Planning for Security

Chapter 5

Information Security

- Quality security programs begin & end with policy.
- Primarily management problem, not technical one.

Information Security Policies

- Form basis for all IS security planning
- Direct how issues should be addressed
- Don't specify proper operation of equipment or software
- Should never contradict law
- Obligates personnel to function in manner that adds to security of info
- Least expensive control to execute
- Most difficult to implement properly
- Standup in court if challenged
- Be properly administered through dissemination and documented acceptance

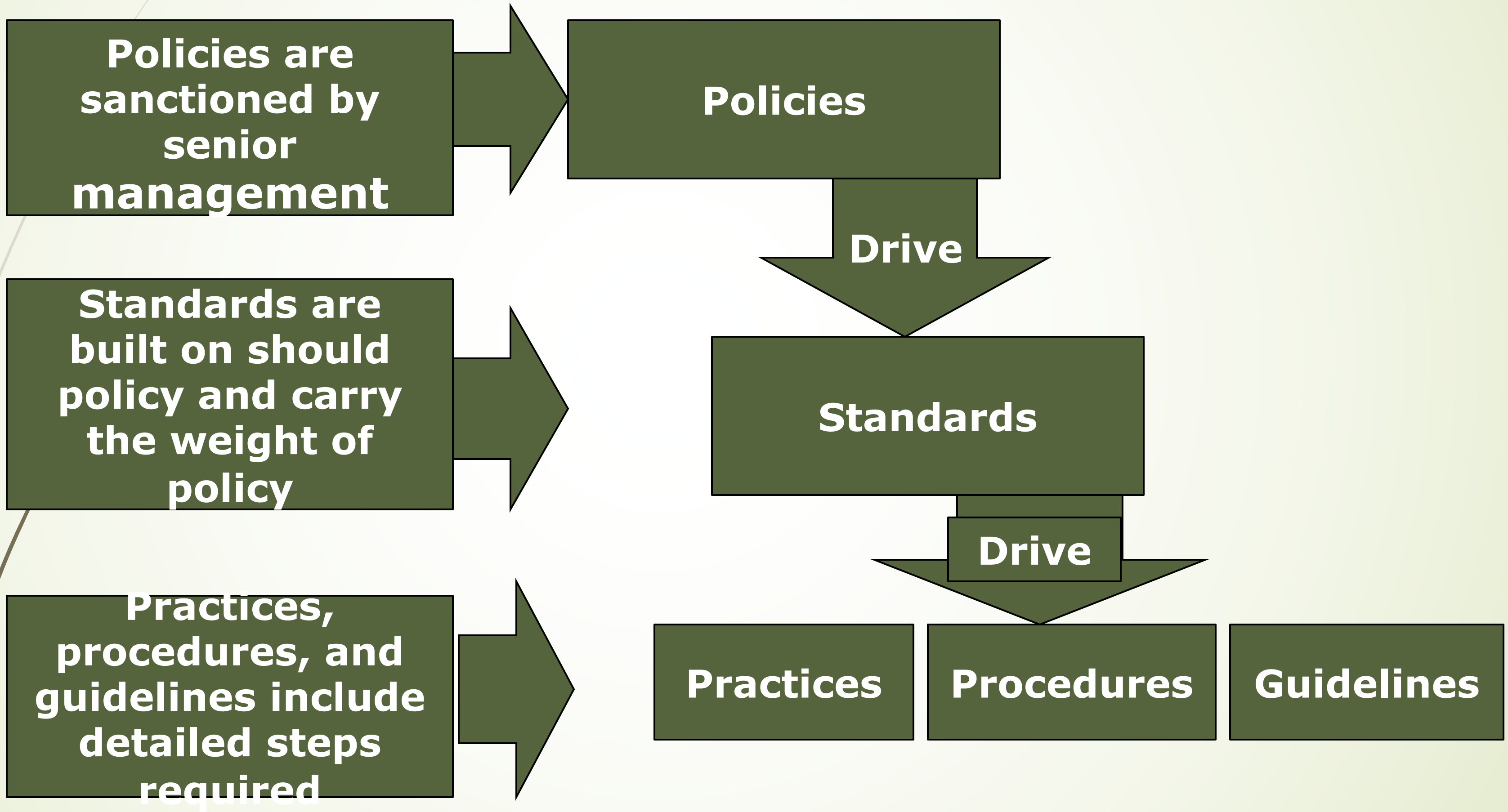
Policy

- Plan or course of action
- Convey instructions
- Organizational laws
- Dictate acceptable and unacceptable behavior
- Define
  - What is right
  - What is wrong
  - The appeal process
  - What are the penalties for violating policy
- Written to support the mission, vision and strategic plan of org

Standards

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

Policies, Standards, and Practices



Policies are sanctioned by senior management

Policies

Drive

Standards are built on should policy and carry the weight of policy

Standards

Drive

Practices, procedures, and guidelines include detailed steps required

Practices

Procedures

Guidelines

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

Policies

- Security Policy
  - Set of rules that protects & organization's assets
- Information security policy
  - Set of rules protects organization’s information assets
- Three types
  - General or Enterprise
  - Issue-specific
  - System-specific

EISP

- Enterprise Information Security Policy
  - Executive level document
  - General Information Security Document
  - 2-10 pages in length
  - Shapes the philosophy of security in IT
  - Contains requirements to be met
  - Assigns responsibilities
  - Addresses legal compliance

ISSP

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

3 Approaches to ISSP

- Independent document tailored to a specific issue
  - Scattered approach
  - Departmentalized
- Single comprehensive document covering all issues
  - Centralized management and control
  - Tend to over generalize the issue
  - Skip vulnerabilities

3 Approaches to ISSP

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

Elements of Issue-Specific Security Policy Statement

- Statement of Policy
- Appropriate Use
- Systems management
- Violations of policy
- Policy review and modification
- Limitations of Liability

Statement of Policy

- Clear statement of policy
  - Fair and responsible use of the Internet
- What is the scope of the policy?
- Responsible person
- What technologies and issues are addressed?

Appropriate Use

- Who can use the technology
- What it can be used for
- Defines “fair and reasonable use”
- What can it cannot be used for

Systems Management

- Focus on user's relationship to systems management
- Regulating
  - Use of e-mail
  - Storage of materials
  - Authorized monitoring of employees
  - Scrutiny of e-mail and electronic documents

Violations of Policy

- Give guidance on penalties and repercussions of violating policy
- Specifics on penalties
- How to report violations

Policy Review and Modification

- Procedures and a timetable for periodic review
- Specific methodology for review
- Specific methodology for modification

Limitations of Liability

- Set of disclaimers
- If employee violates policy or law, the company will not protect them
- Company is not liable for actions of employees

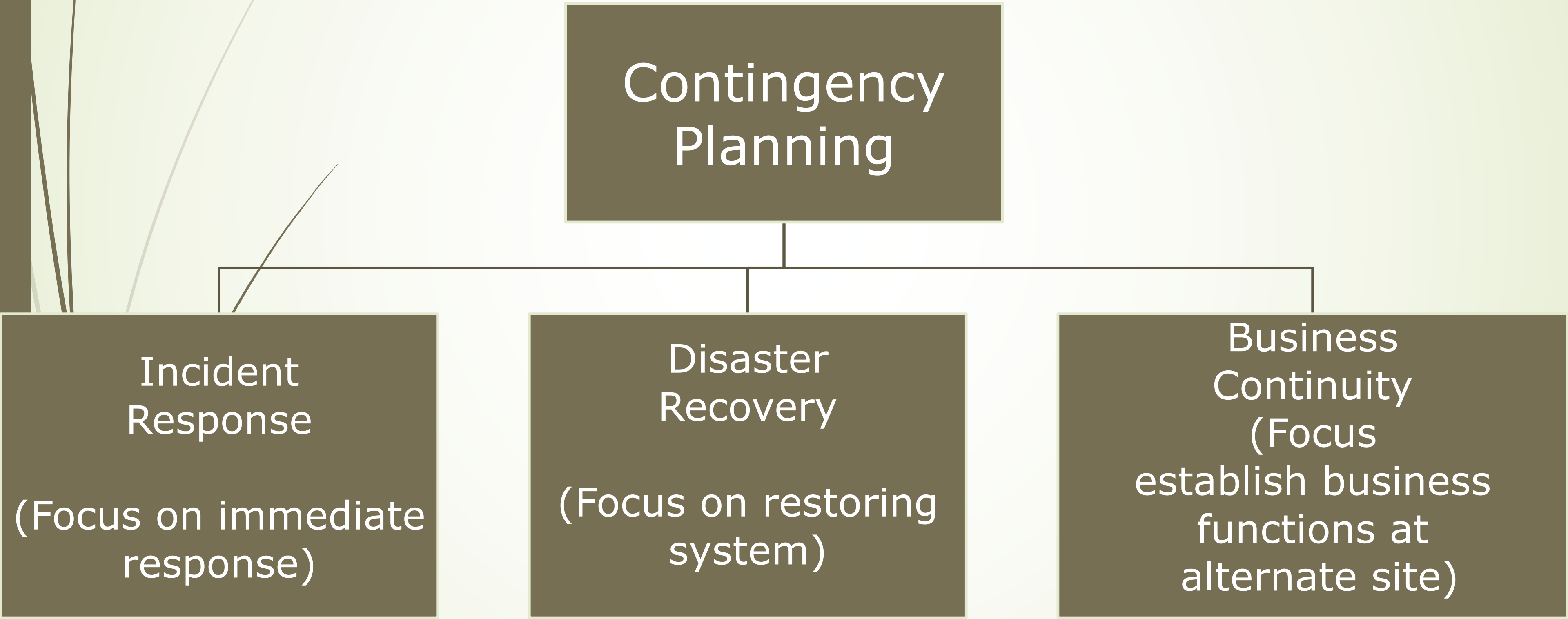
SysSP

- System-Specific Policy
- Frequently codified as standards & procedures
- Used when configuring or maintaining system
- Example
  - Access Control Lists (ACLs)
  - Configuration rules

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


Contingency Planning

Incident Response

(Focus on immediate response)

Disaster Recovery

(Focus on restoring system)

Business Continuity (Focus establish business functions at alternate site)

Figure 5-22 – Contingency Planning Timeline

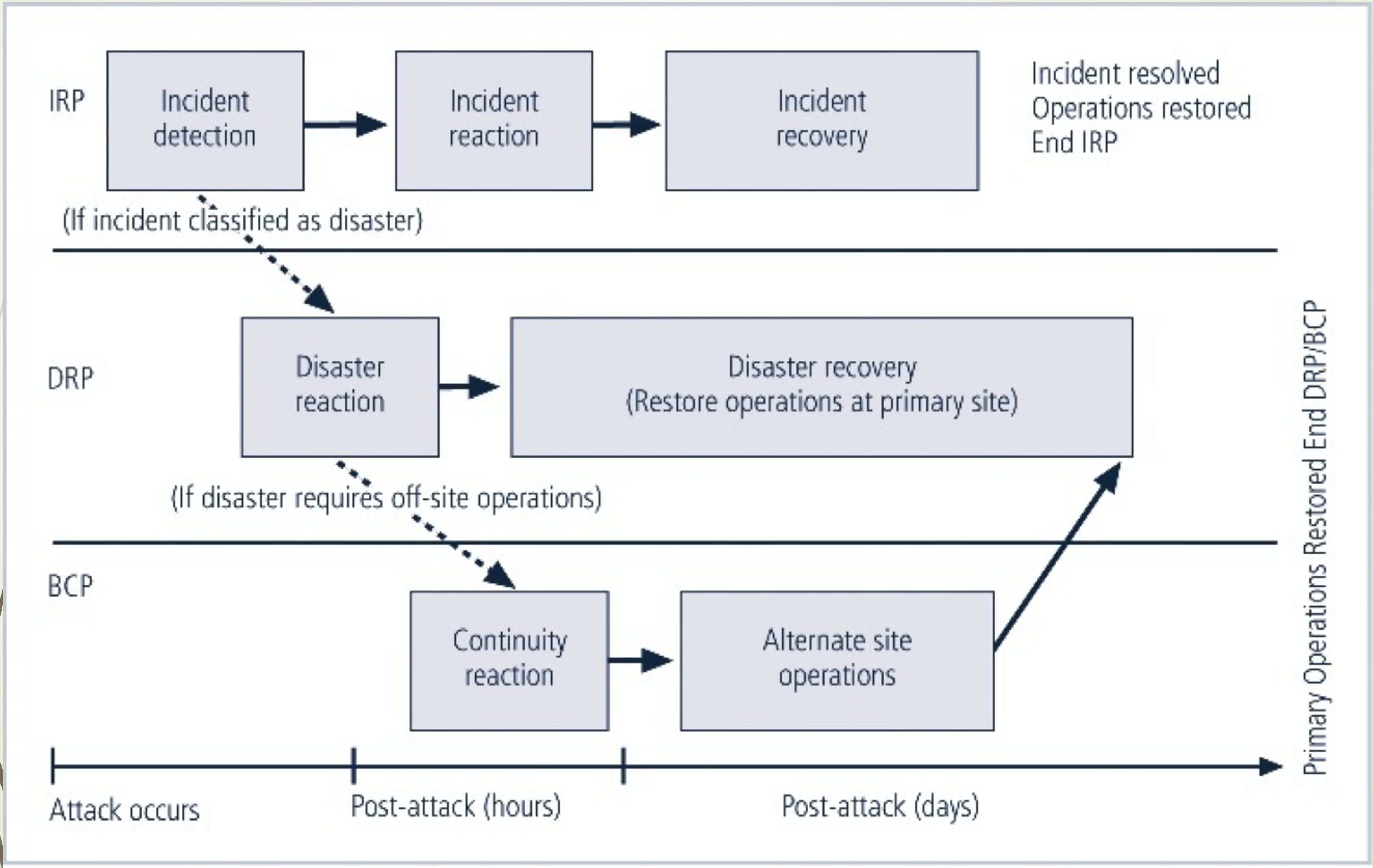
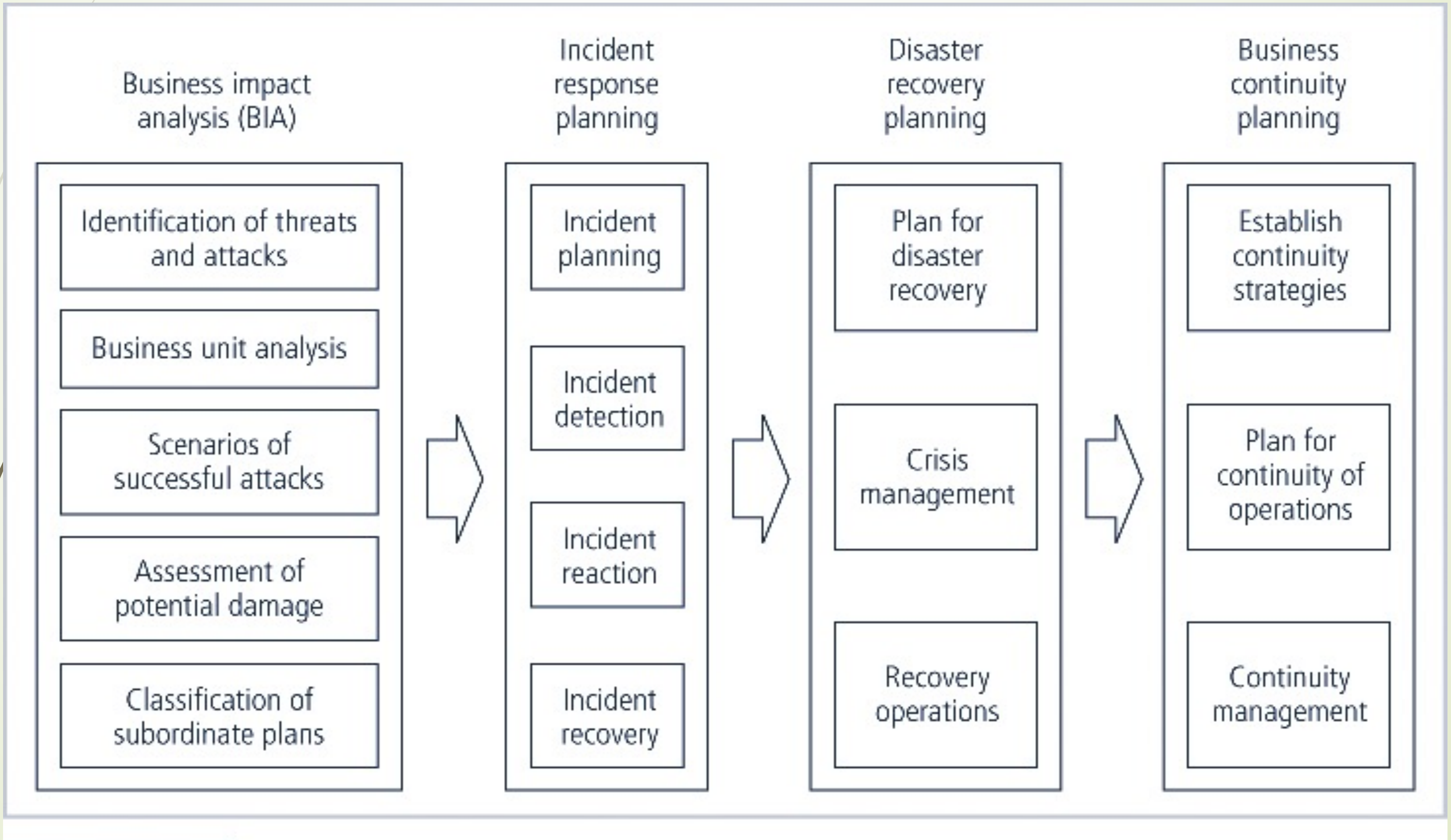


Figure 5-23 – Major Steps in Contingency Planning



Business impact analysis (BIA)

- Identification of threats and attacks
- Business unit analysis
- Scenarios of successful attacks
- Assessment of potential damage
- Classification of subordinate plans

Incident response planning

- Incident planning
- Incident detection
- Incident reaction
- Incident recovery

Disaster recovery planning

- Plan for disaster recovery
- Crisis management
- Recovery operations

Business continuity planning

- Establish continuity strategies
- Plan for continuity of operations
- Continuity management

Incident Response Planning

- Activities to be performed when an incident has been identified
- What is an incident?
  - If action threatens information & completed
  - Characteristics
    - Directed against information assets
    - Realistic change of success
    - Threaten the confidentiality, integrity, or availability of info

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 Response

- 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

Incident Detection

- 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

- 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
- Focus first & foremost -people involved
- Team responsibilities
  - Support personnel and loved ones
  - Determine impact on normal operations
  - Keep public informed
  - Communicate with major players

Business Continuity Planning

- Prepares an organization to reestablish critical operations
- Temporary facilities
- Continuity strategy
- Integration of off-side data storage & recovery functions
- Off-site backup
- Identification of critical business functions
- Identification of critical resources

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

Alternative Site Configurations

- 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
- Rolling mobile site

Off-Site Disaster Data Storage

- “off-site” – how far?
- 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

ACL Policies

- Restrict access from anyone & anywhere
- Can regulate specific user, computer, time, duration, file

ACL Policies

- 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

- More specific operation of a system than ACL
- May or may not deal with user directly
- Define configuration of firewalls, IDS, and proxy servers

Policy Management

- Living documents
- Must be managed
- 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 drafts

Document Configuration Management

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

Information Classification

- Control for the protection of information
- Important facet of policy
- Least
  - "for internal use only"
- Clean desk policy

Information Security Blueprint

- Risk Assessment
  - Quantitative and qualitative analysis
  - Feasibility studies
  - Cost benefit analysis
  - Good idea of systems vulnerabilities
- Specify tasks to be accomplished
- Specify order of performing tasks
- Serve as plan for IS security needs for years not just today

Information Security Blueprint

- Basis for design, selection & implementation
  - All security policies
  - Education
  - Training program
  - Technology controls

Security Models

- ISO (International Organization for Standards)
- IEC (International Electrotechnical Commission)

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

Security Modes

- NIST
  - Available from Computer Security Resource Center of National Institute for Standards & Technology
  - Publically available at no charge
  - Several publications dealing with various aspects

Security Models

- IETF
  - Internet Engineering Task Force
- VISA Internal
  - Focus on system that can and do integrate with VISA
- Base lining and Best Practices
  - Comparison of your organization security with another

Hybrid Framework

- 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

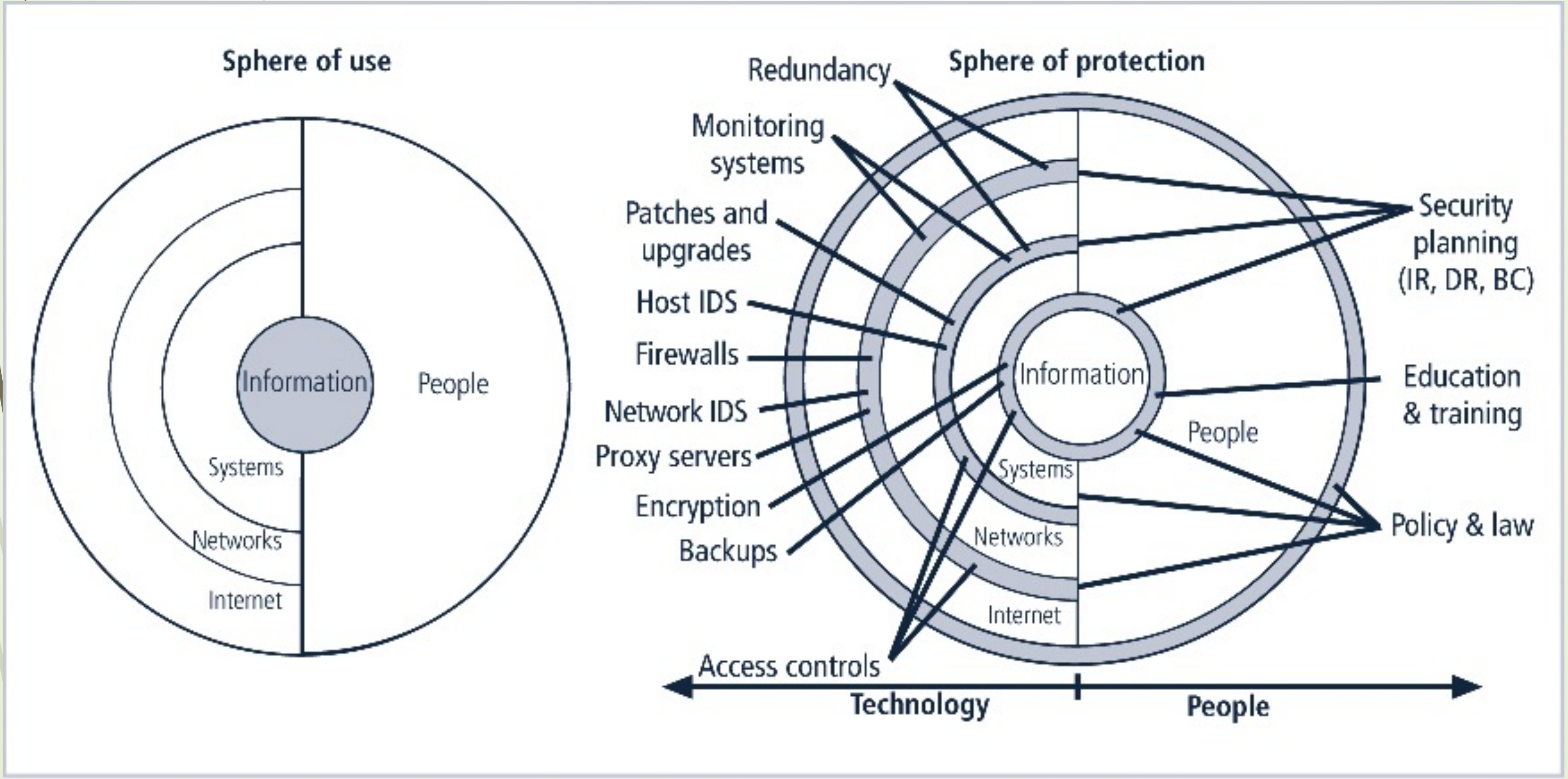


FIGURE 5-15 Spheres of Security

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

Hybrid Framework

- Operational Controls
  - 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 & implementation of audits
  - Covers cryptography
  - Classification of assets and users

Hybrid Framework

- Security Architecture Components
  - Defenses in Depth
    - One of basic tenants
    - Implementation of security in layers
      - Policy
      - Training
      - Technology
  - Security Perimeter
    - Defines the edge between the outer limit of an organization's security and the beginning of the outside world

Hybrid Framework

- 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

- 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

Comparative Framework of SETA

	Education	**Training**	**Awareness**
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction •Discussion seminar •Background reading •Hands-on practice	Practical instruction •Lecture •Case study •Posters	Media •Videos •Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	True or false Multiple choice (identify learning)
Impact timeframe	Long-term	Intermediate	Short-term

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