Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Distributed Analytics & Security Institute
Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Outline (Security Operations) 13%

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Investigations support and requirements

Dr. Patrick Pape, MSU

Dr. C.W. Perr, Sandia Labs

Dr. Drew Hamilton

Investigative Authorities

Identify agencies and offices responsible for investigating security incidents

Explain what information is reported to which agencies and offices

- **The Office of Inspector General - criminal law**
- **Office of Special Investigations**
- **Department of Homeland Security - domestic counterintelligence incidents**
- **Federal Bureau of Investigation - domestic incidents**

Investigation of Security Breaches

- Define security breaches – an act from outside the organization that bypasses security policies, practices, or procedures
- Discuss consequences of security breaches
  - Data loss
  - System compromise
  - Vulnerability exposure
- Discuss security breaches
- Evaluate results of security breaches – potential damages from a security breach
- Evaluate significance of security breaches – how badly would a breach set back the organization
- Implement policy for addressing security breaches

Investigation of Security Breaches

- Prescribe changes resulting from evaluation of security breaches
- Prescribe oversight associated with investigations
- Test security breach detection systems
  - Attempt to circumvent security policies to ensure the proper alarms are raised
  - Useful for both external and internal breaches/violations
- Verify security breach policy is implemented

The short intro

- Computer crime is the natural response of criminals to the dependence on information technology as well as the increase in complexity which helps to mask their nefarious deeds.
- How does this affect the company? You want to ensure compliance with regulation to protect the bottom line and company's image.

The Crux of Computer Crime Laws

- **Three main categories**
  - ***Computer assisted crime*** **– computer was a tool to help carry out the crime**
  - ***Computer targeted crime*** **– the computer was the victim of an attack crafted to harm it (and its owners) specifically.**
  - ***Computer is incidental*** **– a computer just happened to be involved.**

Computer Assisted Crime

Some examples of computer-assisted crimes are:

- **Attacking financial systems to carry out theft of funds and/or sensitive information**
- **Obtaining military and intelligence material by attacking military systems**
- **Carrying out industrial spying by attacking competitors and gathering confidential business data**
- **Carrying out information warfare activities by attacking critical national infrastructure systems**
- **Carrying out hactivism, which is protesting a government or company's activities by attacking their systems and/or defacing their web sites**

Computer-targeted crimes

Some examples of computer-targeted crimes include:

- **Distributed Denial-of-Service (DDoS) attacks**
- **Capturing passwords or other sensitive data**
- **Installing malware with the intent to cause destruction**
- **Installing rootkits and sniffers for malicious purposes**
- **Carrying out a buffer overflow to take control of a system**

NOTE The main issues addressed in computer crime laws are unauthorized modification, disclosure, destruction, or access, and inserting malicious programming code.

Rule of Thumb

One way to look at it is that a computer-targeted crime could not take place without a computer, whereas a computer-assisted crime could.

Now, this in no way means countries can just depend upon the laws on the books and that every computer crime can be countered by an existing law. Many countries have had to come up with new laws that deal specifically with different types of computer crimes. For example, the following are just some of the laws that have been created or modified in the United States to cover the various types of computer crimes:

- **18 USC 1029: Fraud and Related Activity in Connection with Access Devices**
- **18 USC 1030: Fraud and Related Activity in Connection withComputers**
- **18 USC 2510 et seq.: Wire and Electronic Communications Interception and Interception of Oral Communications**
- **18 USC 2701 et seq.: Stored Wire and Electronic Communications and Transactional Records Access**
- **The Digital Millennium Copyright Act**
- **The Cyber Security Enhancement Act of 2002**

NOTE You do not need to know these laws for the CISSP exam; they are just examples.

We have laws, so we should be good, right?

- **Nope. Getting the identity of the criminals is hard. They spoof their addresses and jump through other systems.**
- **VOCABULARY:**
  - ***Botnets* – A group of zombies.**
  - ***Zombies* - The attacker will install malicious software on a computer using many types of methods: e-mail attachments, a user downloading a Trojan horse from a web site, exploiting a vulnerability, and so on. Once the software is loaded, it stays dormant until the attacker tells it what systems to attack and when.**

The Law

- **Even though the FBI and other agencies are charged with investigating cyber crime doesn't mean that they have the time.**

CAUTION Even though financial institutions must, by law, report security breaches and crimes, that does not mean they all *follow* this law. Some of these institutions, just like many other organizations, often simply fix the vulnerability and sweep the details of the attack under the carpet.

Electronic Assets

- **Data is now an asset. Examples: (product blueprints, Social Security numbers, medical information, credit card numbers, personal information, trade secrets, military deployment and strategies, and so on).**

NOTE In many countries, to deal more effectively with computer crime, legislative bodies have broadened the definition of property to include data.

Hacking used to be just for fun.

- **Organized crime made hacking a whole lot worse…**

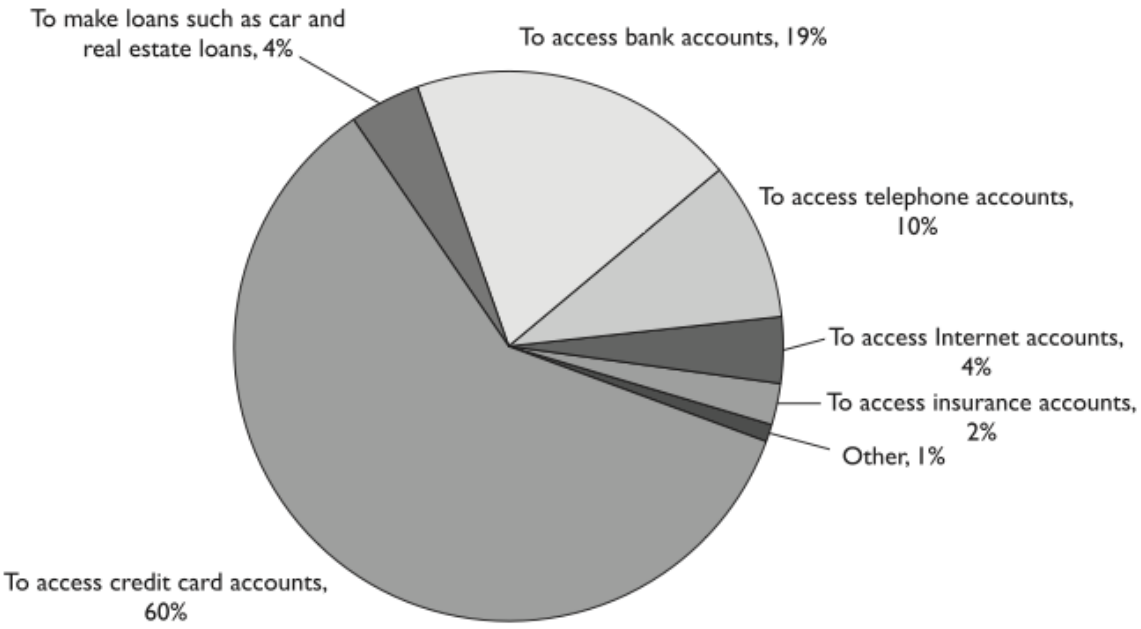
Common Internet Crime Schemes

- Auction fraud
- Counterfeit cashier's check
- Debt elimination
- Parcel courier e-mail scheme
- Employment/business opportunities

- Escrow services fraud
- Investment fraud
- Lotteries
- Nigerian letter, or "419"
- Ponzi/pyramid
- Reshipping
- Third-party receiver of funds

Find out how these types of computer crimes are carried out by visiting www.ic3.gov/crimeschemes.aspx.

How Stolen Information Was Used



In 20% of cases, information was used to open new accounts in the victim's name.

Source: Federal Trade Commission, Identity Theft Survey Report

Internet Crime Schemes

Current and ongoing Internet trends and schemes identified by the Internet Crime Complaint Center along with its description:

Auction Fraud
Auction Fraud — Romania
Counterfeit Cashier's Check
Credit Card Fraud
Debt Elimination
Parcel Courier Email Scheme
Employment/Business Opportunities
Escrow Services Fraud
Identity Theft
Internet Extortion
Investment Fraud
Lotteries
Nigerian Letter or "419"
Phishing/Spoofing
Ponzi/Pyramid
Reshipping
Spam
Third Party Receiver of Funds

AUCTION FRAUD

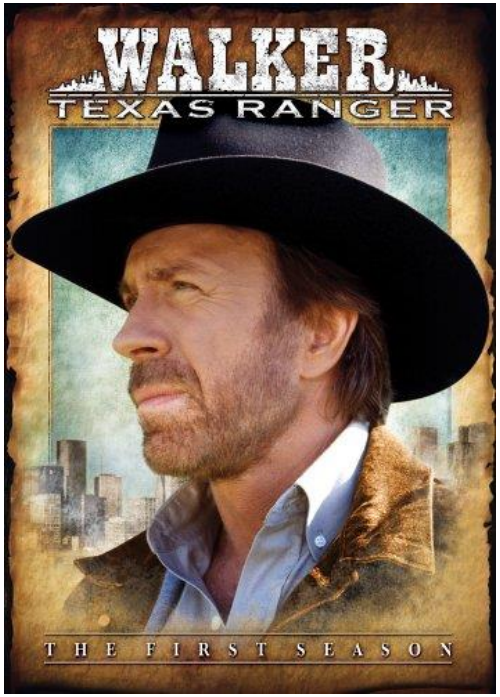
Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Consumers are strongly cautioned against entering into Internet transactions with subjects exhibiting the following behavior:

- The seller posts the auction as if he resides in the United States, then responds to victims with a congratulatory email stating he is outside the United States for business reasons, family emergency, etc. Similarly, beware of sellers who post the auction under one name, and ask for the funds to be transferred to another individual.
- The subject requests funds to be wired directly to him/her via Western

Different Countries

- **If a hacker in the Ukraine hacked a bank in France, who has jurisdiction? (Answer: Walker Texas Ranger is on it…).**



Solution

- Little reason for governments to work together
- The Council of Europe (CoE) Convention on Cybercrime is one example of an attempt to create a standard international response to cybercrime.
  - In fact, it is the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation.
  - The Convention's objectives include the creation of a framework for establishing jurisdiction and extradition of the accused. For example, extradition can only take place when the event is a crime in both jurisdictions.

Accountability

- Define who has responsibility for accountability – each user is responsible for their actions, and those who handle access control
- Describe accounting process for hardware, software, and information – auditing is done on user access attempts and activities and parsed for information, such as accessing information not necessary in a user's job, repetitive mistakes, and too many users with rights/privileges to sensitive data
- Outline accountability process/program
- Verify assigned responsibilities are commensurate with underlying information system security policies and are appropriately assigned

Configuration Management

- Address configuration management with SA/staff
- Address SA/staff about legal configuration restrictions
- Address work force about configuration management procedures
- Direct SA to follow proper configuration management procedures
- Direct SA to help work force with configuration management procedures

Configuration Management

- Direct SA/staff to follow appropriate laws and policies for configuration
- Direct SA/staff to follow configuration control software procedures
- Direct SA/staff to follow proper configuration procedures
- Direct SA/staff to restrict access to configuration functions and collected log files
- Direct SA/staff to restrict access to configuration system and collected information
- Direct SA/staff to review relevant policy and procedures for configuration management
- Direct SA/staff to use configuration management procedures

Configuration Management

- Discuss configuration management policies, laws, and penalties with personnel
- Discuss current configuration management with necessary parties
- Explain configuration management plan – Administrative and technical actions taken to identify and document the functional characteristics and physical layer of a computer system.
- Monitor configuration monitoring plan training
- Summarize monitoring management plan
- Verify that necessary parties understand configuration management plan and where it is maintained

Configuration Management

- Develop configuration management plan
  - Controlling and documenting changes to characteristics and layout
  - Recording model and vendor information on discrete parts
  - Setting up and tracking maintenance and testing schedules
- Direct implementation of configuration management plan
- Direct operation of configuration management plan
- Establish configuration management policy
- Implement configuration management policy
- Implement configuration management reporting
- Influence management on importance of having properly trained SA/staff to perform configuration management plan on mission critical systems

Configuration Management

- Interpret legal aspects of configuration systems
- Propose configuration management plan
- Test configuration management plan – used to test for appropriate documentation of functional characteristics, such as drivers, software options, etc.
- Verify adherence to appropriate laws and policies for configuration procedures
- Verify adherence to configuration procedures
- Verify configuration and auditing procedures and ensure that they are being followed
- Verify configuration management plan is executed

Configuration Management

- Verify configuration management plan is executed
- Verify configuration management policy is followed
- Verify current configuration management plan is available and accurate
- Verify SA understands rules for configuration management
- Verify strategic items being under configuration management
- Verify that software configuration is restricted
- Write configuration management plan

Countermeasures – Intrusion Detection (ID)

- Discuss intrusion detection problems
- Direct intrusion detection be implemented
- Explain intrusion detection problems – see intrusion detection in the previous sections
- Evaluate results of intrusion detection process – results of the simulated penetration attempts from testing
- Prescribe changes resulting from evaluation of intrusion detection process
- Prescribe oversight associated with intrusion detection process
- Test intrusion detection system – attempt to bypass security measures and the IDS: state, host, network, statistical/protocol/traffic anomaly based.
- Verify intrusion detection is in accordance with policy

Countermeasures – Protective Technologies (PT)

- Define cryptanalytic techniques – techniques to analyze cryptographic systems and obtain plaintext from ciphertext data, i.e. related-key attack.
- Define cryptographic concepts – the act of hiding data by changing transforming the data using some type of algorithm, i.e. symmetric-key cryptography and public-key cryptography
- Define digital signatures/non-repudiation – mathematical schemes for showing a message or document's authenticity, valid signatures allow the recipient to have some level of confidence that the document came from a known source. Non-repudiation is a property of digital signatures that keeps the source from later denying that they sent the document.
- Define key management – guidelines to proper generation and storage of keys, i.e. proper key length, secure transfer, extremely random key, higher use keys get shorter lifespans, back up keys, etc.

Protective Technologies

- Define message digests (MD5, SHA, HMAC) – one-way hash functions that are used create a fingerprint of a document to verify it's authenticity
- Define methods of encryption – the transformation of plaintext into unreadable ciphertext, i.e. symmetric, asymmetric encryption
- Identify protective technologies – firewalls, anti-virus, IDS, etc.
- Discuss methods of encryption
- Discuss protective technologies implementation
- Explain alternatives (steganography, watermarking)
- Explain cryptanalytic techniques
- Explain cryptographic concepts
- Explain digital signatures/non-repudiation

Protective Technologies

- Explain email security (PGP, PEM)
- Explain internet security (SSL)
- Explain key management
- Explain message digests
- Present protective technologies implementation plan
- Recommend alternatives
- Recommend digital signatures
- Recommend email security
- Recommend internet security

Protective Technologies

- Recommend message digest tools
- Recommend protective technologies
- Recommend public key infrastructure (PKI, certification authorities)
- Summarize protective technologies implementation plan
- Plan protective technologies implementation
- Test alternatives
- Test email security
- Test internet security

Protective Technologies

- Test protective technologies plan
- Test PKI
- Verify countermeasures exist and that countermeasure procedures are being followed
- Verify protective technologies performs as expected

Ensure Facility is Approved

- Define an approved facility – depends on what the organization and system requirements are, an approved facility changes for each system
- Define an approved service – like facilities, services are approved based on the organization or system they will be used on
- Explain what constitutes approved facility/service
- Monitor acquisition of approved facility/service
- Monitor operation of approved facility/service
- Present approved facility/service plan to Senior Systems Managers, viz., Chief Information Officer, Designated Approving Authority, Chief Technology Officer, etc.(SSM, viz.,CIO, DAA, CTO etc.)
- Recommend approved facility configuration

Ensure Facility is Approved

- Summarize major elements of an approved facility/service
- Direct Contracting Officer's Technical Representative (COTR) through facility acquisition process
- Direct COTR through service acquisition process
- Evaluate contracted security services
- Integrate security services

Ensure Facility is Approved

- Plan an approved facility/service
- Plan for acquisition of an approved facility/service
- Report on contracted security services
- Verify facility/service is approved by the appropriate authority
- Write plan for implementing an approved facility/service contract

Operations

- Security Policy
- Agency/Vendor Cooperation/Coordination
- Certification Advocacy
- Conduct Risk Assessment
- Contracting for Security Services
- Ensure Information System is Approved
- Life Cycle System Security Planning
- System Security Architecture Study

Security Policy

- **Ensure Information System is installed, operated, used, maintained, and disposed of in accordance with security policy**

Agency/Vendor Cooperation/Coordination

- Describe agency policy for redeploying classified systems and access by uncleared individuals and vendors to the SA and SSM, viz., CIO, DAA, CTO, etc.
- Explain cooperation concerns to vendors
- Explain cooperation concerns with vendors to SSM, viz., CIO, DAA, CTO, etc.
- Facilitate agency control of access by uncleared individuals and vendors
- Facilitate correct agency redeployment of classified systems.

Agency/Vendor Cooperation/Coordination

- Facilitate vendor cooperation
- Present the agency policy for access by uncleared individuals and vendors
- Present the agency policy for redeploying classified systems
- Present vendor cooperation report
- Summarize vendor cooperation
- Evaluate agency policy for access by uncleared individuals and vendors

Agency/Vendor Cooperation/Coordination

- Evaluate agency policy for redeploying classified systems
- Evaluate vendor cooperation
- Report vendor cooperation
- Verify corrective vendor actions when required

Certification Advocacy

- Define advocacy – when the certification party works with and/or on behalf of the organization to authenticate documents
- Explain advocacy role – the certification advocate acts as a third party, ensuring information authenticity
- Demonstrate compliance with certification plan
- Explain certification to SSM, viz., CIO, DAA, CTO, etc.
- Explain certification to SA
- Coordinate with certifier

Conduct Risk Assessment

- Define information valuation – the estimated value or worth of information, in this case a risk value to be used in system risk assessment, more sensitive data would yield a higher risk value when involved in an action on the system
- Define risk assessment – the process of calculating the risk of a particular action to either the organization or to a system
- Describe risk assessment process
- Describe three states of information – information gathering, interpretation of data and decision making
- Develop policy and procedures for conducting a risk assessment
- Summarize risk profile
- Write risk assessment reports

Conduct Risk Assessment

- Coordinate resources to perform a risk assessment
- Coordinate risk assessment process
- Interpret results of a risk assessment
- Interpret risk assessment report
- Write risk assessment plan and policy
- Analyze threats to and vulnerabilities of an information system

Contracting for Security Services

- Define an approved service – see previous section
- Explain security services to contracting officers
- Direct contracting officers to incorporate security services as required
- Discuss Protection Profiles and Security Target
- Explain what constitutes an approved service – changes based on the requirements of the system
- Monitor acquisition and operation of an approved service

Contracting for Security Services

- Plan an approved service
- Plan for acquisition of an approved service
- Present approved service plan to SSM, viz. CIO, DAA, CTO, etc.
- Summarize major elements of an approved service
- Direct COTR through service acquisition process
- Evaluate contracted security services

Contracting for Security Services

- Integrate security services contracts
- Report on contracted security services
- Verify obligation for security services
- Verify service is approved by appropriate authority
- Write plan for implementing an approved service contract

Life Cycle System Security Planning

- Define life cycle security – system security to ensure that the system was designed, developed, and maintained with formal designs and controls, including: design specification, verification, implementation, testing, configuration management, and distribution
- Describe agency policy for redeploying classified systems
- Explain life cycle security/system security planning
- Explain agency policy for redeploying classified systems
- Direct life cycle system security planning
- Direct SA to incorporate life cycle security planning as required

Life Cycle System Security Planning

- Explain life cycle security plan – the procedures and guidelines to ensure the system is protected for testing, implementation, verification, etc.
- Monitor life cycle security acquisition process
- Monitor life cycle security process
- Plan life cycle security
- Present life cycle security plan to SSM, viz., CIO, DAA, CTO, etc.
- Summarize major elements of life cycle security

Life Cycle System Security Planning

- Evaluate life cycle security implementation
- Implement Data Item Descriptions for life cycle security
- Implement life cycle security process to support CONOPS
- Integrate life cycle security
- Report on life cycle security implementation
- Validate use of appropriate life cycle security process
- Verify life cycle security planning is approved
- Verify life cycle system security planning is implemented

System Security Architecture Study

- Address system security architecture study
- Define system security architecture – how the security controls are positioned and how they relate to the overall system, to maintain confidentiality, integrity and availability
- Explain system security architecture study – the architecture described above that is in place to control access to a system's resources
- Direct SA to incorporate system security architecture study as required
- Direct support of system security architecture
- Direct and Explain system security architecture study

System Security Architecture Study

- Monitor system security architecture and architecture acquisition process
- Present system security architecture study to SSM, viz., CIO, DAA, CTO, etc.
- Summarize major elements of system security architecture
- Evaluate system security architecture implementation
- Implement DIDS for system security architecture
- Integrate system security architecture

System Security Architecture Study

- Report on system security architecture implementation
- Study system security architecture
- Validate appropriate system security architecture process
- Verify results mapped to security CONOPS
- Verify that security architecture study provides for defense in depth
- Verify system security architecture is approved and architecture study is implemented

Logging and monitoring activities

Dr. Drew Hamilton, MSU

Monitoring and Auditing

- Alarms, Signals, & Reports
- Address auditing and logging management with SA/staff
- Address work force auditing and logging management procedures
- Discuss alarms, signals, and reports requirements – alarms and signals send signals to the parsing program or auditor of suspicious activity and are placed into a report
- Discuss auditing and logging management policies, laws, and penalties with personnel – should include the policies dealing with how to handle situations where alarms have been raised because of a user's activity on the system

Monitoring and Auditing

- Discuss current auditing and logging management with necessary parties
- Develop auditing and logging management plan – plan to handle creating a proper program for creating alarms and signals based on user activity
- Direct SA to follow proper auditing and logging management procedures
- Direct SA to implement auditing and logging management procedures
- Direct SA/staff to follow proper auditing and logging procedures

Monitoring and Auditing

- Direct SA/staff to follow proper monitoring and auditing procedures
- Direct SA/staff to restrict access to auditing and logging functions and collected log files
- Direct SA/staff to restrict access to auditing and logging system and collected information
- Direct SA/staff to review policy and procedures for auditing and logging management

Monitoring and Auditing

- Direct SA/staff to restrict access to auditing and logging functions and collected log files
- Direct SA/staff to restrict access to auditing and logging system and collected information
- Direct SA/staff to review policy and procedures for auditing and logging management
- Direct SA/staff to review relevant policy and procedures for auditing and logging management

Monitoring and Auditing

- Direct SA/staff to use auditing and logging management
- Explain alarms, signals, and reports requirements
- Explain auditing and logging management plan
- Monitor auditing and logging management plan training
- Summarize auditing and logging management plan

Monitoring and Auditing

- Use analysis of intrusion indicators and generate results
- Verify that necessary parties understand auditing and logging management plan and where it is maintained
- Direct implementation of auditing and logging management plan
- Direct operation of auditing and logging management plan – the auditing and logging plan consists of both manual and automated auditing or user activity and logging the resulting reports
- Establish auditing and logging management policy for infractions – creating a proper plan for disciplinary actions against personnel

Monitoring and Auditing

- Implement auditing and logging management policy
- Implement auditing and logging management reporting
- Influence management on importance of having properly trained SA/staff to perform auditing and logging management plan on mission critical systems
- Interpret legal aspects of logging and auditing systems

Monitoring and Auditing

- Prescribe changes that result from analysis
- Prescribe oversight associated with alarms and signals
- Propose auditing and logging management plan
- Test alarms, signals, and reports – force the alarms and signals to activate using a test account and ensure the activity is logged and reported appropriately
- Test auditing and logging management plan – tests the organization of the system rather than the specific parts
- Verify adherence to auditing and logging procedures

Monitoring and Auditing

- Verify auditing and logging plan is executed
- Verify current auditing and logging management plan is available and accurate
- Verify monitoring and auditing procedures and that they are being followed
- Verify SA understands rules for auditing and logging management
- Verify strategic items being audited and logged
- Verify strategic placement of auditing and logging systems
- Write auditing and logging management plan

Audit Trail and Logging, Error/System Logs

- **Prescribe changes resulting from evaluation alarms, signals, & reports – make the appropriate changes to the system after the testing is complete.**

Intrusion Detection

- Address intrusion detection management with SA/staff
- Address SA/staff about monitoring and auditing intrusion detection policies
- Address work force about intrusion detection management procedures
- Develop intrusion detection management plan - the ID plan should consist of how the information taken from the IDS is sent to the necessary parties and how those parties handle the alerts.
- Direct implementation of intrusion detection management plan

Intrusion Detection

- Direct operation of intrusion detection management plan
- Direct SA/staff to follow proper intrusion detection management procedures
- Direct SA/staff to implement intrusion detection management procedures
- Direct SA/staff to follow proper monitoring and auditing procedures
- Direct SA/staff to restrict access to intrusion detection system and collected information
- Direct SA/staff to review relevant policy and procedures for intrusion detection management

Intrusion Detection

- Direct SA/staff to review relevant policy and procedures for intrusion detection management
- Direct SA/staff to use intrusion detection management
- Discuss current intrusion detection management plans, policies, and procedures with necessary parties
- Discuss intrusion detection management policies, laws, and penalties with personnel

Intrusion Detection

- Explain intrusion detection management plan
- Monitor intrusion detection management plan training
- Summarize intrusion detection management plan
- Verify that necessary parties understand intrusion detection management plan and where it is maintained
- Establish intrusion detection management policy for infractions

Intrusion Detection

- Implement intrusion detection management policy and reporting
- Influence management on importance of having properly trained SA/staff to execute intrusion detection management plans, policies, and procedures on mission critical systems
- Interpret legal aspects of intrusion detection systems
- Propose intrusion detection management plan

Intrusion Detection

- Test intrusion detection management plan
- Verify current intrusion detection management plan is available and accurate
- Verify intrusion detection management plan is executed
- Verify intrusion detection management policy is followed
- Verify monitoring and auditing procedures and that they are being followed
- Verify SA understands rules for intrusion detection management
- Verify strategic placements of intrusion detection systems
- Write intrusion detection management plan

Monitoring

- Address monitoring management with SA/staff
- Address SA/staff about legal monitoring restrictions
- Address work force about monitoring management procedures
- Develop monitoring management plan – ensures proper organization of monitoring of user access accounts and their activity

Monitoring

- Direct SA/staff to follow proper monitoring management procedures
- Direct SA/staff to help work force with monitoring management procedures
- Direct SA/staff to follow appropriate laws and policies for monitoring
- Direct SA/staff to follow proper monitoring procedures
- Direct SA/staff to restrict access to monitoring functions and collected log files
- Direct SA/staff to restrict access to monitoring system and collected information
- Direct SA/staff to review relevant policy and procedures for monitoring
- Direct SA/staff to use monitoring management procedures

Monitoring

- Discuss current monitoring management with necessary parties
- Discuss monitoring management policies, laws, and penalties with personnel
- Explain monitoring management plan
- Monitor monitoring management plan training
- Summarize monitoring management plan
- Verify that necessary parties understand monitoring management plan and where it is maintained

Monitoring

- Direct implementation of monitoring management plan
- Direct operation of monitoring management plan
- Establish policy infractions for monitoring management
- Implement monitoring management policy
- Implement monitoring management reporting
- Influence management on importance of having properly trained SA/staff to perform monitoring management plan on mission critical systems.

Monitoring

- Interpret legal aspects of monitoring systems
- Propose monitoring management plan
- Test monitoring management plan
- Verify adherence to appropriate laws and policies for monitoring
- Verify adherence to monitoring procedures
- Verify current monitoring management plan is available and accurate
- Verify monitoring and auditing procedures and that they are being followed.
- Verify monitoring management plan is executed

Monitoring

- Verify monitoring management policy is followed
- Verify SA understands rules for monitoring management
- Verify strategic items being monitored
- Verify strategic placement of monitoring systems
- Verify that consent to monitoring banners are in place
- Verify that process for maintaining signed consent to monitoring forms exists
- Write monitoring management plan – see auditing section for more details

Provisioning of resources

Dr. Chris Harrison, Sandia Labs

Contingency Plans ⇨ Contingency Plan Reporting

- Contingency plan reporting is notification of an incident.
- An example of procedures (EPA): "must note in the operating record the time, date and details of any incident that requires implementing the contingency plan.”
- In addition, within 15 days after the incident, the operating facility must notify the state's director.

Continuity Plans ⇨ Reconstitution ⇨ Continuity Plan Reporting

- **Benchmarking the continuity plan sets forth expectations to be met as well as plans established by similar organizations.**
- **Example: A continuity plan survey found that most of the banks (94%) have back-up operations for member service in place but only two-thirds have full data redundancy and real-time replication of transaction systems in place.**
  - **Banks tend to over-focus on their transaction processing, as a result, many overlook the full backup operations required to maintain business as usual.**
  - **Knowing this, the ISSO can examine his bank's continuity plan and make adjustments.**

http://www.cuinsight.com/media/doc/WhitePaper_CaseStudy/wpcs_Ongoing%20BusinessContinuityBenchmarking%208-2010.pdf

Continuity Plans ⇨ Reconstitution ⇨ Reconstitution

- **Reconstitution reporting involves analysis of the reconstitution plan as well as status reports on ongoing reconstitution of systems post incident.**

- **The primary concerns of reconstitution reporting involve the efficacy of the reconstitution plan, resources required, and a methodology to both update reconstitution methods and verify that reconstitution efforts will be successful.**

Continuity Plans ⇨ Reconstitution ⇨ Backup Reports

Backup reports constitute information regarding the backups. In the status report, typical concerns are how quickly can the backups be implemented, how much data will be lost (aka when was the last backup taken), is there redundancy, how far back do the backups go, and the methodology on backup integrity verification.

Continuity Plans ⇨ Reconstitution ⇨ Restoration Reports

Restoration time is a critical issue for developing back-up systems and appropriate staffing and the restoration report addresses the expected restoration time.

Two measurements useful for reporting on restoration is the recovery time, which measures how quickly the organization can put critical systems back online, while the recovery point, measures effective data loss/asset losses upon restoration on data.

Disposition of Classified Material & Emergency Destruction Procedures (EDP)

A disposition report certifies that all classified material was returned or destroyed. The report serves during verification to ascertain any discrepancies between the evidence and the report. Any discrepancies found must be subsequently reported to the proper investigative agency.

An EDP report is an assessment of the EDP plan and verifies that the efficacy of the plan is valid. A secondary report regarding EDP occurs post incident and determines how successful the EDP was and identifies what information may be at risk. It can also serves as a recommendation for modifying the EDP plan.

Monitoring and Auditing ⇨ Audit ⇨ Auditing Reports

Establish the Terms of the Engagement

This will allow the auditor to set the scope and objectives of the relationship between the auditor and the organization. The engagement letter should address the responsibility (scope, independence, deliverables), authority (right of access to information), and accountability (auditees' rights, agreed completion date) of the auditor.

Preliminary Review

This phase of the audit allows the auditor to gather organizational information as a basis for creating their audit plan. The preliminary review will identify an organization's strategy and responsibilities for managing and controlling computer applications.

Establish Materiality and Assess Risks

In order to plan the audit, a preliminary judgment about materiality and assessment of the client's business risks are made to set the scope of the audit.

Monitoring and Auditing ⇨ Audits (Cont)

Plan the Audit: Proper planning of the audit will ensure the audit is conducted in an effective and efficient manner. When developing the audit plan, the auditor should take into consideration the results of their understanding of the organization and the results of the risk assessment process.

Consider Internal Control: To develop their understanding of internal controls, the auditor should consider information from previous audits, the assessment of inherent risk, judgments about materiality, and the complexity of the organization's operations and systems.

Perform Audit Procedures: Audit procedures are developed based on the auditor's understanding of the organization and its environment. A substantive audit approach is used when auditing an organization's information system.

Issue the Audit Report: Once audit procedures have been performed and results have been evaluated, the auditor will issue either an unqualified or qualified audit report based on their findings.

IS Auditing Standard 070 (Reporting) states, "The IT auditor should provide a report in an appropriate form, upon the completion of the audit. The report should state the scope, objectives, period of coverage, and the nature, timing, and extent of the audit work performed. The report should state the findings, conclusions, and recommendations and any reservations, qualifications or limitations of scope that IT auditor has with respect to the audit."

Identification & Authentication ⇨ Account Administration ⇨ Unauthorized Accounts

1. The incident response process is initiated when there is a reasonable basis to conclude an unauthorized account may be in use.
2. Preliminary report on unauthorized account is made by a member of the IRT and given to the ISSO.
3. ISSO determines if an Incident Response Team is needed to identify and
4. resolve the security breach.
5. ISSO informs management.
6. The Incident Response Team will research the unauthorized account(s) and agree on an action plan.
7. The Information Security Officer reviews all findings of the Incident Response Team.
8. Document its findings in a written report along with recommendations to management.

Identification & Authentication ⇨ Unauthorized Access

- The report on unauthorized access must identify the where, when, who, and how regarding the breach.
- Second, the report must cover the assets potentially examined, the assets potentially exfiltrated, how vulnerable the organization is to a similar event.
- Notification of unauthorized access follows the same procedures of unauthorized accounts.

Configuration Management

- **Configuration management (CM) problems can negatively impact product profitability by effecting product quality, delaying product launches, and increasing product development, direct product, and product lifecycle costs. Important questions must be addressed in a Configuration management report:**

1. **Where are the resources used?**
2. **What are the dependencies between applications and infrastructure?**
3. **Which systems and components are near their maximum capacity now?**
4. **Can we modify the configuration without disruption?**
5. **What software applications are installed?**

- **SAP Crystal Reports and Microsoft's Configuration Manager reporting are automated tools that expedite this process.**

Foundational security operations concepts

Dr. Drew Hamilton

Threats to Operations Security

- Many of the tools used by hackers can be used for good or evil
- For the purposes of the book, if a tool is used by black hats it is called hacking, if it is used by white hats then it's ethical hacking or penetration testing

Threats to Operations Security

- **General Threats**
  - **Script Kiddies**
  - **Trojans**
  - **Backdoors**
  - **DDoS attacks**
  - **OS fingerprinting**
  - **DoS attacks**
  - **Man-in-the-Middle**
  - **Mail bombing**
  - **War dialing**
  - **Ping of Death**
  - **Fake Login Screens**
  - **Teardrop attack**
  - **Traffic analysis**
  - **Slamming and cramming**

Threats to Operations Security

- **Operating System Scanning**
  1. **Find out what systems are running (ping sweep)**
  2. **Port scan the hosts**
  3. **Correlate the services that are running**
  4. **Run a vulnerability scan**

Threats to Operations Security

- An additional layer of protection can be applied in Unix-like systems by using “wrappers”
- Information gathering
  - Browsing – a general technique used by intruders to obtain information they are not authorized to access
    - Perusing file listings on devices
    - Dumpster diving
    - Shoulder surfing

Threats to Operations Security

- A network sniffer is a tool that monitors traffic as it traverses a network
  - Also referred to as network analyzers or protocol analyzers
  - Runs with the NIC in promiscuous mode
- Secure versions of services and protocols should be used when possible in order to combat sniffers
  - Example: Secure RPC (S-RPC): uses Diffie-Hellman public key cryptography to determine the shared secret key
  - R-utilities (rlogin, rexec, rsh, rcp) in Unix all have several weaknesses and should be replaced by a service that requires stronger authentication such as secure shell

Threats to Operations Security

- **Session Hijacking**
  - **Can be countered with IPSec or Kerberos**
- **Loki attack**
  - **Uses ICMP protocol for covert channel communications**
  - **Writes data behind the ICMP header (which is designed for status and error messages)**
  - **Successful because ICMP is not typically scanned by firewalls**

Threats to Operations Security

- **Password Cracking**
  - **Static passwords are the technique of choice, both for familiarity and cost reasons**
  - **Easily cracked, other options would be smart cards or biometrics (at a greater cost)**
  - **Password cracking tools (i.e.: John the Ripper, Crack, Ophcrack) attack encoded hashes**
  - **Dictionary or brute force attacks on stolen password files (rainbow tables not addressed)**
  - **Strong password policies: at least 8 characters, upper case, lower case, at least 2 special characters**

Resource protection techniques

Dr. Chris Harrison, Sandia Labs

Information Technology Testing

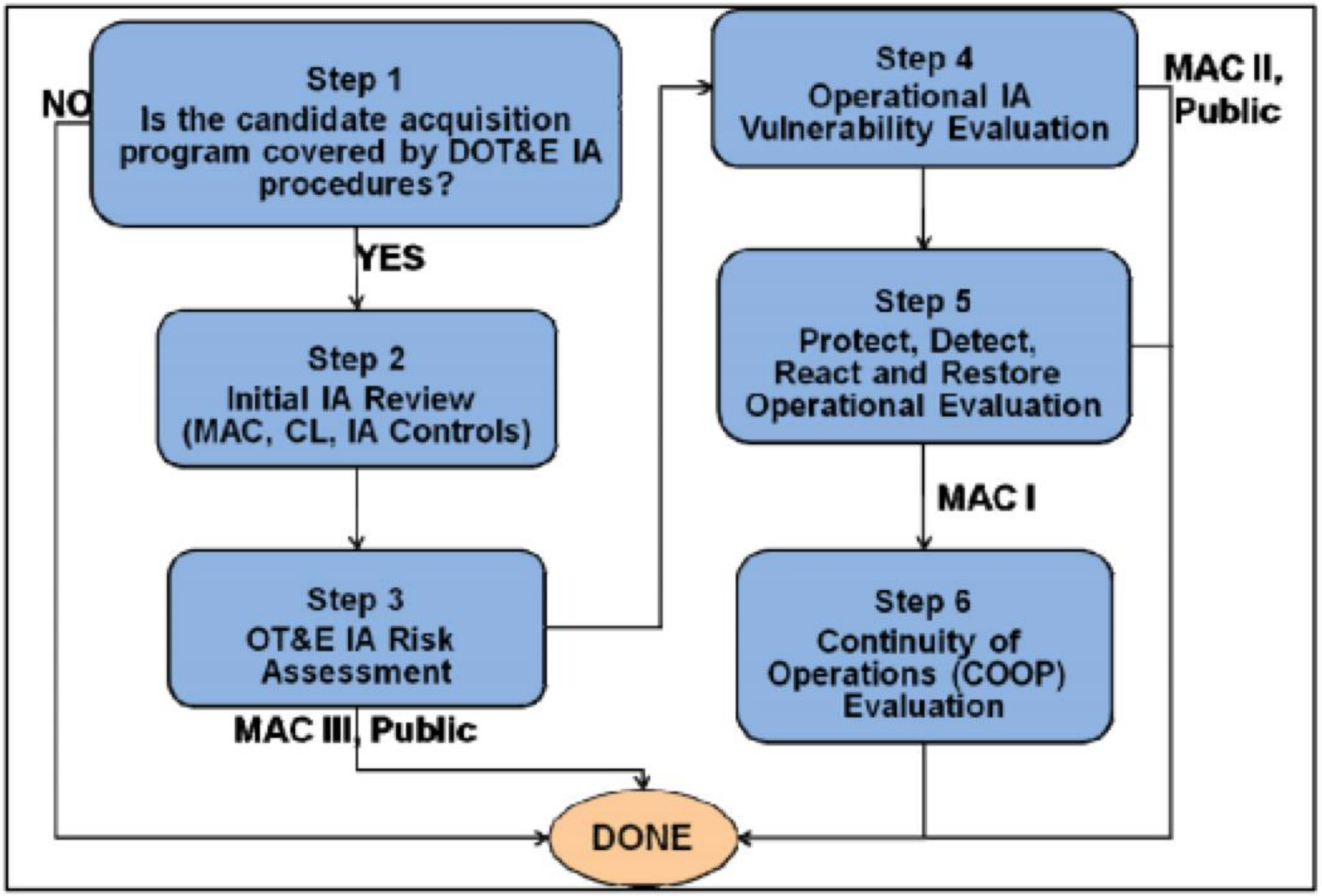


Figure 6. Summary of DOT&E Six-Step Process

Information Technology Testing

- An ITT should be established as early as possible in the acquisition process, and should consist of representatives from the developmental, operational, security, threat and interoperability, and T&E communities. The collaboration of the ITT members is critical to achieving the vision of "test by one, accept by many."
- The ITT should collaborate with the acquisition and engineering communities to ensure that meaningful, measurable T&E criteria are identified to evaluate IA capabilities.
- The ITT should be an active participant in the systems engineering process and participate in program and technical reviews.
- The ITT should convene with the development team to strategize on an integrated DT and OT T&E plan. IA and CND T&E criteria should not only establish minimum technical thresholds, but also address the operational criteria suggested in the DOT&E Six-Step process.
- IA capabilities and requirements should be addressed in the early Systems Engineering Technical Reviews (SETRs) and translated into robust system requirements, RFPs, and the IT system preliminary design. Translating IA requirements into system requirements and specifications early on will enable more positive T&E outcomes during later acquisition test phases.

Information Technology Testing

- IA T&E criteria should include minimum technical thresholds such as Measures of Performance (MOP) and Measures of Effectiveness (MOE) that address the operational criteria as suggested in the T&E Six-Step process in order to evaluate end-to-end IA capabilities.
- The technical and operational thresholds should be used to evaluate significant IA controls and concerns, including the ability to protect, detect, react and restore systems to sustain continuity of operations.
- IA T&E should be conducted during Step 4 of the T&E IA OT process concurrent with DT using operationally realistic testing environments and representative threats.
- Earlier IA testing will allow more time to correct technical IA and CND issues prior to IA and CND Protect, Detect, React, Restore (PDRR) operational assessments.
- Step 4 IA T&E should not be confused with penetration testing using Red Teams that is usually performed in Step 5 and is only applied to the SUT.
- http://www.acq.osd.mil/dte/docs/IA_Cross_Walk_WG_Report-3-30-10.pdf

Computer Organizational/Agency Systems Emergency/Incident Response Team

1. The incident response process is initiated when there is a reasonable basis to conclude any security incident has occurred.
2. Preliminary report on security incident is made by a member of the IRT and given to the ISSO.
3. ISSO determines if an Incident Response Team is needed to identify and resolve the security breach.
4. ISSO informs management.
5. The Incident Response Team will research the security incident and agree on an action plan.
6. The Information Security Officer reviews all findings of the Incident Response Team.
7. Document its findings in a written report along with recommendations to management.

Incident management

Dr. Drew Hamilton

The Spirit of Forensic Discovery

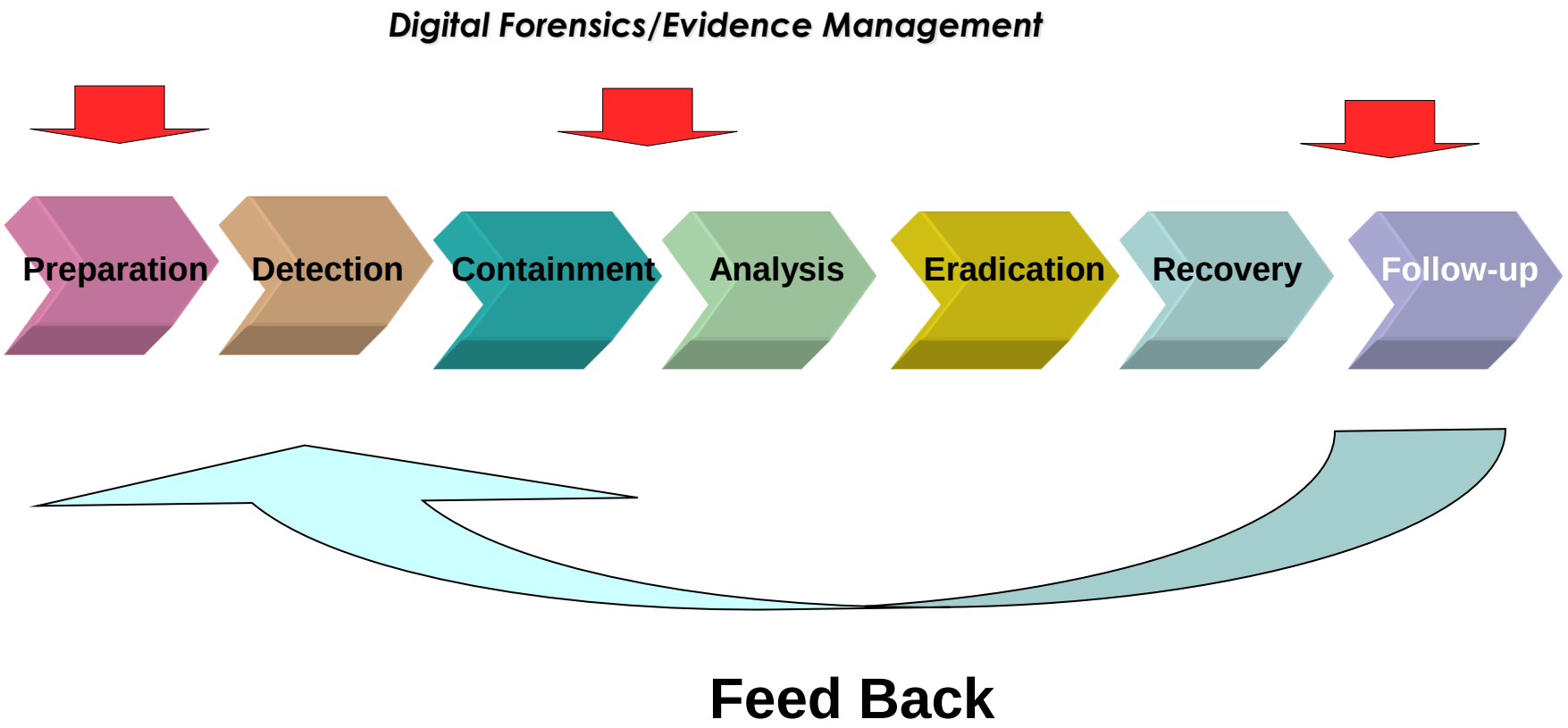
- **Now, a few words on looking for things:**
  - **When you go looking for something specific, your chances of finding it are very bad.**
  - **Because, of all the things in the world, you're only looking for one of them.**
  - **When you go looking for anything at all, your chances of finding it are very good.**
  - **Because, of all the things in the world, you're sure to find some of them.**

-- Darryl Zero, The Zero Effect

Myths & Misconceptions

- Cyber-criminals are computer experts with a high technical ability
- Cyber-criminals have higher than average IQs
- All cyber-criminals are introverts
- Cyber-criminals are never violent
- Cyber-criminals are not “real” criminals
- Cyber-criminals fit one “neat” profile

Incident Response Methodology (PDCAERF)



The Process of Digital Forensic Science

- The primary activities of DFS are investigative in nature.
- The investigative process encompasses
  - Identification
  - Preservation
  - Collection
  - Examination
  - Analysis
  - Presentation
  - Decision

Computer Forensic Activities

Computer forensics activities commonly include:

- **the secure collection of computer data**
- **the identification of suspect data**
- **the examination of suspect data to determine details such as origin and content**
- **the presentation of computer-based information**
- **the application of a country's laws to computer practice.**

The 3 As

- **The basic methodology consists of the 3 As:**
  - **Acquire the evidence without altering or damaging the original**
  - **Authenticate the image**
  - **Analyze the data without modifying it**

"The Computer"

- Computer as *Target* of the incident
  - Get to instructor's test preparation
  - Access someone else's homework
  - Access/Change a grade
  - Access financial information
  - "Denial of Service"
- Computer as *Tool* of the incident
  - Word processing used to create plagiarized work
  - E-mail sent as threat or harassment
  - Printing used to create counterfeit material
- Computer as *Incidental* to the incident
  - E-mail/file access used to establish date/timelines
  - Stored names and addresses of contacts or others potentially involved in the incident

Locard Principle of Exchange

- **“..when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived.”**

- **(Edmund Locard, 1910)**

Forensic Principles

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An Individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

General Evidence Dos & Don'ts

1. Minimize Handling/Corruption of Original Data
2. Account for Any Changes and Keep Detailed Logs of Your Actions
3. Comply with the Five Rules of Evidence
4. Do Not Exceed Your Knowledge
5. Follow Your Local Security Policy and Obtain Written Permission
6. Capture as Accurate an Image of the System as Possible
7. Be Prepared to Testify
8. Ensure Your Actions are Repeatable
9. Work Fast
10. Proceed From Volatile to Persistent Evidence
11. Don't Run Any Programs on the Affected System
12. Document Document Document!!!!

- Source: AusCERT 2003 (www.auscert.org)

Preventative measures

Dr. Drew Hamilton

General Principles

- Discuss access control models:
  - Discretionary Access Control (DAC) – data owners decide who has access to resources, and ACLs are used to enforce the security policy
  - Mandatory Access Control (MAC) – OS enforce the system's security policy with security labels
  - Role-based Access Control (RBAC) – access decisions are based on each subject's role and/or functional position
    - Core and Hierarchical
- Explain approval to operate – when a user has the right to access and make changes to a data object, by the access control method
- Verify SSM, viz, CIO, DAA, CTO, etc can discuss approval to operate

General Principles

- Explain attack, backdoor routines, DOS attacks, remote explorer attack, attack root exploits, session hijacking tools, and war dialer/THC-scan
- Explain business aspects of information security
- Discuss and Explain common criteria – a framework where computer system users can specify their security functional and assurance requirements, vendors can implement security attributes and testing labs can evaluate the products
- Discuss Evaluation Assurance Levels – the level of assurance given by a product is ranked based on how well it meets specification, implementation and evaluation qualities by a third party tester
- Summarize common criteria
- Verify security services as defined by common criteria are implemented

General Principles & Defense in Depth

- Explain computer network attack
- Explain criminal prosecution
- Give examples of defense in depth methods – using more than one of a defense layer, such as physical security (deadbolts), hashing passwords, anti virus, DMZ, Firewalls etc.
- Discuss and explain defense in depth – defending a system against any particular attack, by utilizing several methods, essentially layering levels of prevention
- Explain the role of vendors and uncleared individuals in defense in depth
- Explain the Model for Information Assurance: An Integrated Approach
- Summarize defense in depth

Defense in Depth & Due Care

- Verify implementation of defense in depth
- Verify security architecture provides defense in depth
- Address questions from users about due care
- Monitor adherence to due care rules
- Remind users of due care rules
- Explain generally accepted systems security principles (GASSP)
- Identify standards upon which GASSP are based
- Integrate GASSP into standard operating procedures
- Interpret due care rules

General Principles – Due Care

- Verify due care concerns are addressed
- Verify GASSP is implemented
- Verify implementation of due care rules
- Report to management and SA of status of due care rules
- Report on GASSP implementation
- Report violations of due care rules

General Principles

- List topics for inclusion into education, training and awareness plan:
  - (Post)Implementation
  - Monitoring Compliance
  - Evaluation and Feedback
  - Managing Change
  - Program Success Indicators
- Recognize AT&E is a countermeasure
- Develop education, training, and awareness plan
- Explain industrial security
- Explain and discuss INFOWAR concepts
- Explain intellectual property rights

General Principles

- Explain interim approval to operate
- Explain investigative authorities
- Verify SSM, viz., CIO, DAA, CTO, etc. understands intellectual property rights, can discuss IATO and investigative authorities

General Principles – Knowledge of Security Laws

- **Discuss:**
  - **Clinger-Cohen**
  - **Computer Fraud and Abuse Act**
  - **Computer Security Act**
  - **Copyright Law of the US and related laws**
  - **Copyright protection and licenses**
  - **Electronic Freedom of Information Act**
  - **Electronic Records Management and Federal Records Act**
  - **Federal Information System Management Act**
  - **Federal Managers Financial Integrity Act**
  - **Federal Property and Administration Service Act**

General Principles – Knowledge of Security Laws

- **Discuss:**
  - **Freedom of Information Act**
  - **Government Paperwork Elimination Act/Paperwork Reduction Act**
  - **Government Information Security Reform Act**
  - **Millennium Copyright Act**
  - **National Archives and Records Act**
  - **Privacy Act issues**
  - **USA Patriot Act**
  - **Computer crimes and various methods**
  - **International legal issues which can affect IA**
  - **Legal responsibilities of the SS, viz., etc.**

General Principles

- Define lattice model – structure of particles interconnected in linear branches formed by the results of mathematical differential equations used as a security policy model, with data as the particles and data channels as the branches
- Explain and discuss law enforcement interfaces
- Discuss access control models
- Explain need for system certification – a system needs to be certified in order to give the users some level of assurance when using the system. The level of certification shows a security rating based on how well the security policy is implement throughout the design, implementation and testing of the system.
- Verify SSM, viz., CIO, etc. can discuss system certification requirements and processes
- Explain operating security features

General Principles

- Explain and discuss risk management – the procedures and guidelines used to handle the assessment of risks
- Explain risks associated with agency policy for access by uncleared individuals/vendors and for redeploying classified systems
- Define security awareness for information system users – individual user responsibility and sufficient understanding to comply with security policies
- Develop security awareness plan and materials for information system users
- Discuss requirements for security awareness – requirements establish the who, what and how of security awareness.

General Principles

- Encourage employees to seek education in IA as a countermeasure
- Discuss security education – done through training and exercises based on the organization's security policies
- Monitor changing security education requirements for information system users
- Develop/design information system education programs
- Define security training for information system users

General Principles

- Develop security training plan and materials for information system users
- Discuss requirements for security training – depends on the security policy, see previous slides
- Explain and discuss software licensing
- Explain and discuss software piracy
- Explain and discuss SSAA
- Explain and discuss Systems Security Plan

General Principles

- Explain standards of conduct
- Discuss ITSEC/Common Criteria
- Explain and discuss Waive Policy to Continue Operation

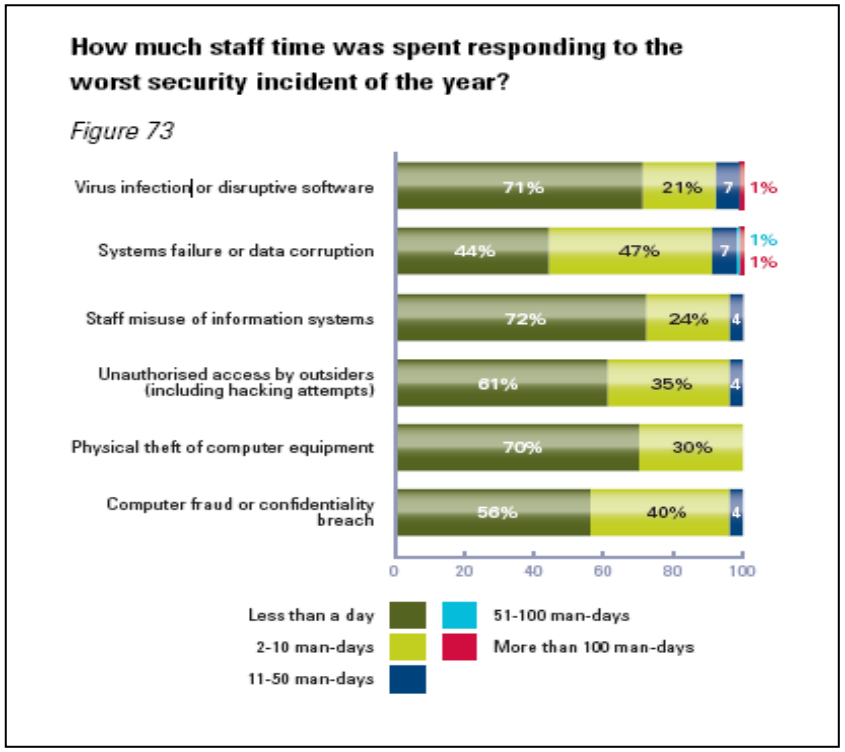
Patch and vulnerability management

Reference: Marcus Alldrick

Patch Management

- **Knowledge of patches**
  - Know when patches for all software you own are released by the vendor
- **Testing**
  - Test all patches, and new software, in a test environment prior to going live
- **Deployment**
  - Can be challenging. Should be automated to insure no machine is missed.
- **Zero-day challenges**
  - Vulnerable time between patch pushed out and able to apply

Reactive remediation



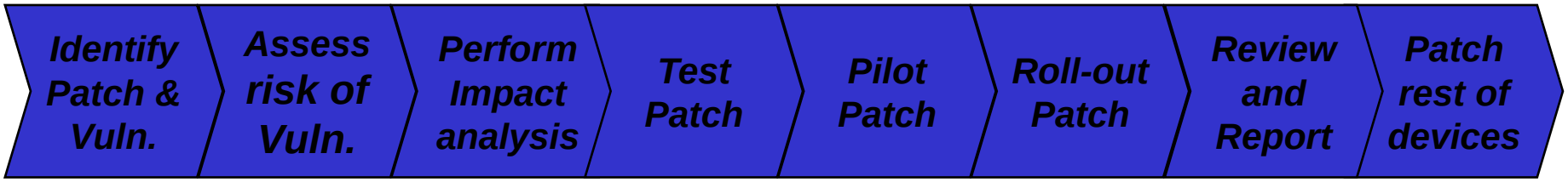
- **Malware infection and system failure remain the incident types that require most staff time to fix**
- **7% of infections took 11-50 man days to recover**
- **1% of infections took >100 man days**

Source: Information Security Breaches Survey 2008, BERR

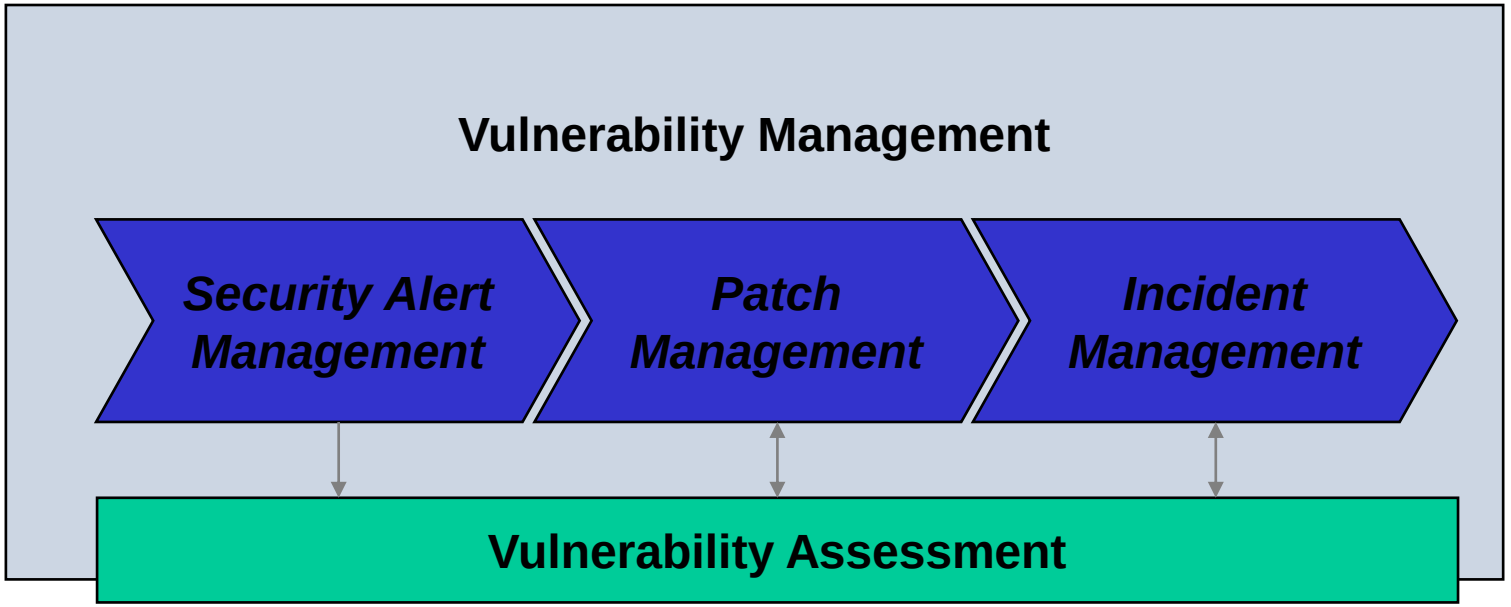
Constraints

- Patch overload
- Different builds
- Complexity of patches
- Device connectivity
- Resource constraints
- Testing timescales
- Testing infrastructure
- Application dependency
- Lack of / inadequate asset inventories
- Lack of / inadequate configuration management
- Scheduling / downtime / business impact

Patch Management process



Vulnerability Management



- Security alerts – proactive
- Patch management - preventative
- Security incidents – reactive / curative
- Vulnerability assessment – indicative monitoring

Key considerations

- Mandate through agreed Patch Management strategy and policy
- Senior Management buy-in and support essential
- Conflicts between patching and business operations must be resolved
- Schedule patch activity as BAU but allow for emergencies
- Prioritise patches based on risk to organisation
- Implement standard builds
- Reduce local admin privileges
- Maintain asset inventories / configuration management
- Consider application whitelisting
- Formulate integrated process and automate wherever possible
- Allocate adequate resource, both management and line

Change management processes

Reference: SAMHSA

Change Management Overview

- Define and identify basic principles of change management
- Two levels
  - Organizational readiness for change
  - Project Schedule Activity/Task changes that impact constraints
- Example of a Change Management model
- Link Change Management to workflow diagramming

Change Management

- Projects make changes to processes, systems, tools, job roles and even organizational structures
  - Require individuals to change how they do their jobs
- Change management is the application of the "set of tools, processes, skill and principles for managing the people side of change to achieve the required outcomes…"
- Goal is to support individuals through the required changes – not impose change

•(Prosci, Inc. 1996. Retrieved February 2012 from www.change-management.com)

Change Management

- Goal is always to keep project on time, on budget and in scope without sacrificing quality
- Integrated throughout Plan:
  - Communication Plan - includes project sponsor, project manager and project team/stakeholders
  - Risk Management Plan - based on validated change management tools applied to common and expected project risks
  - Project Schedule – requires time and space for implementation, so considered in the project duration

10 Principles of Change Management

1) Address change systematically and proactively
2) Start with executive level leadership (via the Project Steering Committee)
3) Involve every layer of the organization
4) Make a formal case – why and how
5) Leadership has "ownership" of the change
6) Communicate the change plan
7) Consider the organizational culture
8) Address the organizational culture
9) Expect the unexpected
10) Engage the individual

•**Ten Guiding Principles of Change Management (2004).* Reggie Van Lee, John Jones, Paul Hyde, Gary Neilson, Andrew Tipping, DeAnne Aguirre, Wolfgang Schirra, Jörg Krings, and Claudia Staub. Booz Allen Hamilton, 2004.

Recovery strategies

Redundancy and Fault-Tolerant Systems

- **Backup and availability solutions**
  - **Redundant hardware ready for "hot swapping"**
  - **Fault-tolerant technologies**
  - **Service Level Agreements**
  - **Solid Operational Procedures**
- **Mean Time Between Failures (MTBF) is the estimated lifespan of a piece of equipment.**
- **Mean Time to Repair (MTTR) is the amount of time expected to get a device repaired and back into production**

Redundancy and Fault-Tolerant Systems

- Avoid single points of failure
- Direct Access Storage Device (DASD): a general term for magnetic disk storage devices, historically used in mainframe and minicomputer environments

Redundancy and Fault-Tolerant Systems

- **Redundant Array of Inexpensive Disks (RAID)**
  - **Striping: divides and writes data over several drives**
  - **Hot swapping: drives can be replaced while the system is running**
  - **Most common RAID levels are 1, 3, and 5**
  - **NOTE: Level 5 is the most commonly used mode**

Redundancy and Fault-Tolerant Systems

RAID Level	Activity	Name
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data are written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data are created with a hamming code, which identifies any errors. This level specifies that up to 39 disks can be used: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.	Byte-level parity
4	Same as level 3, except parity is created at the block level instead of the byte level.	Block-level parity
5	Data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data are simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring

Table 12-2 Different RAID Levels

Redundancy and Fault-Tolerant Systems

- **NOTE: RAID Level 15 is actually a combination of levels 1 and 5, and RAID 10 is a combination of levels 1 and 0**
- **Massive Array of Inactive Disks (MAID)**
  - **A several hundred TB storage area that performs mostly write operations**
  - **Tapes provide the most cost effective solution**
  - **Inactive devices are powered down when not used**

Redundancy and Fault-Tolerant Systems

- **Redundant Array of Independent Tapes (RAIT) – a RAID array with tapes**
- **Storage Area Networks (SAN) – a large amount of storage devices linked together by a high-speed private network**
  - **Provides redundancy, fault tolerance, reliability, and backups**
  - **NOTE: Tape drives, optical jukeboxes, and disk arrays may also be attached to, and referenced through, a SAN**

Redundancy and Fault-Tolerant Systems

- **Clustering: a fault-tolerant server technology in which each server in a redundant server configuration takes part in processing services that are requested**
- **Server cluster: a group of servers viewed logically as a single server and can be managed as a single system**

Redundancy and Fault-Tolerant Systems

- **Grid Computing: a load-balanced parallel means of massive computation implemented with loosely coupled systems that may join and leave the grid randomly**
- **<u>Highlighted Note:</u> Rainbow Tables consist of all possible passwords in hashed formats. This allows attackers to uncover passwords much more quickly than carrying out a dictionary or a brute force attack (I have no idea why this note was placed here unless it was a mistake)**

Redundancy and Fault-Tolerant Systems

- **Backups – Covered in Chapters 6 & 9**
- **Hierarchical Storage Management (HSM): provides continuous online backup functionality that combines hard disks with optical or tape jukeboxes.**
  - **Faster media holds data accessed more often**
  - **Slower media holds rarely accessed data (called near-line devices)**

Redundancy and Fault-Tolerant Systems

- **Caution: TFTP servers are commonly used to save the configuration settings from the network devices.**
- **However, TFTP is an insecure protocol, some network settings are sensitive and should be kept confidential, and a coordinated attack is possible against network devices that load their configurations using TFTP by first causing the network device to fail and then attacking the TFTP download of the configuration to cause a malicious configuration to be loaded.**
- **Alternatives to TFTP should be sought.**

Redundancy and Fault-Tolerant Systems

- **Know the difference between Contingency Planning and Business Continuity Planning**
  - **BCP addresses how to keep the organization in business after a disaster takes place**
  - **Contingency plans address how to deal with small incidents that do not qualify as disasters, as in power surges, server failures, a down communication link to the Internet, or the corruption of software**

Redundancy and Fault-Tolerant Systems

Summary of Technologies Used to Keep the Juices Flowing

The following are the items you will most likely run into when taking the CISSP exam.

- Disk shadowing (mirroring)
- Redundant servers
- RAID, MAID, RAIT
- Clustering
- Backups
- Dual backbones
- Direct Access Storage Device
- Redundant power
- Mesh network topology instead of star, bus, or ring

Redundancy and Fault-Tolerant Systems

- **Mainframes**
  - **Still in use**
  - **Designed from the standpoint of massive I/O**
  - **Not maintenance intensive**
  - **Usually perform batch processing rather than interactive**
  - **Can be configured to load into a different type of system at IPL**
  - **May include supercomputers**

Business Continuity and Disaster Recovery

Dr. C.W. Perr, Sandia Labs

Reference: Shon Harris

What we will cover…

- Project initiation steps
- Recovery and continuity planning requirements
- Business impact analysis
- Selecting, developing, and implementing disaster and continuity plans
- Backup and offsite facilities
- Types of drills and tests

What do we do if everything blows up?

- **The goal of *disaster recovery* is to minimize the effects of a disaster and to take the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner. (Usually very IT focused).**

- **The short: make it not hurt so bad, and get it fixed right away.**

Business Continuity Plan

- ***Availability, integrity, and confidentiality*…a running theme through the ISC2 materials.**
- **These items need to be considered just as important during and after an emergency.**
- **Might be more vulnerable after a disaster.**
- **The plan for this is the Business Continuity Plan (BCP).**

Business Continuity Planning

- **This is a preplanned activity which allows us to…**
  - **Provide and immediate and appropriate response to an emergency**
  - **Protect lives and ensure safety**
  - **Reduce business impact**
  - **Resume critical business functions**
  - **Work with outside vendors during the recovery period**
  - **Reduce confusion during a crisis**
  - **Ensure survivability of the business**
  - **Get “up and running” quickly after a disaster**

Business Continuity Planning (continued)

- **Part of business decisions today should include the following:**
  - **Letting business partners know your company is prepared**
  - **Reassuring shareholders and boards of trustees about your company's readiness**
  - **Making sure a BCP is in place if industry regulations require it**

7 Steps for Business Continuity

1. **Develop the continuity planning policy statement.**
   - **Write a policy that provides the guidance necessary to develop a BCP and that assigns authority to the necessary roles to carry out these tasks.**
2. **Conduct the business impact analysis (BIA).**
   - **Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities, threats, and calculate risks.**
3. **Identify preventive controls.**
   - **Once threats are recognized, identify and implement controls and countermeasures to reduce the organization's risk level in an economical manner.**

*best practices are developed by the National Institute of Standards and Technology(NIST).

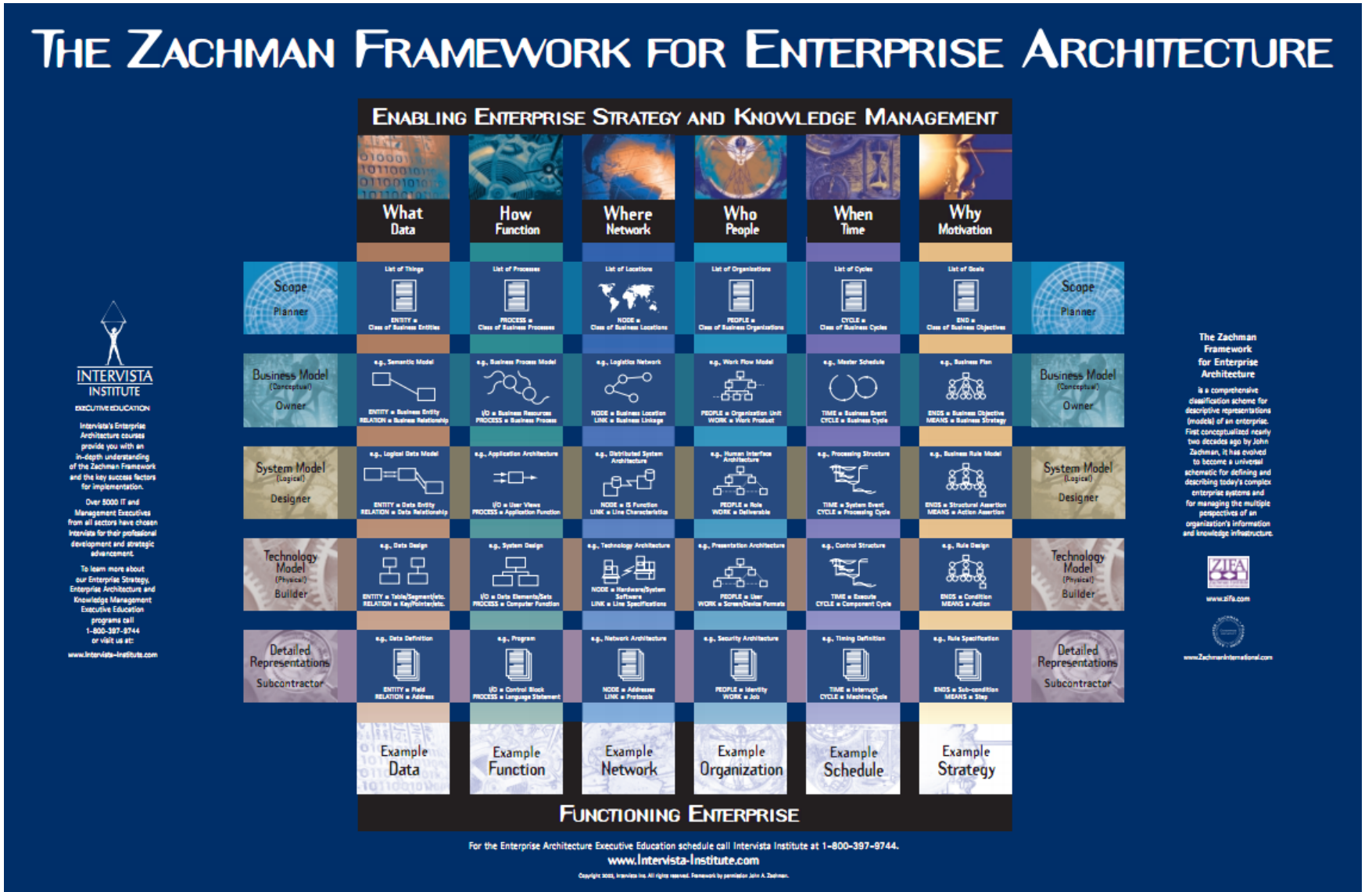
7 Steps for Business Continuity

4. **Develop recovery strategies**
   - Formulate methods to ensure systems and critical functions can be brought online quickly.
5. **Develop the contingency plan.**
   - Write the procedures and guidelines for how the organization can still stay functional in a crippled state.
6. **Test the plan and conduct training and exercises.**
   - Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.
7. **Maintain the plan.**
   - Put in place steps to ensure the BCP is a living document that is updated regularly.

…another Company's version

- $(ISC)^2$
  1. Project initiation
  2. BIA (business impact analysis)
  3. Recovery strategy
  4. Plan design and development
  5. Implementation
  6. Testing
  7. Continual maintenance

Understand the Organization First



Making BCP Part of the Security Policy and Program

- Why do we need to combine business continuity and security plans anyway?
- Response: They both protect the business, unenlightened one. (Their words…not mine).
- BCP = Business Continuity Planning

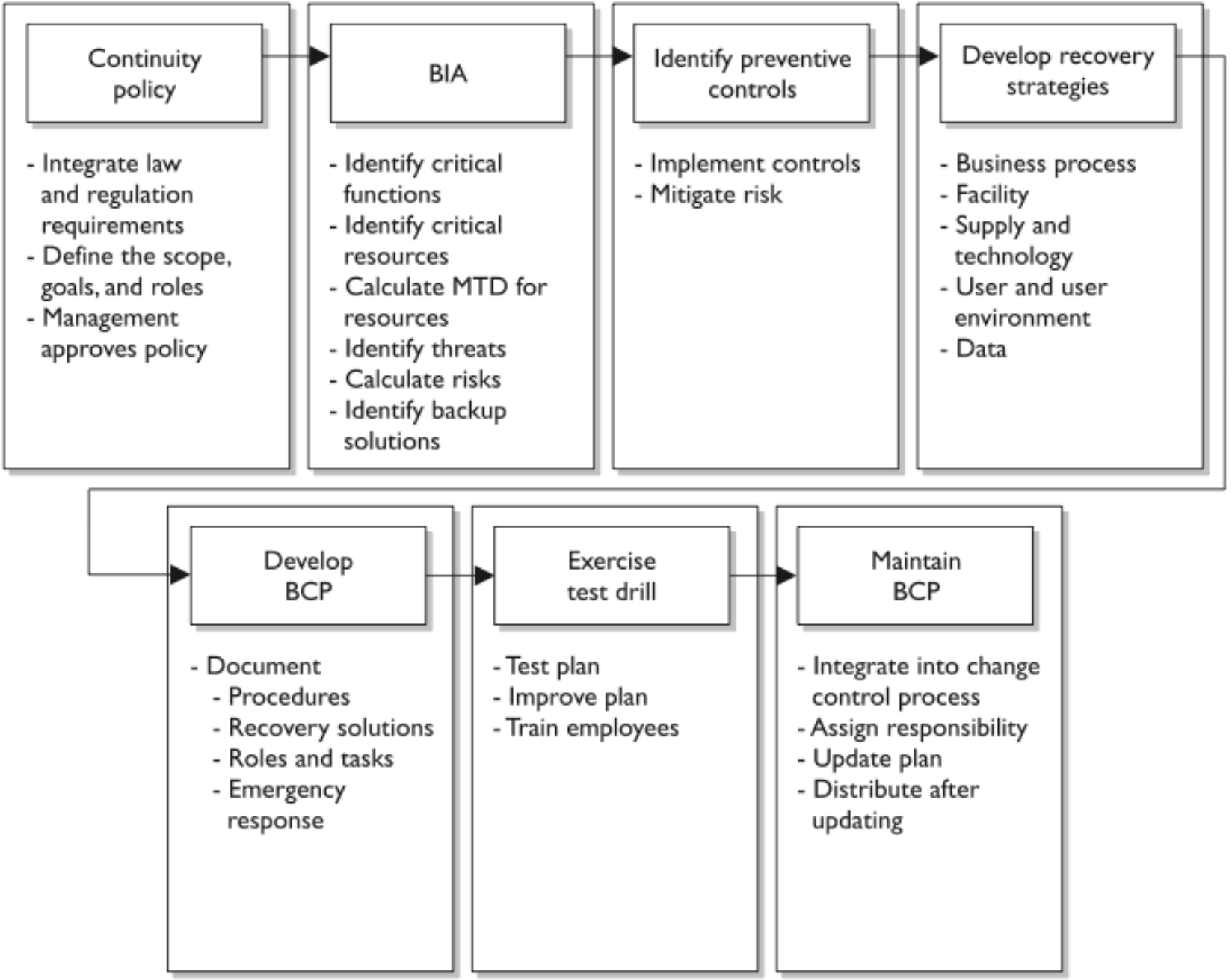


Figure 9-1 The process components of developing a business continuity plan

Why are we doing this? (Warning: Busy Slide)

- A very important question to ask when first developing a BCP is why it is being developed.
- This may seem silly and the answer may at first appear obvious, but that is not always the case.
- You might think that the reason to have these plans is to deal with an unexpected disaster and to get people back to their tasks as quickly and as safely as possible, but the full story is often a bit different. Why are most companies in business?
- To make money and be profitable. If these are usually the main goals of businesses, then any BCP needs to be developed to help achieve and, more importantly, maintain these goals.
- The main reason to develop these plans in the first place is to reduce the risk of financial loss by improving the company's ability to recover and restore operations.
- This encompasses the goals of mitigating the effects of the disaster.

1. Project Initiation

- **After the coffee and donuts have been fetched it is time to get down to business.**
  - **Solidify management support**
  - **Select a *business continuity coordinator* (needs to have direct access to management, and the ability to carry out decisions)**
  - **Bring all issues and threats to the table (representatives from Business units, Senior management, IT department, Security department, Communications department, and the Legal department) –give a sense of ownership here…**

Project Initiation (continued)

- The people who develop the BCP should be the ones to execute it.
- Work with management to develop goals.
- What should the plan address? (natural disaster, terrorist attack, communication outage, etc?)

Continuity planning statement – the scope of the business continuity plan, roles of team members, and goals. [like a mission statement for everything else]

Most companies outline the scope of their BCP to encompass only the larger threats. The smaller threats are then covered by independent departmental contingency plans.

The BCP Coordinators product

BCP Activity	Start Date	Required Completion Date	Completed? Initials/Date	Approved? Initials/Date
Initiating the project				
Continuity policy statement				
Business impact analysis				
Identify preventive controls				
Recovery strategies				
Develop BCP and DRP documents				
Test plans				
Maintain plans				

Table 9-1 Steps to Be Documented and Approved

Project Plan Components

- Objective-to-task mapping
- Resource-to-task mapping
- Milestones
- Budget estimates
- Success factors
- Deadlines

Convince them of value…

- Documents potential loss for the threats involved
- Lip service equals false sense of security…bad
- Legal obligation to due diligence
- Business is the drive to deliver a product, and the sense to anticipate disaster
- Management sets the goals and is responsible for follow up

2. Business Impact Analysis

- ***How bad will this hurt and how long can we deal with this level of pain?***
- **Business impact analysis answers this.**
  - **Functional analysis: based on business, functions, activities, and transactions.**
  - **Threats are mapped based on:**
    - **Maximum tolerable downtime**
    - **Operational disruption and productivity**
    - **Financial considerations**
    - **Regulatory responsibilities**
    - **Reputation**

NOTE A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.

Business Impact Analysis (continued)

- **Data collection comes from asking the committee what they think the threats are**

BIA Steps

The more detailed and granular steps of a BIA are outlined here:

1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

We cover each of these steps in this chapter, but many times it is easier to comprehend the BIA process when it is clearly outlined in this fashion.

Loss Criteria

The committee needs to step through scenarios that could produce the following results:

- Equipment malfunction or unavailable equipment
- Unavailable utilities (HVAC, power, communications lines)
- Facility becomes unavailable
- Critical personnel become unavailable
- Vendor and service providers become unavailable
- Software and/or data corruption

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

- Loss in reputation and public confidence
- Loss of competitive advantages
- Increase in operational expenses
- Violations of contract agreements
- Violations of legal and regulatory requirements
- Delayed income costs
- Loss in revenue
- Loss in productivity

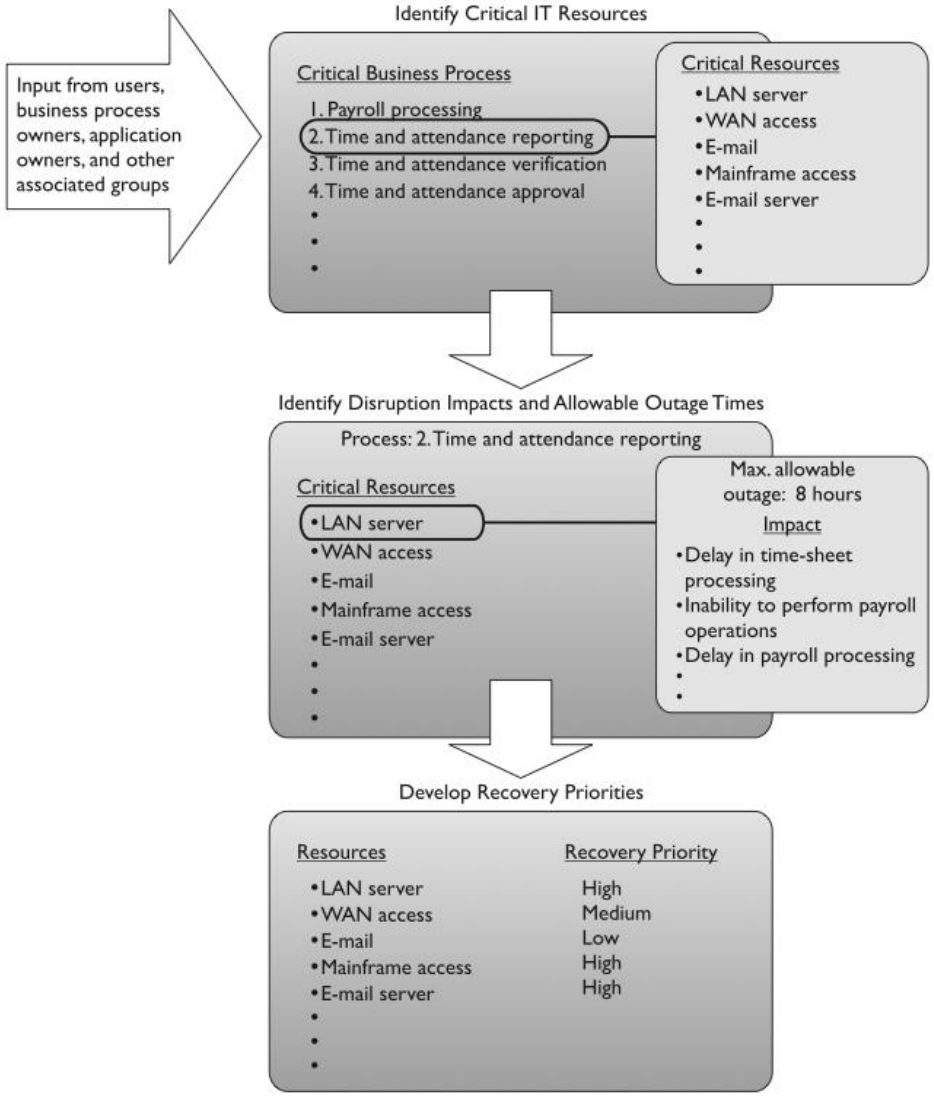
Maximum Tolerable Downtime

- ***Maximum tolerable downtime(MTD)*** **– the outage time that can be endured by the company.**

The following are some MTD estimates that may be used within an organization:

- **Nonessential** 30 days
- **Normal** Seven days
- **Important** 72 hours
- **Urgent** 24 hours
- **Critical** Minutes to hours

Dependency…


Identify Critical IT Resources
Input from users, business process owners, application owners, and other associated groups
Critical Business Process
1. Payroll processing
2. Time and attendance reporting
3. Time and attendance verification
4. Time and attendance approval
Critical Resources
•LAN server
•WAN access
•E-mail
•Mainframe access
•E-mail server
Identify Disruption Impacts and Allowable Outage Times
Process: 2. Time and attendance reporting
Critical Resources
•LAN server
•WAN access
•E-mail
•Mainframe access
•E-mail server
Max. allowable outage: 8 hours
Impact
•Delay in time-sheet processing
•Inability to perform payroll operations
•Delay in payroll processing
Develop Recovery Priorities
Resources
•LAN server
•WAN access
•E-mail
•Mainframe access
•E-mail server
Recovery Priority
High
Medium
Low
High
High

Dependency (continued)

The following interrelation and interdependency tasks should be carried out by the BCP team and addressed in the resulting plan:

- Define essential business functions and supporting departments.
- Identify interdependencies between these functions and departments.
- Discover all possible disruptions that could affect the mechanisms necessary to allow these departments to function together.
- Identify and document potential threats that could disrupt interdepartmental communication.
- Gather quantitative and qualitative information pertaining to those threats.
- Provide alternative methods of restoring functionality and communication.
- Provide a brief statement of rationale for each threat and corresponding information.

Responsibilities (more)

Up until now, we have established management's responsibilities as the following:

- Committing fully to the BCP
- Setting policy and goals
- Making available the necessary funds and resources
- Taking responsibility for the outcome of the development of the BCP
- Appointing a team for the process

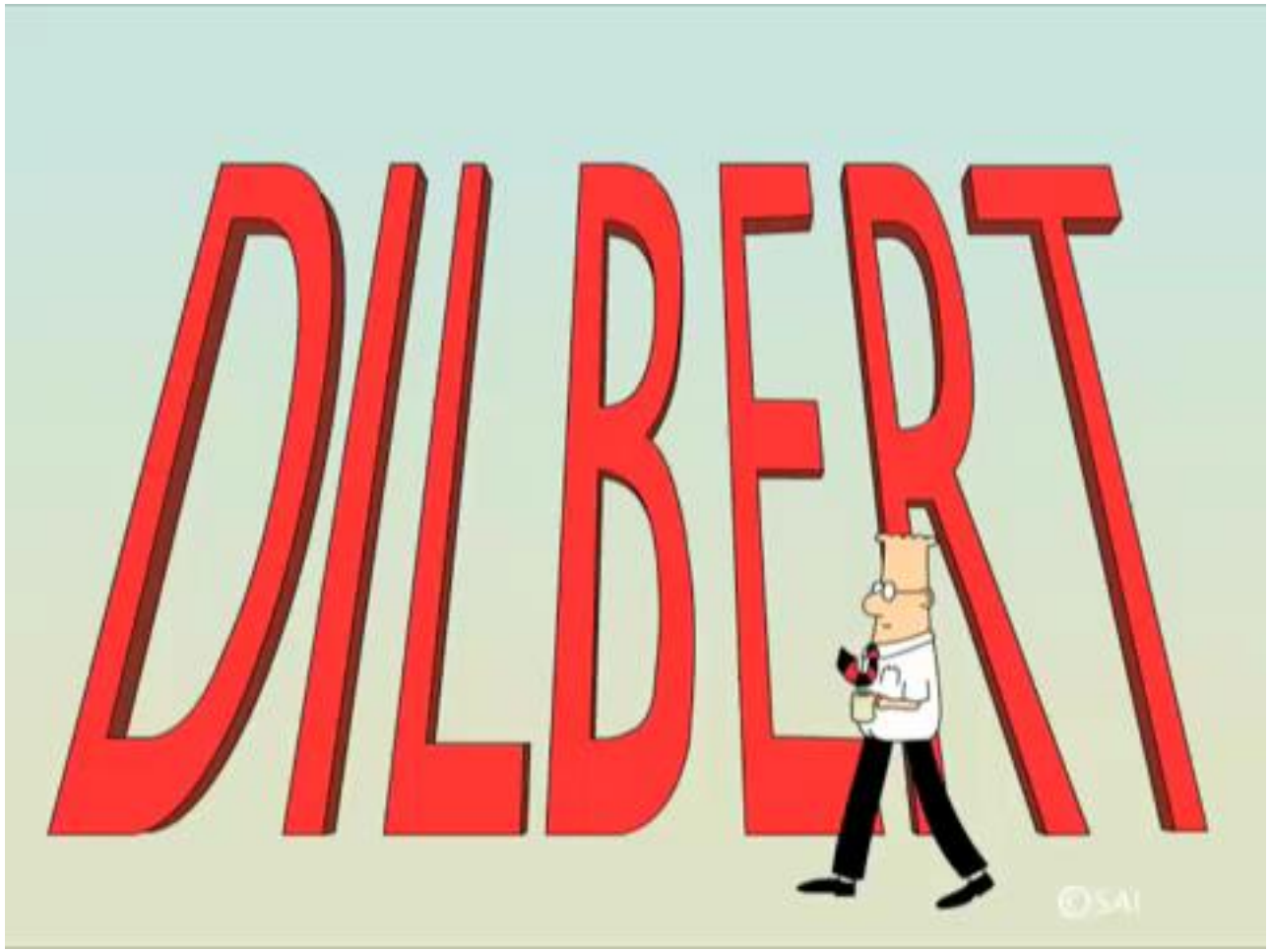
The BCP team's responsibilities are as follows:

- Identifying regulatory and legal requirements that must be met
- Identifying all possible vulnerabilities and threats
- Estimating the possibilities of these threats and the loss potential
- Performing a BIA
- Outlining which departments, systems, and processes must be up and running before any others
- Developing procedures and steps in resuming business after a disaster

The BIA gives us…

- **a guide as to how we should protect ourselves from the things that will cost us the most should they happen.**
- **EX:**
  - Fortification of the facility in its construction materials
  - Redundant servers and communications links
  - Power lines coming in through different transformers
  - Redundant vendor support
  - Purchasing of insurance
  - Purchasing of UPS and generators
  - Data backup technologies
  - Media protection safeguards
  - Increased inventory of critical equipment
  - Fire detection and suppression systems

3. Recovery Strategy



Business Process Recovery

- The books example was an e-commerce site selling cars…lame…
- So here is mine – the Emperor wants to blow up a planet…
  - Validate that the DS is available
  - How long to get to range of the planet?
  - Provide with an estimate
  - Validate the order
  - Send receipt, and tracking info
  - Send coordinates to flyer dudes
  - Send command to destroy that planet

BCP Team needs to know these steps…

- Required roles
- Required resources
- Input and output mechanisms
- Workflow steps
- Required time for completion
- Interfaces with other processes

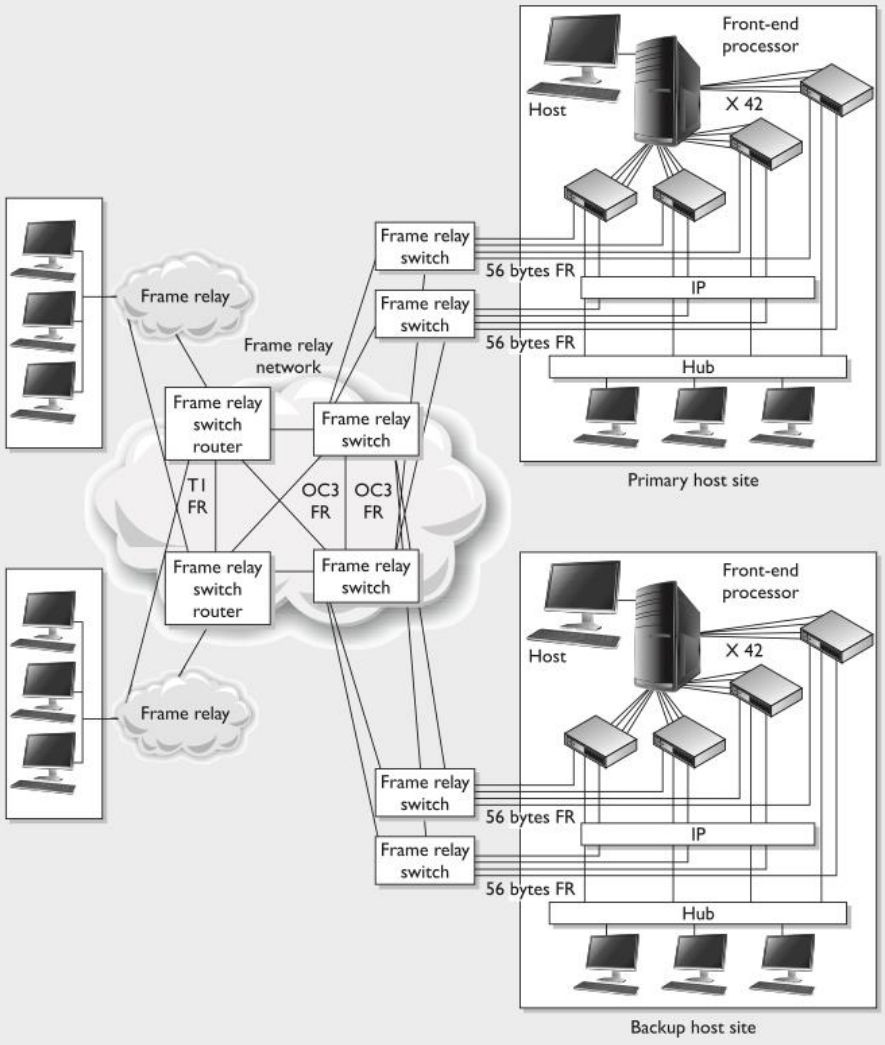
4. Plan Design and Development

- **Non-disaster: A disruption in service due to a device malfunction or failure.**
- **Disaster: An event that causes the entire facility to be unusable.**
- **Catastrophe: A major disruption which destroys the facility.**

Tertiary Sites Backups

Tertiary Sites

During the BIA phase, the team may recognize the danger of the primary backup facility not being available when needed, which could require a tertiary site. This is a secondary backup site, just in case the primary backup site is unavailable. The secondary backup site is sometimes referred to as a "backup to the backup." This is basically plan B if plan A does not work out.



More vocabulary

- **Hot site** A facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues. These sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible. Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state. This is the most expensive of the three types of offsite facilities and can have problems if a company requires proprietary or unusual hardware or software.

- **Warm site** A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment. Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices. This is the most widely used model. It is less expensive than a hot site and can be up and running within a reasonably acceptable time period. It may be a better choice for companies that depend upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after the disaster hits. The odds of finding a remote site vendor that would have a Cray supercomputer readily available in a time of need are pretty slim. The drawback, however, is that the annual testing available with hot-site contracts is not usually available with warm-site contracts, and thus a company cannot be certain that it will in fact be able to return to an operating state within hours.

- **Cold site** A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks, but would require the receipt of equipment from the client, since it does not provide any. The cold site is the least expensive option, but takes the most time and effort to actually get up and functioning right after a disaster. Cold sites are often used as backups for call centers, manufacturing plants, and other services that either can be moved lock, stock, and barrel in one shot or would require extensive retooling and building.

NOTE It is important to understand that the different site types listed here are provided by service bureaus, meaning a company pays a monthly subscription fee to another company for this space and service. A *hot* site is a subscription service. A *redundant* site is a site owned and maintained by the company, meaning the company does not pay anyone else for the site. A redundant site might be "hot" in nature, meaning it is ready for production quickly, but the CISSP exam differentiates between a hot site (subscription service) and a redundant site (owned by the company).

Don’t do this…

Offsite Location

When choosing a backup facility, it should be far enough away from the original site so one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed. There is a rule of thumb that suggests that alternate facilities should be at a bare minimum at least five miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50–200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

Reciprocal Agreement

Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

- How long will the facility be available to the company in need?
- How much assistance will the staff supply in integrating the two environments and ongoing support?
- How quickly can the company in need move into the facility?
- What are the issues pertaining to interoperability?
- How many of the resources will be available to the company in need?
- How will differences and conflicts be addressed?
- How does change control and configuration management take place?
- How often can drills and testing take place?
- How can critical assets of both companies be properly protected?

Supply and technology recovery

- **Granular level backup items:**
  - Network and computer equipment
  - Voice and data communications resources
  - Human resources
  - Transportation of equipment and personnel
  - Environment issues (HVAC)
  - Data and personnel security issues
  - Supplies (paper, forms, cabling, and so on)
  - Documentation

NOTE Many organizations are moving to Voice over IP (VoIP), which means that if the network goes down, network and voice capability are unavailable. The team should address the possible need of redundant voice systems.

The BCP team needs to take into account several things that are commonly overlooked, such as hardware replacements, software products, documentation, environmental needs, and human resources.

Hardware backups

- **Usually a plan of keeping machine images and buying equipment as it is needed.**
- **Service level agreement needs to specify a delivery time for the equipment.**

NOTE MTBF is the estimated lifetime of a piece of equipment and is calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced. MTTR is an estimate of how long it will take to fix a piece of equipment and get it back into production. These concepts are further explained in Chapter 12.

Documentation

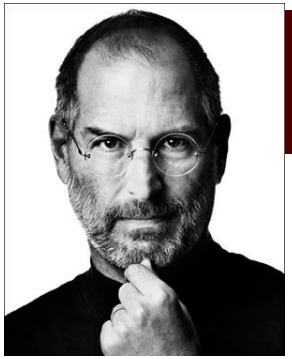
- **Write down the plan…(seriously, this was a whole page in the book…der)**

Plans

Once the business continuity and disaster recovery plans are completed, where do you think they should be stored? Should the company have only one copy and keep it safely in a file cabinet next to Bob so that he feels safe? Nope. There should be two or three copies of these plans. One copy may be at the primary location, but the other copies should be at other locations in case the primary facility is destroyed. Typically, a copy is stored at the BCP coordinator's home, and another copy is stored at the offsite facility. This reduces the risk of not having access to the plans when needed.

These plans should not be stored in a file cabinet, but rather in a fire-resistant safe. When they are stored offsite, they need to be stored in a way that provides just as much protection as the primary site would provide.

NOTE An organization may need to solidify communications channels and relationships with government officials and emergency response groups. The goal of this activity is to solidify proper protocol in case of a city- or regionwide disaster. During the BIA phase, local authorities should be contacted so the team understands the risks of its geographical location and how to access emergency zones. If the company has to initiate its BCP, many of these emergency response groups will need to be contacted during the recovery stage.



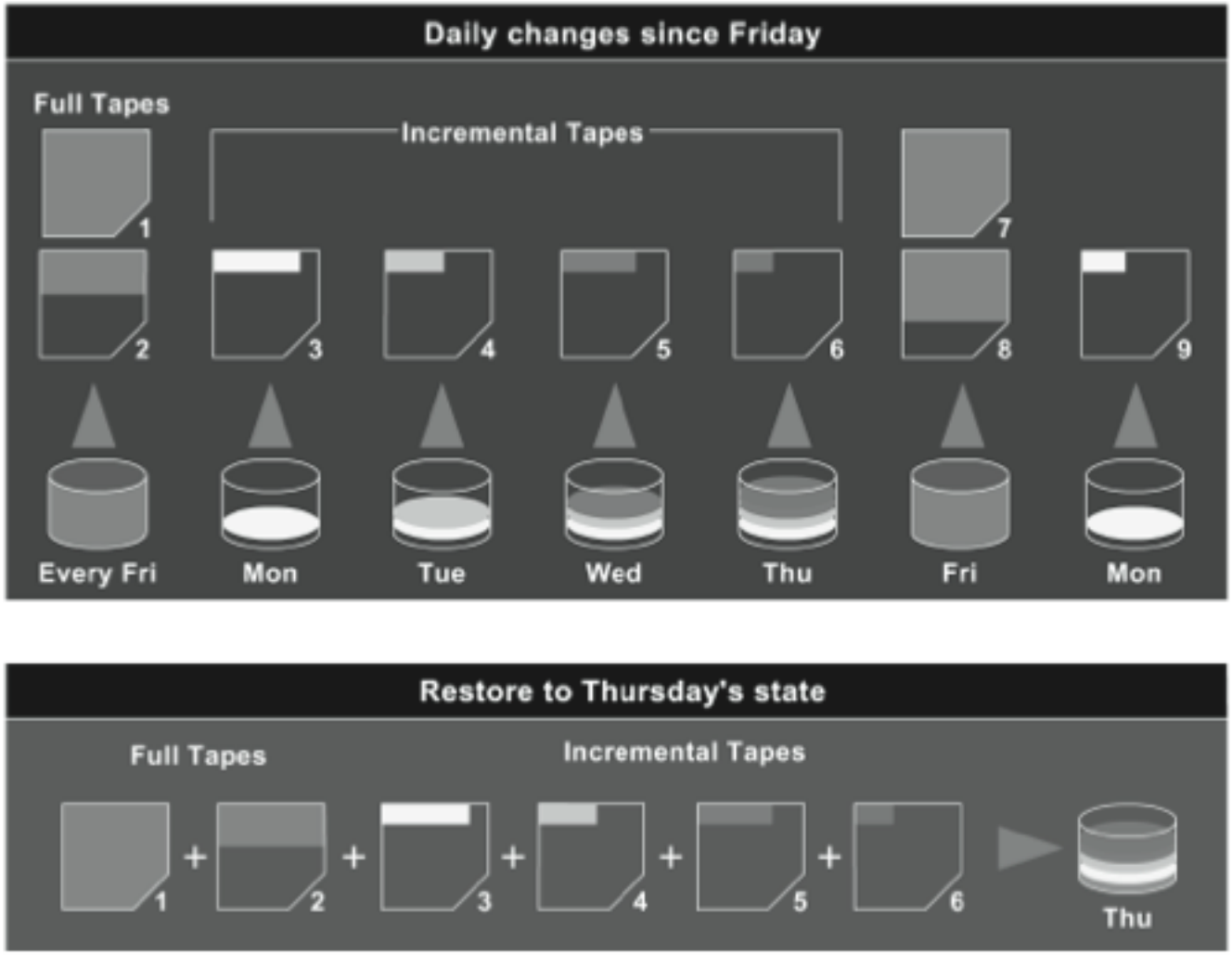
Human resources

- *Executive succession planning* – deputies, replacements, etc. Still has an effects…
- How are you going to get people to work a backup site 250 miles away?
- Usually a skeleton team, so need to identify the critical functions.

5. Implementation

- **Data Backups**
- **Different types of media stored in different locations**
- **Definitions and steps –**
  - **1) *full backup* – all data saved**
  - **2) *differential process* – saves the modified files since↓, restore full, then differential**
  - **3) *last full backup* – last full backup**
  - **4) *incremental process* – back up all the files that have changed since the last full backup**

Figure 9-2
Backup software may alter the archive bit.

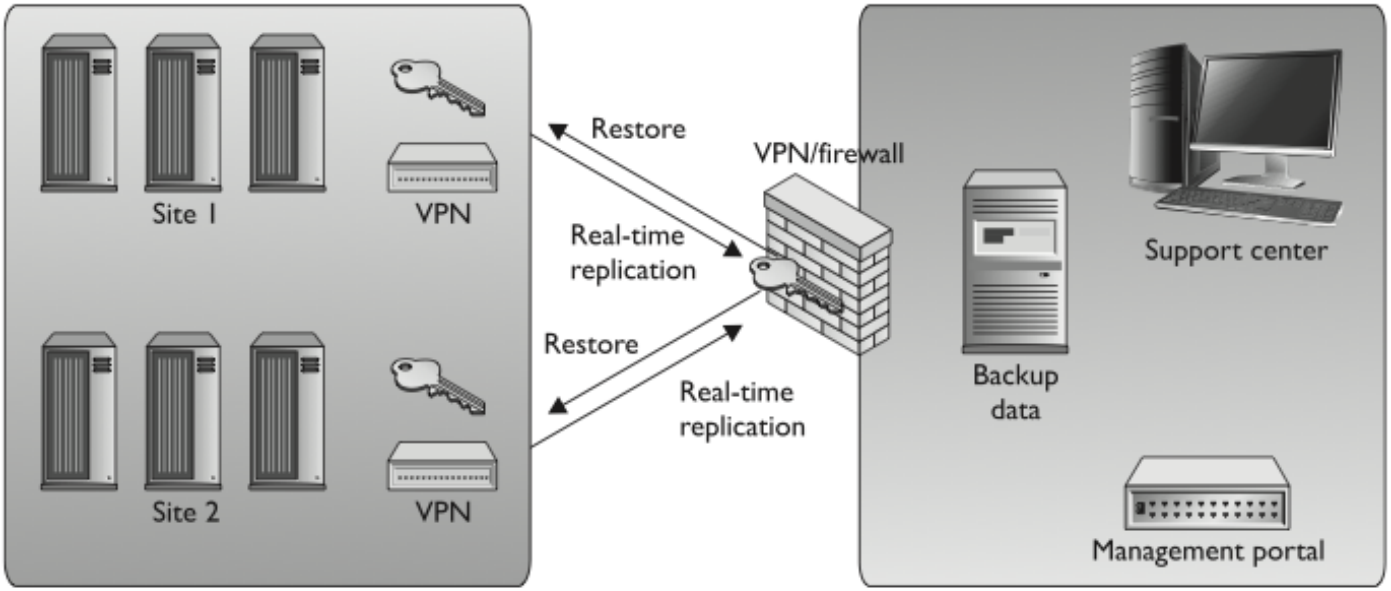


More vocabulary

- ***Electronic vaulting*** **– makes copies of files as they are modified and periodically transmits them to an offsite backup site**
- ***Disk shadowing*** **– similar to data mirroring, provides fault tolerance by duplicating hardware and maintaining more than one copy**
- ***Remote journaling*** **– another method of transmitting data offsite, but this usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data.**

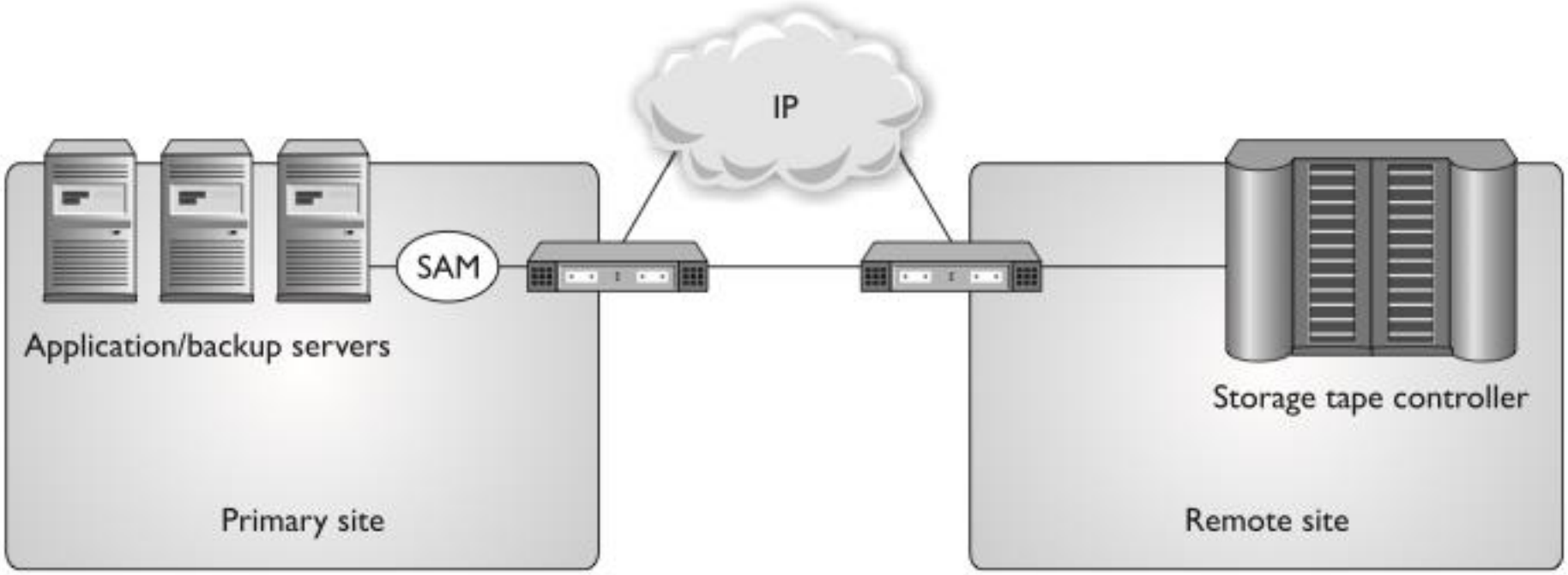
NOTE *Disk duplexing* means there is more than one disk controller. If one disk controller fails, the other is ready and available.

Make sure you can restore…



NOTE Remote journaling takes place in real time and transmits only the file deltas. Electronic vaulting takes place in batches and moves the entire file that has been updated.

Tape Vaulting - the data are sent over a serial line to a backup tape system at the offsite facility



So, basically using magic to the management…awesome diagram

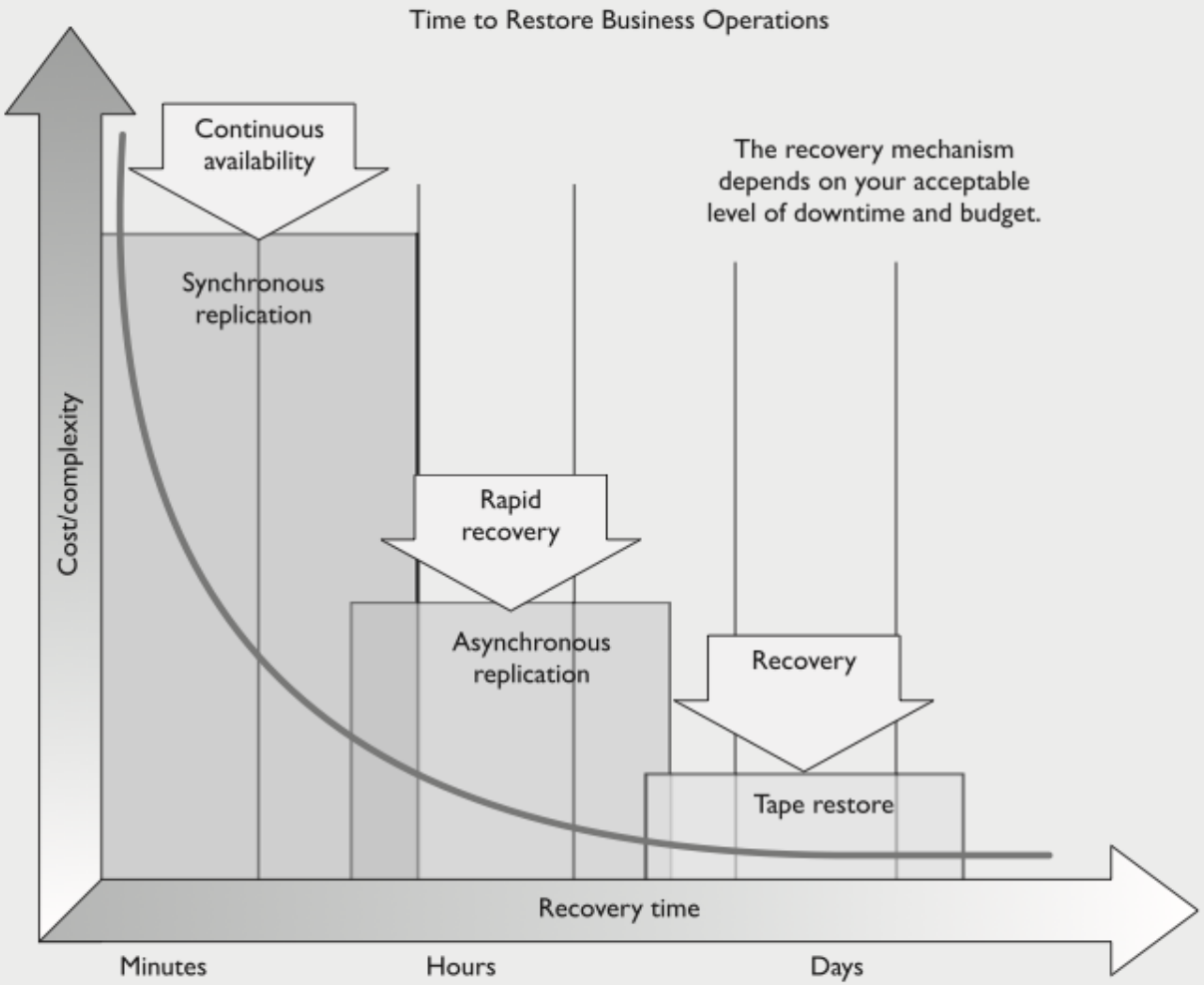
Choose a backup facility

- Can the media be accessed in the necessary timeframe?
- Is the facility closed on weekends and holidays, and does it only operate during specific hours of the day?
- Are the access control mechanisms tied to an alarm and/or the police station?
- Does the facility have the capability to protect the media from a variety of threats?
- What is the availability of a bonded transport service?
- Are there any geographical environmental hazards such as floods, earthquakes, tornadoes, and so on?
- Is there a fire detection and suppression system?
- Does the facility provide temperature and humidity monitoring and control?
- What type of physical, administrative, and logical access controls are used?

Which Data Recovery Solution?

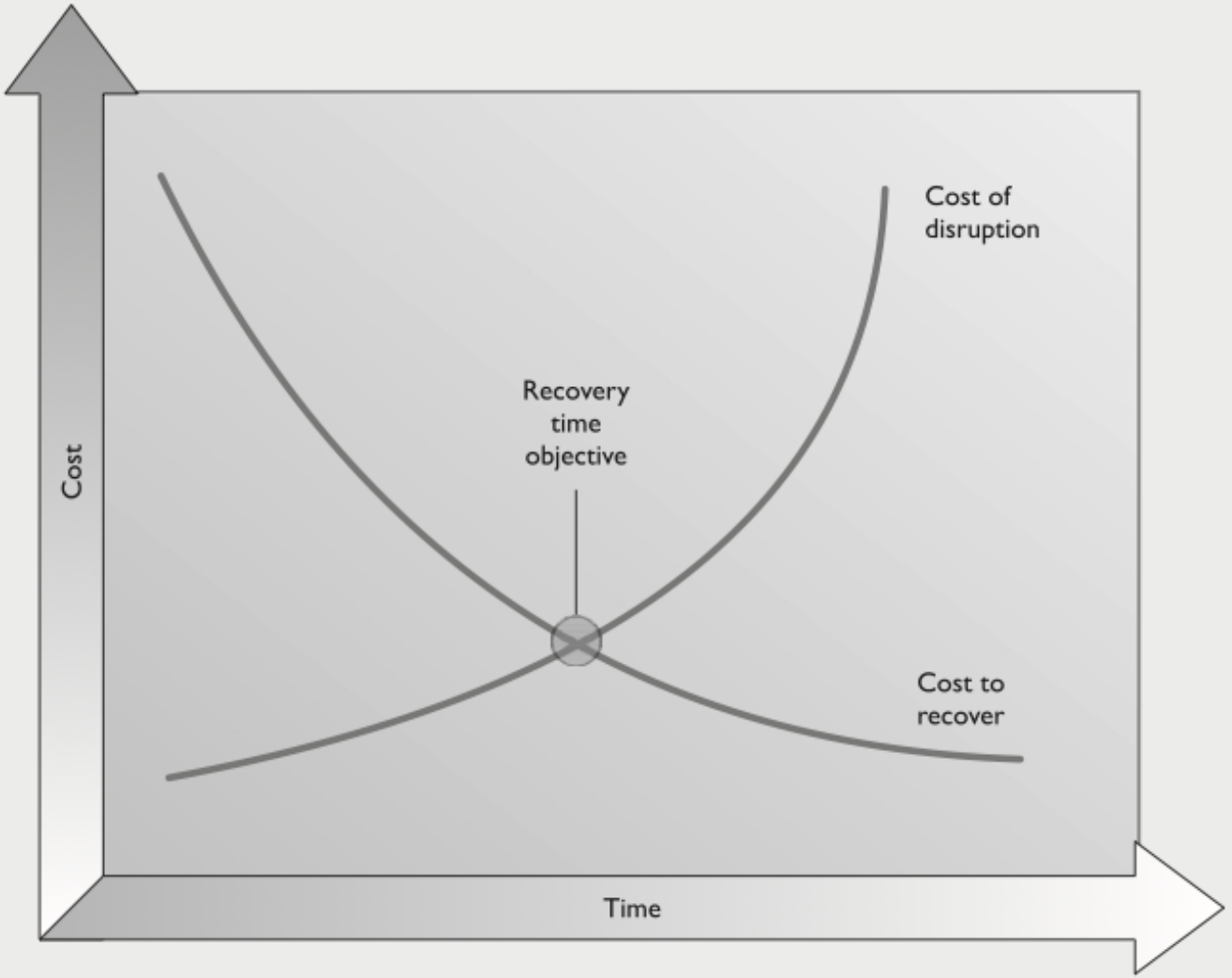
Data classification based on business criticality should have been performed by now.

- The BCP project team needs to divide the data by importance of fast recovery.
- Critical data that need to be continuously available can be restored via electronic vaulting (or remote journaling).
- Other data types can be restored via tapes or mirror systems.



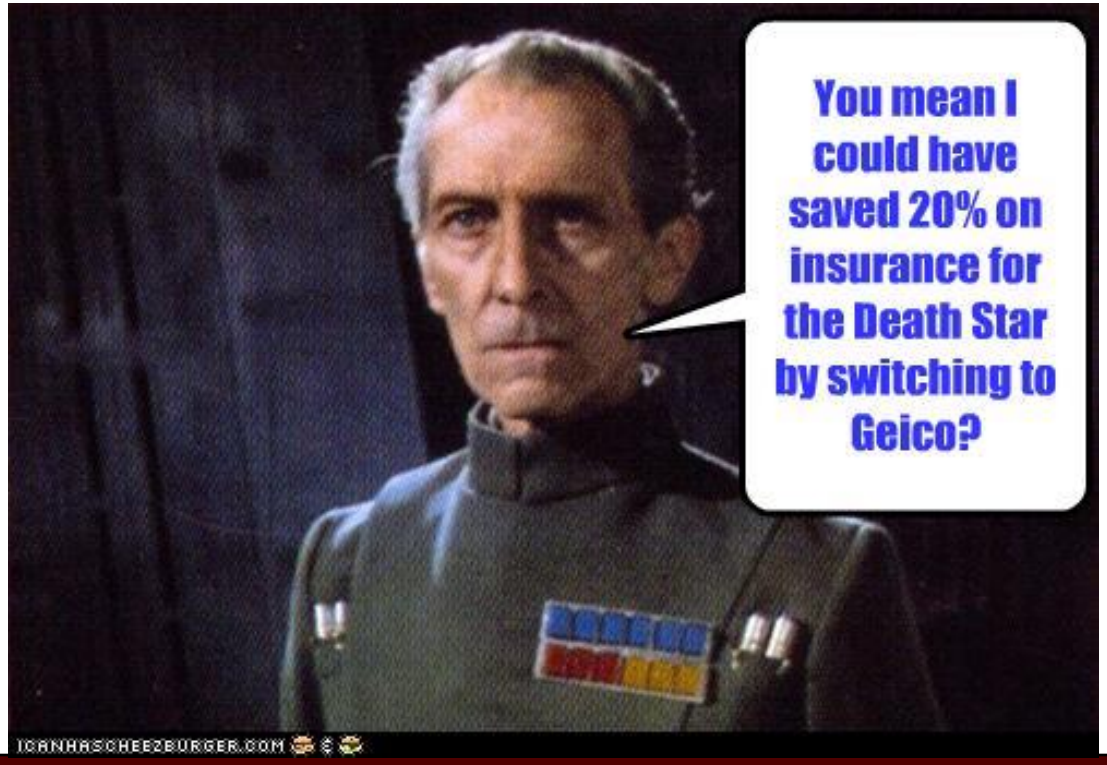
Asynchronous replication means the primary and secondary data volumes are only a few milliseconds out of sync, so the replication is nearly real-time. With synchronous replication, the primary and secondary copies are always in sync, which provides true real-time duplication. Synchronous means replication does not take place in real time, such as in electronic vaulting or batch jobs.

The team must balance the cost to recover against the cost of the disruption. The balancing point becomes the recovery time objective.



Cyberinsurance?

- Not even kidding…Cyberinsurance is a new type of coverage that insures losses caused by denial-of-service attacks, malware damages, hackers, electronic theft, privacy-related lawsuits, and more.
- A company could also choose to purchase a business interruption insurance policy.



Restoration Teams

- The *restoration team* should be responsible for getting the alternate site into a working and functioning environment, and the *salvage team* should be responsible for starting the recovery of the original site.
- A role, or a team, needs to be created to carry out a damage assessment once a disaster has taken place. The assessment procedures should be properly documented and include the following steps:
  - Determine the cause of the disaster.
  - Determine the potential for further damage.
  - Identify the affected business functions and areas. Identify the level of functionality for the critical resources.
  - Identify the resources that must be replaced immediately.
- Estimate how long it will take to bring critical functions back online.
- If it will take longer than the previously estimated MTD values to restore operations, then a disaster should be declared, and the BCP should be put into action.

What team to call? Reconstruction phase…

Different organizations have different criteria, because the business drivers and critical functions will vary from organization to organization. The criteria may comprise some or all of the following elements:

- **Danger to human life**
- **Danger to state or national security**
- **Damage to facility**
- **Damage to critical systems**
- **Estimated value of downtime that will be experienced**

NOTE Examples of possible templates can be found in *NIST's Contingency Planning Guide for Information Technology Systems*, which is available online at http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

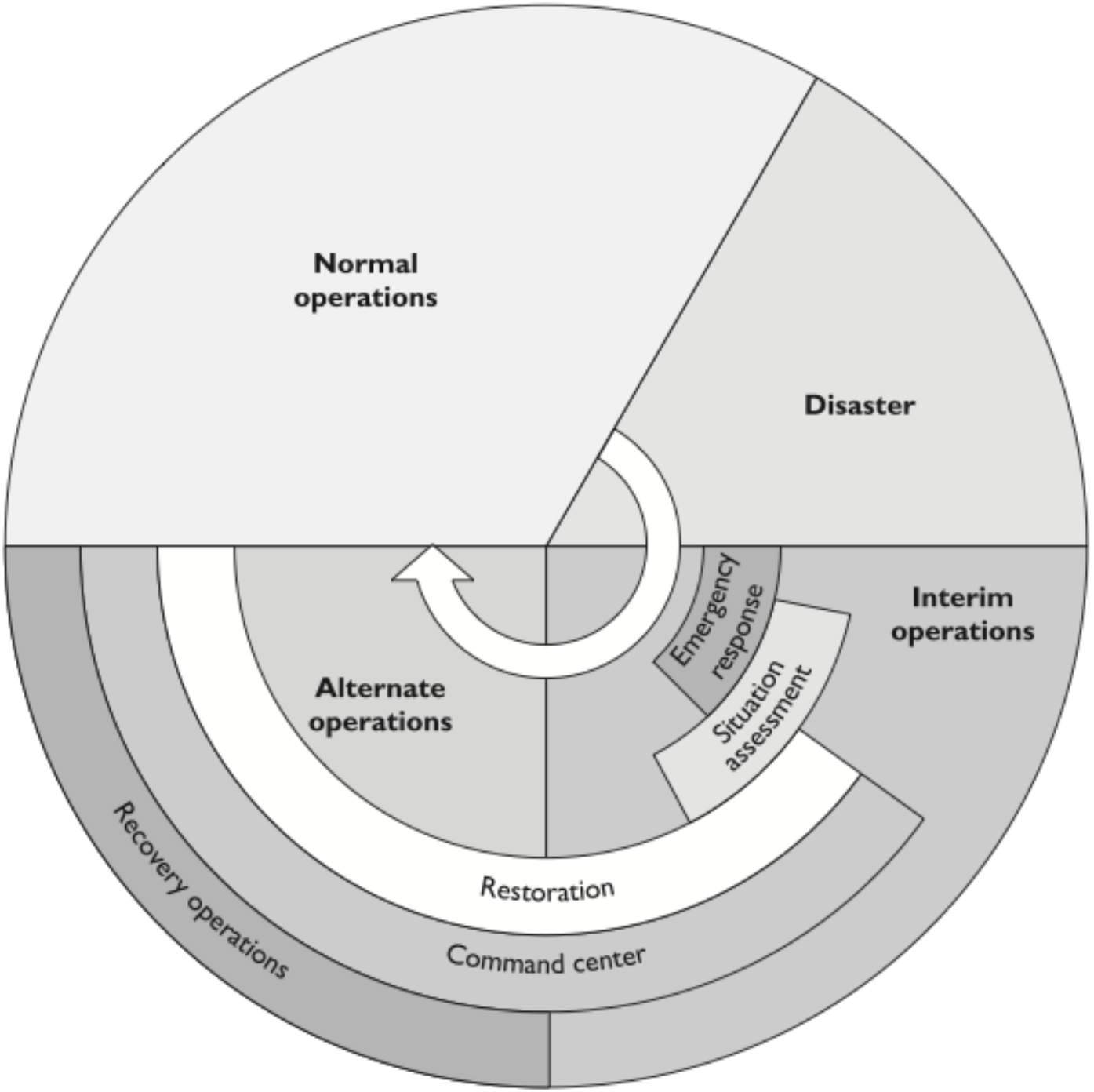
Reconstruction Issues

The following lists a few of these issues:

- **Ensuring the safety of employees**
- **Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)**
- **Ensuring that the necessary equipment and supplies are present and in working order**
- **Ensuring proper communications and connectivity methods are working**
- **Properly testing the new environment**

Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should carry out the following steps:

  - **Back up data from the alternate site and restore it within the new facility.**
  - **Carefully terminate contingency operations.**
  - **Securely transport equipment and personnel to the new facility.**


Normal operations
Disaster
Interim operations
Emergency response
Situation assessment
Alternate operations
Recovery operations
Restoration
Command center

BCP Development Products

Since there is so much work in collecting, analyzing, and maintaining DRP and BCP data, using a product that automates these tasks can prove to be extremely helpful.

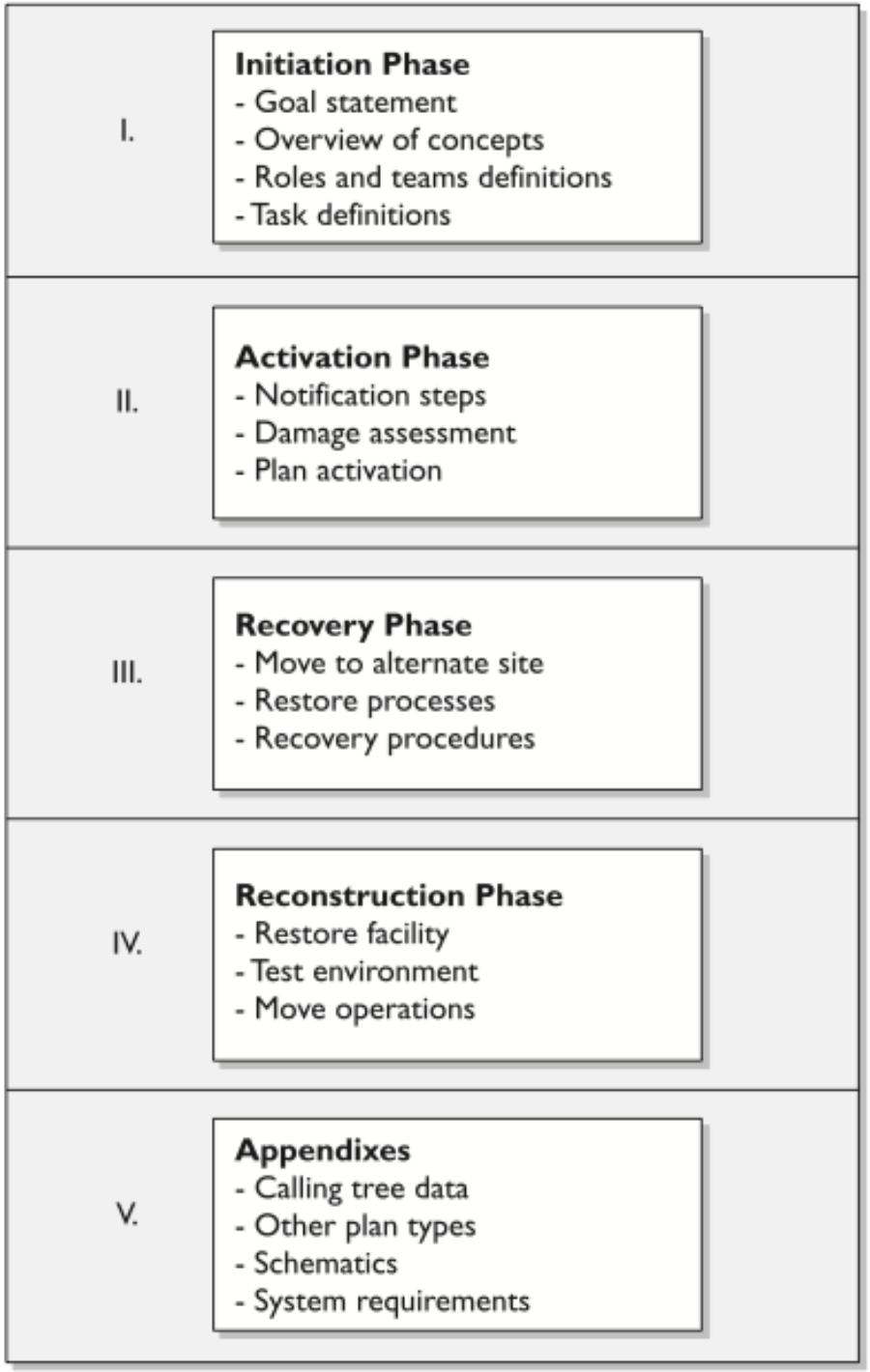
"Automated" plan development can help you create

- Customizable questionnaires through the use of expert-system templates
- Timetables for disaster recovery procedures
- What-if scenario modeling
- Reports on financial and operational impact analysis
- Graphic representations of the analysis results
- Sample questionnaires, forms, and templates
- Permission-based plan maintenance
- Central version control and integration
- Regulatory compliancy

Goals

- **To be useful, a goal must contain certain key information, such as the following:**
- **Responsibility**
  - **Each individual involved with recovery and continuity should have their responsibilities spelled out in writing to ensure a clear understanding in a chaotic situation. Each task should be assigned to the individual most logically situated to handle it. These individuals must know what is expected of them, which is done through training, drills, communication, and documentation. So, for example, instead of just running out of the building screaming, an individual must know that he is responsible for shutting down the servers before he can run out of the building screaming.**
- **Authority**
  - **In times of crisis, it is important to know who is in charge. Teamwork is important in these situations, and almost every team does much better with an established and trusted leader. Such leaders must know that they are expected to step up to the plate in a time of crisis and understand what type of direction they should provide to the rest of the employees. Clear- cut authority will aid in reducing confusion and increasing cooperation.**
- **Priorities**
  - **It is extremely important to know what is critical versus what is merely nice to have. Different departments provide different functionality for an organization. The critical departments must be singled out from the departments that provide functionality that the company can live without for a week or two. It is necessary to know which department must come online first, which second, and so on. That way, the efforts are made in the most useful, effective, and focused manner. Along with the priorities of departments, the priorities of systems, information, and programs must be established. It may be necessary to ensure that the database is up and running before working to bring the file server online. The general priorities must be set by the management with the help of the different departments and IT staff.**
- **Implementation and testing**
  - **It is great to write down very profound ideas and develop plans, but unless they are actually carried out and tested, they may not add up to a hill of beans. Once a continuity plan is developed, it actually has to be put into action. It needs to be documented and put in places that are easily accessible in times of crisis. The people who are assigned specific tasks need to be taught and informed how to fulfill those tasks, and dry runs must be done to walk people through different situations. The drills should take place at least once a year, and the entire program should be continually updated and improved.**

Figure 9-3
The general structure of a business continuity plan



6. Testing

Plan Type	Description
Business resumption plan	Focuses on how to re-create the necessary business processes that need to be reestablished instead of focusing on IT components (i.e., process oriented instead of procedural oriented).
Continuity of operations plan (COOP)	Establishes senior management and a headquarters after a disaster. Outlines roles and authorities, orders of succession, and individual role tasks.
IT contingency plan	Plan for systems, networks, and major applications recovery procedures after disruptions. A contingency plan should be developed for each major system and application.
Crisis communications plan	Includes internal and external communications structure and roles. Identifies specific individuals who will communicate with external entities. Contains predeveloped statements that are to be released.
Cyber incident response plan	Focuses on malware, hackers, intrusions, attacks, and other security issues. Outlines procedures for incident response.
Disaster recovery plan	Focuses on how to recover various IT mechanisms after a disaster. Whereas a contingency plan is usually for nondisasters, a disaster recovery plan is for disasters that require IT processing to take place at another facility.
Occupant emergency plan	Establishes personnel safety and evacuation procedures.

Table 9-2 Different Types of Recovery Plans

Testing Factoids -

- Should be performed annually
- Exercises vs. test. Test pass/fail. Exercises to learn.
- Prepare personnel for what they might face.
- The team of testers must agree upon what exactly is getting tested and how to properly determine success or failure. The team must agree upon the timing and duration of the exercise, who will participate in the exercise, who will receive which assignments, and what steps should be taken. Also, the team needs to determine whether hardware, software, personnel, procedures, and communications lines are going to be tested, and whether it is some, all, or a subset combination.
  - Choose a subset to train a small sub-group at first, and then when everyone is ready take the time of the whole group.

Types of tests

Checklist Test

Okay, did we forget anything?

In this type of test, copies of the BCP are distributed to the different departments and functional areas for review. This is done so each functional manager can review the plan and indicate if anything has been left out or if some approaches should be modified or deleted. This is a method that ensures that some things have not been taken for granted or omitted. Once the departments have reviewed their copies and made suggestions, the planning team then integrates those changes into the master plan.

Structured Walk-Through Test

Let's get in a room and talk about this.

In this test, representatives from each department or functional area come together to go over the plan to ensure its accuracy. The group reviews the objectives of the plan, discusses the scope and assumptions of the plan, reviews the organization and reporting structure, and evaluates the testing, maintenance, and training requirements described. This gives the people responsible for making sure a disaster recovery happens effectively and efficiently a chance to review what has been decided upon and what is expected of them.

The group walks through different scenarios of the plan from beginning to end to make sure nothing was left out. This also raises the awareness of team members about the recovery procedures.

Types of tests (continued)

Simulation Test

Everyone take your places. Okay, action!

This type of test takes a lot more planning and people. In this situation, all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario. The scenario is used to test the reaction of each operational and support representative.

Parallel Test

Let's do a little processing here and a little processing there.

A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility. Some systems are moved to the alternate site and processing takes place. The results are compared with the regular processing that is done at the original site. This points out any necessary tweaking, reconfiguring, or steps that need to take place.

The mother of all tests…

Full-Interruption Test

Shut down and move out!

This type of test is the most intrusive to regular operations and business productivity. The original site is actually shut down, and processing takes place at the alternate site. The recovery team fulfills its obligations in preparing the systems and environment for the alternate site. All processing is done only on devices at the alternate offsite facility.

This is a full-blown drill that takes a lot of planning and coordination, but it can reveal many holes in the plan that need to be fixed before an actual disaster hits. Full-interruption tests should be performed only after all other types of tests have been successful. They are the most risky and can impact the business in very serious and devastating ways if not managed properly; therefore, senior management approval needs to be obtained prior to performing full-interruption tests.

The type of organization and its goals will dictate what approach to the training exercise is most effective. Each organization may have a different approach and unique aspects. If detailed planning methods and processes are going to be taught, then specific training may be required, rather than general training that provides an overview. Higher-quality training will result in an increase of employee interest and commitment.

During and after each type of test, a record of the significant events should be documented and reported to management so it is aware of all outcomes of the test.

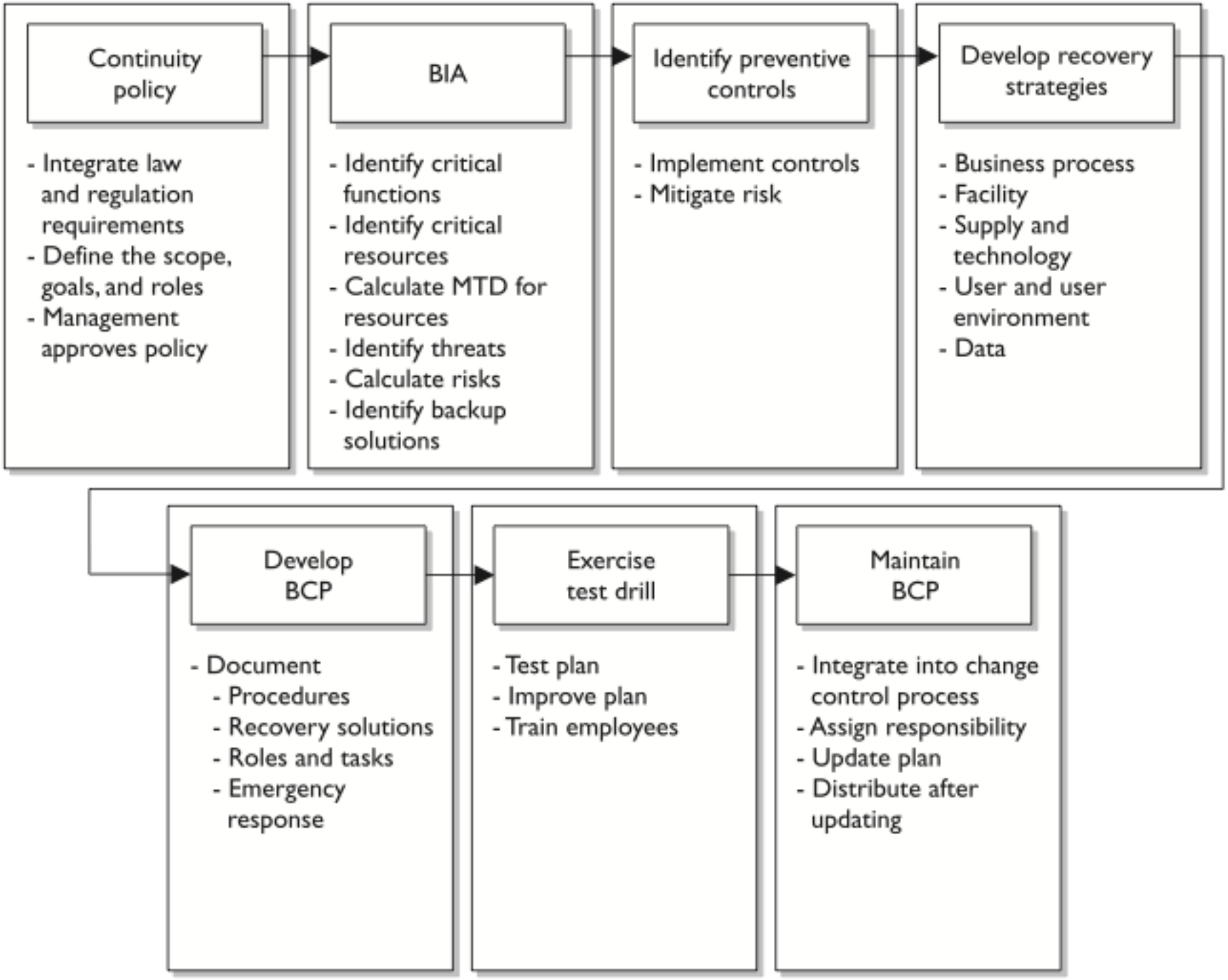
Procedure: Personnel Evacuation Description	Location	Names of Staff Trained to Carry Out Procedure	Date Last Carried Out
Each floor within the building must have two individuals who will ensure that all personnel have been evacuated from the building after a disaster. These individuals are responsible for performing employee head count, communicating with the BCP coordinator, and assessing emergency response needs for their employees.	West wing parking lot	David Miller Mike Lester	Drills were carried out on May 4, 2005.
Comments: These individuals are responsible for maintaining an up-to-date listing of employees on their specific floor. These individuals must have a company-issued walkie-talkie and proper training for this function.			

Table 9-3 Sample Emergency Response Procedure

7. Maintain the Plan!

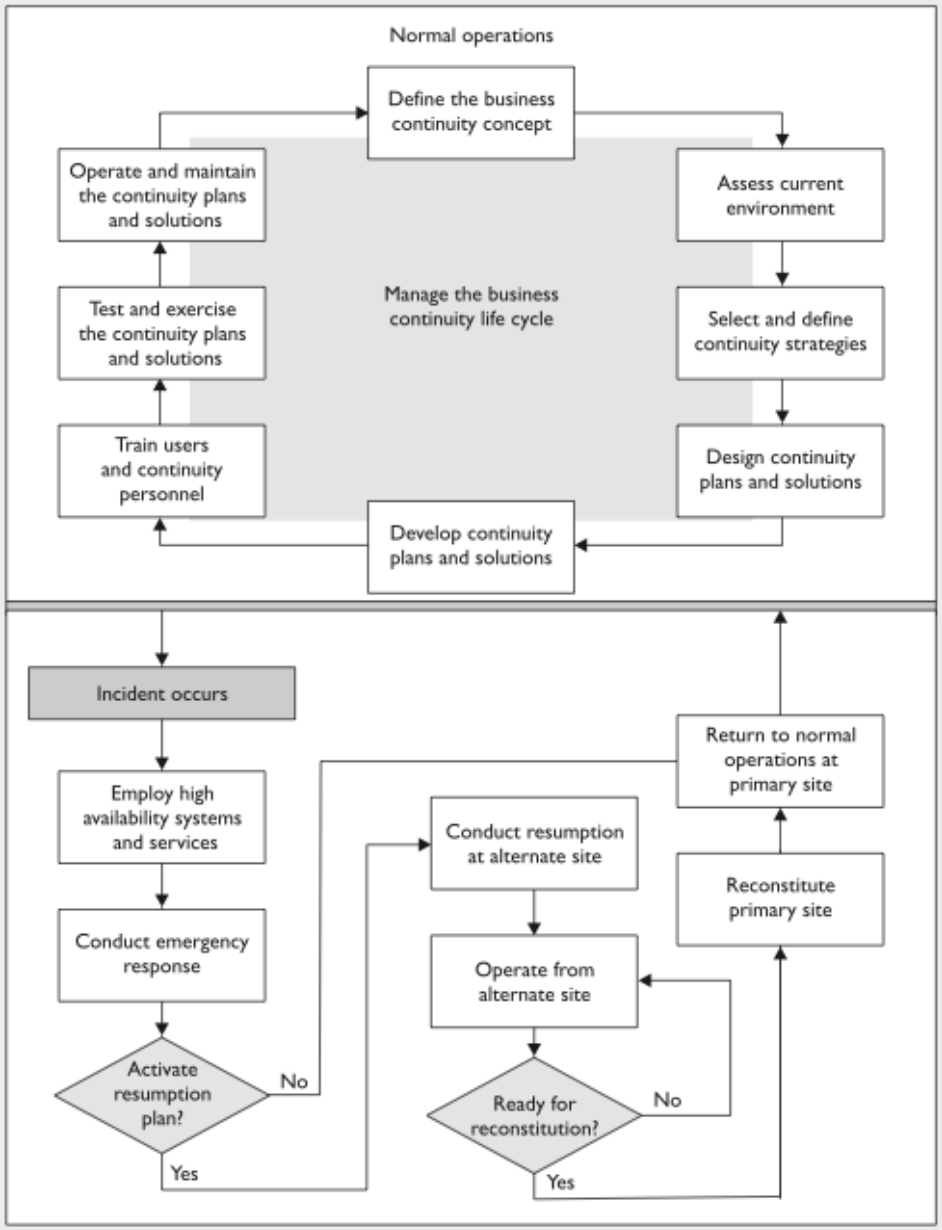
- **The main reasons plans become outdated include the following:**
  - **The business continuity process is not integrated into the change management process.**
  - **Infrastructure and environment changes occur.**
  - **Reorganization of the company, layoffs, or mergers occur.**
  - **Changes in hardware, software, and applications occur.**
  - **After the plan is constructed, people feel their job is done.**
  - **Personnel turns over.**
  - **Large plans take a lot of work to maintain.**
  - **Plans do not have a direct line to profitability.**

- **Organizations can keep the plan updated by taking the following actions:**
  - **Make business continuity a part of every business decision.**
  - **Insert the maintenance responsibilities into job descriptions.**
  - **Include maintenance in personnel evaluations.**
  - **Perform internal audits that include disaster recovery and continuity documentation and procedures.**
  - **Perform regular drills that use the plan.**
  - **Integrate the BCP into the current change management process.**


Continuity policy
- Integrate law and regulation requirements
- Define the scope, goals, and roles
- Management approves policy
BIA
- Identify critical functions
- Identify critical resources
- Calculate MTD for resources
- Identify threats
- Calculate risks
- Identify backup solutions
Identify preventive controls
- Implement controls
- Mitigate risk
Develop recovery strategies
- Business process
- Facility
- Supply and technology
- User and user environment
- Data
Develop BCP
- Document
- Procedures
- Recovery solutions
- Roles and tasks
- Emergency response
Exercise test drill
- Test plan
- Improve plan
- Train employees
Maintain BCP
- Integrate into change control process
- Assign responsibility
- Update plan
- Distribute after updating

Life Cycles

Remember that the DRP and BCP have life cycles. Understanding and maintaining each step of the life cycle is critical if these plans are to be useful to the organization.



Quick Tips

- A business continuity plan (BCP) contains strategy documents that provide detailed procedures that ensure critical business functions are maintained and that help minimize losses of life, operations, and systems.
- A BCP provides procedures for emergency responses, extended backup operations, and post-disaster recovery.
- A BCP should reach enterprisewide, with individual organizational units each having their own detailed continuity and contingency plans.
- A BCP needs to prioritize critical applications and provide a sequence for efficient recovery.
- A BCP requires senior executive management support for initiating the plan and final approval.
- BCPs can quickly become outdated due to personnel turnover, reorganizations, and undocumented changes.
- Executives may be held liable if proper BCPs are not developed and used.
- Threats can be natural, manmade, or technical.
- The steps of recovery planning include initiating the project; performing business impact analyses; developing a recovery strategy; developing a recovery plan; and implementing, testing, and maintaining the plan.
- The project initiation phase involves getting management support, developing the scope of the plan, and securing funding and resources.
- The business impact analysis is one of the most important first steps in the planning development. Qualitative and quantitative data needs to be gathered, analyzed, interpreted, and presented to management.
- Executive commitment and support are the most critical elements in developing the BCP.
- A business case must be presented to gain executive support. This is done by explaining regulatory and legal requirements, exposing vulnerabilities, and providing solutions
- Plans should be prepared by the people who will actually carry them out.
- The planning group should comprise representatives from all departments or organizational units.
- The BCP team should identify the individuals who will interact with external entities such as the press, shareholders, customers, and civic officials. Response to the disaster should be done quickly and honestly, and should be consistent with any other employee response.
- Disaster recovery and continuity planning should be brought into normal business decision-making procedures.
- The loss criteria for disasters include much more than direct dollar loss. They may include added operational costs, loss in reputation and public confidence, loss of competitive advantage, violation of regulatory or legal requirements, loss in productivity, delayed income, interest costs, and loss in revenue.
- A survey should be developed and given to the most knowledgeable people within the company to obtain the most realistic information pertaining to a company's risk and recovery procedures.
- The plan's scope can be determined by geographical, organizational, or functional means.
- Many things need to be understood pertaining to the working environment so it can be replicated at an alternate site after a disaster.
- Subscription services can supply hot, warm, or cold sites.
- A reciprocal agreement is one in which a company promises another company it can move in and share space if it experiences a disaster and vice versa. Reciprocal agreements are very tricky to implement and are unenforceable. However, they are cheap and sometimes the only choice.
- A hot site is fully configured with hardware, software, and environmental needs. It can usually be up and running in a matter of hours. It is the most expensive option, but some companies cannot be out of business longer than a day without detrimental results.
- A warm site does not have computers, but it does have some peripheral devices such as disk drives, controllers, and tape drives. This option is less expensive than a hot site, but takes more effort and time to get operational.
- A cold site is just a building with power, raised floors, and utilities. No devices are available. This is the cheapest of the three options, but can take weeks to get up and operational.
- When returning to the original site, the least critical organizational units should go back first.
- An important part of the disaster recovery and continuity plan is to communicate its requirements and procedures to all employees.
- Testing, drills, and exercises demonstrate the actual ability to recover and can verify the compatibility of backup facilities.
- Before tests are performed, there should be a clear indication of what is being tested, how success will be determined, and how mistakes should be expected and dealt with.
- A checklist test is one in which copies of the plan are handed out to each functional area to ensure the plan properly deals with the area's needs and vulnerabilities.
- A structured walk-through test is one in which representatives from each functional area or department get together and walk through the plan from beginning to end.
- A simulation test is one in which a practice execution of the plan takes place. A specific scenario is established, and the simulation continues up to the point of actual relocation to the alternate site.
- A parallel test is one in which some systems are actually run at the alternate site.
- A full-interruption test is one in which regular operations are stopped and where processing is moved to the alternate site.
- Remote journaling involves transmitting the journal or transaction log offsite to a backup facility.

Disaster recovery processes and plans

Contingency Plans

- Develop contingency plan – procedures and guidelines for how the organization can still stay functional in a crippled state
- Discuss current contingency plan with necessary parties
- Explain contingency plan
- Monitor contingency plan training
- Propose contingency plan
- Summarize contingency plan

Contingency Plans

- Direct implementation of contingency plan
  - Object-to-task mapping
  - Resource-to-task mapping
  - Milestones
  - Budget estimates
  - Success factors
  - Deadlines
- Direct operation of contingency plan
- Influence management on importance of having properly trained SA/staff to perform contingency plan on mission critical systems
- Test contingency plan – highlights deficiencies in the plan

Contingency Plans

- Verify current contingency plan is available and accuracy
- Verify that necessary parties understand contingency plan and where it is maintained, parties include:
  - Business units
  - Senior management
  - IT department
  - Security department
  - Communications department
  - Legal department
- Write contingency plan

Reconstitution

- Discuss current reconstitution plan with necessary parties to ensure they understand their respective reconstitution roles and responsibilities
- Explain reconstitution plan – plan for handling the situation when an organization moves to a new site or returns to the original site
- Explain restoration – placing information onto the new site through the use of proper protection, detection, and reaction capabilities defined in the plan
- Monitor reconstitution plan training
- Monitor restoration/reconstitution
- Summarize restoration/reconstitution plan

Reconstitution

- Verify that necessary parties understand restoration/reconstitution plans and where they are maintained
- Develop restoration/reconstitution plan
  - Ensuring adequate environment and necessary equipment and supplies are present and functional
  - Proper communications, connectivity and testing procedures
  - Backup data from alternate site to new site
- Direct implementation of reconstitution plan – facility restoration, environment testing, and moving of operations
- Direct operation of reconstitution plan
- Implement and maintain recovery procedures
- Implement recovery procedures

Reconstitution

- Implement testing and assessment
  - Checklist test – has anything been forgotten?
  - Structured walk-through test – all parties meet and talk through scenarios step by step
  - Simulation test – drills are done to practice executing disaster recovery plans
  - Parallel test – ensures that specific systems can run at the alternate offsite facility
  - Full-Interruption test – original site is shutdown and offsite is used
- Implement training
- Influence management on importance of having properly trained SA/staff to perform reconstitution plan on mission critical systems
- Propose reconstitution plan

Reconstitution

- Test/exercise restoration/reconstitution plan
- Verify current restoration/reconstitution plan is available and accurate
- Write restoration/reconstitution plan
- Evaluate test/execution of reconstitution plan

Recovery

- Address recovery procedures with SA/staff
- Develop recovery plan
  - Business process recovery
  - Facility recovery
  - Supply and technology recovery
  - User environment recovery
  - Data recovery
- Direct SA/staff to use recovery plan during recovery
- Discuss current recovery plan with necessary parties
- Explain recovery plan
- Monitor recovery plan training

Recovery

- Summarize recovery plan
- Verify that necessary parties understand recovery plan and where it is maintained
- Direct implementation of recovery plan
- Direct operation of recovery plan
  - Move to alternate site
  - Restore processes
  - Recovery procedures
- Influence management on importance of having properly trained SA/staff to perform recovery plan on mission critical systems
- Propose recovery plan

Recovery

- Test recovery plan
- Verify current recovery plan is available and accurate
- Verify SA understands rules for restoring files
- Write recovery plan
  - Required roles
  - Required resources
  - Input and output mechanisms
  - Workflow steps
  - Required time for completion
  - Interfaces with other processes

Business continuity planning and exercises

Reference: Gerald Isaacson

Business Continuity Planning

- a "disaster" is:
  - Trying to make red chili ribs in a crock pot
  - He lost a laptop with the only copy of his thesis
  - She lost her research and papers in the lab fire
  - Payroll system failed the day before payday
  - Asbestos released in a dorm renovation
  - The death of a student
  - The Northeast blackout
  - Hurricane Katrina

Business Continuity Planning

- **Disaster**
  - **is an event, often unexpected, that seriously disrupts your usual operations or processes and can have long term impact on your normal way of life or that of your organization.**
- **RTO [Recovery Time Objective]**
  - **the point in time when you must have at least the critical aspects of your business operational again.**
- **RPO [Recovery Point Objective]**
  - **The last copy of your data that is out of harm's way – hopefully it is recently current.**

Business Continuity Planning

is:

- **a process to minimize the impact of a major disruption to normal operations**
- **a process to enable restoration of critical assets**
- **a process to restore normalcy as soon as possible after a crisis.**

not just:

- **recovery of information technology resources**
  - **and it is the phase of crisis management that follows the immediate actions taken to protect life and property and contain the event**
  - **it begins when the situation has been stabilized.**

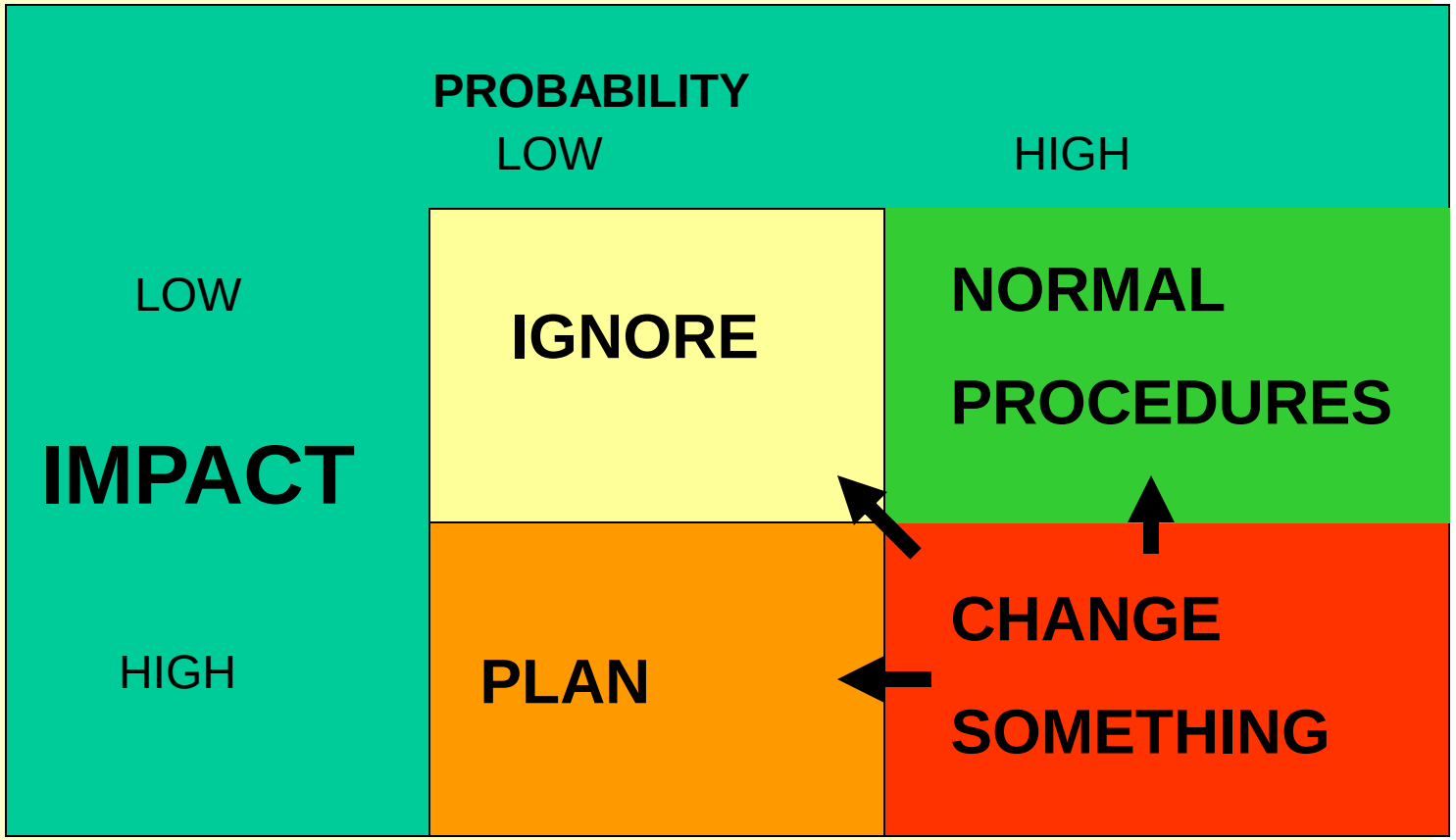
Business Continuity Planning

Key Questions to Ask

- In an emergency, how will the institutional leaders communicate with each other? What are the protocols and procedures? How and where will they find an up-to-date contact list? Where should they convene (initial and back-up locations)?
- Which institutional business processes are considered critical with respect to what needs to be restored first?
- How can the institution manage incidents in ways to minimize risk to current operations, future enrollment, and donor support?
- What would happen if the systems that control security and alarms in residence halls, classroom buildings, and administrative facilities are compromised?
- What are the consequences if environmental pollutants make access to campus facilities impossible?
- What would result from the complete or partial destruction of key buildings and the records they contain?
- How will the institution operate in the face of long-term inaccessibility to communication systems?

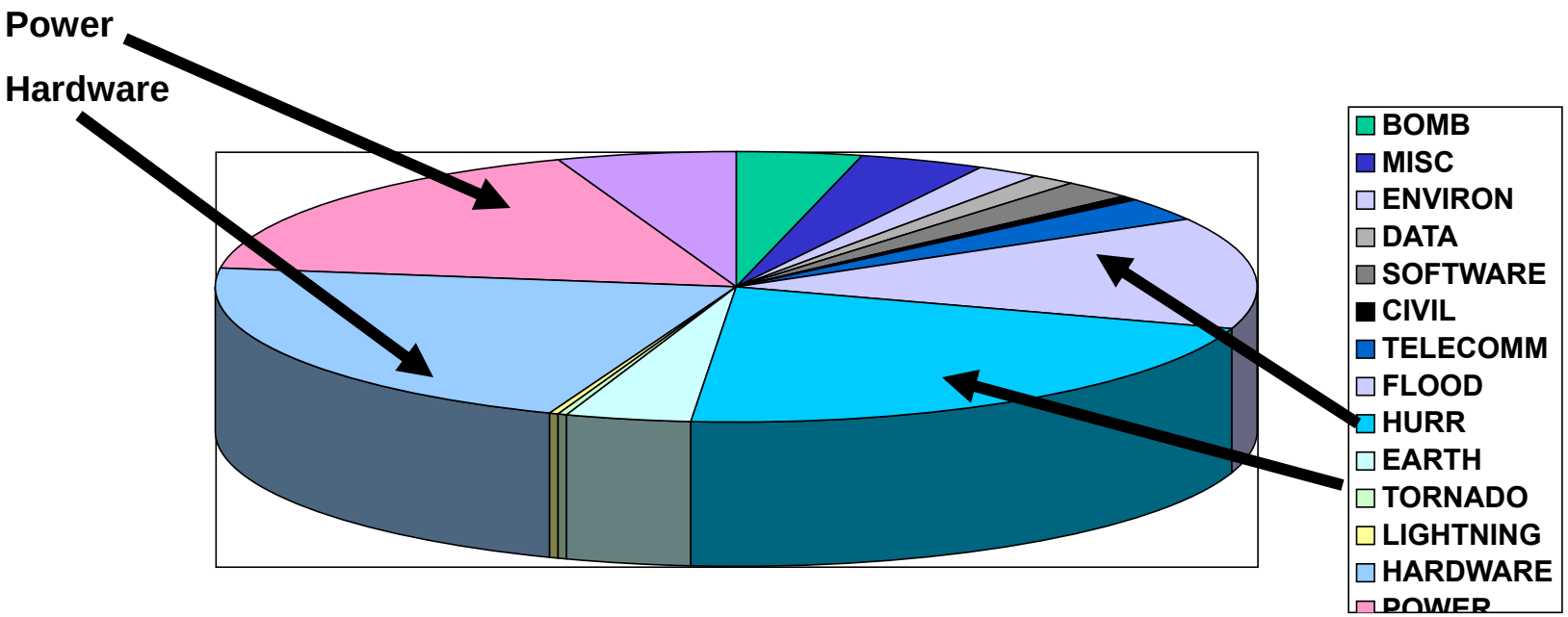
Business Continuity Planning

The Risk Matrix



Business Continuity Planning

Network Operations Disruptions



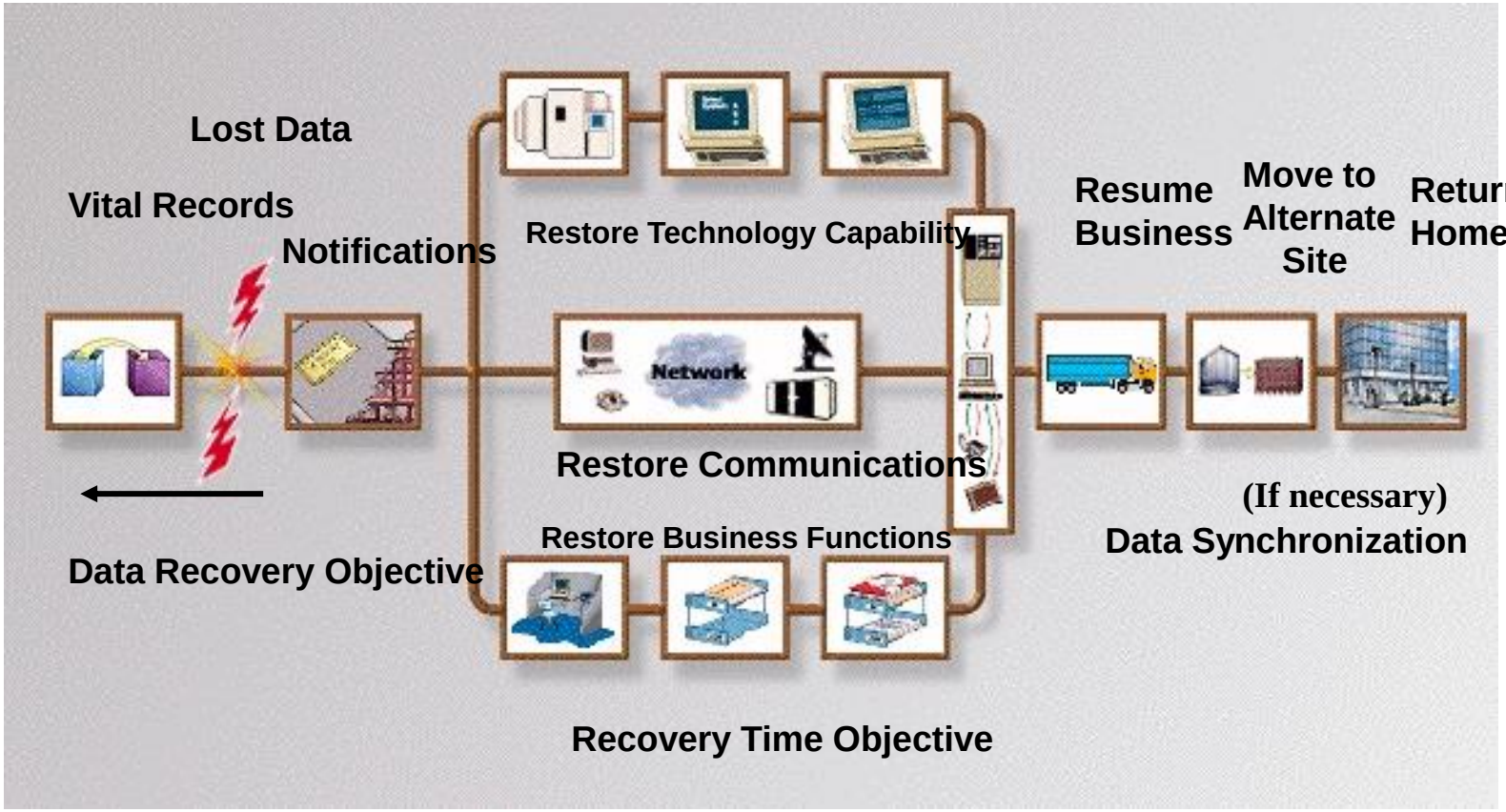
Source: Gartner Group and Comdisco

Business Continuity Planning

Mt. St. Helens – May 1980 – new threats arise

Business Continuity Planning

High Level Look at a Recovery Effort



Physical security

Master Sergeant Alex Applegate, USAF (ret)

Shon Harris

Overview

- Introduction to Physical Security
- The Planning Process
- Protecting Assets
- Internal Support Systems
- Perimeter Security

Introduction to Physical Security

- Most people in the information security field do not think as much about physical security as they do about computer security
- Many people have to specialize in facility construction, risk assessment and analysis, secure data center implementation, fire protection, IDS and CCTV implementation, personal emergency response and training, and legal and regulatory issues

Introduction to Physical Security

Physical threats to an organization are broken into four broad categories:

- **Natural environmental threats – floods earthquakes, storms and tornadoes, fires, extreme temperature**
- **Supply system threats – power outages, communications interruptions, interruption of natural resources such as water, steam, and gas**
- **Manmade threats – unauthorized access (internal or external), explosions, damage by employees, employee errors and accidents, vadalism, fraud, and theft**
- **Politically motivated threats – strikes, riots, civil disobedience, terrorist attacks, and bombings**

Introduction to Physical Security

- **Key Note: Nothing should ever impede life safety goals (protecting human life)**
- **Book example: Barring a door to prevent unauthorized physical intrusion might prevent individuals from being able to escape in the event of a fire**

Introduction to Physical Security

The Planning Process

- Designers work with management to define objectives, design needs, and performance-based metrics
- Objectives depend on the level of protection required for the various assets and the organization
- Level of protection depends on the organization's acceptable risk level
- The acceptable risk level should be based on applicable laws and regulations, as well as the threat profile of the organization

The Planning Process

- **Highlighted Note: Remember that a vulnerability is a weakness and a threat is the potential that someone will identify this weakness and use it against you. The threat agent is the person or mechanism that actually exploits this identified vulnerability**

The Planning Process

- Threats are grouped into two types: internal and external
- Internal threats – misbehaving devices, fire hazards, employees who aim to damage the company
- External threats – political adversaries, organized crime, competitors, protesters, hackers
- Definition: Collusion – two or more people work together to carry out fraudulent activity

The Planning Process

An organization's physical security program should address the following goals:

- Crime and disruption prevention through deterrence – fences, security guards, warning signs
- Reduction of damage through the use of delaying mechanisms – locks, security personnel, barriers
- Crime or disruption detection – smoke detectors, motion detectors, CCTV
- Incident assessment – A plan to be used by security guards to determine proper response to detected incidents and determination of damage level
- Response procedures – Fire suppression mechanisms, emergency response processes, law enforcement notification, and consultation with outside (third party) security professionals

The Planning Process

Steps to establish an effective physical security program:

- **Identify a team to build the program**
- **Carry out a risk analysis**
- **Define an acceptable level of risk**
- **Derive required performance baselines from acceptable risk level**
- **Create countermeasure performance metrics**

The Planning Process

Steps (cont'd)

- Develop criteria for required protection and performance for:
  - Deterrence
  - Delaying
  - Detection
  - Assessment
  - Response
- Identify and implement countermeasures for each category
- Continuously evaluate success of countermeasures

The Planning Process

- **Crime Prevention Through Environmental Design (CPTED) – a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior**
- **Target Hardening – Denying access through physical and artificial barriers (alarms, locks, fences)**

The Planning Process

CPTED has three constituent strategies:

- **Natural Access Control**
- **Natural Surveillance**
- **Natural Territorial Reinforcement**

These are described in the next few slides

The Planning Process

- **Natural access control – the guidance of people entering and leaving a space by the placement of doors, fences, and landscaping**

- **Highlighted definition: Bollards – short posts commonly used to prevent vehicular access and to protect a building or people walking on a sidewalk from vehicles. They can also be used to direct foot traffic**

The Planning Process

- **Natural Surveillance – the use and placement of physical environmental features, personnel walkways, and activity areas in ways that maximize visibility**
- **The goal of natural surveillance is to make criminals feel uncomfortable by providing many ways observers could potentially see them and to make all other people feel safe and comfortable by providing an open and well-designed environment**

The Planning Process

- **Natural Territorial Reinforcement – physical designs that emphasize or extend the company's physical sphere of influence so legitimate users feel a sense of ownership of that space**
- **The goal of territorial reinforcement is to create a sense of a dedicated community. Companies implement these elements so employees feel proud of their environment and have a sense of belonging, which they will defend if required**

The Planning Process

If evaluating the protection level of an existing facility, consider the following:

- **HVAC systems**
- **Construction materials of walls and ceilings**
- **Power distribution systems**
- **Communication paths and types (copper, telephone, fiber)**
- **Surrounding hazardous materials**

The Planning Process

Security considerations – External Components

- **Topography**
- **Proximity to airports, highways, and railroads**
- **Potential electromagnetic interference from surrounding devices**
- **Climate**
- **Soil**
- **Existing fences, detection sensors, cameras, barriers**
- **Working hours of employees**
- **Operational activities that depend upon physical resources**
- **Vehicle activity**
- **Neighbors**

The Planning Process

- **Highlighted Topic**

Activity Support

CPTED also encourages activity support, which is planned activities for the areas to be protected. These activities are designed to get people to work together to increase the overall awareness of acceptable and unacceptable activities in the area. The activities could be neighborhood watch groups, company barbeques, block parties, or civic meetings. This strategy is sometimes the reason for particular placement of basketball courts, soccer fields, of baseball fields in open parks. The increased activity will hopefully keep the bad guys from milling around doing things the community does not welcome.

The Planning Process

Issues to consider when selecting a facility site:

- **Visibility**
  - Surrounding terrain
  - Building markings and signs
  - Types of neighbors
  - Population of the area
- **Surrounding area and external entities**
  - Crime rate, riots, terrorism attacks
  - Proximity to police, medical, and fire stations
  - Possible hazards from surrounding area
- **Accessibility**
  - Road access
  - Traffic
  - Proximity to airports, train stations, and highways
- **Natural disasters**
  - Likelihood of floods, tornadoes, earthquakes, or hurricanes
  - Hazardous terrain, such as mudslides, falling rock from mountains, or excessive snow or rain

The Planning Process

Considerations with regard to physical security

- **Walls**
  - **Combustibility of material (wood, steel, concrete)**
  - **Fire rating**
  - **Reinforced materials**

Building materials:

- **Light frame construction material**
- **Heavy timber construction material**
- **Incombustible material (such as steel)**
- **Fire-resistant material (rebar in concrete)**

Rebar are metal rods encased in concrete

The Planning Process

Considerations (cont'd)

- **Doors**
  - Combustibility (wood, pressed wood, aluminum)
  - Fire rating
  - Resistance to forcible entry
  - Emergency marking
  - Placement
  - Locked or controlled entrances
  - Alarms
  - Secure Hinges
  - Directional Opening
  - Electric door locks that revert to unlocked in power outage
  - Type of glass (shatterproof or bulletproof glass requirements)

The Planning Process

Different door types:

- **Vault doors**
- **Personnel doors**
- **Industrial doors**
- **Vehicle access doors**
- **Bullet-resistant doors**

Doors may also be hollow-core or solid core, and their automatic locks may be fail-safe or fail-secure. Fail-safe defaults to unlocked when power is lost, whereas fail-secure defaults to locked.

The Planning Process

Considerations (cont'd)

- **Ceilings**
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
  - Weight-bearing rating
  - Drop-ceiling considerations

Drop ceilings may be used as a point-of-entry to a secured area by intruders

The Planning Process

Considerations (cont'd)

- Windows
  - Translucent or opaque requirements
  - Shatterproof
  - Alarms
  - Placement
  - Accessibility to intruders

The Planning Process

Types of window glass:

- **Standard – no extra protection**
- **Tempered – heated then cooled suddenly to increase integrity and strength**
- **Acrylic – Plastic rather than glass. Polycarbonate acrylics are stronger than normal acrylics**
- **Wired – Mesh of wire embedded between two sheets of glass. Prevents the glass from shattering**
- **Laminated – Plastic layer between two sheets of glass. Increases strength against breakage**
- **Solar window film – Provides extra security by being tinted and extra strength due to the film's material**
- **Security film – Transparent film applied to glass to improve its strength**

The Planning Process

Considerations (cont'd)

- **Flooring**
  - Weight-bearing rating
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
  - Raised flooring (electrical grounding)
  - Nonconducting surface and material

The Planning Process

Considerations (cont'd)

- **Heating, ventilation, and air conditioning**
  - **Positive air pressure**
  - **Protected intake vents**
  - **Dedicated power lines**
  - **Emergency shutoff valves and switches**
  - **Placement**

Ventilation ducts and utility tunnels can be used by intruders and thus must be properly protected with sensors and access control mechanisms

The Planning Process

Considerations (cont'd)

- **Electrical power supplies**
  - Backup and alternate power supplies
  - Clean and steady power source
  - Dedicated feeders to required areas
  - Placement and access to distribution panels and circuit breakers

Note: Many buildings are not wired properly and have the ground connecter connected to nothing. In such a situation, extra current has nowhere to escape except into equipment or personnel

The Planning Process

Considerations (cont'd)

- **Water and gas lines**
  - Shutoff valves (labeled and brightly painted)
  - Positive flow (material flows out of the building, not in)
  - Placement (proper location and labels)
- **Fire detection and suppression**
  - Placement of sensors and detectors
  - Placement of suppression systems
  - Types of detectors and suppression agents

The Planning Process

- Mantraps and turnstiles can be used so unauthorized individuals entering a facility cannot get in or out if it is activated
- If there is water damage in a data center or facility, mold and mildew could easily become a problem. Instead of allowing things to "dry out on their own," many times it is better to use industry-strength dehumidifiers, water removers, and sanitizers to ensure secondary damage does not occur.
- Also, water detectors should be placed on dropped ceilings and under raised floors

Protecting Assets

Laptop protection mechanisms:

- **Inventory all laptops and their serial numbers**
- **Harden the operating system**
- **Password protect the BIOS**
- **Register all laptops with the vendor and file a report if one is stolen**
- **Do not check a laptop as luggage when flying**
- **Never leave a laptop unattended, and carry it in a nondescript carrying case**
- **Engrave the laptop for proper identification**
- **Use a slot lock with a cable to connect the laptop to a stationary object**
- **Back up the data to a PC or backup media**
- **Use specialized safes if storing laptops in vehicles**
- **Encrypt all sensitive data**

Protecting Assets

Types of organizational safes:

- **Wall safe - embedded in the wall and easily hidden**
- **Floor safe – embedded in the floor and easily hidden**
- **Chest – stand-alone safes**
- **Depository – Safes with slots which allow valuables to easily be slipped in**
- **Vault – Safe large enough to provide walk-in access**

Protecting Assets

- If a combination lock is used on a safe (or for any other type of security) then the combinations should be changed periodically
- Some safes have passive or thermal relocking functionality.
  - Passive relocking causes extra internal bolts to fall into place if someone attempts to tamper with it.
  - Thermal relocking engages an extra lock if a specified temperature is reached.

Protecting Assets

Internal Support Systems

- **Online UPS systems use AC line voltage to charge a bank of batteries.**
  - **When in use, the UPS has an inverter that changes the DC output into AC and regulates the voltage**
- **Standby UPS devices stay inactive until a power line fails**
- **Backup power supplies are used when a power outage lasts longer than a UPS can.**
  - **This includes redundant lines from another electrical substation and generators**

Internal Support Systems

- Clean power contains no interference or voltage fluctuation
- Possible types of interference (or line noise) are electromagnetic interference (EMI) or radio frequency interference (RFI)
- EMI is often caused from wire emissions, motors, and lighting
- RFI is most commonly caused by fluorescent lighting

Internal Support Systems

Power fluctuation terms

- **Power excess**
  - **Spike: momentary high voltage**
  - **Surge: prolonged high voltage**
- **Power loss**
  - **Fault: momentary power outage**
  - **Blackout: prolonged, complete loss of electrical power**
- **Power Degradation**
  - **Sag/Dip: Momentary low voltage condition**
  - **Brownout: Prolonged power supply below normal**
- **In-rush current: initial surge of current required to start a load**

Internal Support Systems

Electrical power definitions

- **Ground – the pathway to earth to enable voltage to dissipate**
- **Noise – electromagnetic or frequency interference that disrupts the power flow**
  - **Voltage regulators and line conditioners can be used to ensure a clean and smooth distribution of power**
- **Transient noise – a short duration of power line disruption**
- **Clean power – electrical current that does not fluctuate**
- **EMI – electromagnetic interference**
- **RFI – radio frequency interference**

Internal Support Systems

Preventative measures and good practices

- **Plug every device into a surge protector**
- **Shut down devices in an orderly manner**
- **Use power line monitors**
- **Use voltage regulators**
- **Protect distribution panels, master circuit breakers, and transformer cables with access controls**
- **Use shielded lines**
- **Use shielded cabling for long cable runs**
- **Do not run data or power lines directly over fluorescent lights**
- **Use three-prong adapters**
- **Do not plug outlet strips and extension cords into each other**

Internal Support Systems

Environmental concerns

- **Water, steam, and gas lines should have emergency shutoff valves and positive drains**
- **Highlighted note:**
  - **The climate issues involved with data processing environments are why it needs its own separate HVAC system.**
  - **Maintenance procedures should be documented and properly followed. HVAC activities should be recorded and reviewed annually**

Internal Support Systems

Environmental concerns (cont'd)

- Highlighted note: Humidity should be kept between 40% and 60% and the temperature should be between 70F and 74F
- Preventative steps against static electricity
  - Use antistatic flooring in data processing areas
  - Ensure proper humidity
  - Have proper grounding for wiring and outlets
  - Don't have carpeting in data centers, or use static-free carpets if necessary
  - Wear anti-static bands when working inside computer systems

Internal Support Systems

Ventilation concerns

- Use a closed-loop air conditioning system
  - Closed-loop means the air is reused after it has been properly filtered
- Implement positive pressurization
  - Positive pressurization means the air flows out of the room when the door is opened, not into the room

Fire prevention

- Employee education
- Proper storage of combustible materials
- Non-combustible building materials
- Fire containment measures

Internal Support Systems

Internal Support Systems

Fire Detection

- Manual – Red pull boxes
- Automatic – Sensor based
  - Smoke Activated
    - Early warning system
    - Uses a photoelectric device / optical detector to detect variations in light intensity
  - Heat Activated
    - Fixed temperature – alarm sounds when pre-defined temperature is reached
    - Rate-of-Rise – alarm sounds when the temperature increases over a period of time

Internal Support Systems

Fire Detection (cont'd)

- Automatic dial-up alarms – systems can be configured to call the local fire station and police station
- Detectors should be placed in enclosures, air ducts, and plenum areas
- Plenum Area – an area through which cables are strung, such as above dropped ceilings, inside wall cavities, and under raised floors.
  - Also, only plenum-rated cabling (does not let off hazardous gases if burning) should be used in plenum areas.

Internal Support Systems

Fire Suppression

Class	Type	Elements	Suppression Method
A	Common Combustibles	Wood, paper, laminates	Water, foam
B	Liquid	Petroleum products and coolants	Gas, CO_2, foam, dry powders
C	Electrical	Electrical equipment and wires	Gas, CO_2, dry powders
D	Combustible Metals	Magnesium, sodium, potassium	Dry powder

Internal Support Systems

Fire Suppression (cont'd)

- **Highlighted note:** There is actually a class K fire, for commercial kitchens.
  - These fires should only be put out with a wet chemical, which is usually a solution of potassium acetate. This chemical works best when putting out cooking oil fires
- **Highlighted note:** Halon has not been manufactured since January 1, 1992, by international agreement.
  - The Montreal Protocol banned halon in 1987, and countries were given until 1992 to comply with these directives.
  - The most effective replacement is FM-200, which is similar to halon but does not damage the ozone

Internal Support Systems

Fire Suppression (cont'd)

- Halon was widely used because it interfered with chemical combustion, but did not harm computers and electronics
- EPA-approved replacements:
  - FM-200
  - NAF-S-III
  - CEA-410
  - FE-13
  - Inergen
  - Argon
  - Argonite

Internal Support Systems

Fire Suppression (cont'd)

Combustion Elements	Suppression Methods	How Suppression Works
Fuel	Soda acid	Removes fuel
Oxygen	Carbon dioxide	Removes oxygen
Temperature	Water	Reduces temperature
Chemical Combustion	Gas – Halon or halon substitute	Interferes with the chemical reactions between elements

Internal Support Systems

Fire Suppression (cont'd)

- **Water Sprinklers**
  - Wet pipe: water kept in pipes and discharged by temperature control sensors. Also called closed-head systems
  - Dry pipe: water kept in a holding tank, pipes filled with pressurized air. Activated by heat or smoke detectors. Used in cold climates so pipes don't freeze
  - Preaction: Water held in holding tank, but when released a thermal-fusible link must break before the water is released.
  - Deluge: Sprinkler heads are kept wide open to allow larger volume of water in a shorter period

Perimeter Security

- **Highlighted note: It is also important to have a diversity of controls. For example, if one key works on four different door locks, the intruder has to obtain only one key. Each entry should have its own individual key or authentication combination.**

Perimeter Security

Locks

- Considered delaying devices
- Mechanical locks
  - Warded Locks: the basic padlock
  - Spring-loaded bolt with notches cut in it
  - Tumbler locks
    - Pin tumbler lock
    - Wafer tumbler lock
    - Lever tumbler lock

Perimeter Security

Locks (cont'd)

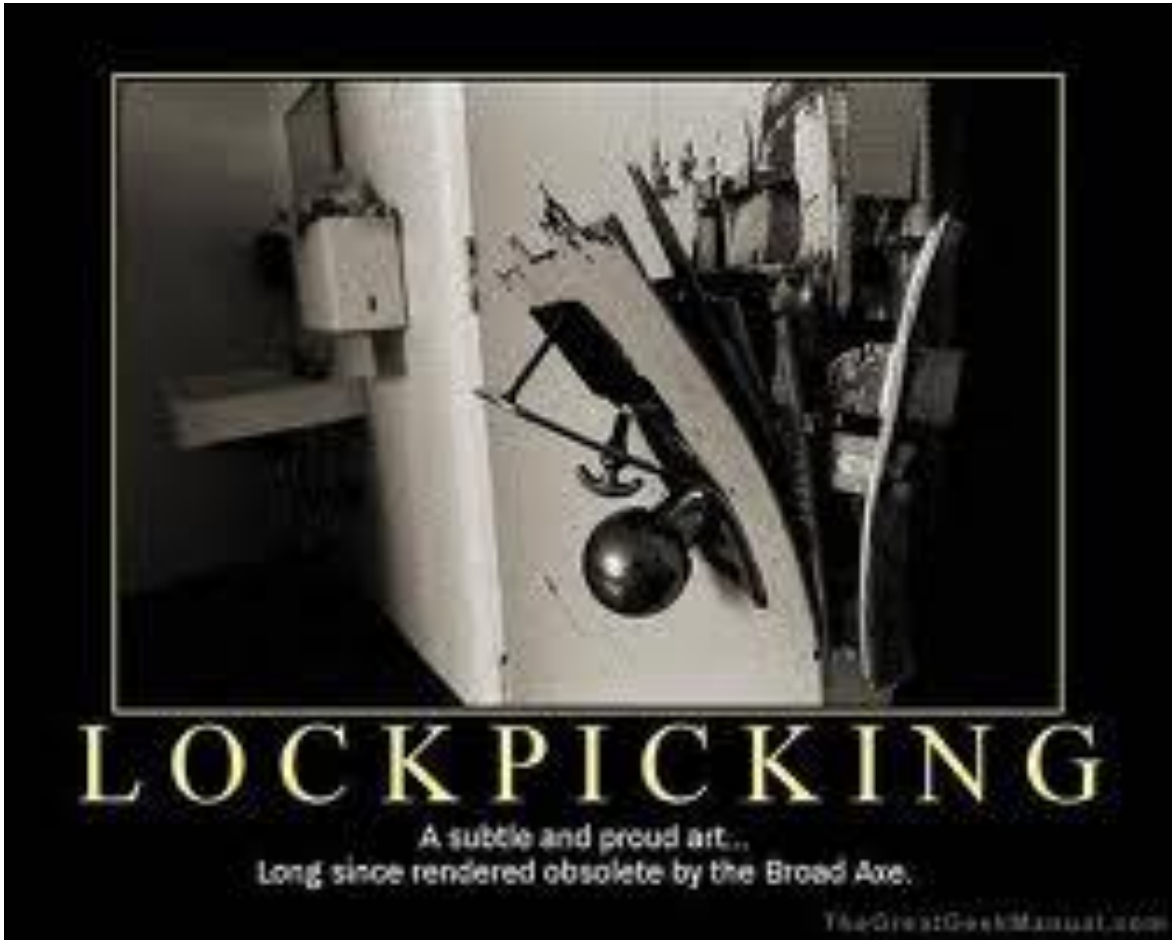
- **Pin tumbler lock**
  - **Most common tumbler lock**
  - **Requires the key to have just the right grooves to put all the spring-loaded pins in the right position**
- **Wafer tumbler lock**
  - **Also called disc tumbler locks**
  - **Use flat discs instead of pins**
  - **Easily Circumvented**

Perimeter Security

Locks (cont' d)

- **Highlighted note: The delay time provided by the lock should match the penetration resistance of the surrounding components (door, door frame, hinges). A smart thief takes the path of least resistance, which may be to pick the lock, remove the pins from the hinges, or just kick down the door**

Perimeter Security



Perimeter Security

Locks (cont'd)

- **Highlighted note: Some locks have interchangeable cores, which allow for the core of the lock to be taken out. You would use this type of lock if you wanted one key to open several locks. You would just replace all the locks with the same core**

Perimeter Security

Locks (cont'd)

- **Combination locks**
  - Require the proper combination
  - Use internal wheels that must line up
  - Electronic combination locks have a key pad to type in the combination instead of wheels
- **Cipher locks**
  - Also called programmable locks
  - Requires combination by key pad, and sometimes a swipe card as well

Perimeter Security

Locks (cont'd)

- **Functions of cipher locks**
  - **Door delay: after door is open for so long, an alarm triggers**
  - **Key override: a specific combination can be used to override normal procedures or for supervisory override**
  - **Master keying: enables supervisory personnel to change access codes and lock features**
  - **Hostage alarm: a specific combination can be used to open the door and simultaneously transmit a duress message to guards and/or police station**

Perimeter Security

Locks (cont'd)

- **Highlighted note: It is important to change the combination of locks and to use random combination sequences.**
  - **Often, people do not change their combinations or clean the keypads, which allows an intruder to know what key values are used in the combination, because they are the dirty and worn keys.**
  - **The intruder then just needs to figure out the right combination of these values.**

Perimeter Security

Locks (cont'd)

- Cipher locks that can assign specific codes to unique individuals are sometimes called smart locks
- Highlighted note: Hotel key cards are also known as smart cards. They are programmed by the nice hotel guy or gal behind the counter. The access code on the card can allow access to a hotel room, workout area, business area, and yes – the mini bar

Perimeter Security

Locks (cont'd)

- **Device locks**
  - Cable locks: a vinyl-coated steel cable to connect a device to a stationary object
  - Switch controls: a cover for power switches
  - Slot locks: similar to cable locks mounted to a bracket mounted in a spare expansion slot
  - Port controls: block access to disk drives or unused connection ports
  - Peripheral switch controls: secures a keyboard by placing a power switch between the system and the keyboard port
  - Cable traps: prevents the removal of I/O devices by passing their cables through a lockable unit

Perimeter Security

Locks (cont'd)

- **Lock strengths**
  - Grade 1: Commercial and industrial use
  - Grade 2: Heavy-duty residential/light-duty commercial
  - Grade 3: Residential/consumer expendable
- **Lock cylinder categories**
  - Low security: No pick or drill resistance
  - Medium security: uses tighter and more complex keyways (notch combinations)
  - High security: Pick resistance protection through many different mechanisms (grade 1 & 2 locks only)

Perimeter Security

Locks (cont'd)

- Circumventing locks
  - Lock picks / tension wrenches
  - Raking: push lock pick is pushed to the back of a tumbler pin lock and quickly slid out with upward pressure and tension wrench is used to hold set pins in place
  - Lock bumping: a special bump key is used to force the pins of a tumbler pin lock to the open position

Perimeter Security

Perimeter Security

Personnel Access Controls

- Identification and authentication can be verified by anatomical attribute (biometric), smart or memory card (swipe card), presenting photo ID, using a key, or providing a card and entering a password or PIN
- Piggybacking: an individual gains unauthorized access by using someone else's legitimate credentials (often by following closely through a door)

Perimeter Security

Personnel Access Controls (cont'd)

- **Highlighted note: Electronic access control (EAC) tokens is a generic term used to describe proximity authentication devices, such as proximity readers/transponders, programmable locks, or biometric systems, which identify and authenticate users before allowing them entrance into physically controlled areas**

Perimeter Security

External Boundary Protection Mechanisms

- **Control pedestrian and vehicle traffic flow**
- **Various levels of protection for different security zones**
- **Buffers and delaying mechanisms to protect against forced entry attempts**
- **Limit and control entry points**

Perimeter Security

Perimeter Security

External Boundary Protection Mechanisms (cont'd)

- Services provided by the following control types:
  - Access control mechanisms: locks, electronic card access, personnel awareness
  - Physical barriers: fences, gates, walls, doors, windows, protected vents, vehicular barriers
  - Intrusion detection: perimeter sensors, interior sensors, annunciation mechanisms
  - Assessment: guards, CCTV cameras
  - Response: guards, local law enforcement
  - Deterrents: signs, lighting, environmental design

Perimeter Security

Fences

- **Fence heights**
  - **3-4’ high deter only casual trespassers**
  - **6-7’ high are considered too high to climb easily**
  - **8’ and higher (perhaps with barbed or razor wire) deter more determined intruders**
- **Posts should be buried sufficiently deep and secured with concrete**

Perimeter Security

Fences (cont'd)

- Gauge sizes
  - 11 gauge: 0.0907" diameter
  - 9 gauge: 0.1144" diameter
  - 6 gauge: 0.162" diameter
- Common mesh sizes
  - 2"
  - 1"
  - 3/8"

Perimeter Security

Fences (cont'd)

- **Common fence configurations**
  - **Extremely high security: 3/8" mesh, 11 gauge**
  - **Very high security: 1" mesh, 9 gauge**
  - **High security: 1" mesh, 11 gauge**
  - **Greater security: 2" mesh, 6 gauge**
  - **Normal industrial security: 2" mesh, 9 gauge**

Perimeter Security

Fences (cont'd)

- **Perimeter Intrusion Detection and Assessment System (PIDAS) is a type of fencing that has sensors located on the wire mesh and at the base of the fence.**
  - **It is used to detect if someone attempts to cut or climb the fence.**
  - **It has a passive cable vibration sensor that sets off an alarm if an intrusion is detected.**
  - **PIDAS is very sensitive and can cause many false alarms**

Perimeter Security

Fences (cont'd)

- Gates come in four distinct classifications
  - Class I: Residential
  - Class II: Commercial where general public access is expected
  - Class III: Industrial where limited access is expected
  - Class IV: Restricted access
- Highlighted note: UL standards can be found at www.ul.com. A good introduction to the UL-325 standard, which deals with gates, can be found at www.abrpaint.com/services/GatesFencing/ul325intro.htm

Perimeter Security

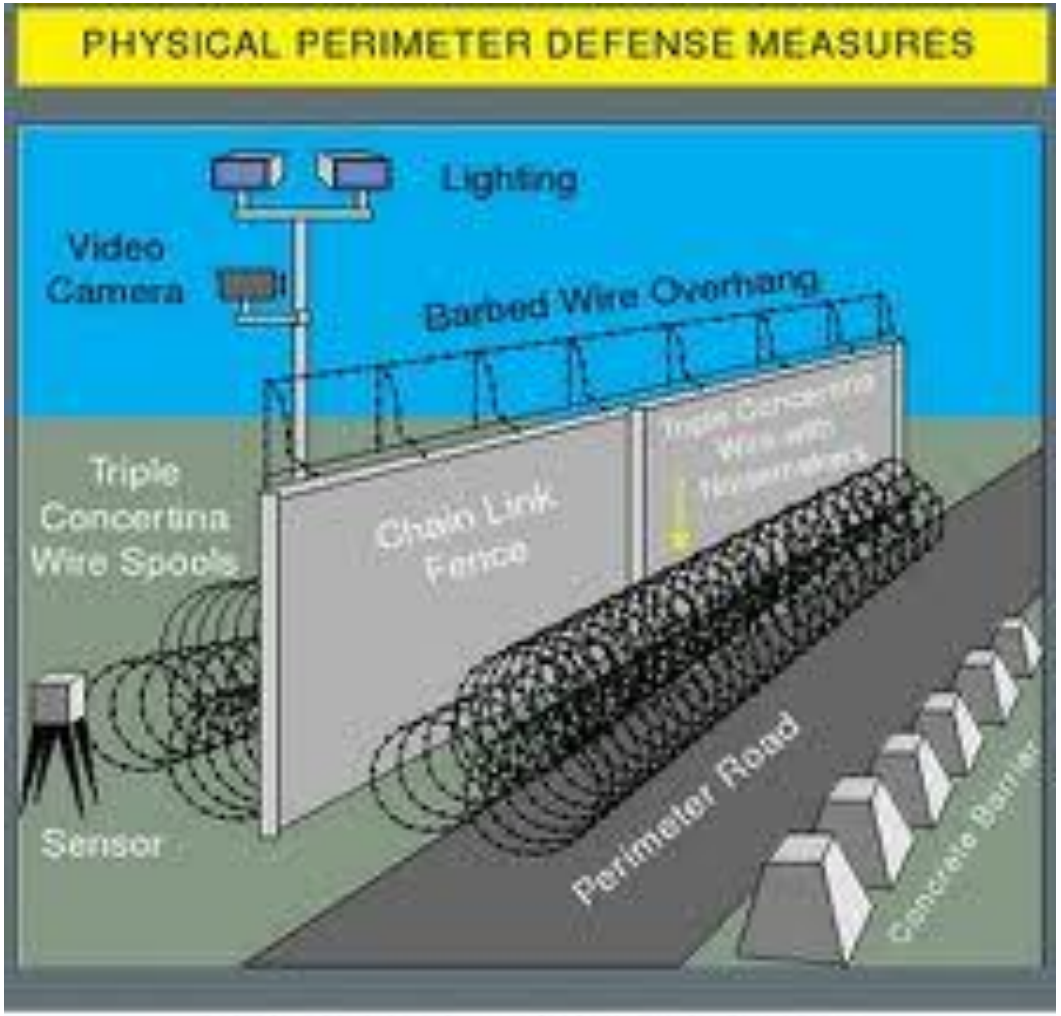


Figure IV-7. Physical Perimeter Defense Measures

Perimeter Security

- **Bollards – discussed earlier**
- **Lighting**
  - **Should overlap**
  - **Glare protection: security lights should point away from security guard posts and toward gates or exterior access points**
  - **Continuous lighting: array of lights that provides even illumination across an area**
  - **Standby lighting: configurable to turn on and off at predetermined times**
  - **Responsive area illumination: IDS detects suspicious activity and turns on the lights in a specific area**

Perimeter Security

- **Lighting (cont'd)**
  - **Highlighted note: Critical areas need to have illumination that reaches at least eight feet with the illumination of two foot-candles**
  - **Highlighted note: Redundant or backup lights should be available in case of power failures or emergencies. Special care must be given to understand what type of lighting is needed in different parts of the facility in these types of situations. This lighting may run on generators or battery packs**

Perimeter Security

- **Closed-circuit television (CCTV)**
  - **The purpose of CCTV is to detect, assess, and/or identify intruders**
  - **Made up of cameras, transmitters, receivers, a recording system, and a monitor**
  - **Most modern CCTV cameras use light-sensitive chips called charged coupled devices (CCDs) in the lens which converts the light received into an electrical signal**
  - **Two types of lenses: fixed focal length and zoom (varifocal)**

Perimeter Security

CCTV (cont'd)

- **Highlighted note: CCTVs should have some type of recording system. Digital recorders save images to hard drives and allow advanced search techniques that are not possible with videotape recorders. Digital recorders use advanced compression techniques, which drastically reduce the storage media requirements**

Perimeter Security

CCTV (cont'd)

- **Highlighted note: Fixed focal length lenses are available in various fields of view – wide, medium, and narrow. A lens that provides a "normal" focal length creates a picture that approximates the field of view of the human eye. A wide-angle lens has a short focal length, and a telephoto lens has a long focal length. When a company selects a fixed focal length lens for a particular view of an environment, it should understand that if the field of view needs to be changed (wide to narrow), the lens must be changed.**

Perimeter Security

CCTV definitions

- Focal length: effectiveness in viewing objects from a horizontal and vertical view
- Zoom lens: allow the viewer to change the field of view
- Depth of field: portion of the environment that is in focus
- Manual iris lens: a lens with a ring around the lens that can be manually turned and controlled
- Automatic iris lens: a lens that senses brightness and adjusts itself accordingly
- Fixed mounting: camera cannot move in response to security personnel commands
- PTZ capabilities: ability for a camera to pan, tilt, and zoom

Perimeter Security

- **Intrusion detection systems**
  - **Electromechanical or volumetric**
  - **Volumetric IDSs are more sensitive**
  - **IDSs can detect changes in:**
    - **Beams of light**
    - **Sounds and vibrations**
    - **Motion**
    - **Different types of fields (microwave, ultrasonic, electrostatic)**
    - **Electrical circuits**

Perimeter Security

IDSs (cont'd)

- **Electromechanical systems work by detecting a change or break in a circuit**
  - **Strips of foil embedded or connected to windows**
  - **Vibration detectors**
  - **Magnetic contact switches**
  - **Pressure pads**

Perimeter Security

IDSs (cont'd)

- **Volumetric systems**
  - **Photoelectric or photometric: detects changes in a beam of light**
  - **Passive infrared (PIR): identifies changes in heat waves**
  - **Acoustical detection: detects sounds with very sensitive microphones (Vibration sensors??)**
  - **Wave-pattern motion detectors: monitors a microwave, ultrasonic, or low frequency wave**
  - **Proximity detector or capacitance detector: detects changes in an emitted magnetic field caused by static electricity of subatomic particles**

Perimeter Security

IDSs (cont'd)

- **Characteristics**
  - **Expensive and require human intervention to respond to alarms**
  - **A redundant power supply and emergency backup power are necessary**
  - **Can be linked to a centralized security system**
  - **Should have a fail-safe configuration that defaults to "activated"**
  - **Should detect and be resistant to tampering**

Perimeter Security

Other security measures

- **Bollards**
- **Patrol force and security guards**
- **Dogs**
- **Audits of physical access**
- **Testing and drills**

Summary

- Introduction to Physical Security
- The Planning Process
- Protecting Assets
- Internal Support Systems
- Perimeter Security

Personnel safety concerns

Personnel Safety

- **The number one concern in any disaster response operation**
  - **Emergency evacuation**
  - **Accounting for all personnel**
  - **Administering first-aid**
  - **Emergency supplies**
    - **Water, food, blankets, shelters**
    - **On-site employees could be stranded for several days**

Public Utilities and Infrastructure

- **Often interrupted during a disaster**
  - **Electricity: UPS (Uninterruptible Power Supply), generator**
  - **Water: building could be closed if no water is available for fire suppression**
  - **Natural gas: heating**
  - **Wastewater: if disabled, building could be closed**
  - **Steam heat**

Logistics and Supplies

- Food and drinking water
- Blankets and sleeping cots
- Sanitation (toilets, showers, etc.)
- Tools
- Spare parts
- Waste bins
- Information
- Communications
- Fire protection (extinguishers, sprinklers, smoke alarms, fire alarms)

Summary

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns