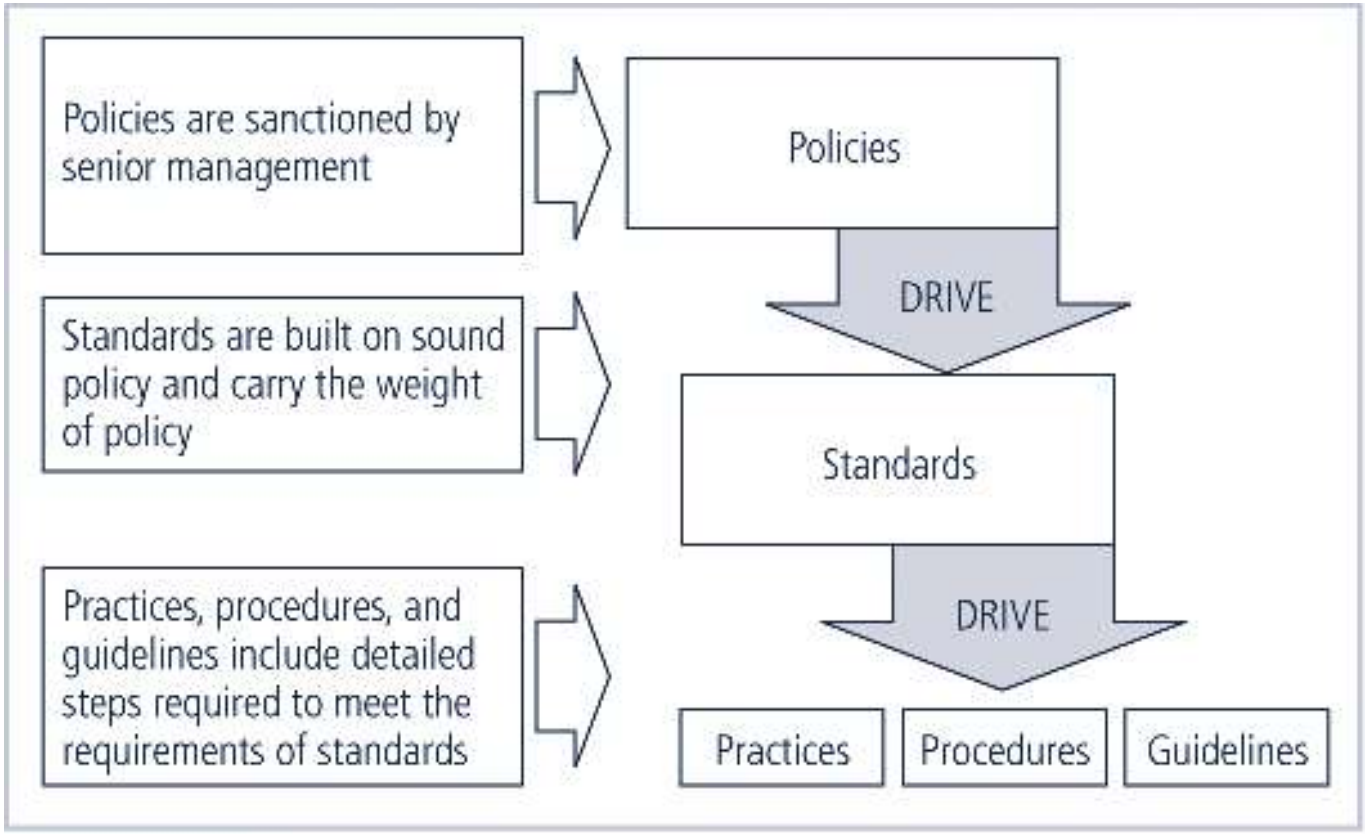
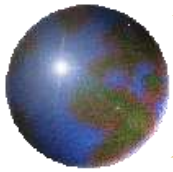
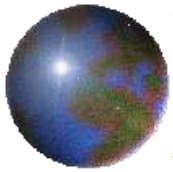


FIGURE 5-1 Policies, Standards, and Practices



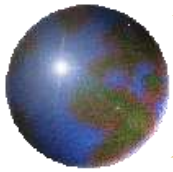
Policies

- Security Policy – set of rules that protects and organization's assets
- Information security policy – set of rules that protects an organization’s information assets
- Three types
  - General Issue-specific
  - System-specific



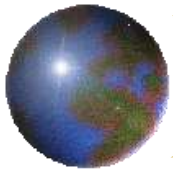
Enterprise Information Security Policy (EISP)

- General Information Security Document
- Shapes the philosophy of security in IT
- Executive-level document, usually drafted by or with CIO of the organization, 2-10 pages
- Typically addresses compliance in two areas
  - Ensure *meeting requirements* to establish program
  - *Responsibilities* assigned therein to various organizational components
  - Use of specified *penalties and disciplinary action*



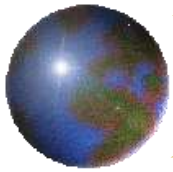
ISSP

- Issue-Specific Security Policy
- Addresses specific areas of technology
- Requires frequent updates
- Contains a statement on the organization's position on a specific issue



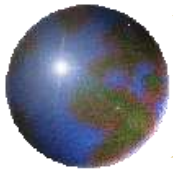
3 Approaches to ISSP

- Create independent document tailored to a specific issue
  - Scattered approach
  - Departmentalized
- Create single comprehensive document covering all issues
  - Centralized management and control
  - Tend to over generalize the issue
  - Sip vulnerabilities



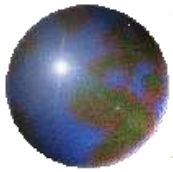
3 Approaches to ISSP

- Create a modular plan
  - Unified policy creation and administration
  - Maintain each specific issue's requirements
  - Provide balance



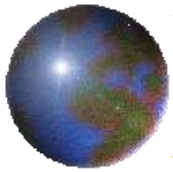
ISSP

- Statement of Policy
- Authorization Access & Equipment Use
- Prohibited Equipment Use
- System Management
  - Focus on user's relationship
- Violations of Policy
- Policy review & modification
- Limitations & Liability



Systems-Specific Policy (SysSP)

- SysSPs frequently codified as standards and procedures
- used when configuring or maintaining systems
- Systems-specific policies fall into two groups
  - Access control lists (ACLs)
  - Configuration rules

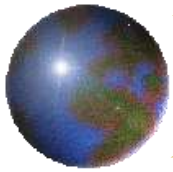


ACL Policies

- Restrict access from anyone & anywhere
- Can regulate specific user, computer, time, duration, file
- What regulated
  - Who can use the system
  - What authorization users can access
  - When authorization users can access
  - Where authorization users can access

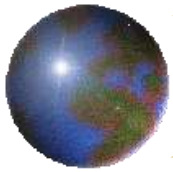
ACL Policies

- Authorization determined by persons identity
- Can regulated specific computer equipment
- Regulate access to data
  - Read
  - Write
  - Modify
  - Copy
  - Compare



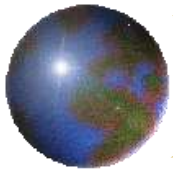
Rule Policies

- Rule policies are more specific to operation of a system than ACLs
- May or may not deal with user directly
- Many security systems require specific configuration scripts telling systems what actions to perform on each set of information they process



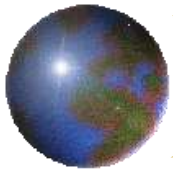
Policy Management

- Living documents
- Must be managed as they constantly changed and grow
- Must be properly disseminated
- Must be properly managed
- Responsible individual
  - Policy administrator
  - Champion & manager
  - Not necessarily a technically oriented person



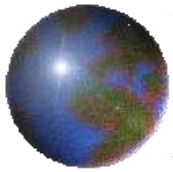
Reviews

- Schedule
  - Retain effectiveness in changing environment
  - Periodically reviewed
  - Should be defined and published
  - Should be reviewed at least annually
- Procedures and practices
  - Recommendations for change
  - Reality one person draft



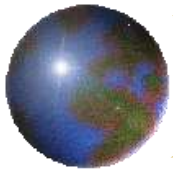
Document Configuration Management

- Include date of original
- Includes date of revision
- Include expiration date



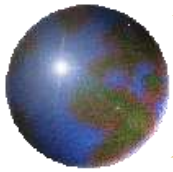
Information Classification

- Classification of information is an important aspect of policy
- Policies are classified, least for “internal use only”.
- *A clean desk policy* stipulates that at end of business day, classified information must be properly stored and secured
- In today’s open office environments, may be beneficial to implement a clean desk policy



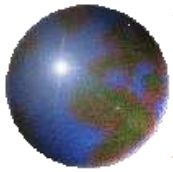
The Information Security Blueprint

- Security Blueprint is the basis for design, selection, and implementation of
  - all security policies,
  - education and training programs, and
  - technological controls
- More detailed version of security framework (outline of overall information security strategy for organization)
- Should specify tasks to be accomplished and the order in which they are to be realized
- One approach to selecting a methodology by which to develop an information security blueprint is to adopt a published model or framework for information security.



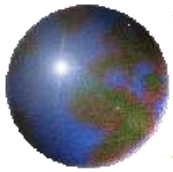
ISO 17799/BS7799

- Information technology – code of practice for information security management from
- ISO (International Organization for Standards)
- IEC (International Electro-technical Commission)
- One of the most widely referenced and often discussed security models
- ISO/IEC 17799
  - Purpose – "give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization.
  - Provides a common basis
  - Must pay for these



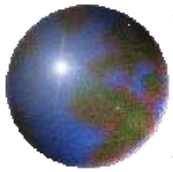
NIST Security Models

- Another possible approach described in documents available from Computer Security Resource Center of National Institute for Standards and Technology (NIST)
- Public ally available at no charge
- Several publications dealing with various aspects



NIST Special Publication 800-14

- Security supports mission of organization; is an integral element of sound management
- Security should be cost-effective; owners have security responsibilities outside their own organizations
- Security responsibilities and accountability should be made explicit; security requires a comprehensive and integrated approach
- Security should be periodically reassessed; security is constrained by societal factors
- 33 Principles enumerated



IETF Security Architecture

- Internet Engineering Task Force
- Security Area Working Group acts as advisory board for protocols and areas developed and promoted by the Internet Society
- *RFC 2196: Site Security Handbook* covers five basic areas of security with detailed discussions on development and implementation

VISA International Security Model

- VISA Internal
  - Developed two important documents that improve and regulate information systems: “Security Assessment Process”; “Agreed Upon Procedures”
  - Focus on system that can and do integrate with VISA
- Base lining and Best Practices
  - Comparison of your organization security with another

Hybrid Framework for a Blueprint of an Information Security System

- Result of a detailed analysis of components of all documents, standards, and Web-based information described previously
- Offered here as a balanced introductory blueprint for learning the blueprint development process
- People must become a layer of security
- Human firewall
- Information security implementation
  - Policies
  - People
    - Education, training, and awareness
    - Technology

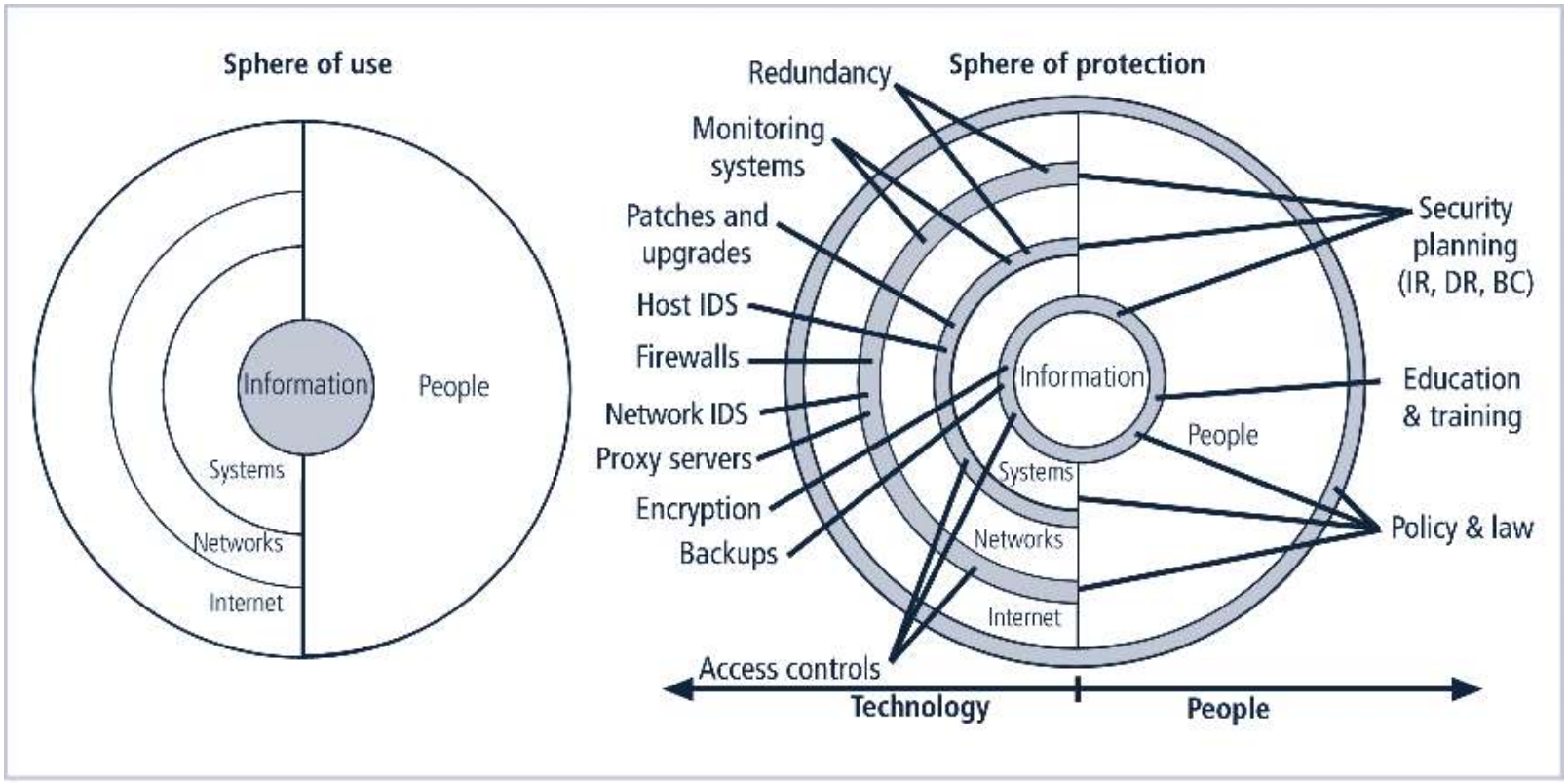
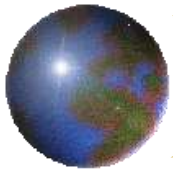
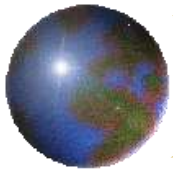


FIGURE 5-15 Spheres of Security



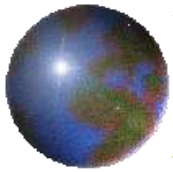
Hybrid Framework

- Managerial Controls
  - Cover security process
  - Implemented by security administrator
  - Set directions and scope
  - Addresses the design and implementation
  - Addresses risk management & security control reviews
  - Necessity and scope of legal compliance



Hybrid Framework

- Operational Controls
  - Operational functionality of security
  - Disaster recovery
  - Incident response planning
  - Personnel and physical security
  - Protection of production inputs and outputs
  - Development of education, training & awareness
  - Addresses hardware and software system maintenance
  - Integrity of data

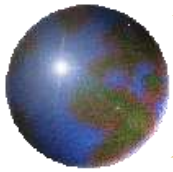


Hybrid Framework

- Technical Controls
  - Addresses the tactical & technical issues
  - Addresses specifics of technology selection & acquisition
  - Addresses identification
  - Addresses authentication
  - Addresses authorization
  - Addresses accountability

Hybrid Framework

- Technical Controls
  - Addresses development and implementation of audits
  - Covers cryptography
  - Classification of assets and users

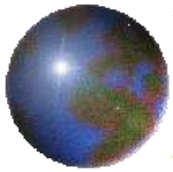


Design of Security Architecture

- Security Architecture Components
  - Defenses in Depth,
    - Implementation of security in layers, policy, training, technology.
    - Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls
  - Security Perimeter
    - Point at which an organization's security protection ends and outside world begins
    - Does not apply to internal attacks from employee threats or on-site physical threats

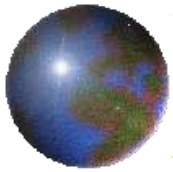
Design of Security Architecture

- Security Architecture Components
  - First level of security – protects all internal systems from outside threats
  - Multiple technologies segregate the protected information
  - Security domains or areas of trust



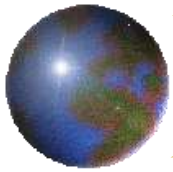
Key Technology Components

- Firewall
  - Device that selectively discriminates against information flowing in and out
  - Specially configured computer
  - Usually on parameter part of or just behind gateway router
- DMZ
  - Buffer against outside attacks
  - No mans land between computer and world
  - Web servers often go here



Key Technology Components

- Proxy Server
  - Performs actions of behalf of another system
  - Configured to look like a web server
  - Assigned the domain name
  - Retrieves and transmits data
  - Cache server



Key Technology Components

- IDS
  - Intrusion Detection System
  - Host based
    - Installed on machines they protect
    - Monitor host machines
  - Network based
    - Look at patterns of network traffic
    - Attempt to detect unusual activity
    - Requires database of previous activity
    - Uses “machine learning” techniques
    - Can use information form similar networks

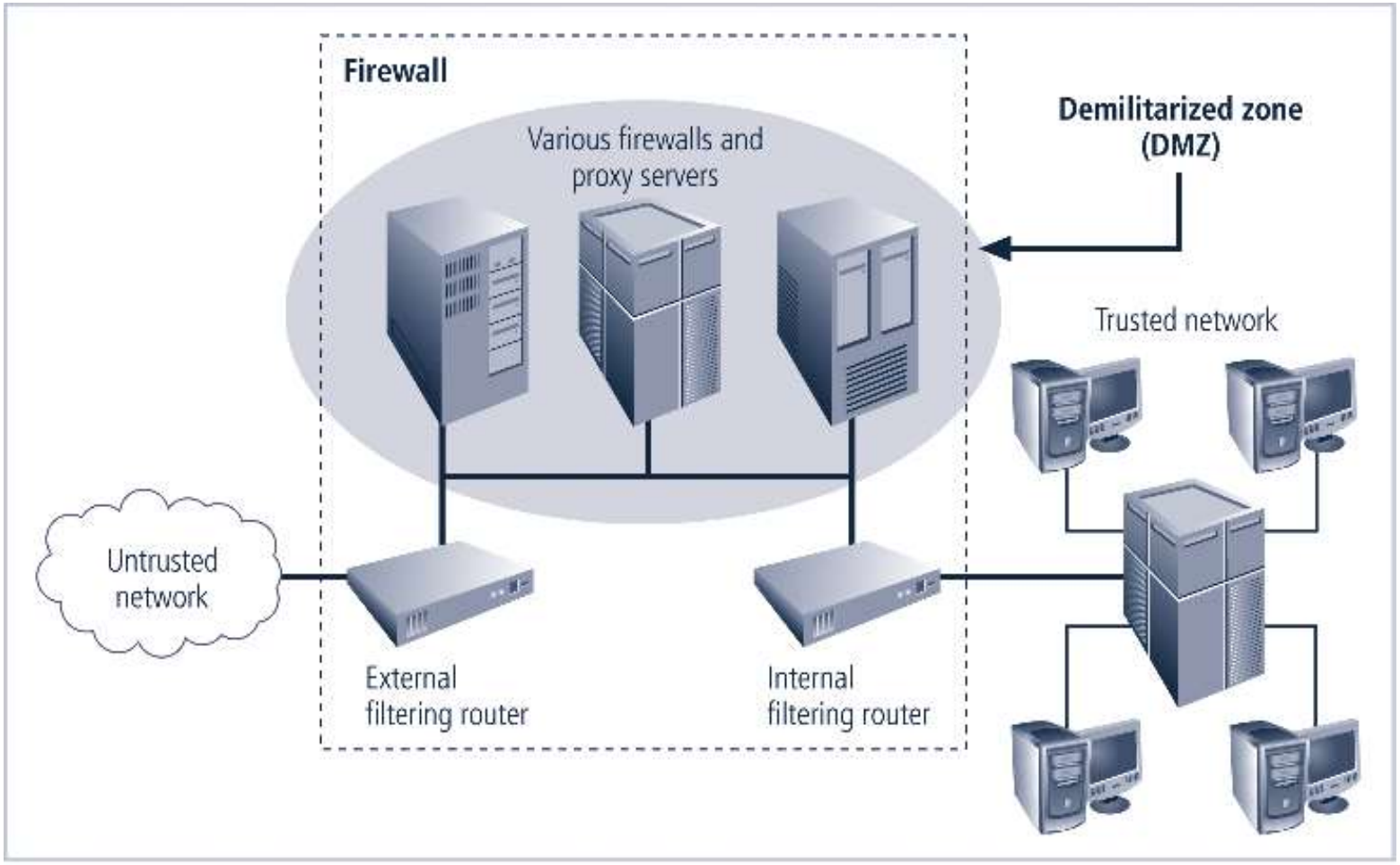
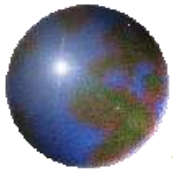
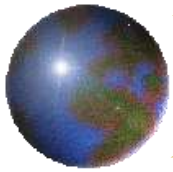


FIGURE 5-18 Firewalls, Proxy Servers, and DMZs



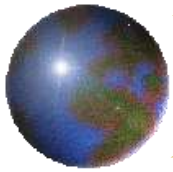
Key Technology Components

- SETA
  - Security education, training and awareness
  - Employee errors among top threats
  - Purpose
    - Improve awareness of need to protect
    - Develop skills and knowledge
    - Build in-depth knowledge to design, implement, or operate security programs



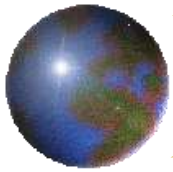
Security Education

- Everyone in an organization needs to be trained and aware of information security; not every member needs formal degree or certificate in information security
- When formal education for individuals in security is needed, an employee can identify curriculum available from local institutions of higher learning or continuing education
- A number of universities have formal coursework in information security



Security Training

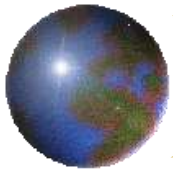
- Involves providing members of organization with detailed information and hands-on instruction designed to prepare them to perform their duties securely
- Management of information security can develop customized in-house training or outsource the training program



Security Awareness

- One of least frequently implemented but most beneficial programs is the security awareness program
- Designed to keep information security at the forefront of users' minds
- Need not be complicated or expensive
- If the program is not actively implemented, employees begin to "tune out" and risk of employee accidents and failures increases

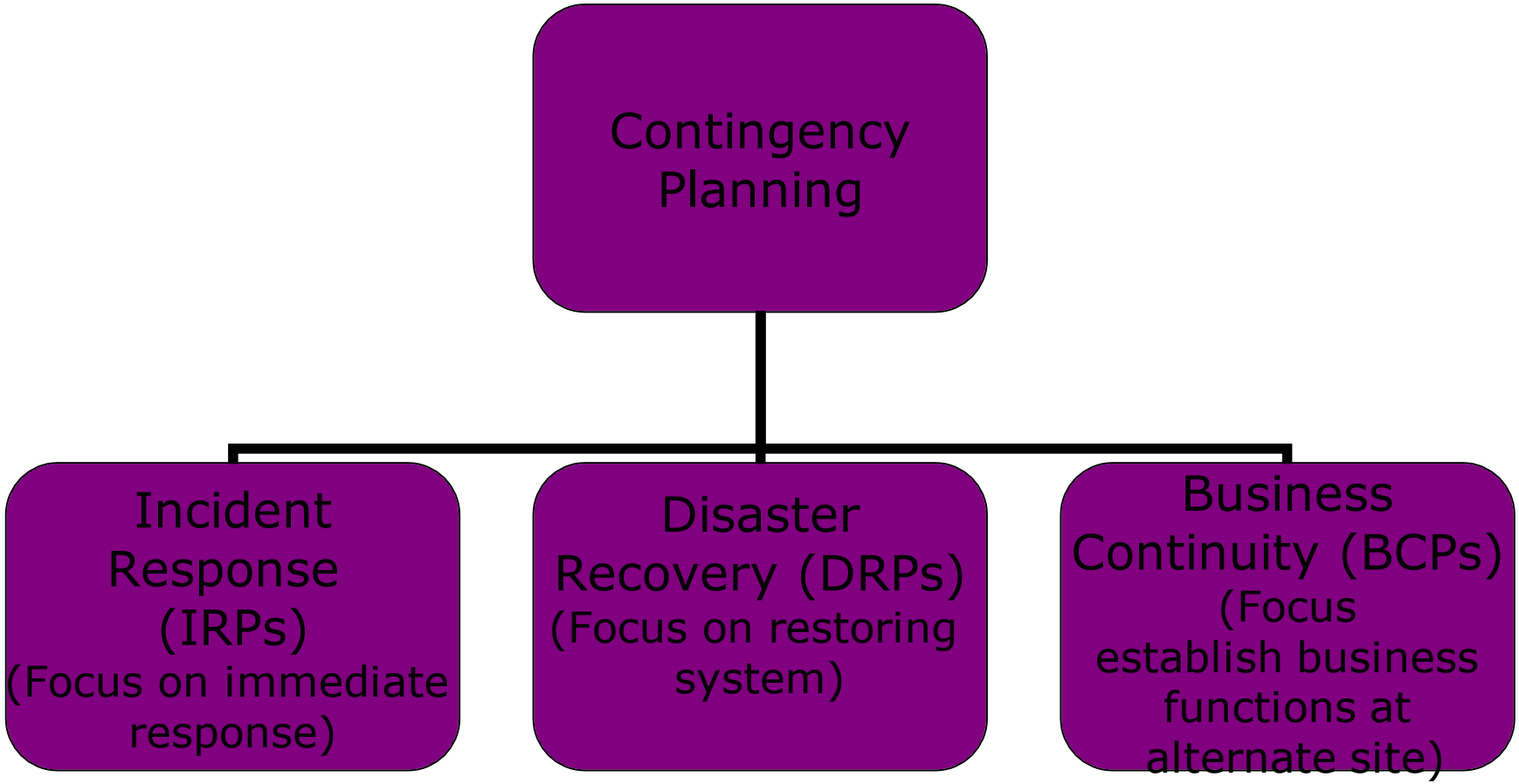
Continuity Strategies



Continuity Strategies

- Continuous availability of info systems
- Probability high for attack
- Managers must be ready to act
- Contingency Plan (CP)
  - Prepared by organization
  - Anticipate, react to, & recover from attacks
  - Restore organization to normal operations

Components of Contingency Plan



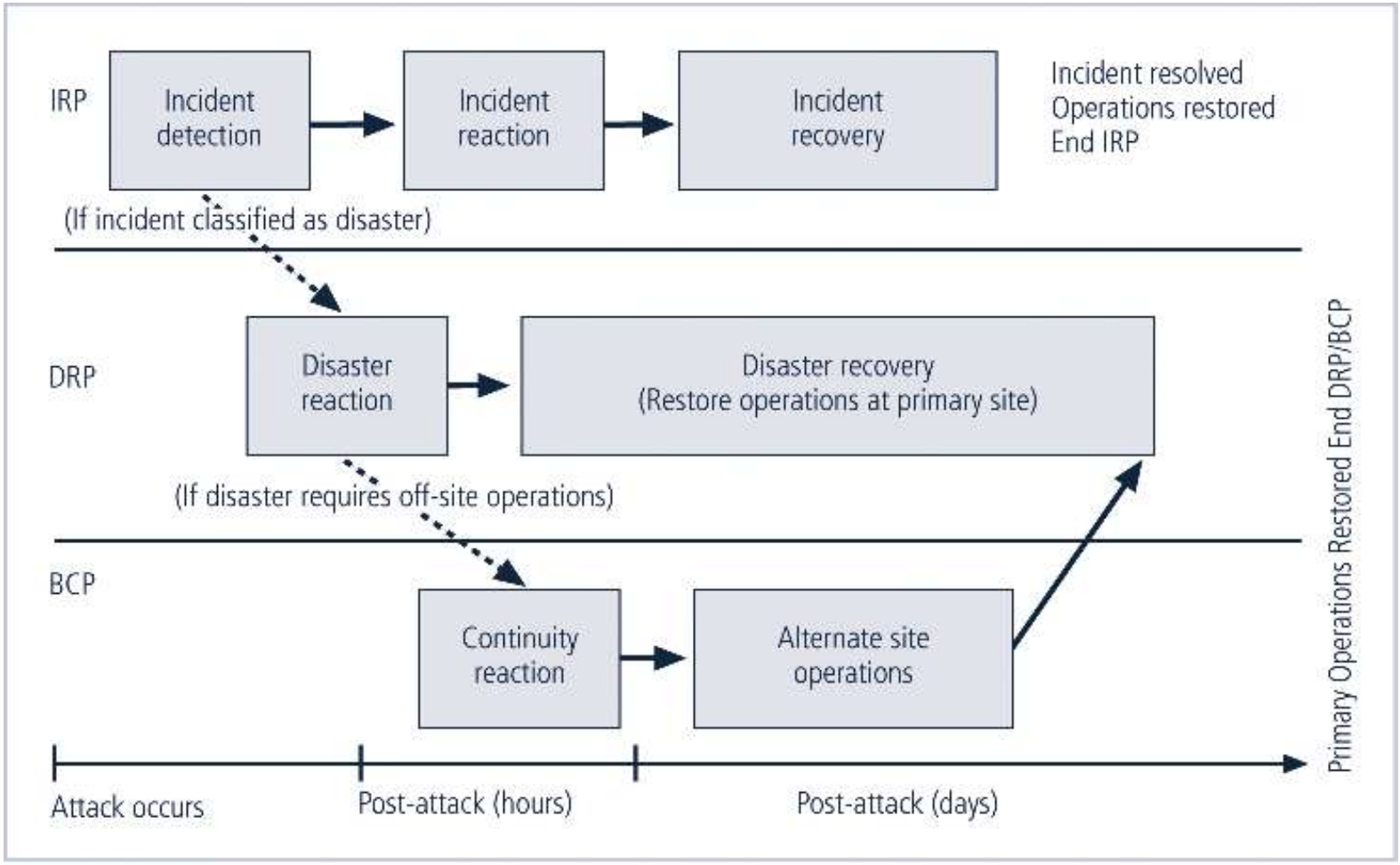
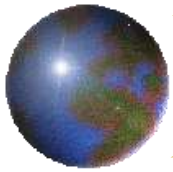


FIGURE 5-22 Contingency Planning Timeline



Continuity Strategies (continued)

- Before planning can begin, a team has to plan effort and prepare resulting documents
- 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

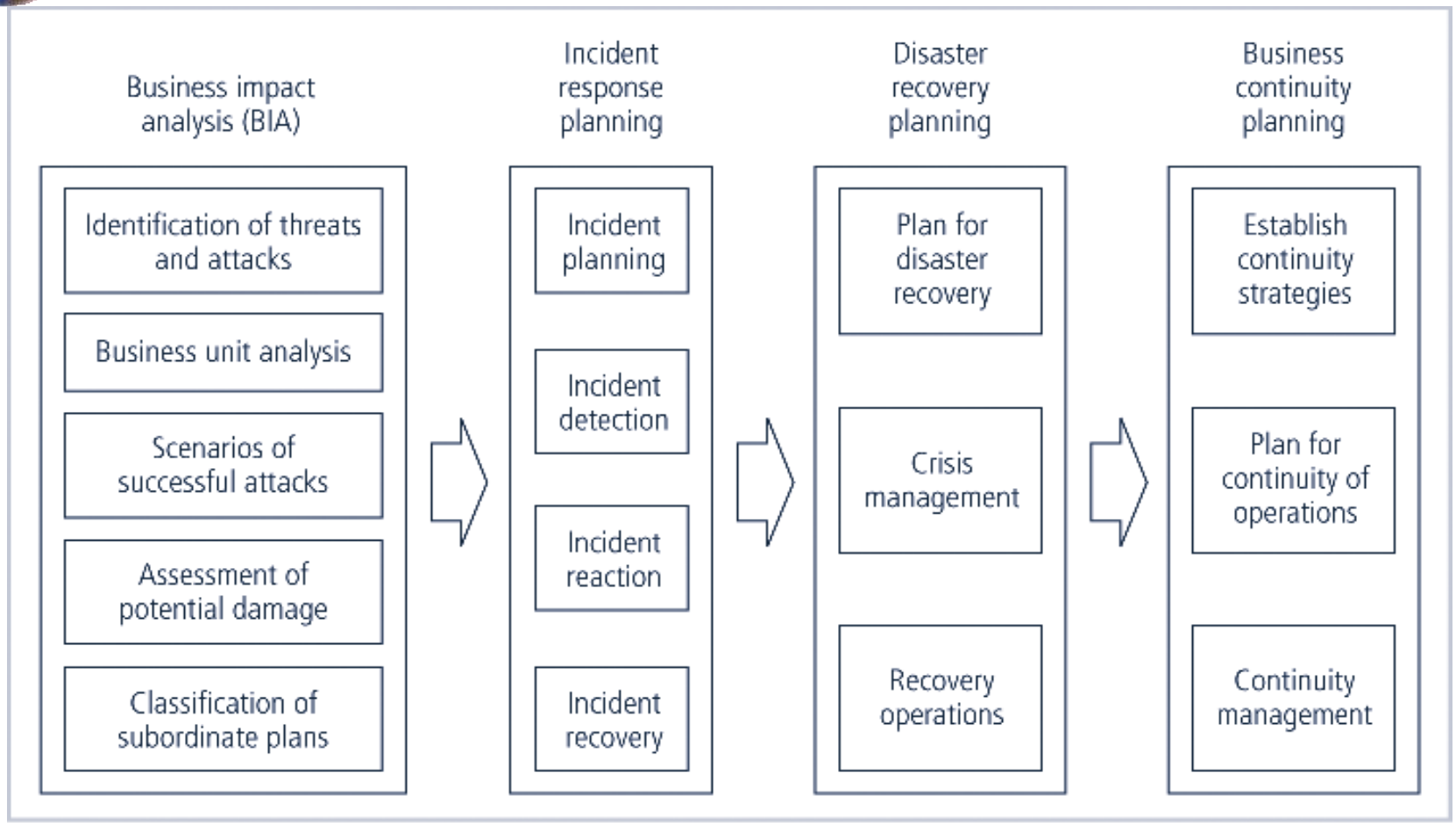


FIGURE 5-23 Major Steps in Contingency Planning

Business Impact Analysis (BIA)

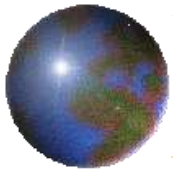
- Investigate & assess impact of various attack
- First risk assessment – then BIA
- Prioritized list of threats & critical info
- Detailed scenarios of potential impact of each attack
- Answers question
  - "if the attack succeeds, what do you do then?"

BIA Sections

- Threat attack identification & prioritization
  - Attack profile – detailed description of activities that occur during an attack
  - Determine the extent of resulting damage
- Business Unit analysis
  - Analysis & prioritization-business functions
  - Identify & prioritize functions w/in orgs units

BIA Sections

- Attack success scenario development
  - Series of scenarios showing impact
  - Each treat on prioritized list
  - Alternate outcomes
    - Best, worst, probable cases
- Potential damage assessment
  - Estimate cost of best, worst, probable
  - What must be done under each
  - Not how much to spend
- Subordinate Plan Classification
  - Basis for classification as disastrous not disastrous

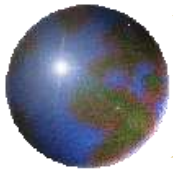


Incident Response Planning (IRPs)

- Incident response planning covers identification of, classification of, and response to an incident
- Attacks classified as incidents if they:
  - Are directed against information assets
  - Have a realistic chance of success
  - Could threaten confidentiality, integrity, or availability of information resources
- 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

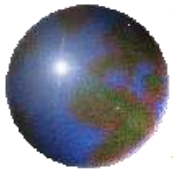
Incident Response

- Set of activities taken to plan for, detect, and correct the impact
- Incident planning
  - Requires understanding BIA scenarios
  - Develop series of predefined responses
  - Enables org to react quickly
- Incident detection
  - Mechanisms – intrusion detection systems, virus detection, system administrators, end users



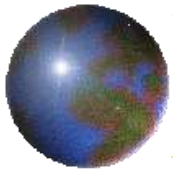
Incident Detection

- Possible indicators
  - Presence of unfamiliar files
  - Execution of unknown programs or processes
  - Unusual consumption of computing resources
  - Unusual system crashes



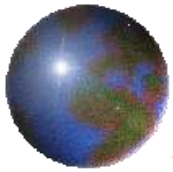
Incident Detection

- Probable indicators
  - Activities at unexpected times
  - Presence of new accounts
  - Reported attacks
  - Notification form IDS
- Definite indicators
  - Use of dormant accounts
  - Changes to logs
  - Presence of hacker tools
  - Notification by partner or peer
  - Notification by hackers



Incident Detection

- Predefined Situation
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality
  - Violation of policy
  - Violation of law

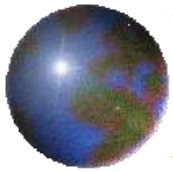


Incident Reaction

- Actions outlined in the IRP
- Guide the organization
  - Stop the incident
  - Mitigate the impact
  - Provide information recovery
- Notify key personnel
- Document incident

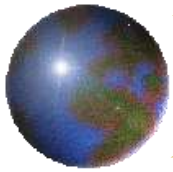
Incident Containment Strategies

- Sever affected communication circuits
- Disable accounts
- Reconfigure firewall
- Disable process or service
- Take down email
- Stop all computers and network devices
- Isolate affected channels, processes, services, or computers



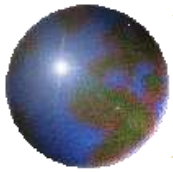
Incident Recovery

- Get everyone moving and focused
- Assess Damage
- Recovery
  - Identify and resolve vulnerabilities
  - Address safeguards
  - Evaluate monitoring capabilities
  - Restore data from backups
  - Restore process and services
  - Continuously monitor system
  - Restore confidence



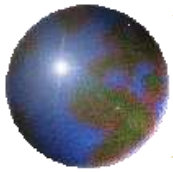
Disaster Recovery Plan (DRPs)

- Provide guidance in the event of a disaster
- Clear establishment of priorities
- Clear delegation of roles & responsibilities
- Alert key personnel
- Document disaster
- Mitigate impact
- Evacuation of physical assets



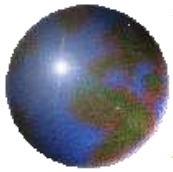
Crisis Management

- Disaster recovery personnel must know their responses *without any supporting documentation*
- Actions taken during and after a disaster *focusing on people involved* and *addressing viability of business*
- Crisis management team responsible for managing event from an enterprise perspective and covers:
  - Support personnel and loved ones
  - Determine impact on normal operations
  - Keep public informed
  - Communicate with major players such as major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties



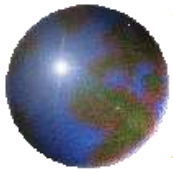
Business Continuity Planning (BCPs)

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, there must be a plan to allow business to continue functioning
- Development of BCP somewhat simpler than IRP or DRP; consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy



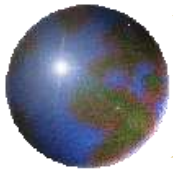
Continuity Strategies

- There are a number of strategies for planning for business continuity
- Determining factor in selecting between options usually cost
- In general there are three exclusive options: hot sites; warm sites; and cold sites
- Three shared functions: time-share; service bureaus; and mutual agreements



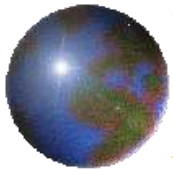
Alternative Site Configurations

- Hot sites
  - Fully configured computer facilities
  - All services & communication links
  - Physical plant operations
- Warm sites
  - Does not include actual applications
  - Application may not be installed and configured
  - Required hours to days to become operational
- Cold sites
  - Rudimentary services and facilities
  - No hardware or peripherals
  - empty room



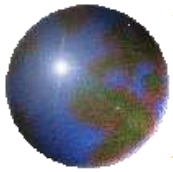
Alternative Site Configurations

- Time-shares
  - Hot, warm, or cold
  - Leased with other orgs
- Service bureau
  - Provides service for a fee
- Mutual agreements
  - A contract between two or more organizations that specifies how each will assist the other in the event of a disaster.



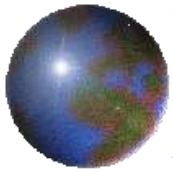
Off-Site Disaster Data Storage

- To get sites up and running quickly, organization must have ability to port data into new site's systems
- Electronic vaulting
  - Transfer of large batches of data
  - Receiving server archives data
  - Fee
- Journaling
  - Transfer of live transactions to off-site
  - Only transactions are transferred
  - Transfer is real time



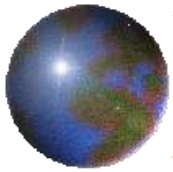
Off-Site Disaster Data Storage

- Shadowing
  - Duplicated databases
  - Multiple servers
  - Processes duplicated
  - 3 or more copies simultaneously



Model For a Consolidated Contingency Plan

- Single document set supports concise planning and encourages smaller organizations to develop, test, and use IR and DR plans
- 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

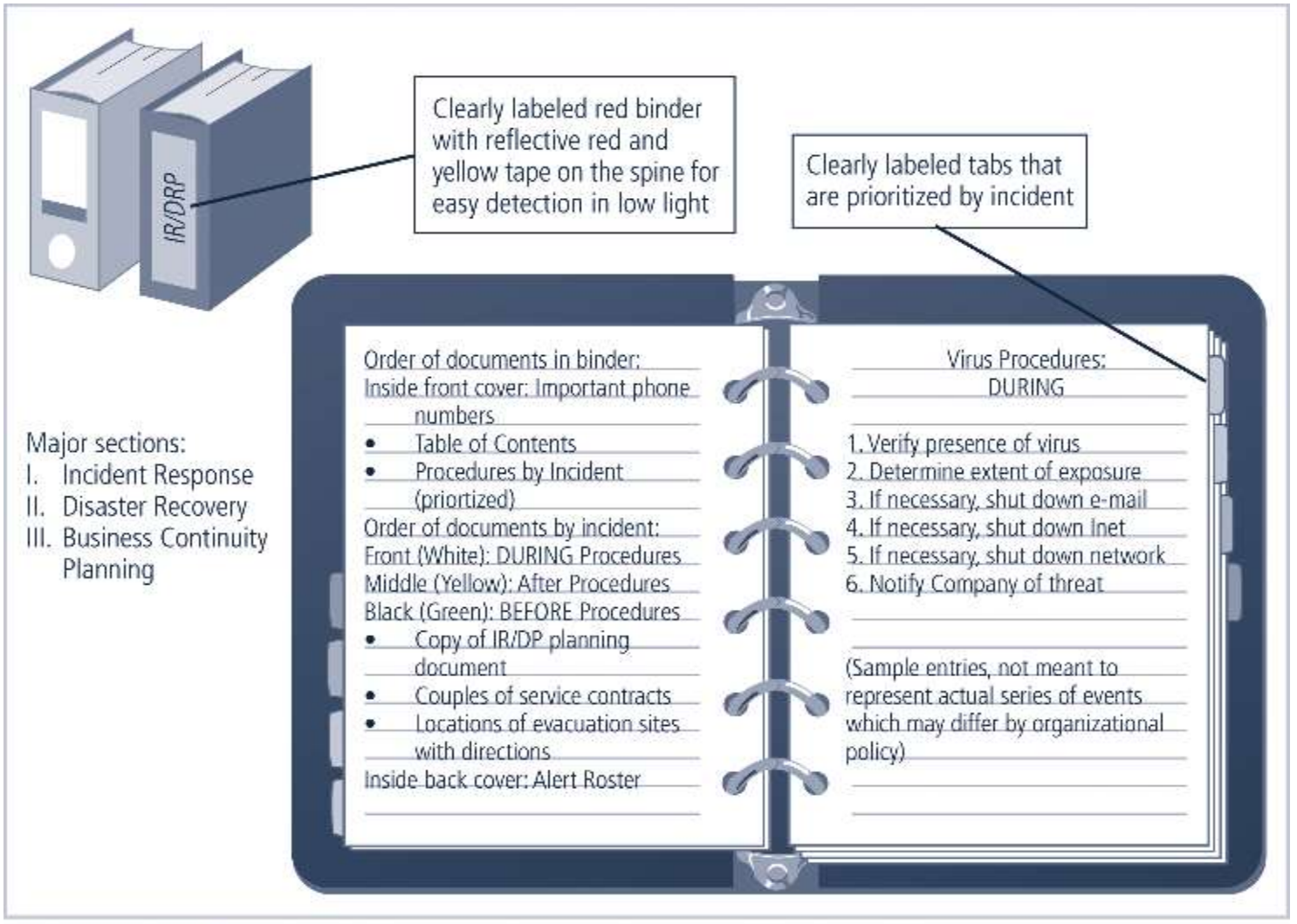
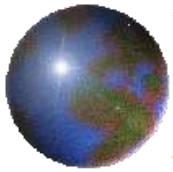
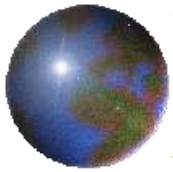


FIGURE 5-24 Contingency Plan Format



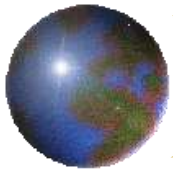
Law Enforcement Involvement

- When incident at hand constitutes a violation of law, organization may determine involving law enforcement is necessary
- Questions:
  - 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?
- Some questions are best answered by organization's legal department



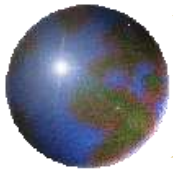
Benefits and Drawbacks of Law Enforcement Involvement

- Involving law enforcement agencies has advantages:
  - Agencies may be better equipped at processing evidence
  - Organization may be less effective in convicting suspects
  - Law enforcement agencies prepared to handle warrants and subpoenas needed
  - Law enforcement skilled at obtaining witness statements and other information collection



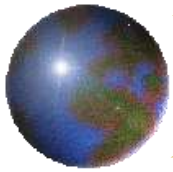
Benefits and Drawbacks of Law Enforcement Involvement (continued)

- Involving law enforcement agencies has disadvantages:
  - Once a law enforcement agency takes over case, organization loses complete control over chain of events
  - Organization may not hear about case for weeks or months
  - Equipment vital to the organization's business may be tagged evidence
  - If organization detects a criminal act, it is legally obligated to involve appropriate law enforcement officials



Summary

- Management has essential role in development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Information security blueprint is planning document that is basis for design, selection, and implementation of all security policies, education and training programs, and technological controls



Summary

- Information security education, training, and awareness (SETA) is control measure that reduces accidental security breaches and increases organizational resistance to many other forms of attack
- Contingency planning (CP) made up of three components: incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP)