CISSP® 2015

Domain 7: Security Operation

V1

Domain 7: Security Operation

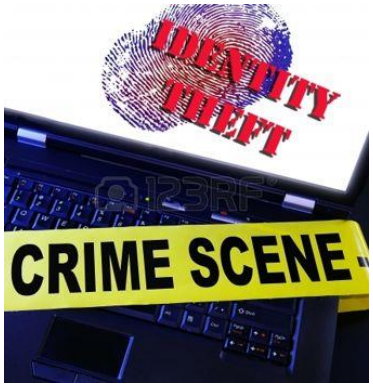
- Operation Security incudes:
  - Investigation
  - Logging Monitoring
  - Asset protection
  - Incident management
  - Operation
  - Patch management
  - Change management
  - Recovery strategies
  - Disaster recovery

A. Understand and support investigations

- **Investigations**
  - **Many names**: Computer forensics, Digital forensics, Network forensics, Cyber forensics and Electronic data discovery….
  - Security Professional should understand Legal requirement, **chain of custody for evidence**, what type of evidence is admissible in court, **incident response procedure** and escalation process.

Crime Scene

- **Before investigation**, agents must handle the crime scene
- **Crime scene =** an environment in which potential evidence may exist
- **Criminalistics principles:**
  1. **Identify** the scene
  2. **Protect** the environment
  3. Identify **evidence** and potential sources of evidence
  4. **Collect** evidence
  5. **Minimize** the degree of **contamination**



General Principles

- Cannot be **too detail** or rigid as a checklist
- Apply general forensic and **procedural** principles
- **Protect** evidence
- All activity **log** (seizure, access, storage or transfer etc.) must be documented, preserved and available for review
- **Training** is required
- Individual is responsible for **compliance** with principles

Investigations

- **Incident Response**
  - **Incident** is a series of events that **negatively affects** the company and/or impacts its security.
  - **Example**: virus, insider attack, terrorist attack….
  - Prevent for **destroying** evidence (such as reboot…)
  - Develop incident response team (include senior mgt, Network, security officer, ….)

Incident Handling and Response Procedure

1. Triage Phase:

- **Detection**: false-positive? Severity? Prepare for escalation
- **Identification**: type of incident, apparent source
- **Notification**: determine what type of notification is required, to senior management, vendor, manager….

2. Investigative Phase

- **Containment**: migrate the damage, example physically take out infected workstation from network
- **Analysis**: Root cause; how, who, when and why the incident happens
- **Tracking**: parallel with Analysis; to track internal or external; eg. Log review

3. Recovery Phase

- Recovery and Repair

Chain of Custody (CoC)

- In legal contexts, CoC (=log) refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

A2. Reporting and documenting

- If suspected crime related, **report to senior management** immediately to decide whether it should conduct internally or report to law enforcement.
- **If Report to law enforcement** seizure
  - Company loses control over investigation
  - Become public
  - May effect on reputation
  - Evidence will be custodied for long period of time

A2. Reporting and documenting

- **Five rules** of evidence in the court:
  - Be authentic
  - Be accurate
  - Be complete
  - Be convincing
  - Be admissible

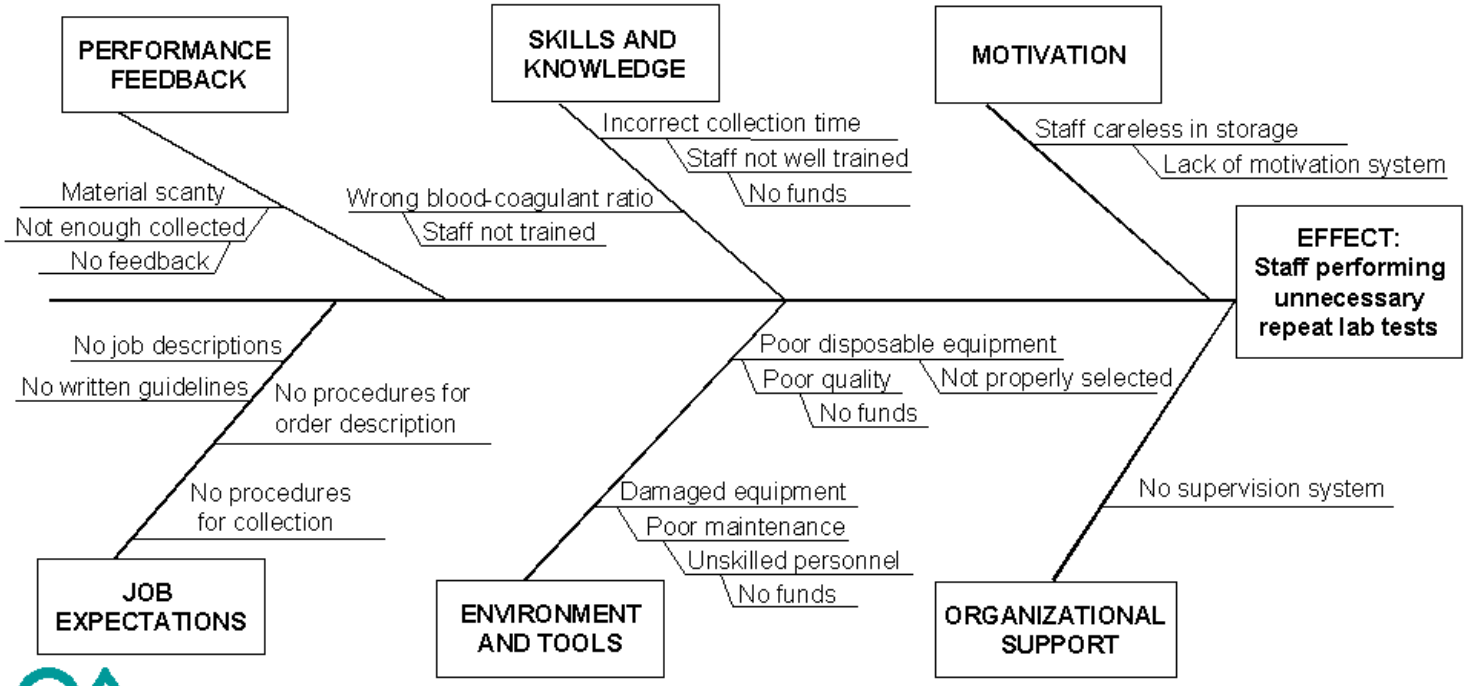
A3 Investigative techniques

- **Root-cause analysis**: identifying the root causes of faults or problems.
- **Purpose**: Prevent the final undesirable event from recurring; Continuous improvement.
- **Limitation** of RCA: too few source data, data quality, lack of trust, openness, and honesty.
- Examples: **5 Whys** is an iterative question-asking technique used to explore the cause-and-effect relationships underlying a particular problem.
  - The vehicle will not start. (the problem)
  - 1.Why? - The battery is dead. (first why)
  - 2.Why? - The alternator is not functioning. (second why)
  - 3.Why? - The alternator belt has broken. (third why)
  - 4.Why? - The alternator belt was well beyond its useful service life and not replaced. (fourth why)
  - 5.Why? - The vehicle was not maintained according to the recommended service schedule. (fifth why, a root cause)

Example of RCA - Fishbone

MAQ EXCHANGE

Using Fishbone Technique in Root-Cause Analysis



QUALITY ASSURANCE PROJECT

14-16

A4. Digital forensics
(Media, Network, Software, embedded devices)

- **Computer Forensics and Proper Collection of Evidence**
  - **Digital Forensics:** The use of scientifically derived and proven **methods** toward the **preservation, collection, validation, identification, analysis, interpretation, documentation and presentation** of digital evident derived from digital source for the **purpose** of facilitating or furthering the reconstruction of events found to be **criminal**…….
  - Investigation **without corrupting original evidence**

The Forensics Investigation Process

- Make two copies, **primary image** stored in library; **working image** (for analysis and collection)
- Must be in **bit level copy** to capture deleted file, slack space and unallocated cluster
- Marking and labeling of evidence
- Handle with gloves and placed into containers and sealed

Digital forensics - Networks

- **Network forensics** is relating to the monitoring and analysis of computer network traffic for the purposes of (1) information gathering, (2) legal evidence, or (3) intrusion detection.
- It is often a **pro-active** investigation, as Network traffic is transmitted and then lost.
- An attacker **might erase all log files on a compromised host**, so investigators might therefore base on the only evidence available for identifying for traffic and intrusions.
- **Examples**: transferred files, searching for keywords, emails or chat sessions to collect evidence.

Digital Forensics – Software Analysis

- Software forensics is to collect evidence from the examination of software **source code, binary, decompiled code.**
- Purposes:
  - **Author identification** of malware (virus, worm etc.) by analysis of program style, language, development toolkits, embedded comment and address etc.
  - Determine **intention**: Carelessness bug?
  - Find the destination address of **Trojan Horse** program
  - Provide expert opinion on how similar programs in **intellectual property disputes**

Digital forensics – Embedded devices

- **Examples** of embedded devices: Mobile, smartphone, PDA etc.
- Use special **tools and techniques** to image/copy the information on motherboard, CMOS chip etc.
- Then examine the content
- But many embedded devices cannot be read or copied

Other considerations of Investigation

- **Role of the First-Responde**r: Certain precautions, Simple shutting-down may destroy evidence
- **3I:**
  - Information: always needed
  - Instrumentation: Investigate financial crime involving digital forensic, such as review money transaction for money laundering
  - Interviewing: Directly gather information from related people
- **Evidence Collection and processing**: Lawfully, warrant is required
- **Jurisdiction**: authority; Complicated in cross-border environment

B5. Electronic discovery (eDiscovery)

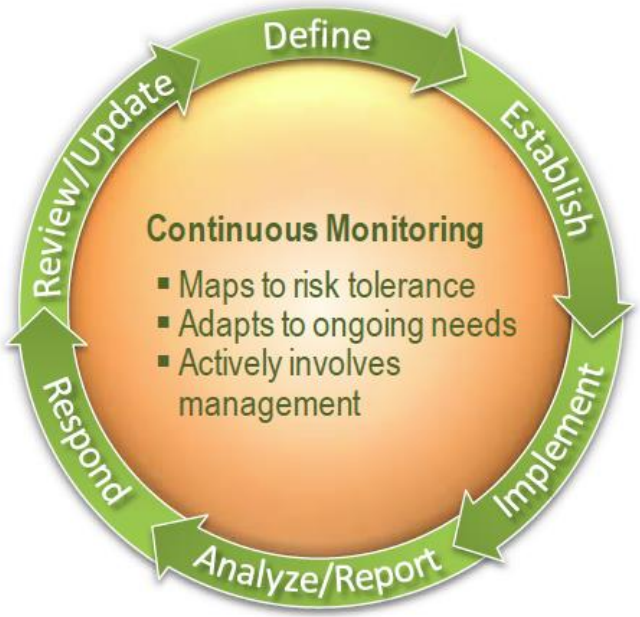
- eDiscovery refers electronic data is **sought, located, secured, and searched** with the intent of using it as evidence in a civil or criminal **legal** case.
- Digital data is difficult or impossible to completely destroy, particularly if it gets into a network.
- **Evidence types** include text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites, computer programs, email, etc.
- E-discovery is applied in the fields of legal, political, security and personal privacy issues, etc.

C. Logging & Monitoring Activities Through IDS, IPS and SIEM

- **IDS & IPS**: contains log, rules to detect or prevent intrusion.
- **SIEM: Security Information and Event Management**
  - Store **raw** information form various system logs
  - **Aggregate** information in a single repository
  - **Normalize** information to make comparisons more meaningful
  - **Analytical** tools can process, map and extract target information
  - **Alerting and reporting** tools

C3. Continuous monitoring

- **Continuous monitoring** is the process and technology used to **detect** compliance and risk **issues**.
- **Benefit**: **detects** weak or poorly designed or implemented controls, then to **correct** or **replace**, thus enhancing the organization's risk profile.
- Purpose: **Continuous Improvement**



C4. Egress Monitoring

- **Egress Control**: **monitoring** and potentially **restricting** the flow of information outbound from one network to another (Typically, Internal network to Internet).
- Allow/limit certain servers and protocols, such as HTTP/HTTPS, SMTP etc. to transit to Internet.
- On-going maintenance of Egress filter list is required for new server or service.
- Beware of spoofing, DoS (as filtering is required), Single Point Of Failure (SPOF)

Data Leak/Loss Prevention (DLP)

- **DLP is a technical solution** by focusing **location, classification and monitoring** of information at-rest, in-use and in-motion.
- **At-rest:** DLP solution can identify and log where sensitive information such as Credit card info are stored, open spreadsheet and document to search
- **Data-in-Motion (Network):** by monitor traffic, reconstruct files, scan any sensitive information
- **Data-in-Use (End Point):** ability to monitor copying to thumb drive, printing, even cutting and pasting between applications for any sensitive information
- **Classification:** what is sensitive information, such as Customer, employee, financial data, intellectual property

Steganography

- **Steganography** is the science of hiding information
- **Steganography**: Ancient Greek words, “steganos” meaning "covered, concealed, or protected", and “graphein” meaning "writing".
- **Digital form**: Text in JPEG, video, voice,
  - **Control**: compare original copy, compression errors may detect some unusual format
- **More sophisticated**: (1) hide information within image or audio files (2) encryption
- This may create Data Leak/Loss

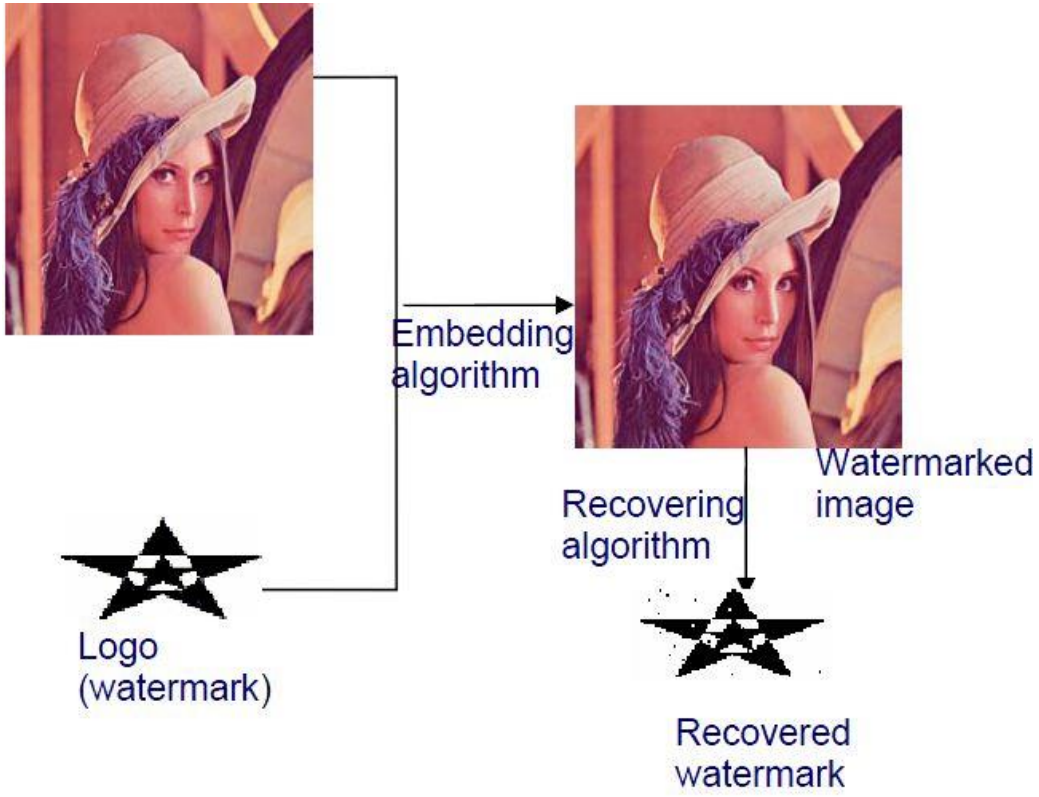
Steganography

hidden in

a subsequent **normalization** of color is required.

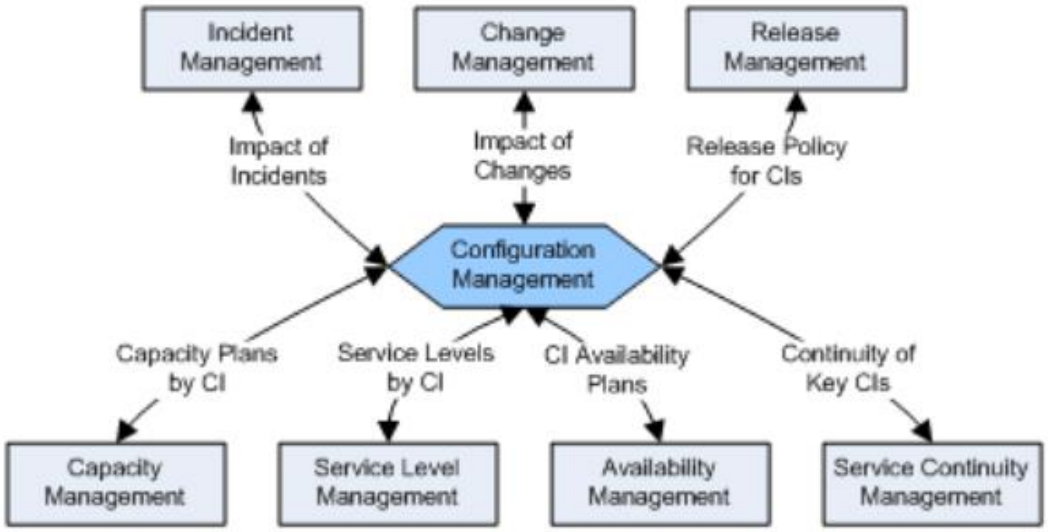
Watermarking

- **Digital watermark** is to identify ownership of the copyright of Document, Video, Voice signal by embedding a **noise-tolerant** signal.
- Example: Graphic artist posted sample images on website with an embedded signature, so that he can later prove their ownership in case others attempt to violate the copy rights



D. Secure the provisioning of resources

- **Configuration Management (CM)** is the discipline of identifying, recording, evaluating, tracking, coordinating, reporting, and controlling Configuration Items (CI)
- CI can be Hardware device, applications, programs and source codes etc.
- CM can maintain the program version, ownership, relationship, previous change history etc.
- **Asset Inventory** is a simplified version of CM.



D. Secure the provisioning of resources

- A full configuration management system includes:
  - **Physical assets**: server, laptop, tablet, smartphone etc.
  - **Virtual assets**: Software Defined Network (SDN), Virtual SAN (vSAN), Virtual machine (VM)
  - **Cloud assets**: Service, Fabric, Storage network, Tenant
  - **Applications**: workload (application type) in private clouds, Web service, Software as a Service (SaaS)

E. Understand and apply foundational security operations concepts

- **Key Themes (of Operation)**
  1. **Maintaining Operational Resilience**
  2. **Protecting Valuable Assets**
  3. **Controlling System Accounts**
  4. **Managing Security Services Effectively**

- **Least Privilege**: **absolutely** require in order to perform job duties.
- **Need-to-know**: business need to have access to resources, normally based on Position.

E. Understand and apply foundational security operations concepts (E1 to E4)

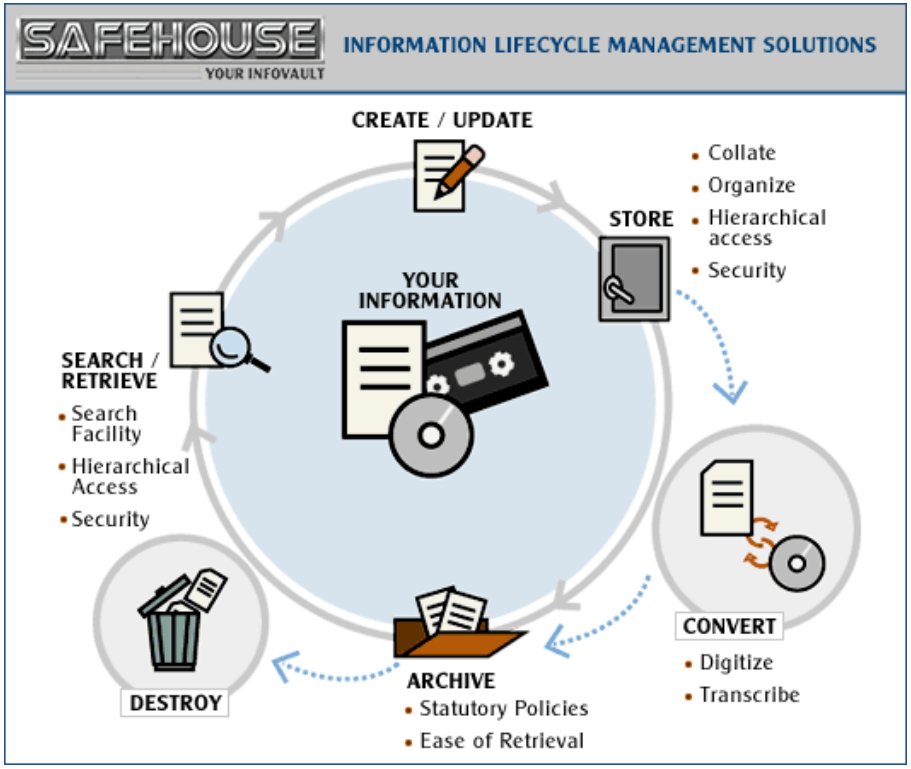
- **Rotation of duties** (Rotation of assignments): prevent key man dependency
- **Separation (Segregation) of duties**: dual control (eg. Input, check, approve done by different staff)
- **Monitor special privileges:** high security significant (such exceptions or administrator activities) must be monitored
- **Clearances, Suitability and Background Checks** for privileged accounts
- **Account Validation**: review of account activity, Inactive account may be due to departure, long leave or no use.

E. Understand and apply foundational security operations concepts (E1 to E4)

- **Managing Accounts Using Groups and Roles:** Role-based access control is more effective
- **Account types:**
  - **Root or Built-in Administrator Accounts**
  - **Service Accounts**
  - **Administrator Accounts**
  - **Power Users**
  - **Ordinary or Limited User Accounts**
  - **Operators**
  - **Help/Service Desk Personnel**

E5. Information lifecycle

- Information Lifecycle
  - **Creation**: ownership
  - **Use**: classification
  - **Destruction**: securely



E6. Service-level agreements (SLA)

- **Service-level agreement (SLA)** is document describing the level of service **expected** by a customer from a supplier.
- Particular aspects of the service - **Scope, Quality, Responsibilities, Metrics, Bonus/Penalty, Indemnity** etc**.**
- **An indemnity** is an **obligation** by a service provider to provide **compensation** for a particular loss suffered by customer.
- **Metric**: Service Availability, Defect rates, Technical Quality, Security

F. Employ resource protection techniques

F1. Media Management

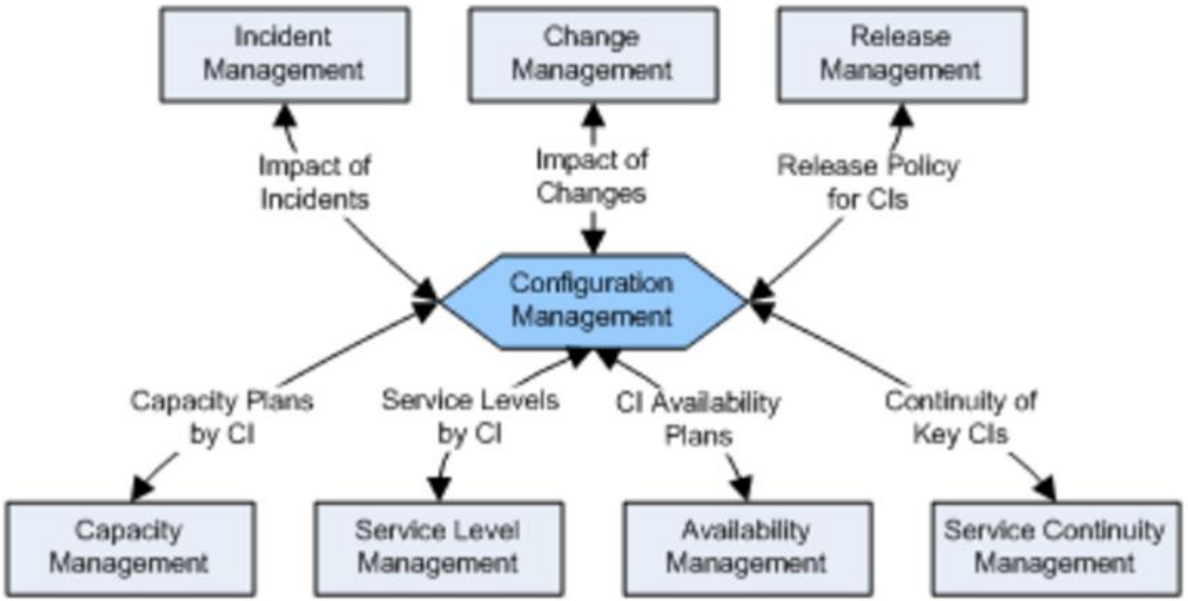
- **Media includes** soft copy & hard copy, Magnetic, Optical, Solid-state (flash drives and memory cards)
- Consider **encryption**: built-in, not only storage, but transmission, snapshots, shadowing, backup, vaulting
- **Removable Media**: pay more attention:
  - Easy to leave, to breach, not willing to report
- **Archival vs. Backup**
  - **Archival**: information for historical purpose only; saved and removed from system
  - **Backup**: regular basis, useful in recovering when disaster

F. Employ resource protection techniques
F1. Media Management

- **Hard Copy Records:**
  - **Risks:** fire, flood, hurricane, explosions, smoke, contamination, water damage etc.
  - **Controls:** Secure, clean and stable containers, making copies (scan or microfiche), off-site,
- **Reassign or reuse or disposal:**
  - **Delete, format**: not actually remove information
  - **Degausser**: reduce magnetic field to zero
  - **Software overwrite**: may need multiple times
  - **Destruction**: shedding, burning, grinding (磨) , pulverizing (使成粉末)

F2. Hardware and software asset management

- Again, Asset Management keep track the inventory of assets.



G. Conduct incident management (IcM)

- **IcM** is to **restore** a normal service operation as **quickly** as possible and to **minimize** the **impact** on business operations, thus ensuring that the **best** possible levels of service quality and availability are maintained.
- General Steps:
  - **Detection**: alert, user report
  - **Response**: understand and analysis
  - **Mitigation**: minimize the impact (eg. detach virus pc from Network)
  - **Reporting**: Ticketing, Escalation, to Senior Management
  - **Recovery**: Restore the service
  - **Remediation**: try to prevent (or escalate to Problem Management)
  - **Lessons Learned**: Continuous improvement

Problem Management

- **Problem Management**
  - Aim to **resolve** issue through investigation & in-depth analysis to **identify root cause**
  - Mainly cover major incident or several repeated incident

H. Operate and maintain preventative measures (H1..H4)

- **Firewall & Router**: Boundary Control
  - Rules change management, patch management
- **Whitelisting / Blacklisting**: email, LAN, Protocol, Application, Telephone #, FAX #
  - Maintain updated list
- **Third-Party Security services**
  - Regular Review; Update procedure, SLA and Contract

H2: Intrusion Detection & Prevention System

- **IDS**: Designed to **spot** something suspicious or to **determine** whether attack is underway, then send **alerts** or perform very limited **response**, say reconfigure Firewall
- **Two targets:**
  - **Network-Based IDS (NIDS):**
    - To detect **network** traffic, packet or protocol
  - **Host-Based IDS (HIDS):**
    - to detect any inappropriate or anomalous activities of **host or application**, such as deleting system file, reconfigure important setting etc.

IDS Methods - Signature

- **Signature- or Pattern-Matching systems**
  - **Signature**: how attacks are carried out are developed
  - **Example**: A packet has the same source and destination IP
  - Require **regular update** of signature
  - **Weakness**: only identify known attacks

IDS Methods - Anomaly

- **Anomaly approach:**
  - Learning mode to build “normal” activity profile (a period of time, say 2 to 4 weeks)
  - Future traffic will be compared to “normal” profile
  - Can detect “zero day” attack or “low and slow” attack
  - Higher false positive error

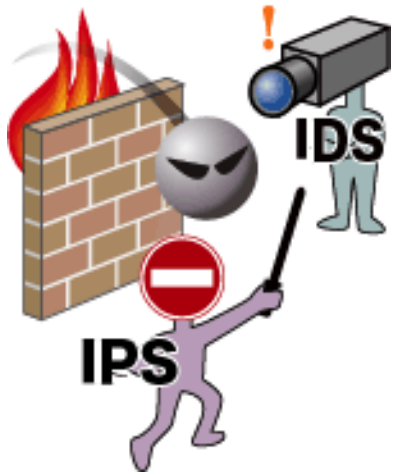
  1. Statistical Anomaly-based IDS
    - **Examples:** Multiple failed log-on attempts; Users logging in a strange hours; Unexplained changes to system clocks; shutdowns, etc.

  2. Protocol Anomaly-Based IDS
    - But many vendor don’t strictly follow the protocol rule

  3. Traffic Anomaly- Based IDS
    - Changes in traffic pattern (Denial-of-service attack (DoS))
    - Highly dynamic environment, it may be difficult or impossible

Intrusion Prevention Systems (IPS)

- **IDS is copying** traffic and perform analysis & let original data goes thru, **detective** & **after-the-fact**
- **Intrusion Prevention Systems (IPS)**
  - to **detect** the intrusion activity, **send** alerts and **block** the intrusion
  - **IPS is preventive**, but can be traffic bottleneck



H. Operate and maintain preventative measures (cont.) (H5. Sandboxing)

- **Sandboxing**: security mechanism for separating running programs (untested, untrusted or unverified code) in a form of software virtualization.
- Typically provides a **tightly** controlled resources (disk, memory, network) for guest programs to run in
- **Example**: Virtualization, Jail, Capability

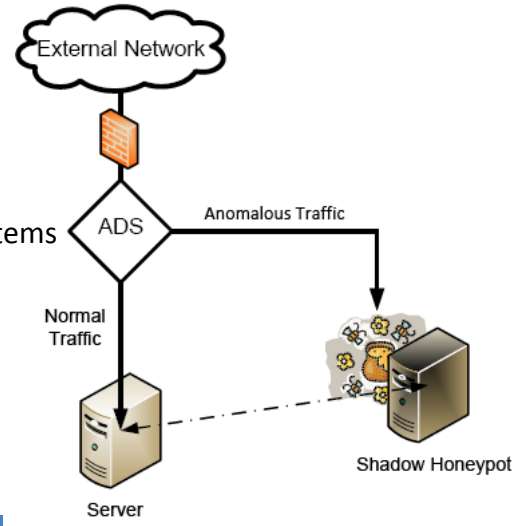
Change Management & Configuration Management

- **Change Management**
  - Request
  - Impact assessment
  - Approval/Disapproval
  - Build and test
  - Notification: notify users about proposed change and schedule of deployment
  - Implementation
  - Validation
  - Documentation
- **Configuration Management**
  - Record or inventory of Configuration Item (CI)
  - **Hardware**: Make, model, MAC, Serial number, OS, Firmware, Location, IP, CPU, HD size, etc.
  - **Software**: Name, Vendor, Version, License expiration, Contact, etc.
  - Extension of Change Management

H6. Honeypot/Honeynet/Honeyfarm

- **Honeypot**
  - Pretend vulnerability to lure the hackers, but no real information inside
  - enable administrator to know any potential attack is happening
  - **enticement** (legal): open ports
  - **entrapment** (illegal): saying web page to download illegal software
- **Honeynet**
  - **Two or more honeypots** on a network form a honeynet.
  - Typically, a honeynet monitors a **larger** and/or more diverse network in which one honeypot may not be sufficient.
- **Honeyfarm** is a centralized collection of honeypots and analysis tools.

ADS: Anomaly Detection Systems



H7. Anti-malware

- Anti-Malware
  - Signature update, version upgrade, patch, procedure

I. Implement & support patch & vulnerability Mgt.

- patch to production in a controlled fashion and always have a rollback plan
- **Step 1: Infrastructure**
  - create strategy
  - assemble a team
  - including software and hardware
- **Step 2: Research**
  - verify source by fingerprint or digital signature etc.
- **Step 3: Assess and Test**
  - test environment which is close to production
  - test plan
- **Step 4: Mitigation (Rollback)**
  - all necessary step to get back to the operational state prior to the installation

Patch Management

- **Step 5: Deployment (Rollout)**
  - phased approach
  - pilot less critical group first
  - use automated script or deployment tools to reduce human error
  - patching windows should be outside of peak hour
- **Step 6: Validation, Reporting and Logging**
  - log what, where when and how
  - document standard build and configuration
  - confirmation of all systems: manual inspection or scanning tools

Patch Management

- **Limitation to Patching**
  - doesn’t guarantee success
  - incompatible or inoperable with unpatched system
- **Best Practices**
  - patch management tools
  - backup before patch
  - update inventory
- **Anything else?**
  - to buy time for patch, ensure other measures such as hardening, least privilege, firewall and end-point security

Question

A system has been patched many times and has recently become infected with a dangerous virus. If antivirus software indicates that disinfecting a file may damage it, what is the correct action?

A. Disinfect the file and contact the vendor

B. Back up the data and disinfect the file

C. Replace the file with the file saved the day before

D. Restore an uninfected version of the patched file from backup media

J. Participate in and understand change management processes

- **Change Management**
  - Request
  - Impact assessment
  - Approval/Disapproval
  - Build and test
  - Notification: notify users about proposed change and schedule of deployment
  - Implementation
  - Validation
  - Documentation
- **Configuration Management**
  - Record or inventory of Configuration Item (CI)
  - **Hardware**: Make, model, MAC, Serial number, OS, Firmware, Location, IP, CPU, HD size, etc.
  - **Software**: Name, Vendor, Version, License expiration, Contact, etc.
  - Extension of Change Management

K. Implement recovery strategies

K1. Backup storage strategies

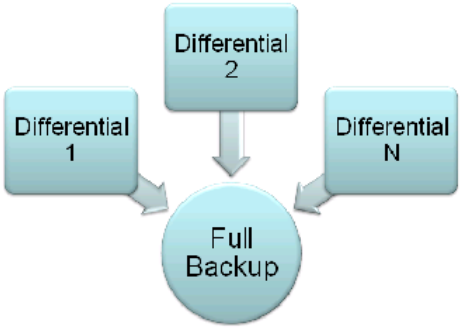
- **Choosing Offsite storage facility:**
  - Balance the risk of site lost and convenience of offsite access (such as single disaster damage vs. access timeframe)
  - Physical security: cannot be lowered
  - Bonded transport and storage service
  - Administrative control: how, who, when can get the tapes?

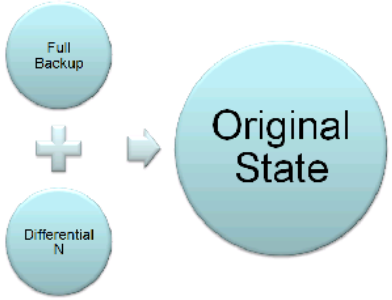
Electronic Backup Solutions

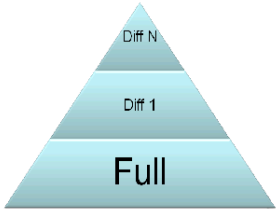
- **SAN (Storage Area Network) / NAS (Network Attached Storage): own system resilience**
- **RAID (Redundant Array of Independent Disk)**
  - **RAID 0 –** No protection
  - **RAID 1 –** Mirror
  - **RAID 5 –** Data & parity are stored across all drives. If lost one, can be rebuilt
- **RAIT (Redundant Array of Independent Tape)**

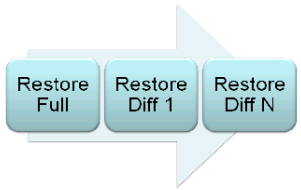
Tape rotation

- **Full:** all data, archive bit is clear
- **Differential**: backup files modified since the last full backup, ***does not change archive bit***. Restore requires Full & Differential backup. Differential backup is getting bigger.
- **Incremental**: backup files modified since last full or differential backup; **change archive bit**. Restore requires Full and n Incremental backup.









Data Backup

- **Considering:**
  - Backup policy & **procedure**: daily, weekly, monthly, yearly, transaction log, online backup etc.
  - Stored onsite and offsite
  - Stored in fire-resistant, heat-resistant waterproof safe

K2. Recovery site strategies

- **Different Strategies – Operation Alternatives**
  - **Surviving Site:** Operated in **at least two geographically** dispersed buildings; fully equipped and staffed; Service level may drop, but never ceased.
  - **Self-Service: Transfer work** to another own location
  - **Internal Arrangement:** staff travels to training room, cafeterias, conference room of another site
  - **Reciprocal agreement (or Mutual Aid Agreement)**: company A agrees to allow company B to use its facility if company B is hit by disaster and vice versa. Difficult in configuration management; security issue in missing of operation; not suitable for very specific technology and equipment (newspaper printing);
  - **Dedicated alternate sites**: built by company to accommodate business functions
  - **Work From Home**:
  - **External suppliers**: by Disaster Recovery vendor
  - **No arrangement**: for low priority business functions

Facility Recovery

- **Different Strategies – Data Center:**
  - **Hot site**: A facility is fully configured and ready to operate within a few hours. Equipment and software must be ***compatible*** from main site. Only missing resources are usually data (need restore), people (relocation). Can be tested annually; **Can be internal (by company) or external (by DR vendor)**
  - **Warm site**: usually partially configured with some equipment, but **not computers**; cannot be tested; less expensive
  - **Cold site**: supplies **basic environment**, electrical wiring, air conditioning, plumbing and flooring, but none of the equipment or additional services. May take weeks to get ready;
  - **Tertiary Site**: secondary backup site if primary backup site failed as well; usually network infrastructure ready (say in frame relay network); backup to the backup; **Plan B if Plan A does not work out**.
  - **Redundant Site (or Mirror Site)**: is equipped and configured **exactly** like the primary site; most expense;
  - **Rolling hot (or Mobile) site**: implemented by truck or trailer has all necessary power, telecommunication and system to allow processing
  - **Multiple processing centers (or Dual data center)**: backup by other data center in the organization; **operationally redundant system**

Questions

Which of the following is the best way to ensure that the company's backup tapes can be restored and used at a warm site?

A. Retrieve the tapes from the offsite facility and verify that the equipment at the original site can read them.

B. Ask the offsite vendor to test them and label the ones that were properly read

C. Test them on the vendor's machine, which won't be used during an emergency

D. Inventory each tape kept at the vendor's site twice a month

Which best describes a hot-site facility versus a warm- or cold-site facility?

A. A site that has disk drives, controllers, and tape drives

B. A site that has all necessary PCs, servers, and telecommunications.

C. A site that has wiring, central air, and raised flooring

D. A mobile site that can be brought to the company's parking lot

K4. Staffing for Resilience

- Considering
  - Proper training
  - Adequate level of staff
  - Cross training for key man dependency
  - Call tree
  - Hotel arrangement

L. Implement disaster recovery processes

1. Response
2. Personnel
3. Communications
4. Assessment
5. Restoration
6. Training and Awareness

L1. Response

- **Consideration,** once an event is identified
  - Prepare for **24 X 7** as events happen 24 X 7
  - **Assessment** of damage
  - Notify **senior management**
  - **Declare** disaster if necessary
  - **Call tree**: (1) safety (2) employee need to understand
  - Organize and control **Command Centers**
  - Organize and provide **administrative** support to the recovery effort
  - Administer and direct the **problem management** function
  - Require to predefine **who, when, what, where, how**

L2 Personnel

- **Human Resource**: get HR involves, say temporary housing; new hire; executive succession Planning; travel different plane; keep senior executive in distance
- **Disaster recovery teams**
  - Various teams: such as Damage Assessment team, Legal team, Media relation team, Network recovery team, relocation team, restoration team, salvage team, security team, telecommunication team understand
  - Pre-assigned and properly **trained** and let team members understand the responsibility, task etc.

L3. Communications

- **Crisis Communication**: can turn risk to opportunity
- **Rosenthal U. & Charles M.:** "A serious threat which, under **time pressure** and highly **uncertain** circumstances, necessitates making critical decisions.
- Has to be simple, direct & honest
- Predefined Spokesperson(s)
- **Targets**: Employee, Customer, vendor, contractor, regulator, media, External Stakeholder, etc.

L4. Assessment

- **Assessment**: Preliminary but fairly accurate onsite **evaluation** of damage for **disaster declaration and claim.**
- **Example of Categorization**
  - **Non-Incident**: System malfunction or human error → **minor** disruptions
  - **Incident**: Cause entire facility or service to be **inoperative**
  - **Severe Incident**: **Significant** interruption to organization's mission, facility and personnel.

L5. Restoration

- **Restoration** of the **primary** environment and transition back to normal operations
- **Pre-planned** and documented
- Need to **contact legal and insurance** companies
- Evidence & **photo** for damage before anything is removed, repaired, or replaced

L6. Training & awareness

- Assist in providing an understanding of, as well as developing skills and competencies in, business continuity management.

M. Exercise, Assess, and Maintain the Plan

- test regularly (**at least annually**) or **significant changes** in the organization
- **Tabletop Exercise / Structured Walk-Through Test:** through discussion; **purpose**: responsibility, training, awareness
- **Walk-Through Drill / Simulation Test:** practice and validation specific functional response
- **Functional Drill / Parallel Test:** a full drill, parallel processing is performed and compare to production results
- **Full-Interruption / Full-Scale Test**: ***shut-down original site*** and processing takes place at the alternate site for **longer period of time**; a lot of planning, but can reveal many holes

Question

How often should a business continuity plan be tested?

A. At least every ten years

B. Only when the infrastructure or environment changes

C. At least every two years

D. Whenever there are significant changes in the organization.

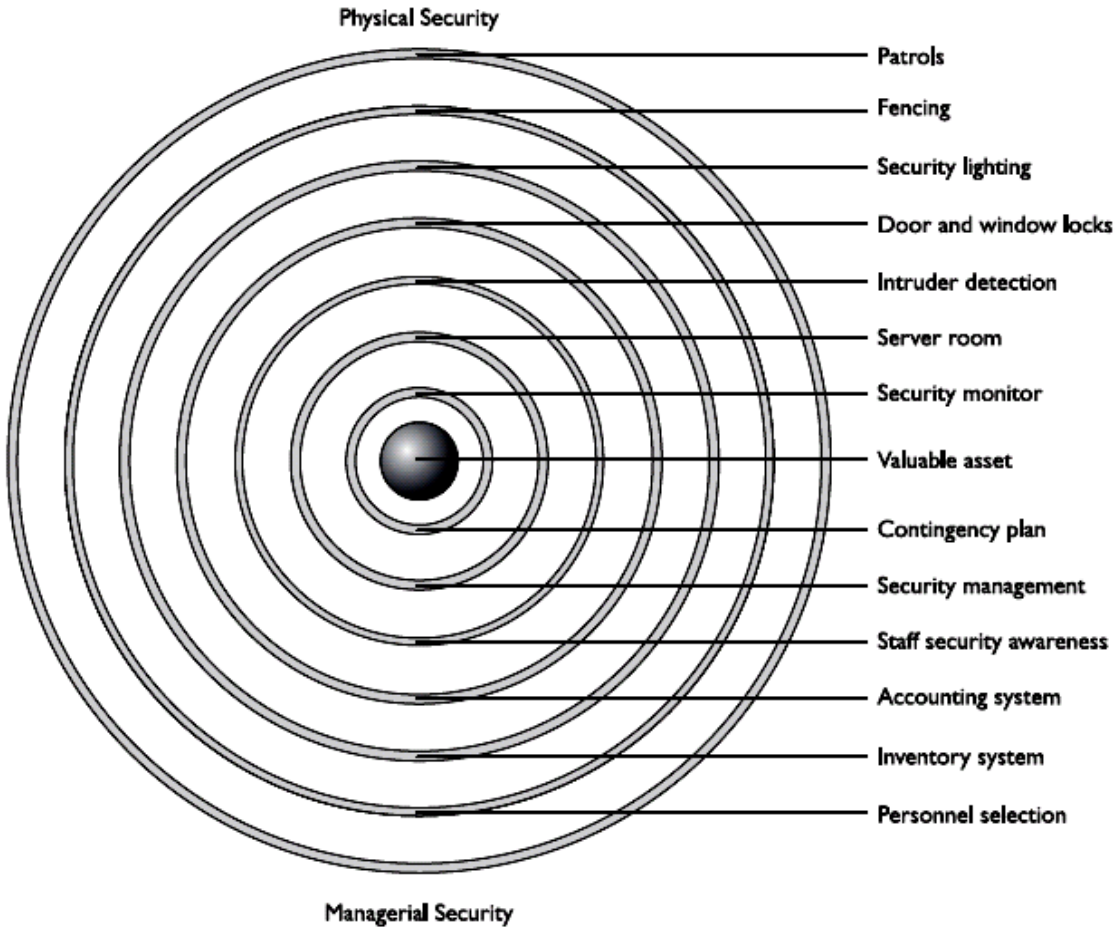
N. Participate in BCP and exercises

- BCP is company specific and **company wide** project.
- Departments should participate in every part of BCP, such as BIA, planning, developing, exercising, training, revising etc.
- The purpose of BCP is **not from audit**.
- BCP Drill is **not just a rehearsal**, but to ensure the company ability.
- Participants should **follow the plan** during exercise.

O. Implement & manage physical security

- **Layer defense approach**, from outer to the protected asset
- **Two modes**: One for **normal operation**, another one for facility is **closed**

§ Deals with facility, personnel access control, external boundary protection mechanism, intrusion detection and corrective actions



O1. Perimeter

- **External boundary Protection Mechanism**
- control types:
  - access control mechanism: lock, key, card, personnel awareness
  - Physical barrier: fence, gate, wall, door, window….
  - Intrusion detection: sensor
  - Assessment: guard, cctv
  - Response: guard, local law enforcement
  - Deterrent: sign, lighting, environmental design

External

- **Barriers**
  - **Natural:** River, dense growth (of brushwood), culvert, ditch (溝)
  - **Man-made:** Wall, **Fence**, door, gate, building itself
- **Fences**
  - Effective physical barrier
  - Only delay or psychological deterrent
  - Crowed control and access control
  - Can be costly (maintenance) and unsightly (not good looking)
  - **Gauge of the metal**: thickness of the wire diameter
  - **Mesh size**: distance between the wires
  - **Height of fence**

External

- **PIDAS** (Perimeter Intrusion Detection and Assessment System): sensor located on the wire mesh and the base of the fence; detect cutting and climbing
  - **Infrared Sensors**: detect heat; consider change in temperature
  - **Microwave**: detect by sending and receiving wave
  - **Coaxial Strain-Sensitive Cable**: Detect climbing or cutting
  - **Time Domain Reflectometry (TDR) System**: send radio frequency (RF) signal to fence fabric; when climbing or flexing will create signal path flaw
  - **Video Content Analysis and Motion Path Analysis**
- **Bollard**
  - small concrete pillar outside the building
  - prevent vehicle driving to exterior wall

Lighting

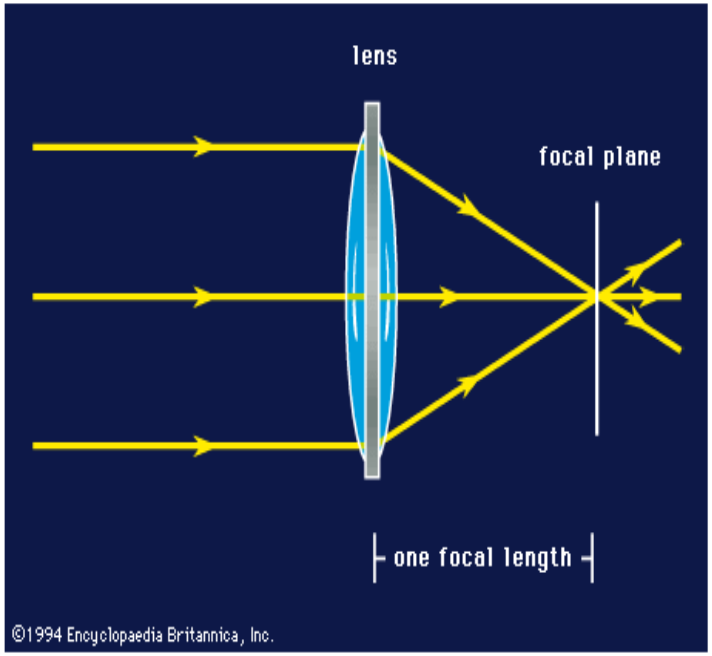
- criminal in dark area
- **Light coverage**: depending on wattage capacity of the bulb, should be positioned in correct distance
- **Continuous lighting:** provide even amount of illumination across an area
- If near airport, highway, railway, does not “bleed over”
- **Standby lighting**: even when resident are away
- **Responsive area illumination**: IDS detect something and turn on the light
- Lighting control and switch should be protected, locked and centralized area
- **Glare Protection:** light directed toward intruder coming from and directed away from the security force.

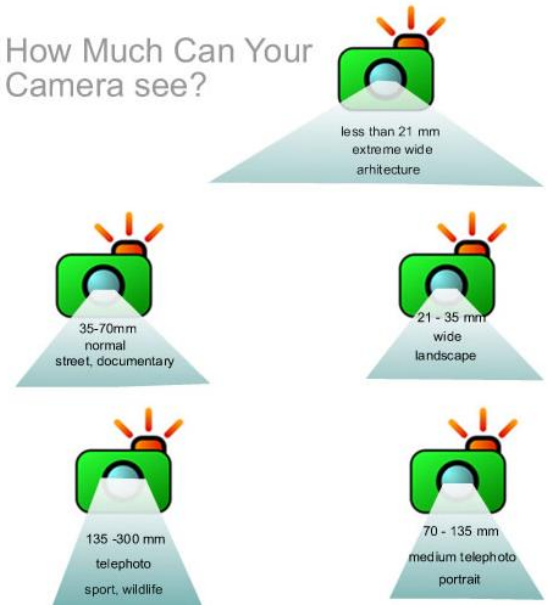
CCTV

- can be visual detection or sophisticated means of detecting abnormal behavior.
- **Visual Recording Devices**
  - Closed-circuit TV (**CCTV**): commonly used monitoring device
  - **Consider**: purpose, internal or external, large or small area, lighting, guard, ids, alarm etc.
  - CCTV made of camera, transmitter, receiver, recording system and monitor
  - **Provide**: Surveillance, Assessment, Deterrence, Evidentiary Archives
  - Multiple camera connect to one **multiplexer**
  - Camera's transmitter to the monitor's receiver, usually a coaxial cable, **closed circuit**
  - Common **attack**: replay previous recording
  - CCTV camera use light-sensitive chips called "**Charged-Coupled Device** (CCD)"
  - CCD receive light from lens and convert into electronic signal.
  - CCD also use in fax, photocopier, barcode reader…

CCTV

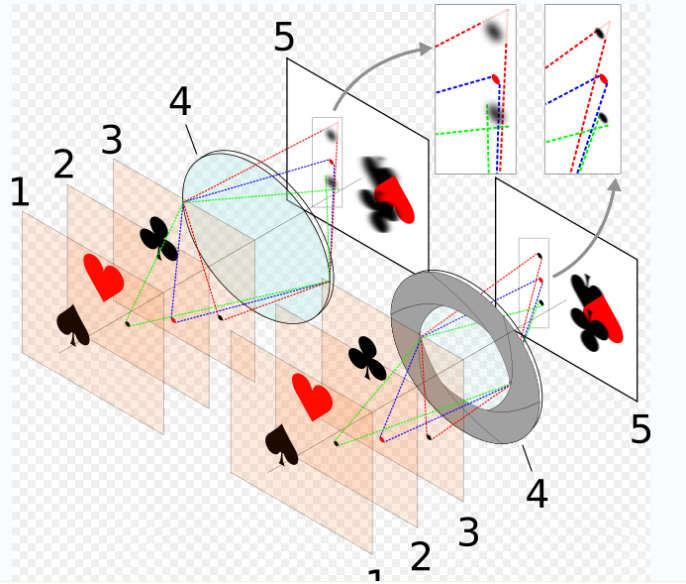
- **Focal length of a lens** defines effectiveness in viewing object
  - Short focal length provide wider-angle view
  - Can be fixed and zoom (varifocal) of focal length





CCTV

- **The depth of field**: the portion of environment that is in focus
  - Depth of field increase as the size of lens opening decrease, the subject distance increase or the focal length of the lens decrease
  - If want to cover large area and not focus on specific items, better use wide-angle lens and a small lens opening.



CCTV

- **Iris**: control the amount of light that enter lens
  - Iris can be manual or auto
  - Manual: fix lighting or normal inside
  - Consider Lighting requirement;
    - **Light-to-Dark Ratio**
    - **Black/White Switching**: auto switch to color at day and B&W at night
- **Mounting camera**: can be fixed or movable
- **PTZ** capabilities: Pan (up/down/left/right), tilt (rotate), zoom (in/out)

CCTV

- Other specification: **Resolution, Frames per Second (FPS) and Compression**
- **Annunciator** system: Notification system; either “listen” or motion detector, then activate lights, sirens, or cctv camera
- **Internet Protocol (IP) Cameras**: different from CCTV
  - **Pros**: can view anywhere in the network (ie internet)
  - **Cons**: least secure (within internet), high bandwidth,

IDS

- **Intrusion detection system**
  - Surveillance to watch unusual behavior; IDS sense changes
  - IDS can detect changes in the followings:-
    - Beams of light
    - Sound and vibration
    - Motion
    - Electrical circuit
    - Different type of field (microwave, ultrasonic, electrostatic)

2 X IDS

1. Volumetric System (by Wave)

- **Photoelectric system (or photometric system or Infrared Linear Beam Sensors):** detect change in infrared light beam; emit a beam hits the receiver; can be invisible or visible beam (or use special goggles); can be cross sectional by mirror; like Mission Impossible or James Bond movies
- **Passive infrared system (PIR**): detect change of heat wave
- **Acoustical detection system**: to detect sound; install floor, wall; false alarm by picking up noises from Air Conditioner or telephone ringer.
- **Wave-pattern motion detector**: send diff waves (microwave, ultrasonic and low frequency), reflect back, if return pattern altered, something is moving.
- **Proximity detector (or capacitance detector**): emit measurable magnetic field, alarm if the field is disrupted, used to protect specific objects (eg. artwork or safe)

2 X IDS

2. Electromechanical system: break circuit

- **Magnetic contact switch (or Balanced Magnetic Switch [BMS])**: alarm if contact is separated, used in window, door
- **Vibration detector**: detect movement on wall, ceiling which wires embedded with the structure are broken
- **Pressure pad**: someone step on the pad

- **Dual-technology Sensors**:
  - two independent technology devices; such **Microwave + Passive infrared system (**PIR)

- IDS: expense, **human intervention is required**; redundant power, **fail-safe** (default to “activated”)

Question

If an access control has a fail-safe characteristic but not a fail-secure characteristic, what does that mean?

A. It defaults to no access

B. It defaults to being unlocked

C. It defaults to being locked

D. It defaults to sounding a remote alarm instead of a local alarm

Patrol & Dog

- **Patrol force and guard**
  - one of the best security mechanism
  - more **flexible**; provide good **response**
  - costly, sometimes unreliable
  - fully trained
  - IDS and physical protection ultimately require human intervention
  - Consider**: Proprietary (employee), Contract & Hybrid**
- **Dogs**
  - proven highly useful in detecting intruder
  - hearing and sight and intelligence and loyalty
  - intensive training, can smell smoke
  - provide good supplementary security mechanism

Audit & drill

- **Auditing Physical Access**
  - **log**: should include date, time, entry point, user id, unsuccessful access…..
  - periodically review
  - **detective not preventive**
- **Testing & drills**
  - evacuation and emergency response plan must be developed and documented
  - easily accessible
  - provide training
  - test or drill at least once a year
  - predetermined scenario and specific parameter and scope

Questions

When is a security guard the best choice for a physical access control mechanism?

A. When discriminating judgment is required

B. When intrusion detection is required

C. When the security budget is low

D. When access controls are in place

What is a common problem with vibration-detection devices used for perimeter security

A. They can be defeated by emitting the right electrical signals in the protected area.

B. The power source is easily disabled

C. They cause false alarms

D. They interfere with computing devices

Questions

Which of the following is an example of glare protection?

A. Using automated iris lenses with short focal lengths

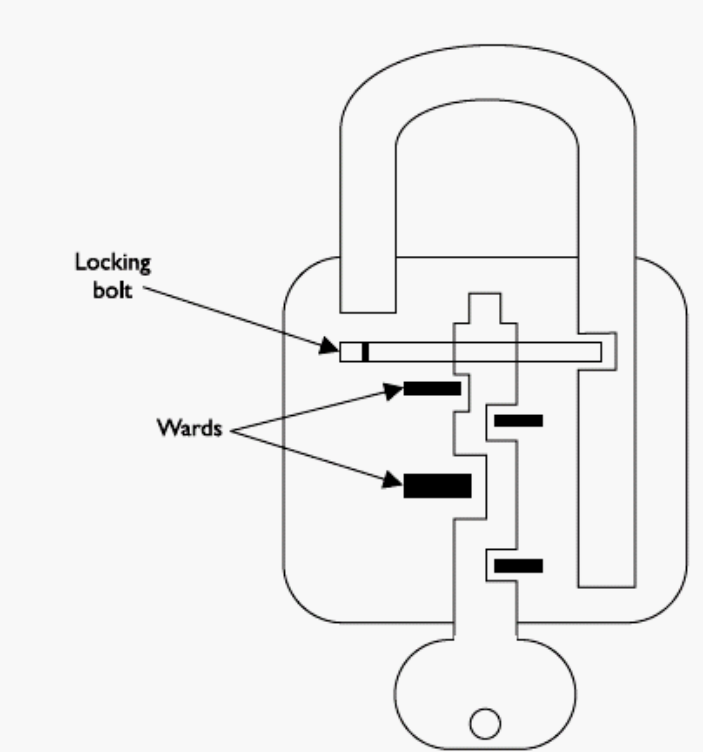
B. Using standby lighting, which is produced by a CCTV camera

C. Directing light toward entry points and away from a security force post

D. Ensuring that the lighting system uses positive pressure

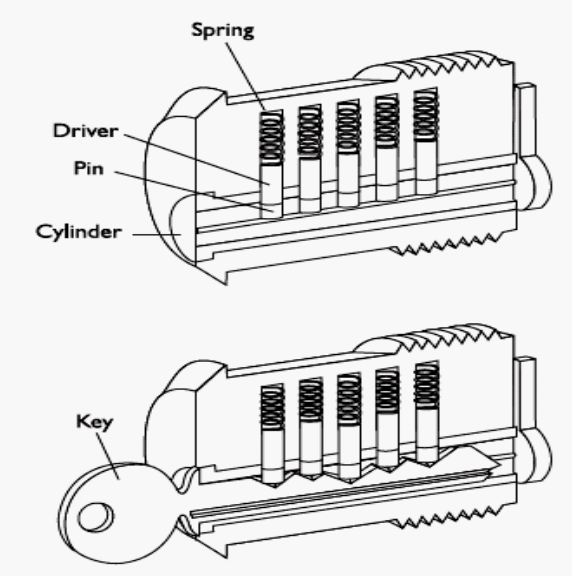
O2. Internal security

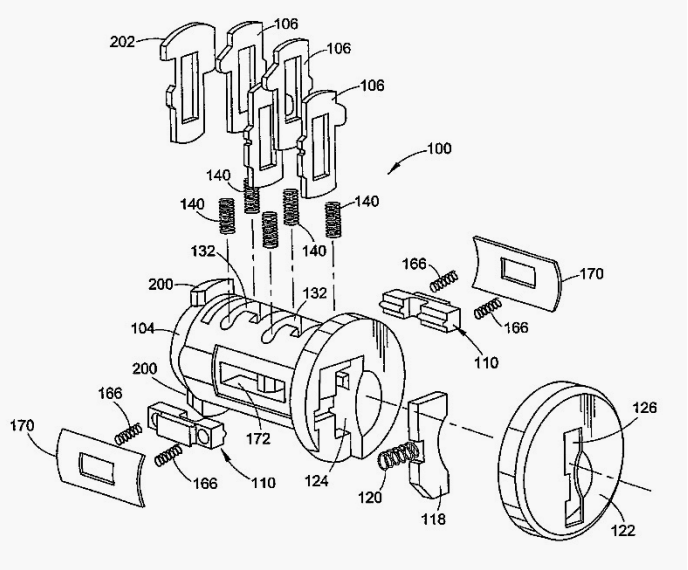
- **Facility access control**
  - enforced through physical and technical components here
- **Locks**
  - inexpensive; widely accepted,
  - **delaying** device to intruder, not a deterrent
  - **Mechanical Locks**
    - **1. Warded lock**: has spring-loaded bolt with a notch cut in it. Cheapest locks, easiest to pick,



Lock

- **2. Tumbler lock (or Locking Cylinders)**:
  - key fits into a cylinder, which raises the lock metal pieces to the correct height so the bolt can slide to the locked or unlocked position.
  - 2 types of tumbler locks: **Pin** tumbler, **Wafer** tumbler (or **Disc** tumbler





§ **Combination lock**: use combination of number, left and right spin;

Lock

- **Electronic Locks**
  - **Electronic Combination Lock** has key pad
  - **Cipher lock**: or programmable lock, keyless, use keypad, combination + possibly swipe card
    - **Door delay**: alarm if door open for a given time
    - **Key override**: programmed emergency combination to override normal procedure
    - **Master Keying**: enable supervisor to change access code and other features
    - **Hostage Alarm**: a combination can open and alarm to guard or police station, in case under hostage
    - Can be same combination or unique individual and audit log
    - Or call “smart lock”
  - Must have backup battery system and set to unlock during a power failure (for person safe)

Other Locks

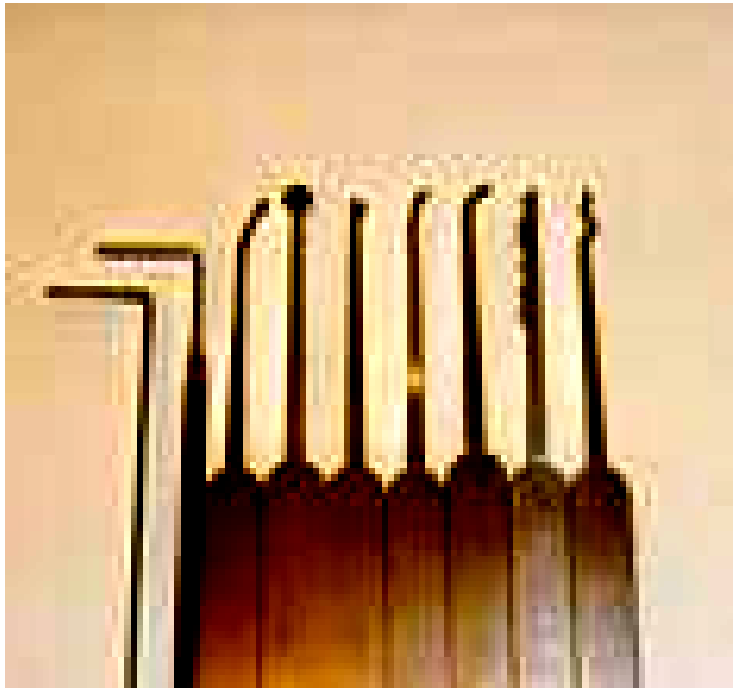
- **Device Locks**
  - **Slot locks**: use of steel cable, eg notebook, projector etc
  - **switch control**: cover on/off power switches
  - **Port control**: block access to disk driver and ports
  - **Peripheral switch control**: Secure keyboard by inserting an on/off switch
  - **Cable traps**: prevent the removal of input/output devices by locking cable
- **Biometric Readers**
  - Fingerprint, Facial Image, Hand Geometry, Voice Recognition, Iris Patterns, Retinal Scanning, Signature Dynamics, Vascular Patterns (血管), Keystroke Dynamics

Lock

- **Administrative Responsibilities**
  - **procedure** how to assign, inventory, destroy the key and document key holder
  - master key: open all locks
  - sub-master key: open one or more locks
  - key should be properly guarded and **not widely share**

Lock

- **Circumventing Lock**
  - **Pick** the lock: open without the key
  - **Tension Wrench**: a tool; L shaped, use to figure out the correct setting for each pin
  - **Raking**: a technique; push to the back of the lock and quickly slid out while providing upward pressure
  - http://www.youtube.com/watch?v=JZJe23UD8wU



Question

Which of the following best describes the difference between a warded lock and a tumbler lock?

A. A tumbler lock is more simplistic and easier to circumvent than a warded lock

B. A tumbler lock uses an internal bolt and a warded lock uses internal cylinders

C. A tumbler lock has more components than a warded lock

D. A warded lock is mainly used externally and a tumbler lock is used internally

Escort requirement / visitor control

- Understand visitor's purpose and SOW.
- Visitor need to be **registered** and **authenticated**, say checking contract, name card, staff card etc.
- Provide visitor **minimum** physical and logical **access** (such waiting area, meeting room, broadband, visitor pass etc.)
- **Detective**: Visitor log and log review
- **Preventive**: Escort

P. Participate in addressing personnel safety concerns

- CISSP #1 concern is people safety and life
- **Duress** (or coercion): a situation whereby a person performs an act as a result of violence, threat or other pressure against the person.
- **Travel restrictions**: government announced alert or warning
- Do not travel on the **same plane** for senior managements
- Put the senior managements in **different locations**