Final Exam Study Notes Week 8-9

SENG 460

Spring 2021

8 Identity, Access Management, Logging, Policies, Standards, Audits, Compliance

8.1 Key Terms

- Authentication
  - Proof of identity which allows a user access to a system
- Authorization
  - Determines the privileges users will have
- Least privilege
  - Person should have the minimum privileges or access to do their job, no more, no less
- Job rotation
  - Move people between jobs to limit fraud
- Mandatory vacations
  - Reduce fraud
- Privilege creep
  - Gaining more access than you should have (aggregation of privileges)
- Separation of duties
  - Requiring more than one person to complete a task
- Collusion
  - Two people working together to defeat SoD
- Password
  - String of characters used to authenticate access
- Passcode
  - Often used interchangeably with password
  - May refer to pin
- Passphrase
  - Longer string of text
- Password length
  - Password must be X characters or more
- Password complexity
  - Upper and lower case
  - Numbers
  - Punctuation
  - Special characters
- Password aging
  - Must change password after X days
  - Password expiry
- Password history
  - Can't use the same password as last **X** times
- Multi-factor authentications (2 or more of...)
  - Something you know
  - Something you have
  - Something you are
- Biometrics
  - Fingerprints
  - Retina
  - Iris
  - Vascular
  - Gait
  - Typing
  - Voice
  - Etc
- False reject rate (FRR)
  - Type 1 error
  - When authorized users are falsely rejected

- False accept rate (FAR)
  - Type 2 error
  - When unauthorized persons are falsely accepted
- Username
- Separation of duties (SoD)
- Two factor (2FA), Multifactor (MFA)
- Crossover error rate (CER)
  - Point at which false rejection rates and false acceptance rates are equal
  - Smaller the CER the more accurate the system

Two or more of

- Something you know
  - Password
  - PIN
- Something you have
  - Phone
  - Hardware token
- Something you are
  - Biometrics
  - Typing pattern
  - Facial recognition

Access control

- Allowing only authorized users, programs, or other computer systems to gain access
  - Specify which users can access a system
  - What resources the users can access
  - What operations the users can perform
  - Enforce accountability for user actions

8.2 Access Terms

- Access request
  - Access is needed
  - Access request submitted
  - Request is reviewed and approved/denied
  - Request is implemented
  - Requester notified
- Employee identification cards vs. access cards
  - Magnetic stripes
  - Smart cards
  - Proximity cards
- Identity proofing
  - Verifying claimed identity matches actual identity
- Credentials
  - Username
  - Identification number
  - Password
  - License or security key
  - PIN
  - Etc.
- Background checks
  - Employment
  - Education
  - Criminal records
  - Credit history
  - Motor vehicle and license record checks

- Access Rules
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
  - Non-Discretionary Access Control
- Issuing credentials
  - Providing credentials to a person or business
- Account management
  - Creating user accounts
  - Modifying accounts
  - Decommissioning accounts

8.3 Onboarding/Offboarding

- Onboarding
  - Individual joining the organization
- Offboarding
  - Individual leaving the organization
- Transfer between roles
  - Individual changing jobs
- Provisioning
  - Providing access
- Deprovisioning
  - Removing access
- Requests, approvals
  - Part of the access request process

8.4 Tips

- Maintain least privilege
- Centralized record of who has what access
- Regular review, SoD violations
- Identity management solution
  - Knowledge of who has access to what
  - Alerts, remediates discrepancies
  - Maintains concept of roles
  - Pros/Cons
    - Is it feasible to do for all systems?

8.5 Logging

- Record who did what and when
- Ensure accurate time, synchronized
- Restrict access, store remotely
- Correlation, monitoring, alerting
- Different levels of logging maturity
  - Logs enabled
  - Centralized logging
  - Security information and event management (SIEM)

8.6 Types of Controls

Administrative

- Policies and procedures
- Disaster recovery plans
- Awareness training
- Security reviews and audits
- Background checks
- Review of vacation history
- Separation of duties
- Job rotation

Logical or Technical

- Restrict access to systems and the protection of information
  - Encryption
  - Smart cards
  - Anti-virus software
  - Audit trails
  - Log files
  - ACLs
  - Biometrics
  - Transmission protocols (Kerberos, IPSec)
- Physical
  - Guards and building security
  - Biometric access restrictions
  - Protection of cables
  - File backups

8.7 Mandatory Access Control (MAC)

- Authorization of subject's access to an object depends on labels (sensitivity levels), which indicate subject's clearance, and the classification or sensitivity of the object
- Every object is assigned a sensitivity level/label and only users authorized up to that particular level can access the object
- Access depends on rules and not by the identity of the subjects or objects alone
- Only administrator (not owners) may change category of a resource
- Output is labeled as to sensitivity level
- Unlike permission bits or ACLs, labels cannot ordinarily be changed
- Can't copy a labeled file into another file with a different label
- Rule based access control

8.8 Discretionary Access Control (DAC)

- Subject has authority, within certain limits, to specify what objects can be accessible
- User-directed means a user has discretion
- Identity-based means discretionary access control is based on the subjects identity
- Very common in commercial context because of flexibility
- Relies on object owner to control access
- Identity-based access control

8.9 Non-Discretionary Access Control

- Central authority determines what subjects can have access to certain objects based on organization's security policy
- May be based on individual's role in the organization (Role-Based) or the subject's responsibilities or duties (task-based)

8.10 Role-Based Access Control (RBAC)

- Restricting access based on roles
- Notion of "employee" or "base" role
  - Access everyone has

Steps

- Identify systems
- Create library of roles
- Assign users to defined roles

8.11 Web Access Management

Software controls what users can access when using a browser to access a web-app

8.12 Single Sign-on

Allows users to enter credentials one-time and access all resources in same domain (Eg. Kerberos)

8.13 Kerberos

Three components

- Authentication server (AS)
- Ticket granting service (TGS)
- Key distribution center (KDC)

8.14 Security Assertion Markup Language (SAML)

- Doesn't rely on passwords
- Uses crypto and digital signatures to pass secure token from identity provider to application

8.15 Open Authorization

- Open standard for token-based authentication and authorization on the internet
- Allows third party to use information without exposing password
- Just authorization to resources, not supposed to be authentication

8.16 Onboarding

- Provide access to new employees
  - Delay impacts brand of company (desk, laptop, phone, access)
- Concept of an employee role or base role
  - That access that every employee has (Eg. Active directory)
- "Make me look like Bob"
  - Leads to access creep
- Aggregation of privileges
  - Longer an employee is there, the more access they have
- Employee badge, what should be on it?
  - Company
  - Department
  - Name
  - Employee number
  - Signature
  - Picture

8.17 Cards

- Proximity card
  - "Dumb card"
- Smart card

8.18 Offboarding

- Remove access from departing employees
- Remind about obligations regarding assets, info

Consider

- Voluntary Departure
  - Competitor vs. not
  - Exit interview
- Involuntary Departure
  - Policies (eg. straight to the door? respect)
  - Priorities (eg. remove access first)
  - Review last activities

Physical concerns

- Threat to employees?
- Tailgating
- Collect
  - Badge
  - Keys
  - Computer
  - Phone
  - Credit card
  - USB
  - Etc

8.19 Single-Factor Authentiation

- Lockout after unsuccessful attempts
- Password
  - Length
  - Complexity
  - Aging/Expiry
  - History
- Determine whether to detect or prevent concurrent logins
- Passwords are susceptible to attack
  - Dictionary attack
  - Brute force attack
  - Rainbow tables

8.20 Hashing

- Word to hash
- Salt
- Hash with salt

8.21 Rainbow Tables

- Holds a significant number of precomputed hashes
- Can easily look up the hash and know what the original input was

8.22 Salting the hash

- Password management
- Password + salt to hash
  - Less susceptible to attacks
  - Unless the salt is short and have computed all combinations
- Password
  - Susceptible to rainbow tables
- Password creation

8.23 Policies, Standards, and Guidelines

- Policy
  - Document that outlines requirements that must be met (Eg. Acceptable use policy)
- Standard
  - System or procedure specific requirements that must be met (Eg. Server hardening, cryptographic)
- Guideline
  - Collection of system of procedure specific "suggestions" for best practice
- Policy should refer to standards and guidelines

8.24 Information Security Policy

- Policy language
- Know the audience
- Length
- Clarity
- Consumable
- Base on an industry standard

8.25 Personnel Security

- This section identifies security responsibilities and management processes throughout the employment cycle

Supervisors must ensure

- Prior to employment
  - Employee security screening is done in accordance with Public Service Agency policies and practices
- During employment
  - Employees are informed about the information security policies and procedures
  - Information Security roles and responsibilities
- At Termination
  - Employees are reminded of their ongoing confidentiality responsibilities following termination of employment in accordance with the Standards of Conduct
- Potential or actual information security breaches are investigated and reported, and invoke incident management processes where necessary
- Contractor responsibilities for information security are identified in contractual agreements

8.26 Information Systems and Devices

- This section defines requirements for secure management for government information systems and devices

Ministries must

- Maintain an inventory of government information systems and devices, including portable storage devices, and mobile devices
- Validate the measures taken to protect information systems and devices as part of enterprise risk management strategy This includes maintaining, documenting, verifying and valuing asset inventories on a regular basis
- Document the return of government devices in the possession of employees upon termination of their employment
- Remove government information from devices that are no longer needed by government
- Security dispose of devices in a manner appropriate for the sensitivity of the information the device contained

Mobile device security

- Ministries must ensure controls are implemented to mitigate security risks associated with the use of mobile devices
- Mobile device users must lock and/or secure unattended mobile devices to prevent unauthorized use or theft

8.27 Access to Info Systems and Devices

- This section identifies security roles, responsibilities and management processes relating to access and authorization controls for government information systems and devices

- Ministries must define, document, implement, communicate and maintain procedures to ensure access to government information systems and devices are granted to individuals based on business requirement and the principles of "least privilege" and "need-to-know"
- Employee must know and adhere to password security practices given in the Appropriate Use Policy

Supervisors must

- Ensure the assignment and revocation of access rights follow a formal and documented process
- Regularly, and upon change of employment, review, and update where appropriate, employee access rights to ensure they are up to date

8.28 Information Encryption

- This section defines encryption methods for improving the protection of information and for reducing the likelihood of compromised sensitive information
- The Chief Information Security Officer supports, and provides advice on, the use of encryption technologies in government

The Office of the Chief Information Officer must

- Provided direction and leadership in the use of encryption and the provision of encryption services, including those used for user registration
- Set corporate direction for the management (generating, storing, archiving, distributing, retiring and destroying) of encryption keys throughout their lifecycle

Ministries must

- Select information encryption controls during system design to provide appropriate protection commensurate to the information value and security classification
- Register the use of encryption technology products and services with the Chief Information Security Officer

8.29 Physical Security

- This section identifies operational requirements for protecting facilities where government information and information systems are located

Ministries in collaboration with the Ministry of Citizens' Services, must

- Design, document and implement security controls for a facility based on an assessment of security risks to the facility
- Review, and where appropriate test, physical security and environmental control requirements
- Establish appropriate entry controls to restrict access to secure areas, and to prevent unauthorized physical access to government information and devices
- Incorporate physical security controls to protect against natural disasters, malicious attacks or accident
- Ensure security controls are maintained when computer equipment, information or software is used outside government facilities

8.30 Operations Security

- This section establishes a framework for identifying requirements to control, monitor, and manage information security changes to the delivery of government services

Ministries must

- Plan, document and implement change management processes to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems
- Monitor and maintain information systems software throughout the software lifecycle
- Define document, assess, and test backup and recovery processes regularly
- Implement processes for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems
- Ensure operating procedures and responsibilities for managing information systems and information processing facilities are authorized, documented and reviewed on a regular basis
- Establish controls to protect log files from unauthorized modification, access or disposal
- Establish processes to identify, assess, and respond to vulnerabilities
- Enable synchronization of computer clocks to ensure integrity of information system logs and accurate reporting

- The Chief Information Officer must assess, provide advice, monitor response progress, and report vulnerability response activities

8.31 Computer Network and Communication Security

- This section identifies requirements for the protection of sensitive or confidential information on computer networks
- The Government Chief Information Officer must provide direction and leadership on implementation of, and significant modification to, electronic messaging systems
- The Chief Information Security Officer must develop corporate security controls to protect information from interception, copying, misrouting and unauthorized disposal when being transmitted electronically

Ministries in collaboration with the Office of the Chief Information Officer must

- Document network security controls prior to commencement of service delivery
- Ensure security features are implemented prior to commencement of service delivery
- Document, implement and manage changes to network security controls and security management practices to protect government information systems from security threats
- Ensure segregation of services, information systems, and users to support business requirements based on the principles of least privilege, management of risk and segregation of duties
- Ensure implementation of network controls to prevent unauthorized access or bypassing of security control
- Ensure electronic messaging services are protected commensurate to the value and sensitivity of message content, and approved for use by the Government Chief Information Officer
- Ensure information transfers between government and external parties are protected using services approved for use by the Government Chief Information Officer

8.32 Information System Procurement, Development and Maintenance

- This section defines requirements to ensure security controls are included on business and contract requirements for building and operating secure information systems, including commercial off the shelf and custom-built software
- The Office of the Chief Information Officer must provide corporate direction and oversight for developing and implementing security standards to procure, develop and maintain information systems

Ministries must

- Develop, implement and manage the processes and procedures necessary to ensure that information security risks and privacy requirements are taken into account throughout the systems development lifecycle
- Ensure sufficient resources and funding are allocated to complete the necessary information security tasks
- Ensure that system development or acquisition activities are aligned with government information security requirements and standards
- Apply vulnerability scanning, security testing, and system acceptance processes commensurate to the value and sensitivity of the information system

8.33 Supplier Relationships

- This section defines requirements to ensure supplier agreements for information systems and cloud services align with government security policies, standards and processes

Ministries must

- Ensure identified security requirements are agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities
- Ensuring security controls, service definitions, and delivery levels are identified and included in agreements with external parties prior to using external information and technology services
- Ensure that changes to provision of services by suppliers or information system services take into account that criticality of the information and information systems involved and the assessment of risks

- Establish processes to manage and review the information security controls of services delivered by external parties, on a regular basis
- Assess business requirements and associated risks related to external party access to information and information systems
- Ensure the risks of external party access to information and information systems are identified, assessed, mitigated and managed

8.34 Cloud Services Security

The Office of the Chief Information Officer provides corporate direction and leadership on the secure use of cloud services by

- Establishing policy and providing strategic direction on the use of cloud services
- Establishing roles and responsibilities
- Establishing information security and requirements for cloud services

Ministries must

- Notify the Government Chief Information Officer and the Chief Records Officer prior to procuring cloud services
- Consider existing cloud service offerings provided by the Office of the Chief Information Officer prior to procuring new cloud services
- Ensure new cloud services align with the cloud service strategy provided by the Office of the Chief Information Officer

8.35 Information Incident Management

- This section address the response and management of information incidents, including privacy breaches, in order to take the appropriate steps to mitigate the risk of harm
- Employees must immediately report suspected or actual information incidents in accordance with the Information Incident Management Process
- Ministries must establish ministry specific information incident management policies and procedures, as appropriate, to ensure quick, effective and orderly response to information incidents within the ministry

8.36 Business Continuity Management

- This section defines requirements to prepare, and re-establish, business or services as swiftly and smoothly as possible in adverse situation
- Emergency Management BC coordinates government-wide business continuity plans to reconcile recovery priorities, business impacts, security impacts and business resumption processes

Ministries must

- Establish, documents, implement, and maintain processes, procedures and controls to ensure the required level of information security for business continuity and disaster recovery during an adverse situation
- Ensure that vital records and critical systems are identified in business continuity plans

- Review business continuity and recovery plans annually to ensure they are current, valid, functional and readily accessible during a business interruption
- Regularly conduct business continuity and recovery exercises and, where necessary, update business continuity and recovery plan

8.37 Assurance and Compliance

- This section defines requirements to ensure compliance with legislation, government policies and standards

The Chief Information Security Officer must

- Initiate an independent review of the overall government information security program on a regular basis
- In collaboration with ministries, report on each ministry's adherence to the information security policies, and standards

Ministries must

- Ensure the legislative, statutory, regulatory and contractual security requirements of information systems are identified, documented, addressed and maintained
- Regularly review information systems and information security procedures to ensure compliance with security policies and standards

8.38 Information Security Standards

- ISO/IEC 27001
- ISO/IEC 27002
- NIST

8.39 Audits

- Sarbanes Oxley/SOX (Review Slide 86 of Week 8)
- SAS70/ SSAE16 / SSAE18
- PCI - DSS

8.40 SAS70/ SSAE16 / SSAE18

- Can help with SOX compliance
- Service Organization Controls (SOC)

Three SOC Reports

- SOC 1: Financial statement control
- SOC 2: Security; includes auditor testing and result (Most important out of the three)
- SOC 3: less detailed, intended to be publicly available

Two types

- Type 1
  - Controls are suitably designed
- Type 2
  - Controls are suitably designed and operating effectively

8.41 PCI-DSS

- More stringent
- Focused on credit cards
- Avoid if possible
- If must be involved then reduce Cardholder Data Environment (CDE) as much as possible
- Reduce scope (Eg. WiFi, rest of network)
- Outsource if possible

9 AppSec,Security Testing, Physical Security

9.1 Secure Coding

- Principles
  - Least privilege
  - Separation of duties
  - Defense in depth
  - Non-repudiation
  - Strong authentication
- Build security in from the ground up
  - Easier
  - Cheaper
  - Faster
  - More effective
- Don't bolt it on after the face because it's
  - Difficult
  - Expensive
  - Slower/delay
  - Less effective
- Validate your input
  - Never rely on the client
- User secure protocols
  - Utilize encryption at rest and in transit
- Don't make assumptions
  - Trust and verify
- Open Web Application Security Project (OWASP)
- Courses on OWASP on Cybrary
- OWASP Zed Attack Proxy (ZAP)
  - Finds vulnerabilities while you are developing and testing
- Different types of scanning and testing
  - Netstat
  - Tcpdump/snoop
  - Port scanning
  - Fiddler
  - Network vulnerability scanning
  - Web app vulnerability scanning
  - Static code analysis
- Don't proceed with known vulnerabilities
  - Patch new ones that arise
- Never store or pass passwords in plain text

9.2 OWASP top 10 Security Risks

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

Common issues

- Cross-site Request Forgery (CSRF)
- Cross-site Scripting (XSS)
- SQL Injection
- Session Hijacking

9.3 SQL Injection

- Consider the code used to authenticate users and the database call
- Insufficient input validation may allow an attacker to input
  - Password' OR '1=1
- Resulting in
  - SELECT * FROM users WHERE name='john' AND password='password' OR '1=1'
- What about if it was
  - password'; DROP TABLE users;

9.4 Session Hijacking

- Victim visits website
- Attacker sniffs the traffic and captures the session
- Attacker replays the session to the webserver and hijacks the session

9.5 Cross-Site Request Forgery (CSRF)

- Victim visits website
- Victim visits attacker's site
- Page contains CSRF code
- Victim posts CSRF code to website.com

9.6 Buffer Overflows

- Program may become unstable, crash, or return corrupt info
- Can run other malicious code
- When a max of 8 bytes are expected then limit the amount of data written to the buffer to 8 bytes
- Eg. writing 10 bytes of data to an 8 byte buffer

9.7 Nmap

- Port scanner
- nmap -Pn 192.168.10.100-254
- nmap –top-ports 20 192.168.10.100
- nmap -sV <target>
  - Services
- nmap -Pn –script vuln 192.168.10.100
- nmap -A -T4 <target>
  - OS detection
  - Version
  - Script
  - Trace
  - Fast

9.8 Vulnerability Scanning

- Best practice is to scan before and after production launch
  - And after any changes and periodically
- Identify vulnerabilities based on open ports
- Maturity
  - External vulnerability scans
  - Internal vulnerability scans
  - Credentialed scans
  - Databases and network elements

Vulnerabilities exist due to

- End of life systems
- Embedded systems
- Lack of vendor support
- Poor coding
- Improper input/error handling
- Default configuration
- Resource exhaustion
- Etc

9.9 Penetration Testing

- Penetration testing
  - Ethical hacking - attempts to exploit vulnerabilities
  - Aka pen testing
- External
  - Targets external infrastructure to see how far outside attacker would get
- Internal
  - Mimics inside attack behind firewall with standard user access
- Blind testing
  - Pentesters only given company name
  - Takes longer
  - $$$
- Double-blind test
  - Blind testing and only a few people know
- Vulnerability analysis
- Password attacks
- Exploitation
- Blackbox testing
  - Pentester gets no information
- Whitebox testing
  - Pentester gets information
- Future terms?
  - Zero knowledge
  - Partial knowledge
  - Full knowledge
- Pre-engagement
  - Permission
  - Scope
- Reconnaissance
  - Passive
  - Active
- Post-exploitation
- Reporting

9.10 Terms

- White hat
  - Does not have any malicious intent
- Black hat
  - Has malicious intent
- Grey hat
  - Somewhere between white and black

9.11 Other Tools

- VirusTotal (read slide 35 Week 9)
- Security Onion (read slide 36 Week 9)
- Bro (Zeek)
  - Network analysis
  - NIDS
- Rita
  - Real intelligence threat analytics
- Suricata
  - Open source IDS
- pfSense
  - Open source firewall
- Wireshark, Tcpdump, Snoop, Ettercap
  - Packet capture

9.12 Physical Security

- Vancouver Riot
- Call Center/Social Engineering
- Copper Theft
- Encompasses a set of threats, vulnerabilities, and risks
- Similarities in language between physical and logical security
- Guards, fences, gates, cages
- Includes
  - Design and layout
  - Environmental components
  - Emergency response readiness
  - Training
  - Access control
  - Intrusion detection
  - Power and fire protection
- Tailgating
  - Gaining unauthorized access to a facility by following someone in that has access
  - Aka piggybacking
- Dumpster diving
  - Looking through garbage for valuable information
- Locks , safes, secure, cabinets, signs
- Walls, barriers, barricades/bollards, astragals
- Lighting, CCTV
- Access controls
- Air gaps, man traps
- Prevention/deterrent
- Detection, response
- Protect
  - People
  - Data
  - Equipment
  - Systems
  - Facilities
  - Assets
- Shoulder surfing
  - When someone watcher over your shoulder at what you're doing on your computer
- Consider convergence between physical and logical

  - Access controls
  - Access badges
  - Proximity cards for building access shifting to smart cards enabling PC login and multi-factor authentication
- Network security does not mean physical security is obsolete or legacy
  - You need both
  - Consider cases where attacker has physical access or steals your gear
- Device security
  - Docking station
  - Cable locks
  - Screen filters
- Environmental controls
  - HVAC
  - Hot/cold aisles
  - Fire suppression

9.13 Environmental Design

- Crime Prevention Through Environmental Design (CPTED)
- Physical environment can reduce crime by affecting human behavior

Three main strategies

- Natural access control
- Natural surveillance
- Natural territorial reinforcement

9.14 Fences

- 3-4ft
  - Deter casual intruders
- 6-7ft
  - Too tall to climb easily
- 8+ft
  - Deter more determined intruders especially with razor wire

9.15 Guards

- Observe and report
- Escorted access (accompanying visitors into, around, and out of facility), knowing where they are at all times

Visitors sign into "guest book"

- Who
- When
- Where
- Why

9.16 Door Types

- Vault doors, personnel doors, industrial doors
- Vehicle access doors
- Bullet-resistant
- Turnstile
- Mantraps

9.17 Locks

- Warded
- Tumbler
- Combination
- Electronic
- Proximity cards
- Biometrics

9.18 Personnel Security

- RUN
- HIDE
- FIGHT

9.19 Threat Categories

- Natural environment threats
  - Floods
  - Earthquakes
  - Storms and tornadoes
  - Fires
  - Extreme temperature
- Supply system threats
  - Power distribution outages
  - Communications
  - Interruptions
  - Interruption of other resources such as water, gas, air filtration
- Natural territorial reinforcement
  - Promotes feeling of community in the area and extends sense of ownership to the employees (Eg. Parks, courts, fields)
- Manmade threats
  - Unauthorized access (both internal and external)
  - Explosions
  - Employee errors and accidents
  - Vandalism
  - Fraud
  - Theft
  - Collusion
- Politically motivated threats
  - Strikes
  - Riots
  - Civil disobedience
  - Terrorism
  - Bombings
- Natural surveillance
  - Visibility of areas to discourage crime
  - Organized (security guards)
  - Mechanical (CCTV)
  - Large windows
  - Open benches

Assessment

- Construction material of wall and ceilings
- Power distribution systems
- Communication paths and types
- Surrounding hazardous materials
- Regulations and legal issues
- Exterior components (proximity to airports, highways, railroads, electromagnetic, interference, vehicle activity, neighbors)
- Eg. external warehouse door

Selection criteria

- Visibility
  - Desired visibility depends on organization and processes being carried out
- Surrounding area and external entities
  - Consider nature of operations of surrounding businesses
- Accessibility
  - Ease with which employees and responders can access facility
- Natural disaster
  - Likelihood of floods, tornadoes, earthquakes, hurricanes, etc

9.20 Physical Security - Examples

- Store examples
  - Greetings on entry, rulers on doors of stores
  - Too many posters on exterior
- Example
  - Financial organization doesn't have a secure recycling bin/shredder
- Controlling vegetation and bushes
  - Obstructing signs, lights, doors
  - Tailgating examples
- Locked door may not be sufficient
  - Consider the motivation

9.21 Design Goals

1. Deter criminal activity (layout and policies)
2. Delay intruders (add impediments – locks/fences/barriers, slow and monitor people)
3. Detect intruders (allow criminal activity to be detected)
4. Assess situation (actions to be taken when event occurs)
5. Respond to intrusions and disruptions (appropriate responses to intruders and disruptions)

9.22 Design

Natural access control

- Follow the flow of people
- Consider placement of doors, lights, fences and landscaping to satisfy security goals in least obtrusive and most appealing manner
- Consider security zones with different classifications

9.23 Layered Defense

Shouldn't rely on any single physical security concept but on use of multiple approaches that support one another

9.24 Fire Suppression

- Wet pipe
  - Water in the pipes
- Dry pipe
  - Water in a tank not in the pipes
- Preaction
  - Springhead has thermal fusible link
- Deluge
  - Large amounts of water

Halon gas

- Works by chemically reacting with fuel, oxygen, ignition src
- Myth that Halon takes O2 out of air
- Debatable whether it kills people

9.25 Fire Extinguishers

- Class A
  - Stands for Ash
  - Wood and Paper
  - Extinguish with water and soda
- Class B
  - Stands for Boil
  - Liquid, Flammable gasses
  - Extinguish with gas and soda acid
- Class C
  - Stands for Current
  - Electrical Current
  - Extinguish with non-conductive like gas
- Class D
  - Stands for Dilute
  - Combustible Metals
  - Extinguish with dry powder

9.26 Business Continuity Plan (BCP)

- Plans and framework to ensure business can continue in an emergency
- Continuation of critical business processes in an organization using different people, equipment, facilities
- Proactive
- Provide procedures for sustaining essential business operations while recovering from significant disruption
- Long term planning of ensuing business can continue if emergency happens
- Minimize cost associated with disruptive event and mitigate risk

4 Elements

1. Scope and plan initiation
2. Business impact assessment (BIA)
3. Business continuity plan development
4. Plan approval and implementation ..... Maintenance

- Business Impact Analysis
  - Detailed and documented process to identify and prioritize business functions and workflow, including establishing Recovery Time Objectives by assessing impacts over time that might result if an organization was to experience a disruptive event
- Business Priority Service
  - Business function or process that is not mission critical, but should it not be performed, could lead to the loss of a major government service
- Critical Services
  - General term that collectively refers to Business Priority and Mission Critical services
- Recovery Time Objectives (RTO)
  - Amount of time that a business function can withstand an interruption before a negative or unacceptable consequence occurs
  - Time allowed to recover systems
    - Max amount of time process or system will be unavailable
- Recovery Point Objectives (RPO)
  - The point in time, relative to pre-disaster, at which available data from backup can be restored
  - Max amount of data loss or work loss for a given process (Eg. weekly backups RPO = 1 week)
- Mean Time Between Failures (MTBF)
  - How frequent are failures
- Availability Formula
  - MTBF / (MTBF + MTTR) = Availability
- Mean Time to Repair (MTTR)
  - How long to repair equipment on average
- Work Recovery Time (WRT)
  - Time required to configure systems
- Minimum Operating Requirements (MOR)
- Maximum Tolerable Downtime (MTD) Formula
  - MTD = RTO + WRT
  - Period of time after which the organization would suffer considerable pain if the process were unavailable

9.27 Business Impact Assessment (BIA)

Identify the impact of a disruptive event on the business

- Quantitative (Eg. Financial)
- Qualitative (Eg. Brand)

3 Goals of BIA

1. Criticality prioritization
2. Maximum tolerable downtime estimation
3. Resource requirements

- Identify which business units are critical to maintaining operations
- Catalog of important business processes and criticality
- Loss impact analysis quantitative and qualitative
- Ensure remember to establish criticality levels to assist with prioritization

Steps

- 1) Information gathering
- 2) Risk analysis and threat assessment
- 3) Determine key metrics
  - Maximum tolerable downtimes
  - Recovery time objective
  - Recovery point objective
- 4) Develop impact statements

9.28 BCP Development Approach One

1. Identify the business areas
2. Engage the stakeholders
3. Develop and populate the plan
4. Communicate and educate on the plan
5. Test the plan
6. Review and update on a regular basis

9.29 BCP Development Approach Two

1. Identify critical functions and priorities for restoration
2. Identify support systems needed by critical functions
3. Estimate potential outages and calculate the minimum resources needed to recover from the catastrophe
4. Select recovery strategies and determine what vital personnel, systems, and equipment will be needed to accomplish the recovery
5. Determine who will manage the restoration and testing process
6. Calculate what type of funding and fiscal management is needed to accomplish these goals

9.30 Disaster Recovery

- Refers to Information Technology (IT) recovery
- Disaster Recovery Plans (DRPs)
  - Document process to recover and restore technology (computer processing, applications and data) needed to support critical business functions

Mission Critical Services

- Functions and processes that, should the not be performed
  - Could lead to loss of life or injury
  - Personal hardship to citizens
  - Major damage to the environment
  - Significant loss of revenue or assets

9.31 Disaster Recovery Plan (DRP)

- What actions need to be taken to restore IT operations as quickly as possible
- Assessment, salvage, repair, and eventual restoration of damaged facilities and systems
- DRP is the effort to recover IT system and applications whereas BCP is effort to recover business processes
- Reactive
  - When an IT disaster strikes
- Detailed procedures
  - Facilitate recovery of capabilities at an alternate site
- Recover from emergency with minimum impact on business
- Plan for before, during, and after the event
- Objective is to move critical processes to an alternate site and return primary site and normal processing within a timeframe that minimizes loss
- People are the number one priority
- Management approved plan
  - Addresses operational processes for the recovery of damaged facility
- Hot site
  - Fully configured computer facility with electric power, heating, ventilation, and air conditioning (HVAC) and functioning file/print servers and workstations
    - Has all hardware and critical app data mirrored in real time (resume operations in ¡ 1hr)
- Warm site
  - Computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC), limited file/print servers and workstations
    - Data may not be in real time, backups may be required
    - MTD between 1 and 3 days with 24-48 hr recovery time
- Cold site
  - Computer facility available with electrical power, heating, ventilation and air conditioning (HVAC)
    - No computer hardware (long MTD required)

Data Center alternatives

- Electronic Vaulting
  - Transfer of backup data to offsite location (transfer occurs over connectivity)
- Remote Journaling
  - Parallel processing of transactions to alternative site (transfer occurs

live)

  * Provide redundancy for transactions

- Database Shadowing
  - Uses live processing of remote journaling but creates more redundancy by duplicating database set to multiple servers

9.32 Differences between BCP and DRP

BCP

- Activities required to ensure continuation of critical business processes in an organization
- Alternate personnel, equipment, and facilities
- Often includes non-IT aspects of business

DRP

- Assessment, salvage, repair, and restoration of damaged facilities and systems
- Often focuses on IT systems

9.33 Backup Strategies

- Full
  - All files are backed up modified or not (archive bit is reset)
- Incremental
  - Archive data that has changed since the last full or incremental backup (archive bit is rest)
- Differential
  - Archive data that changed since the last full backup only (archive bit isn't reset)