INFO 6010 Lesson 11

Security Operations Part 2

Domain 7 &

Architecture & Engineering Part 3

Domain 3

Site (Physical) Security

Revision 2

Information Security Management & Network Security Architecture

FANSHAWE

Security Operations – Domain 7

- Disaster recovery
- Liability
- Personal safety concerns

Architecture & Engineering Part 3 - Domain 5

- Site and facility design considerations
- Physical security risks, threats, and countermeasures
- Electric power issues and countermeasures
- Fire prevention, detection, and suppression

Disaster Recovery

- Disaster Recovery:
  - Minimizes the effects of a disaster
  - Take steps to ensure business processes are able to resume operation in a timely manner
- Disaster Recovery Plan
  - How to handle problems right after they occur
  - Short term goal to get systems back online
  - Usually IT focused

Disaster Recovery

- Unforeseen events happen
  - Terrorist attacks,
  - Extreme weather events
- Both destroyed many business
- Some events can be predicted
  - Equipment failure
  - Hard drive
  - Equipment eventually wears out from overuse
- Plans can be put in place to reduce impact on business when failures occur
  - Reduce the financial loss
  - Quick recovery from failure by roll over to a redundant system
  - No single point of failure
- Companies that survive major disasters had plans in place to restart business operations.

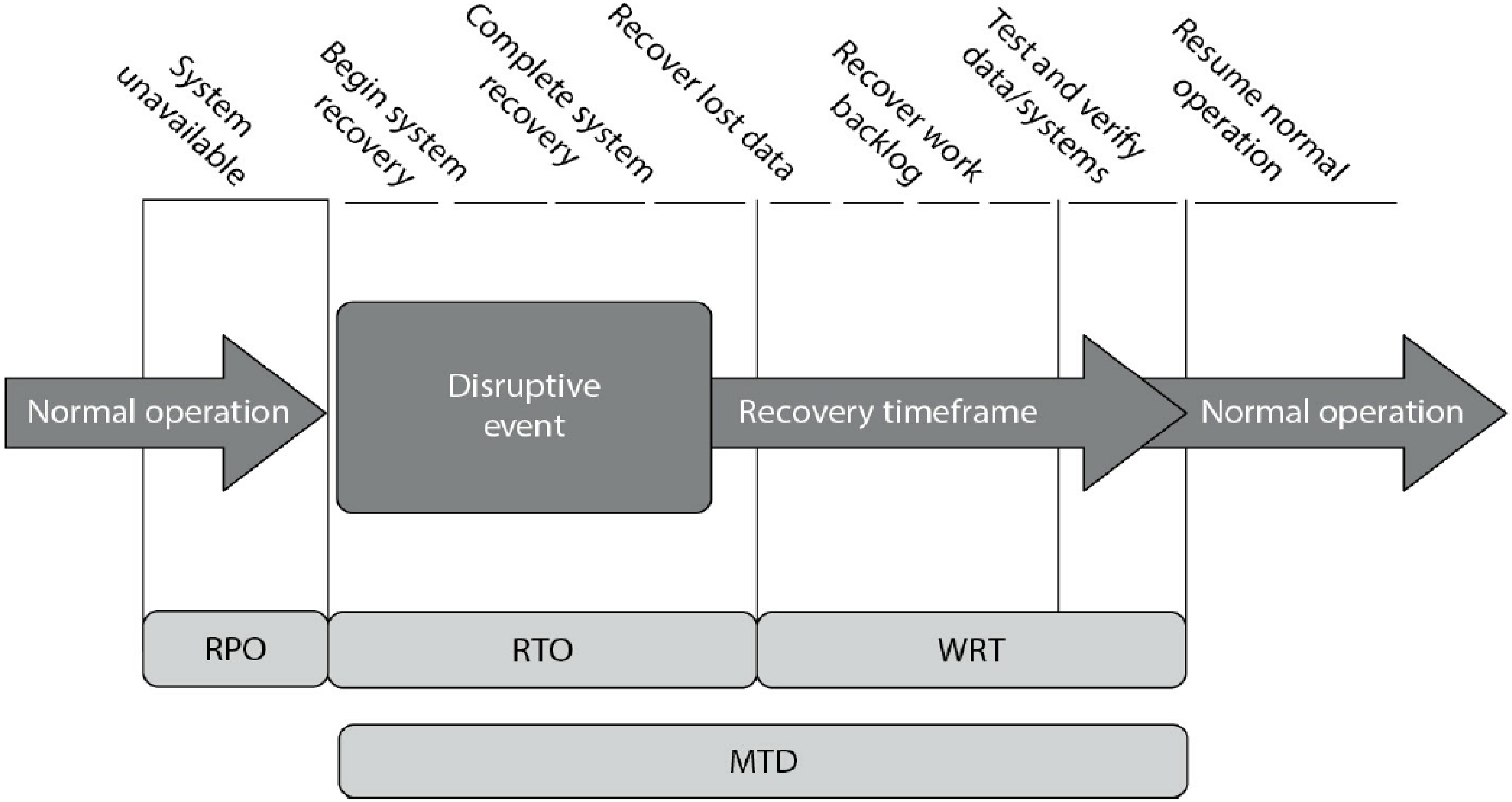
Disaster Recovery

- Identify required resources for critical business processes to take place
  - Personnel, procedures, tasks, computers, suppliers, vendor support
- Estimate maximum ‘outage’ for any of these critical systems before severe company impact
  - This is referred to as *Maximum Tolerable Downtime (MTD)*
- The *recovery time objective (RTO)* is the maximum time period within which a business process must be restored to a designated service level after a disaster to avoid unacceptable consequences.

Disaster Recovery

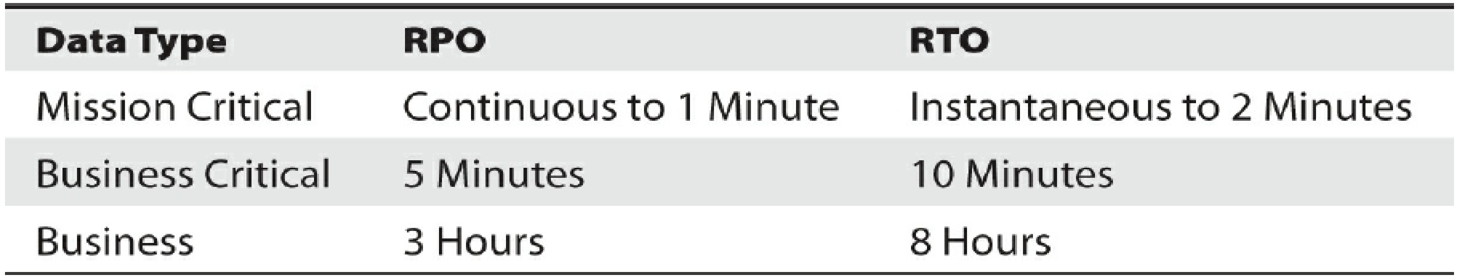
- The *work recovery time (WRT)* is the remainder of the overall MTD value after the RTO has passed. RTO deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything “live” for production purposes.
- The *recovery point objective (RPO)* is the acceptable amount of data loss measured in time. This value represents the earliest point in time at which data must be recovered.

Disaster Recovery Metrics



Disaster Recovery

- Example (MTD) Values
  - Nonessential: 30 days
  - Normal: 7 days
  - Important: 72 hours
  - Urgent: 24 hours
  - Critical: Minutes to hours
- Each asset, process, transaction or service should be placed in one of these categories



Data Type	RPO	RTO
Mission Critical	Continuous to 1 Minute	Instantaneous to 2 Minutes
Business Critical	5 Minutes	10 Minutes
Business	3 Hours	8 Hours

RPO and RTO Value Relationship

Business Process Recovery

Recovery Measures

- Definition: Set of interrelated steps linked through specific decision activities to accomplish a specific task.
- Preventative measures
  - Reduce the possibility of disaster
- Recovery measures
  - Predefined activities to rescue company from disaster

Recovery Site Strategies

- 3 Types of disruptions: Non-disasters, disasters and catastrophes
- Non-disasters
  - Disruption due to device malfunction or failure
  - Solution may include hardware or software replacement
  - File restoration
- Disasters
  - Event where entire facility is unusable for a day or longer
  - Usually requires the use of alternate facility and restoration of data from off site copies
  - Alternate site must be available to company until primary site is repaired

Recovery Site Strategies

- Catastrophes
  - Major event that destroys the primary facility
  - Would require short term solution
    - Carry on business operations from alternate site
  - Would require a long term solution
    - Rebuilding of primary facility

Recovery Site Strategies

- 3 types of alternate sites
  - hot site, warm site and cold site
- **Hot Site**
  - Fully configured, ready to operate within a few hours
  - Up and running once people and data from backup are transferred
  - Most expensive of three, best choice for company which must be operational within hours
  - Must be tested annually

Recovery Site Strategies

- **Warm Site**
  - Partially configured with some equipment, but missing computers
  - Preferred choice for companies which operate unique or proprietary equipment that they must transfer to the backup site
  - Annual testing not possible (no equipment)
- **Cold Site**
  - Has basic environment (electrical, plumbing, air, flooring)
  - No required equipment, site may require weeks before its operational
  - Least expensive site of three types but requires the most time and effort to activate

Recovery Site Strategies

- **Hot Site advantage**
  - Ready within hours
  - High availability
  - Usually used for short term solutions
  - Annual testing available
- **Hot Site disadvantage**
  - Very expensive
  - Limited hardware and software available if company has unique equipment or proprietary systems

Recovery Site Strategies

- **Warm & Cold Site advantage**
  - Less expensive
  - Available for long term engagement because of reduced costs
  - Practical for proprietary hardware or software use
- **Warm & Cold Site disadvantage**
  - Not immediately available
  - Operational testing not usually available
  - Resources for operations not immediately available
- **Rolling Hot Site**
  - Mobile redundant mirror site
  - Usually a truck and trailer filled with expensive equipment ready to go
  - Site can be trucked anywhere and operated from a parking lot

Recovery Site Strategies

- **Redundant Site**
  - A secondary site equipped identically to primary site
  - Sites are exact mirrors of each other
  - Data is mirrored to redundant site
  - Redundant site ready for immediate use should primary site fail
    - No configuration required
    - Most expensive
    - Duplicating all resources, hardware, physical facility equipment and environmental

Alternate Facility Location

- Minimum 5 miles distance
- 15 miles recommended for low to medium
- 50-200 miles for critical operations
- Distance depends on threat
  - Tornado, hurricane, flood, war
- Renting another floor on same building not logical if threat is fire or tornado

Recovery Site Strategies

- **Reciprocal Agreements**
- A *reciprocal agreement* with another company, usually one in a similar field or that has similar technological infrastructure. This means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa.
- This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability.
- There is the potential to introduce all sorts of security issues.

Supply & Technology Recovery

- After identifying critical business processes and backup facility more detailed backup solution required
  - Network and computer equipment
  - Voice and data communications
  - Human resources
  - Transportation of equipment and personnel
  - Environment issues (HVAC)
  - Data and personnel security
  - Supplies such as forms, cabling, paper
  - Documentation

Supply & Technology Recovery

- Financial sector banks, and credit unions utilize specialized software developed by a few unique vendors
- Software is further customized with specific needs for each financial institution
- Should software developer go out of business source code is available through a “Software Escrow Agreement”

Hardware Data Backup

- BCP team must prepare backup strategy
  - Online backups (hot redundant site)
  - Backup tape
  - Full backup image (eg. Ghost)
- Examine implications of each backup strategy
  - Full, partial or image backup
  - How long for complete or partial restore
  - Any required configuration changes or additional software **after** restore

Hardware Data Backup

- Consider implications of hardware replacement
  - Is hardware available at retailer
    - In stock, out of stock, on back order
  - Delivery time of new hardware
  - Set up and configuration time for provision of hardware
- Consider limitations/implications of using custom or legacy equipment
  - Can it be replaced?
  - How easily can we replace it?
  - Can we use anything else if equipment not available?

Software Data Backup

- Inventory required of critical and non critical software used by all business units
  - Hardware is useless without required software
- Ensure software is duplicated and stored off site
- Inventory custom software
  - In house development
  - Store multiple copies - cannot purchase off shelf
- Inventory specialized software developed by 3rd parties
  - Ensure a “Software Escrow” agreement is in place in the event 3rd party developer goes out of business.
  - Company has access to source code held in escrow by an independent entity.

Data Backup

- Plan must provide solutions, how to protect data and how to restore after a disaster.
- BCP team is not responsible for classification of data, but plan for protection and recovery
- BCP team should choose a backup strategy which makes sense for the type of data that is being backed up
- Operations is responsible for timing of backup tasks (how often)

Data Backup

- Typically 3 types of backup available full, differential and incremental
- **Full Backup**
  - All data is saved
  - Archive bit is cleared
    - File attribute that is set when the content of a file is changed
  - Backup is one step
  - Restore is one step
  - Longest process to backup
  - Fastest to restore

Data Backup

- **Differential Backup**
  - Includes all data which has been modified since last full backup.
    - All files with archive bit set
  - Archive bit is not cleared so data will be copied again on next differential backup
    - Differential backups continue to grow
  - Restore procedure requires the full backup then latest differential backup
  - Faster than doing full backup

Data Backup

- **Incremental Backup**
  - Data which has changed since last full or incremental backup.
  - Archive bit is changed after each incremental to indicate the data has been backed up
  - Restore requires full backup then each consecutive incremental in order
  - Fastest backup and slowest restore

Data Backup

- Critical data should be stored on-site and secondary recovery site
- Critical data should be stored in a fire proof vault, storage cabinet
- Backup strategy documentation should be available to operators
  - During disaster recovery original backup operator may not be available
- Data Backups should be tested by performing a full restore to alternate location
  - Without testing you don’t know if your data is actually being backed up properly and is in good shape (corruption)

Data Backup

- Electronic backup technology provides many automated backup solutions
- **Disk Shadowing**
  - Very similar to ‘mirroring’
  - Duplicated hardware maintains more then one copy of data set
  - Dynamically created and copied to two or more identical disks
  - If one disk fails, remaining shadow copies available
  - To the user all these identical disks appear as one single disk
  - Multiple paths are provided to data, can carry our multiple read requests in parallel
  - Expensive solution because multiple drives are used to store same data

Data Backup

- **Electronic vaulting**
  - As data is written to disk, a periodic copy is automatically sent backup recovery site
  - Data changes are batched and transmitted on a schedule
    - hourly, daily, weekly, monthly

Data Backup

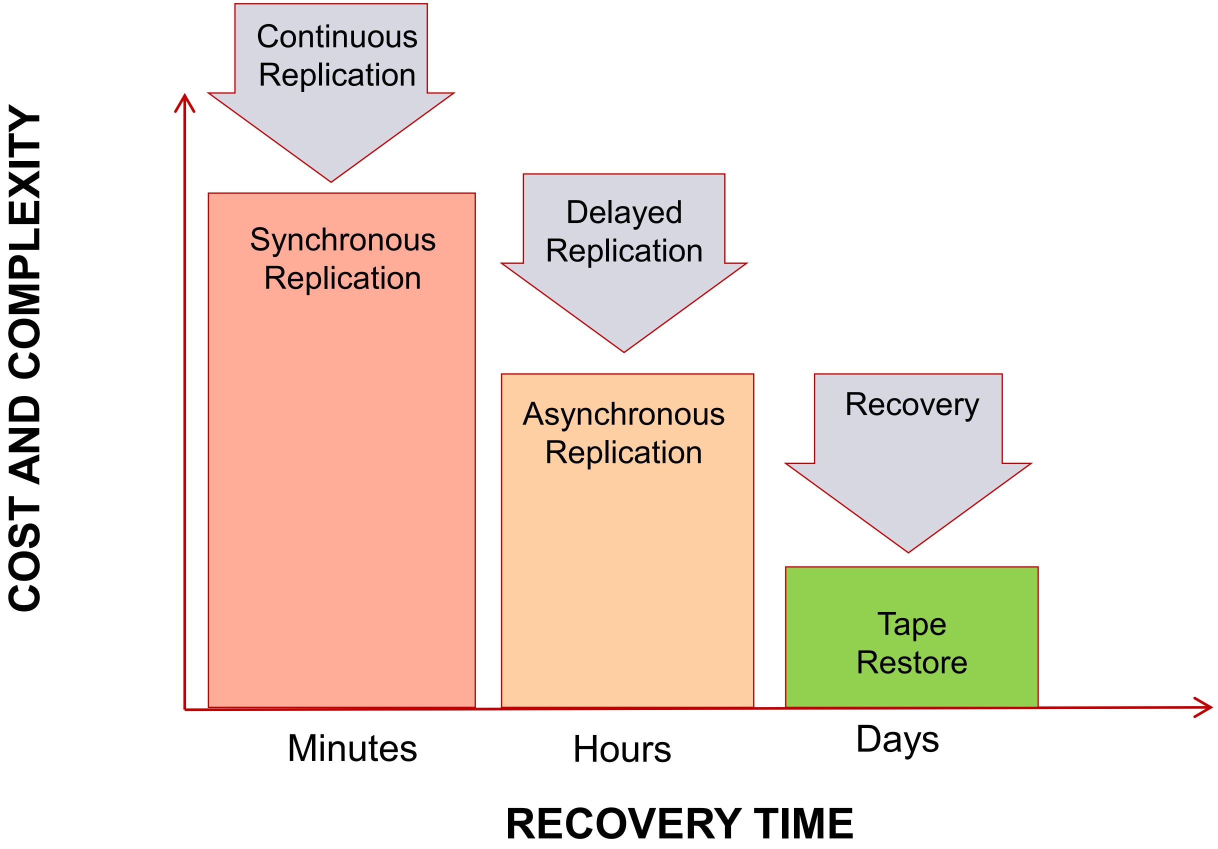
- **Tape Vaulting**
  - Many companies backup data to tape media which is transported to offsite storage
  - With automatic tape vaulting data is sent over dedicated serial lines to tape backup devices at offsite facility.
  - Tape changes and maintenance are done by remote facility staff (usually contracted vendor)
  - Eliminates error of manual tape backup process and you can’t forget to ship tape offsite

Data Backup

- **Remote Journaling**
  - Another method of transmitting data offsite to recovery site
  - Just the journal transaction entry or transaction logs are transmitted offsite
    - Changes to files not complete file
    - Done in real time
    - Best for database backup and recovery
    - Record or log of journal entries is used to rebuild data if required

Data Backup

Cost vs Recovery Time



Source: All-In-One CISSP Exam Guide by Shon Harris

Recovery Documentation

- All procedures for business transaction, services, tasks and processes must be documented
  - Special attention to unique or specialized processes
  - Separate plans for specific processes may be required
  - Crisis communication plan
- Documentation should include all business units
- Include IT specific processes
  - Network and voice communication diagrams
  - Backup restore procedures
  - Hardware provisioning procedure

Recovery Documentation

- Once critical tasks have been identified assign ownership of each task or procedure to a specific individual
  - Ensures accountability
  - Must be included as part of daily duties
  - Ensures constant updates

Human Resource Plans

- Human assets are sometimes harder to replace because of required experience and training
  - BCP includes physical location, equipment, environmental plan
  - Must also consider who will operate equipment
  - What if recovery site is far away
  - How will employees be transported
- Should company hire new employees?
- Should company use temporary employees?

Human Resource Plans

- **Senior management**
- Plan requires an executive succession plan
  - In the event senior management retires, leaves or is killed in accident
  - Defines line of succession
  - How to find replacement and temporary role assignment
- Plan should include things like;
  - CEO and 2nd in command cannot travel in same plane/car

Human Resource Plans

- Devise a method by which employees will be notified of disaster
  - Utilize current management structure within the company to notify employees
  - Managers would be notified (top-down)
- Appoint two or more individuals to be in charge of new facility
  - These individuals should be available to everyone
  - These individuals should be in easily accessible central location
    - Ease confusion during recovery
    - Think of them as traffic cops

End-User Environment

- Plan to recover departments based on criticality level
- During recovery process most companies bring in skeleton crew
  - Most critical department should be recovered first
  - Second most important department recovered next and so on..
- Devise a notification plan in case some technology is not available
  - Email or network may initially be down
  - How do we communicate? (Runners)

Liability and Its Ramifications

- As legislatures, courts and law enforcement develop and refine their respective approaches to computer crimes so too must corporations
- Corporations should follow these principles otherwise be open to litigation:
  - **Due Care**
  - **Due Diligence**

Liability and Its Ramifications

- **Due Care**
  - Means that a company did all it could have reasonably done under the circumstances, to prevent security breaches, and also took reasonable steps to ensure that if a security breach did take place, proper controls or countermeasures were in place to mitigate the damages
- **Due Diligence**
  - Means that the company properly investigated all of its possible weaknesses and vulnerabilities

Liability and Its Ramifications

- Before you can figure out how to properly protect yourself you need to find out what it is you are protecting yourself against
  - This is due diligence - researching and assessing the current level of vulnerabilities so the true risk level is understood
- Only after these steps and assessments take place can effective controls and safeguards be identified and implemented
- Security is developed and implemented to protect an organization’s valuable resources

Liability and Its Ramifications

- Appropriate safeguards need to be in place to protect the company’s mission by protecting its tangible and intangible resources, reputation, employees, customers, shareholders, and legal position
- The costs and benefits of security should be evaluated in monetary and nonmonetary terms to ensure that the cost of security does not outweigh the expected benefits

Liability and Its Ramifications

- Security mechanisms should be employed to reduce the frequency and severity of security-related losses
- Senior management needs to decide upon the amount of risk it is willing to take pertaining to computer and information security, and implement security in an economical and responsible manner

Liability and Its Ramifications

- When companies come together to work in an integrated manner, special care must be taken to ensure that each party promises to provide the necessary level of protection, liability, and responsibility, which should be clearly defined in the contracts
- Auditing and testing should be performed to ensure that each party is indeed holding up its side of the bargain
- Each company has different requirements when it comes to their list of due care responsibilities

Liability and Its Ramifications

- There are a number of circumstances whereby a company could be held liable for negligence in in actions and responsibilities.
  - Personal Information, whether or staff or customers.
  - Health information.
  - Financial information.
  - The company needs to know, understand and comply with all applicable laws and regulations.

  Third Party Risk
  - If engaging service providers, conduct risk assessments before signing contracts.

Contractual Agreements

- It is critical that information security issues are addressed in the contracts organizations use or enter into during regular business activities. Security considerations should be taken for at least the following contracts types:
  - Outsourcing agreements
  - Hardware supply
  - System maintenance and support
  - System leasing agreements
  - Consultancy service agreements
  - Website development and support
  - Nondisclosure and confidentiality agreements
  - Information security management agreements
  - Software development agreements
  - Software licensing

Implementing Disaster Recovery

- Management support is most important before any BCP tasks can begin
- Management should appoint a “Business Continuity Coordinator”
  - Leader of BCP team
  - Will oversee development, implementation, testing and maintenance of BCP
  - Person should have good social skills with political streak
  - Must be credible and have authority as granted by senior management

Implementing Disaster Recovery

- BCP Coordinator must create a number of key teams responsible for recovery tasks
  - Damage assessment team
  - Recovery team
  - Relocation team
  - Restoration team
  - Salvage team
  - Security team

Implementing Disaster Recovery

- Employees should be assigned to respective teams based on their knowledge
- Each team requires a leader
  - Responsible for meeting team objectives
  - Responsible for communicating with other teams and BCP coordinator

Assessment

- Tasks assigned to Damage Assessment Team
  - 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 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.

Restoration

- Once the damage assessment is completed and the plan is activated, various teams must be deployed, which signals the company's entry into the *restoration phase*.
- 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

Communications & Training

- **Emergency communications** plan should be developed and documented
  - Copies of plan must be easily accessible at primary site and recovery site
  - Different formats be available to all recovery teams
    - Electronic and paper
  - Key personnel should have a copy of plan at home with call tree (who to call and how)
- **Training the team on** the execution of a DR plan is critical:
  - Validates that the plan will work.
  - If your team is doing a walk-through exercise in response to a training scenario, it will be obvious whether the plan would work or not.
  - Everyone will know what their role entails.

Emergency Management

- Safety
  - Protect human life
  - Life-safety is the primary goal of security from all threats
  - A physical security program should not compromise safety with security mechanisms
- Security
  - Protection against vandalism, theft and attacks
- In case of emergency or fire alarm an electronic lock has one of two default settings
- Fail-Safe - unlock
  - If power disruption occurs due to fire or emergency lock will open
  - Primary concern human safety
- Fail-Secure - locked
  - If power disruption occurs due to fire or emergency lock will remain closed
  - Primary concern asset security

Architecture & Engineering Part 3 - Domain 3
Site (Physical) Security

FANSHAWE

Physical Security

- Site and facility design considerations
- Physical security risks, threats, and countermeasures
- Electric power issues and countermeasures
- Fire prevention, detection, and suppression

Site and Facility Security

Physical Threat Categories

- **Natural and Environmental**
  - Floods
  - Earthquakes
  - Storms and tornadoes
  - Fires
  - Extreme temperature
- **Supply System Threats**
  - Electrical power outages
  - Communications interruptions,
  - Energy resources such as water, gas, steam

Site and Facility Security

Physical Threat Categories

- **Man Made Threats**
  - Unauthorized access (internal and external)
  - Damage by angry employee
  - Employee errors and accidents
  - Vandalism, fraud, theft, espionage
- **Politically Motivated Threats**
  - Strikes
  - Riots
  - Civil disobedience
  - Terrorist attacks
    - Bombings

Physical Security

- Theft, fraud, sabotage and vandalism are raising costs for companies
  - Laptops or workstations lost or stolen
  - Data lost or stolen
  - Disgruntled employee (shooting, violent attacks)
  - Terrorism, espionage, cyber attacks
- Most IT departments focus on network security not physical security

Physical Security

- Physical security must be implemented based on a layered defense model
  - Physical controls work together in a tiered architecture
  - From perimeter to protected asset
  - Fence
  - Building
  - Locked door card access
  - Guard
  - Locked computers
  - Locked server rooms

Physical Security Goals

- Safety
  - Protect human life
  - Life-safety is the primary goal of security from all threats
  - A physical security program should not compromise safety with security mechanisms
- Security
  - Protection against vandalism, theft and attacks

Threat Categories

- Internal
  - Malfunctioning devices
  - Fire hazards
  - Employees who aim to damage the company
- External
  - Threats originating outside of the company
  - Terrorist threats
  - Religion motivated threats
  - Social or ideological threats
    - Abortion clinic

Physical Security Planning

- Physical security plans depend on the level of protection required for assets and resources
  - Depends on the acceptable level of risk
  - Derived from laws and regulations
    - Identify threats against assets
    - Identify types of attacks
    - Identify and understand business impact of threats
    - Identify types of countermeasures
- Financial institution has a different threat profile than a grocery store or a hospital

Physical Security Planning

- Organization must first define
  - Targets
  - Vulnerabilities
  - Threats
  - Threat agents

Physical Security Planning

- Vulnerability
  - Weakness in procedure, resource, process, asset or transaction
- Threat
  - The potential that someone will identify this weakness an use it against you
- Threat Agent
  - The person or mechanism that actually exploits the identified vulnerability

The Site Planning Process

Physical Security Goals

- Deter, detect, reduce
- **Crime and disruption prevention through deterrence**
  - Fences, security guards, warning signs
- **Crime or disruption detection**
  - Smoke detectors, motion detectors, CCTV cameras
- **Reduction of damage**
  - Layers of defenses that slow down the adversary
  - Fences, locks, security guard and barriers

The Site Planning Process

- **Incident Assessment**
  - Determine level of damage
  - Response of security guards to detected incidents
- **Response Procedures**
  - Fire suppression mechanisms,
  - Emergency response processes
  - Law enforcement notification
- An organization should prevent crimes and disruptions from occurring
- Should plan to deal with them when they do happen

The Site Planning Process

- Possible Performance Metrics:
  - Number of successful crimes
  - Number of successful disruptions
  - Number of unsuccessful crimes
  - Number of unsuccessful disruptions
  - Time between detection, assessment and recovery steps
  - Business impact of disruptions
  - Number of false-positive detection alerts
  - Time it took for a criminal to defeat a control
  - Time it took to restore the operational environment
  - Financial loss of a successful crime
  - Financial loss of a successful disruption

The Site Planning Process

- Physical security plan requires
  - A team of internal employees
  - Risk analysis
    - Identify vulnerabilities and threats
    - Calculate the business impact of each threat
    - Cost of counter measures

An Effective Physical Security Program

1. Identify a team of internal employees and/or external consultants who will build the physical security program through the following steps.

2. Define the scope of the effort: site or facility.

3. Carry out a risk analysis to identify the vulnerabilities and threats and to calculate the business impact of each threat.

4. Identify regulatory and legal requirements that the organization must meet and maintain.

5. Work with management to define an acceptable risk level for the physical security program.

6. Derive the required performance baselines from the acceptable risk level.

7. Create countermeasure performance metrics.

8. Develop criteria from the results of the analysis, outlining the level of protection and performance required for the following categories of the security program:

- Deterrence
- Delaying
- Detection
- Assessment
- Response

9. Identify and implement countermeasures for each program category.

10. Continuously evaluate countermeasures against the set baselines to ensure the acceptable risk level is not exceeded.

Crime Prevention Through Environmental Design (CPTED)

- Crime Prevention Through Environmental Design (CPTED)
  - Common approach to physical security design
  - Proper design of physical environment can directly reduce crime by influencing human behaviour
  - Outlines proper facility construction and environmental components and procedures
  - Landscaping
  - Entrances
  - Facility and neighborhood layout
  - Lighting
  - Road placement and traffic patterns
  - It addresses micro environments such as offices, restrooms

CPTED

- CPTED approach provides 3 main strategies:
  - Natural Access Control
  - Natural Surveillance
  - Natural Territorial Reinforcement

CPTED - Security Zones

- Clear lines of sight and transparency can be used to discourage potential offenders, because of the absence of places to hide or carry out criminal activities.
- The CPTED model shows how *security zones* can be created. An environment's space should be divided into zones with different security levels, depending upon who needs to be in that zone and the associated risk.
- The zones can be labeled as controlled, restricted, public, or sensitive.
- This is conceptually similar to information classification,

CPTED
Natural Access Control

- Is the guidance of people entering and leaving a space by the placement of doors, fences, lighting and landscaping:
  - Limit number of entry points
  - Force all guests to go to front desk and sign in
  - Reduce entry points further after hours, weekends
  - Have security guard validate picture ID before allowing access
  - Require guests to sign in and be escorted
  - Encourage employees to question strangers

CPTED - Perimeter Security

- Bollards
  - Concrete Pillars outside a building
  - Usually placed between facility and parking
  - Protect against car threat
    - Driving through wall or front door

CPTED - Natural Surveillance

- The goal of natural surveillance is to make criminals feel uncomfortable
- Provide many ways observers could potentially see criminal
- Make others in the area feel safe and comfortable by providing an open space

CPTED
Natural Territorial Reinforcement

- Natural Territorial Reinforcement
- Create a sense of a dedicated community through the use of walls, fences, landscaping, light fixtures, flags, clearly marked addresses and decorative sidewalks
- Give potential offenders the impression they do not belong there, they are at risk of being seen and their illegal activities will not be tolerated
- Urban design

Designing a Physical Security Program

If a team is organized to assess the protection level of an existing facility, it needs to investigate the following:

- Construction materials of walls and ceilings
- Power distribution systems
- Communication paths and types (copper, telephone, fiber)
- Surrounding hazardous materials
- Exterior components:
    - Topography
    - Proximity to airports, highways, railroads
    - Potential electromagnetic interference from surrounding devices
    - Climate
    - Soil
    - Existing fences, detection sensors, cameras, barriers
    - Operational activities that depend upon physical resources
    - Vehicle activity
    - Neighbors

Physical Security Framework Outline

I. Deterrence of criminal activity
- **A.** Fences
- **B.** Warning signs
- **C.** Security guards
- **D.** Dogs

II. Delay of intruders to help ensure they can be caught
- **A.** Locks
- **B.** Defense-in-depth measures
- **C.** Access controls

III. Detection of intruders
- **A.** External intruder sensors
- **B.** Internal intruder sensors

IV. Assessment of situations
- **A.** Security guard procedures
- **B.** Damage assessment criteria

V. Response to intrusions and disruptions
- **A.** Communication structure (calling tree)
- **B.** Response force
- **C.** Emergency response procedures
- **D.** Police, fire, medical personnel

Designing a Physical Security Program

- Facility
- When buying, renting or building a facility consider:
  - Location, Location and Location
  - How much protection does a particular location provide?
- Construction
- What level of protection do the materials from which the build is constructed provide?

Construction Guidelines

- Cost vs. benefit
  - Wood steel or concrete
- Material ‘load’ (how much weight) must be considered
- Windows may provide UV protection
  - Lower heating/cooling costs
- Exterior doors and interior doors
  - Different risk ratings
- Raised floors vs. standard flooring (server rooms)
- Electrical considerations
- Cooling considerations

Construction Guidelines

- **Walls**
  - Combustibility and fire rating,
  - Reinforcement for secured areas
- **Ceilings**
  - Combustibility, fire rating
  - Weight-bearing rating
  - Drop-ceiling considerations

Construction Guidelines

Doors:

- Combustibility of material (wood, pressed board, 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 an unlocked state for safe evacuation in power outages
- Type of glass—shatterproof or bulletproof glass requirements

Construction Guidelines

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

Construction Guidelines

- **Flooring**
  - Weight-bearing rating
  - Combustibility and fire rating (wood, steel, concreate)
  - Fire rating
  - Raised flooring
    - Network cables laid below floor
  - Non-conducting surface and material

Construction Guidelines

- **Heating, Ventilation and Air Conditioning** (HVAC)
  - Positive Air Pressure
  - Protected intake vents
  - Dedicated power lines
  - Emergency shutoff valves and switches
  - Placement
- **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

Construction Guidelines

- **Water and Gas Lines**
  - Shutoff valves
  - Positive flow (material flows out of building, not in)
  - Placement – properly located and labeled
- **Fire Detection and Suppression**
  - Placement of sensors and detectors
  - Placement of suppression systems
  - Type of detectors and suppression agents

Construction Guidelines

- **Entry points**
  - Doors & windows
    - weakest portion of any structure
  - Roof access fire escape
  - Chimneys
  - Service delivery access points
- Second and Third entry points
  - Internal doors leading into other portions of the building
  - Elevators
  - Stairwell
  - Ventilation ducts and utility tunnels

Doors

- Different types of doors are available with different functionality and properties
  - Vault Doors
  - Personnel Doors
  - Industrial Doors
  - Vehicle Access Doors
  - Bullet-resistant Doors
- Hinges on doors should have pins that cannot be removed

Doors

- Doors can be hollow or solid core
  - Hollow core only for internal use
- Walls surrounding doors must offer same level of protection
  - Otherwise when faced with a fortified solid core door may choose to go through wall defeating door counter measure

Doors

- In case of emergency or fire alarm an electronic lock has one of two default settings
- Fail-Safe - unlock
  - If power disruption occurs due to fire or emergency lock will open
  - Primary concern human safety
- Fail-Secure - locked
  - If power disruption occurs due to fire or emergency lock will remain closed
  - Primary concern asset security

Windows

- **Standard:**
  - No extra protection
  - The least expensive and lowest level of protection
- **Tempered:**
  - Glass is heated and then cooled suddenly to increase integrity and strength
- **Acrylic:**
  - A type of plastic instead of glass
- **Wired:**
  - A mesh of wire is embedded between two sheets of glass
  - Prevents shattering
- **Laminated:**
  - Plastic layer between two outer glass layers
  - Increases strength
- **Solar window film:**
  - Provides extra security by being tinted and offers extra strength due to the film’s material.
- **Security Film:**
  - Transparent film is applied to the glass to increase its strength

Data Centre & Server Rooms

- Strict access policies should be in place
  - Door codes changed every 6 months
- Data centre should not be located on top floors
  - Difficult for fire crews to reach quickly
- Data centre should not be located in basements
  - flooding
- HVAC and circulation ducts should be protected or made too small for human to crawl
- Positive air pressure
  - Air is not sucked into the room
  - Contaminating computer cooling fans

Data Centre & Server Rooms

- Have separate power system from rest of facility
- Have redundant and backup power
  - On site generator
- Have UPS Power
  - Battery for temporary power and power conditioning
- Shatter-proof glass for walls
- Data centre doors should be solid core and frame should be fixed to adjoining wall studs with three hinges (increase door strength)

Distribution Facilities

- Distribution facilities are systems that distribute communications lines, typically dividing higher bandwidth lines into multiple lower bandwidth ones.

- Buildings generally have one **main distribution facility** (MDF) where one or more external data lines are fed into the server room, data center, and/or other smaller **intermediate distribution facilities** (IDFs).
- Larger IDFs are usually installed in small rooms normally called **wiring closets**.
- It is critical to think of these as the sensitive IT facilities that they are and not as just closets.

Storage Facilities

- The information life cycle includes an archival phase during which information is not regularly used but still needs to be retained.
  - This has to happen in a secure location that meets the requirements required for server rooms and data centers.
  - Media storage is not always given the importance it deserves, which can result in the loss or compromise of important information.
- Evidence storage facilities are even more sensitive because any compromise, real or perceived, could render evidence inadmissible in court.
  - Every organization with a dedicated IT staff should have a secure facility in which to store evidence.
  - The two key requirements for evidence storage facilities are that they are secured and that all access and transfers are logged.

Internal Support Systems

Electrical Power

- Clean Power
  - Electrical power that does not fluctuate
  - No harmonics or distortions
- Onsite power generator for longer term power backup
  - Requires natural gas or diesel
  - Runtime depends on fuel storage supply
  - More expensive solution
- Uninterruptible power supply (UPS) for temporary power backup
  - Requires large batteries
  - Limited amount of power / time

Electrical Power

- Online UPS
  - AC current charge a bank of batteries
  - Batteries provide DC supply
  - Inverters switch power back to AC
  - This conditions power levels to a steady constant level
  - Removes distortions
- StandBy UPS
  - Remains inactive until a power line failure is detected and load is switched from AC to battery

Electrical Power

- Electric power is susceptible to interference creating harmful conditions for some computer controlled equipment
- Line Noise
  - Electromagnetic Interference (EMI)
    - Electric Motors generate EMI noise
  - Radio Frequency Interference (RFI)
    - Office Fluorescent lighting generates RFI noise

Electrical Power

- Plug in every device to a surge protected outlet
- Shutdown and restart devices in an orderly fashion
- Employ power line monitors to detect frequency and voltage fluctuations
- Use voltage regulators or conditioners
- Protect distribution panels, master circuit breakers with access controls

Electrical Power

- Provide protection from magnetic induction through shielded lines
- Use shielded cabling for long cable runs
- Do not run data or power lines directly over fluorescent lights or near elevator shafts
- Do not plug outlet strips and extension cords into each other
- Redundant supply line from power utility

Electrical Power

- **Preventive Measures and Good Practices**

When dealing with electric power issues, the following items can help protect devices and the environment:

- Employ surge protectors to protect from excessive current.
- Shut down devices in an orderly fashion to help avoid data loss or damage to devices due to voltage changes.
- Employ power line monitors to detect frequency and voltage amplitude changes.
- Use regulators to keep voltage steady and the power clean.
- Protect distribution panels, master circuit breakers, and transformer cables with access controls.
- Provide protection from magnetic induction through shielded lines.
- Use shielded cabling for long cable runs.
- Do not run data or power lines directly over fluorescent lights.
- Use three-prong connections or adapters if using two-prong connections.
- Do not plug outlet strips and extension cords into each other.

Electrical Power Issues

- **Power excess:**
  - **Spike** Momentary high voltage
  - **Surge** Prolonged high voltage
- **Power loss:**
  - **Fault** Momentary power outage
  - **Blackout** Prolonged, complete loss of electric power
- **Power degradation:**
  - **Sag/dip** Momentary low-voltage condition, from one cycle to a few seconds
  - **Brownout** Prolonged power supply that is below normal voltage
  - **In-rush current** Initial surge of current required to start a load

Environmental Issues

- Damage to services, hardware and lives.
  - Make certain appropriate controls are in place.
  - During construction or renovation make certain that items such as: water pipes, gas lines, electrical power and so on all have proper shut off valves/switches and are accessible.

Fire Prevention, Detection and Suppression

Fire Issues

- Companies must meet national and local standards pertaining to fire prevention, detection and suppression methods
- Fire Prevention
  - Proper construction materials (non combustible)
- Fire Detection
  - Manual or automatic detection sensors that react when they detect the presence of fire or smoke
- Fire Suppression
  - Agent to put out a fire
  - Manual or automatic

Fire Prevention, Detection and Suppression

Fire Issues

- Fire requires the following to continue to burn
  - Fuel, and oxygen
  - Remove either one and you’ve suppressed a burning fire
- There are 4 classes (A, B, C, D) of fire
  - Each has different suppression agent
- Fire detectors should be installed
  - On and above suspended ceilings
  - Below raised floors and in air ducts and enclosures

Fire Prevention, Detection and Suppression

Fire Class, Fire Type, Fire Characteristics and Suppression

CLASS	CLASS B	CLASS C	CLASS D
Wood Products, Paper and Laminates	Petroleum Products and Coolants	Electrical Equipment and Wires	Magnesium, Sodium, Potassium
Common Combustibles	Liquid	Electrical	Combustible Materials
Water and Foam	Gas, CO2, Foam, Dry Powder	Gas, CO2, Dry Powder	Dry Powder

Source: All-In-One CISSP Exam Guide 8th Edition by Shon Harris

Types of Fire Detection

- **Smoke Detector**
  - Photoelectric
  - Optical detector
  - Beam of light directed at a receiver
  - If light beam is interrupted sensor activates.
- **Heat Activated detectors**
  - Monitor ambient temperature
  - Trigger alarm when temperature reaches a predefined level
  - Rate of increase within a specific amount of time reaches a certain threshold.

Fire Suppression

- Each of the 4 fire classes have a specific suppressing agent
- Suppression agents
  - Water
  - Foam
  - Gas
  - Dry Powder
- Each suppression agent has different properties, requirement
- Can be hazardous if not administered in the right environment.

Plenum Area

- Space between real ceiling and drop ceiling tiles, wall cavities and space under raised floors
- Typically full of wiring
  - Lighting, electrical, network
- Plenum rated wiring should be used in these areas.

Water Sprinklers

- Water sprinkler systems are typically least expensive but cause significant water damage
- There are 4 types of Sprinkler Delivery systems
- **Wet Pipe**
  - Closed head systems
  - Wet pipe systems always contain water in the pipes and are usually discharged by temperature.
  - In colder climates this water may freeze
  - If there is a pipe break or nozzle problem it can cause water damage

Water Sprinklers

- **Dry Pipe**
  - Water is not held in pipes, it is contained in a holding tank until it is required
  - Pipes are air pressurized which is reduced when a fire is detected allowing water to flow from holding tank, through pipes to sprinkler nozzles
  - Best used in colder climates because will not freeze
  - First a heat or smoke sensor activates, filling pipes with water
  - Then a fire alarm is activated, electric power is disconnected and sprinkler nozzles release

Water Sprinklers

- **Preaction**
  - Similar to dry pipe systems, but includes a 2nd safety mechanism which is a thermal-fusible link in the sprinkler nozzle
  - Just like in dry pipe system, when fire is detected air pressure in pipes is reduced, filling pipes with water
  - Water is held at sprinkler nozzle until thermal fuse is melted by fire heat.
  - This system gives more time to respond to smaller fires before activating sprinkler system.
- Often used in data processing centers.

Fire Detectors

- **Deluge**
  - Deluge system has OPEN sprinkler heads to allow greater volume of water in a shorter period of time
  - Typically not used in data processing centers

Summary

- Life-safety number one goal
- The site planning process
- Facility site design using CPTED
- Walls, doors, windows,
- Environmental controls
  - Power supply
- Fire suppression
  - Water, gas system, hand extinguisher

Homework

- Read the relevant chapter in the set book ‘All In One CISSP Exam Guide’ – by Shon Harris.

- Depending on which edition you have the relevant sections will be in different places – so use the index.

- Then identify and do the practice m/c questions relating to this subject.

Questions

- ?