CyIntegriti

UNCOMPLICATE SECURITY

CISSP – Chapter 7 Security Operations

Key Points

- Prudent Person Concept
  - A person who takes responsible, careful, cautious and practical actions
  - He how follows due care and due diligence
- Operations Security
  - All about ensuring People, Process, and Technology are adequately secured
  - It is the practice of continual maintenance to keep the environment running at a necessary security level.
  - Goal is to reduce the possibility of damage that could result from unauthorized access or disclosure
- Administrative Management
  - It is the most important piece of Operations management
  - One aspect is dealing with personnel issues.

Administrative Management

- **Separation of Duties**
  - Objective is to ensure one person acting alone cannot compromise the security of a system in any way
  - Activities should be broken down into different parts and given to different individuals or departments
  - Collusion – more than one person having to work together to commit a fraud
  - It helps prevent mistakes and minimizes conflicts of interest

- **Separation of Privilege**
  - Similar to Separation of duties, but builds upon the principle of least privilege and applies it to applications and processes.
  - Requires the use of granular rights and permissions
- **Segregation of duties**
  - Goal is to ensure the individuals do not have excessive system access that may result in conflict of interest
  - Most common implementation of segregation of duties policy is ensuring that security duties are separate from other duties

Administrative Management

- **Need-to-know Access**
  - Access is granted only to data or resources that are needed to perform a task
  - It is commonly associated with security clearances of subject
  - Restricting access based on need-to-know helps protect against unauthorized access resulting in a loss of ***confidentiality***

Administrative Management

- **Principle of Least Privilege**
  - Subjects are granted only the privileges necessary to perform the assigned task
  - It protects ***confidentiality and Integrity***
  - Typically it is focused on user privileges, but it can also be applied to processes and applications

Administrative Management

- **Entitlement**
  - Amount of privileges granted to the users, typically during first time provisioning
- **Aggregation**
  - Amount of privileges the user collects over time
- **Transitive Trust**
  - Extends the trust relationship between two security domains to all of their subdomains
  - It allows subjects from one domain to access objects in the other domain

- **Nontransitive** trust does not extend the trust relationship to their subdomains. It enforces principle of least privilege and grants the trust to a single domain at a time

Administrative Management

- **Two-Person Control**
  - Also called two-man rule, requires approval of two individuals for a critical task
  - It ensures peer-review and reduces opportunity for collusion and fraud
- **Split knowledge**
  - Combines the concept of separation of duties and two-person control
  - No single person has sufficient privileges to compromise the security of the environment

Administrative Management

- **Job Rotation**
  - Employees are rotated through jobs
  - Provides peer-review, controls fraud and enables cross-training
  - It can act as a deterrent and detective control
- **Mandatory vacation**
  - Employees are required to take one-week or two-week vacations mandatorily
  - Provides peer-review, helps detect fraud and collusion
  - It can act as a deterrent and detective control

Administrative Management

- **Clipping Levels**
  - Predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious
  - To goal is to alert if a possible attack is underway within the network
  - In most cases IDS software is used to track these activities and behavior pattern

Assurance Levels

- **Operational Assurance**
  - Concentrates on the products architecture, features, and functionality
  - Examples: access control mechanisms, separation of privileged and use program code, auditing and monitoring capabilities, covert channel analysis, trusted recovery
- **Life-cycle Assurance**
  - Pertains to how the product was developed and maintained
  - Ex: design specifications, clipping-level configuration, unit and integration testing, configuration management, and trusted distribution

Trusted Recovery

- When an operating system or application crashes, it should not put the system in any type of insecure state
- Types of failures can be classified as
  - **System Reboot**
    - Takes place after a system shuts itself-down in a controlled manner in response to a kernel failure
    - It releases resources and returns the system to a more stable and safe state

Trusted Recovery

- **Emergency System Restart**
  - Takes place after a system failure happens in a ***uncontrolled manner***.
  - It could be caused by lower privileged subject accessing memory segments that are restricted
  - The kernel or user object could be in inconsistent state and data could be lost or corrupted
  - System goes into maintenance mode and recovers from the actions taken
- **System Cold Restart**
  - Takes place when unexpected failure happens and the regular recovery procedure cannot recover the system to a more consistent state
  - Intervention by the user may be required to bring back the system to recover the system

After a system crash

1. **Enter single user or safe mode:**
    1. In this mode the system does not start the services for users or the network
    2. File systems typically remain unmounted and only the local console access is available
    3. Administrator must either be physically at the console or have deployed external technology to connect the system remotely (KVM)
2. **Fix Issue and recover files**
    1. In single user mode, administrator salvages damaged files and also attempts to find the cause of the shutdown to prevent it from happening
    2. Administrator then brings the system out of single user mode
3. **Validate critical files and operations**
    1. Administrator must ensure validate the contents of configuration files and ensure system files are consistent with their expected state

Input and Output Controls

- **Aspects to be considered with I/O**
  - Data entered into a system should be in correct format and validated
  - Transactions should be *atomic* – they cannot be interrupted between the input provided and the output generated
  - Transactions must be timestamped and logged
  - Safeguards should be implemented to ensure output reaches the correct destination securely
  - If a report has no information, it should contain “no output”

Service Level Agreements

- It is an agreement between an organization and an outside entity, such as a vendor
  - It stipulates performance expectations and often includes penalties if the vendor doesn’t meet these expectations
- Memorandum of Understanding (MOU)
  - Documents the intention of two parties to work together; it is less formal and doesn’t include monetary penalties if one of the parties doesn’t meet the responsibilities
- Interconnection Security Agreement (ISA)
  - If two or more parties plan to transmit sensitive data, ISA can be used to specify the technical requirements of the connection
  - It provides information on how the two parties establish, maintain, and disconnect the connection

Managing Hardware and Software Assets

- Hardware Inventories
  - Radio frequency identification (RFID) methods significantly reduce the time needed to perform an inventory
  - They are expensive than the barcode and barcode readers
- Software Licensing
  - Ensuring systems in the organization uses only authorized software installed
  - Installing pirated software is not only a ethical violation but also both a liability risk and a potential vector for introducing malware

Managing Virtual Assets

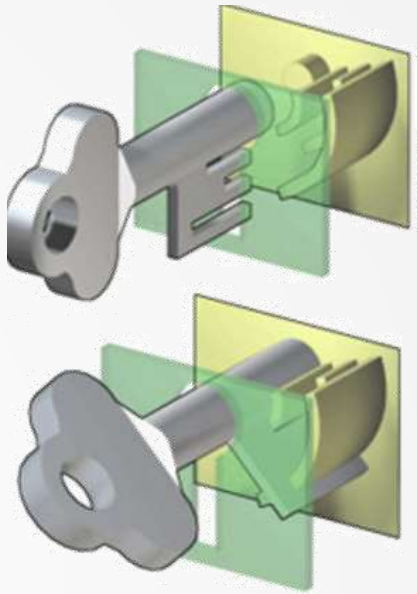
- The primary component in Virtualization is Hypervisor. It manages the VM, data storage, and virtual network components.
- **Virtual Machines (VM)**
  - VMs run as guest OS on physical servers. Physical servers will have extra processing, memory and disk storage to handle the VM Requirements
- **Software-defined Networks (SDN)**
  - Decouples the control plane from the data plane.
  - Control plane uses protocols to decide where to send traffic and the data plane includes rules to decide whether traffic will be forwarded
- **Virtual Storage Area Networks (VSAN)**
  - Virtualizing the SAN environment bypassing the complexity of SAN

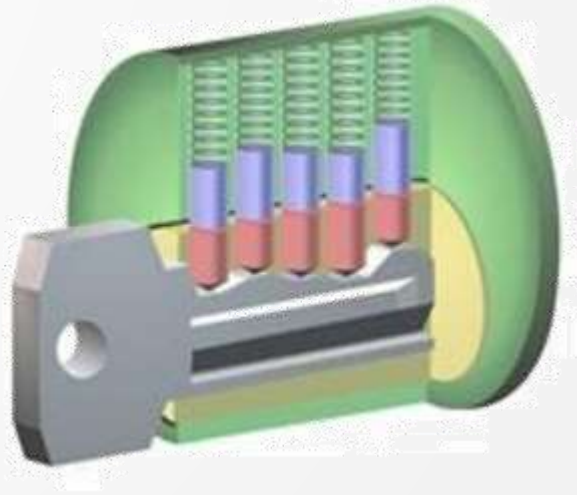
Physical Security - Locks

- Inexpensive access control mechanisms that are widely accepted and used
- They are considered delaying devices to intruders
- **Padlocks** – can be used on chained fences
- **Preset locks** – usually used on doors
- **Programmable locks** – used on doors or vaults

Mechanical Locks

- Two main types of mechanical locks
  - Warded lock
    - It is a basic padlock. It has a spring-loaded bolt with a notch cut in it
    - Cheapest locks, lacks any sophistication and easiest to pick
  - Tumbler Lock
    - Has more pieces and parts than a ward lock
    - The 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





Tumbler Locks

- Pin Tumbler Lock
  - Most commonly used tumbler lock
  - It uses pins of varying lengths to prevent the lock from opening without the correct key
- Wafer Tumbler Lock (disc tumbler lock)
  - Small, round locks found on file cabinets.
  - They use flat discs instead of pins inside the lock
  - Does not provide much protection
- Lever Tumbler Lock
  - uses a set of levers to prevent the bolt from moving in the lock.

Other Locks

- Combination Locks
  - Requires the correct combination of numbers to unlock them

- Cipher Locks
  - Also known as programmable locks
  - Are keyless and use keypads to control
  - Cost more than traditional locks, but has additional features like
    - Lockout, duress alarm etc.

Cipher Locks

- Cipher Locks functionality include
  - Door delay – if door is held open for a given time, an alarm will trigger
  - Key override – specific combination can be programmed for use in emergency situation to override normal procedures
  - Master keying – Supervisory personnel can change access codes and other features
  - Hostage alarm – Duress alarm combination

Circumventing Locks

- Tension wrench
  - A tool shaped like L and is used to apply tension to the internal cylinder of a lock
- Racking
  - To circumvent pin tumbler lock, a lock pick is pushed to the back of the lock and quickly slid out while providing upward pressure, this movement makes the pins fall into place
- Lock bumping
  - Force the pins in a tumbler lock to their open position by using a special key called a bump key

Lock strength

- Grade 1 = Commercial and industrial use
- Grade 2 = Heavy-duty residential/light-duty commercial
- Grade 3 = Residential/consumer
- Three categories of Cylinders
  - Low Security – No pick or drill resistance provided
  - Medium Security – A degree of pick resistance provided
  - High Security – Pick resistance protection through many different mechanisms

Personnel Access control

- Piggybacking
  - Piggybacking is when another person follows through a door WITH the permission of the person who has received access
- Tailgating
  - Tailgating is when another person, whether an employee or not, passes through a secure door without the knowledge of the person who has gained legitimate access through the secure door
- Best preventive measures are security guards, man-trap, user awareness

Fencing

- Delays intruders, psychological deterrent
- Can provide crowd control, helps control access to entrances and facilities.
- Can be costly and unsightly
- Height:
  - 3 to 4 feet – deters casual trespassers
  - 6 to 7 feet – considered too high to climb
  - 8 feet (with barbed wire) – deter more determined intruder
- Barbed wire tilted in is to deter someone exit the premises
- Barbed wire tilted out is to deter someone enter the premises

Fencing

- Gauge of the fence wiring is the thickness of the wiring mesh
- Lower the gauge number, larger the wire diameter
- Mesh sizing is the minimum clear distance between the wires.
- Fencing with smaller the mesh sizing and larger the gauge number are harder to cut
- PIDAS fencing is a type of fencing that has sensors located on the wire mesh and at the base of the fence
- PIDAS is very sensitive and can cause many false alarms

Gates

- Different Types
- Class 1 – Residential Use
- Class 2 – Commercial use, general public access is expected
- Class 3 – Industrial use, Limited public access is expected
- Class 4 – Restricted use, no public access, monitored via CCTV or guards

Lighting

- The higher the lamps wattage, the more illumination it provides
- Zones of illumination coverage should overlap
- Exterior lights provide less illumination intensity than interior working lights
- If the light is going to bounce of dark places, more illumination is required, if it bounces of clean concrete and light coloured surface then not much illumination is required
- Lighting should be directed towards area where potential intruders can gain access
- Glare protection – guards should be in shadows or under low illumination
- Lights should be directed outward
- Continuous lighting – an array of lights that provides even amount of illumination across an area
- Controlled illumination – should erect light such a way that it does not blind others close by
- Standby lighting – configure lighting to turn on and off, so potential intruders think different areas of the facility are populated
- Responsive lighting – lights get turned on specific areas when IDS detects suspicious activities

CCTV

- CCTV is made up of camera, transmitter, receiver, recording system and a monitor
- It sends captured data via the cameras transmitters to the monitors receiver via coaxial cable
- The most common type of attack against CCTV is the replay attack
- Cameras use Charged coupled devices (CCD)
  - Electrical circuit that receives input light from the lens can convert to electronic signal. Images are focused through a lens on to the CCD chip

CCTV

- Lens Types
  - Fixed Focal Length
  - Zoom
- Focal length defines its effectiveness in viewing objects from a horizontal and vertical view
- Shorter focal length provides wider-angle of view
- Fixed focal length lens does not allow the user to change the area that fills the monitor
- Optical zoom lens allow the viewer to change the field of view while maintaining the same number of pixels in the resulting image

CCTV

- Depth of field
  - Refers to the portion of the environment that is in focus when shown in the monitor
  - Small Depth of field is called Shallow focus and large Depth of field is called deep focus
  - Depth of field varies depending on the size of the lens opening, distance of the object, and the focal length of the lens
  - Depth of field increase when
    - Subject distance increases
    - Size of lens opening decreases
    - Focal length decreases

IDS

- Can be used to detect intruders by employing Electromechanical or volumetric systems
- Volumetric systems are more sensitive and can detect changes in subtle environmental characteristics like vibration, microwaves, infrared values and photoelectric changes
- Electromechanical Systems:
  - Work by detecting a change or break in a circuit.
  - Vibration detectors can detect movement on walls, screens, ceilings when the fine wires embedded within the structure are broken
  - Magnetic contact switches can be installed on windows and doors
  - Pressure pad is placed underneath a rug or carpet and is activated during off-hours.

IDS

- Photoelectric system
  - Detects change in the light beam, and hence can be used only in windowless environments
  - Cross-sectional beams can be used to extend the light beams across an area by using hidden mirrors to bounce the beam
- Passive infrared system
  - Identifies change of heat waves in the area
- Acoustic Detection
  - Uses microphones installed in doors, windows, walls; monitors for sounds during forced intrusion
  - Its very sensitive and cannot be used in open areas
  - Vibration sensors are similar to this and are commonly used by financial institutions in vaults

IDS

- Wave-pattern motion detectors
  - These devices generate wave patters that is sent over a sensitive area and reflected back to a receiver.
  - Uses different frequencies to monitor
- Proximity detector or capacitance detector
  - Emits measurable magnetic fields and looks out for disruption
  - It is used to protect specific objects versus protecting a whole room or area
- Electrostatic IDS
  - Creates an electrostatic magnetic field

Tracking Software

- Widely accepted best practices
  - Application Whitelisting
  - Using Gold Masters (Ghost Image)
  - Enforcing least privilege
  - Automated Scanning

Change Control Process

- Change control is important for product not only during its development but throughout its lifecycle
- Change must be effective, orderly, timely
- Change control Steps
  - Request for change
  - Approval of the change
  - Documentation of the change
  - Tested and presented
  - Implementation
  - Report change to management

Network and Resource Availability

- Below are some options to ensure availability of network resources
  - Redundant Hardware
    - HA/ Hot swapping methods allows failover or change of hardware components without causing downtime to the environment
  - Fault-tolerant Technologies
    - Technologies that will try to correct itself after a failure. It is the most expensive solution, primarily used in mission critical infrastructure
  - Service Level Agreements (SLA)
    - Helps in maintaining a agreed service level with internal as well as external providers
  - Solid Operational Procedures
    - Operational procedures, training and continuous improvement are all important aspects in maintaining a healthy environment

Mean Time Between Failure (MTBF)

- Measure of how long an equipment will operate reliably
- Calculated by taking the average of time between failures
- Vendor normally provides this value
- Its is used as a benchmark for reliability
- MTBF implies the device is repairable, if it is not there, then it means Mean Time to Failure (MTTF)
- Mission critical systems will have a higher MTBF value

Mean Time to Repair (MTTR)

- Measure of time to get a device repaired and back into production
- MTTR may pertain to fixing a component, replacing the device or refers to an SLA
- If the MTTR is too high, then redundancy should be used for critical devices
- Systems that cannot be allowed to be down should have redundant systems with high MTBF values.

Single Point of Failure

- If a single device failure brings down a segment or the whole network, then the device is considered a single point of failure
- The defences are
  - Proper maintenance
  - Regular backup
  - Redundancy
  - Fault tolerance

RAID

- Redundant Array of Independent Disks is a technology used for redundancy and/or performance improvement.

RAID	Activity	Name
0	Data **stripped** over serval drives, no redundancy or parity. If one volume fails entire volume may become unusable, primarily used for **performance improvement**	Stripping
1	Data is **written to two drives** at the same time. If one fails, the other drive has the same data	Mirroring
2	Data **stripping** over all drives at **the bit level,** Parity data is created with Hamming code. **Not** used **in Production** today	Hamming code Parity
3	Data stripping over all drives, **parity code in in one drive**. If one drive fails it can be reconstructed using parity code	Byte-level parity
4	Same as RAID 3, parity is created at block level instead of byte level	Block-level parity
5	Data is **written in disk sector** units to all drives. **Parity is also written to all drives**. Ensure no single point of failure	Interleave parity
6	Similar to RAID 5 with **added Fault tolerance**, second set of parity added to all drives	Double parity
10	Data is **mirrored and stripped** simultaneously across several drives and can support multiple drive failure	Stripping and Mirroring

Direct Access Storage Device (DASD)

- Magnetic storage devices which have been used in mainframe and minicomputer environments
- RAID is a DASD
- In DASD, an point ca be reached directly, whereas in SASD every point in between the current and desired position must be traversed in order to reach the desired position

Massive Array of Inactive Disks (MAID)

- Used in environments where several hundred terabytes of data storage is required but it **carries mostly write operations**.
- In a MAID, rack-mounted disk arrays have all been powered down with only the disk controller alive.
- When an application asks for data, the controller powers the appropriate disk drive, transfers the data and then powers the drive down
- This helps in decreased energy consumption and lengthier service life of the disk drives

Redundant Array of Independent Tapes (RAIT)

- Similar to RAID, but uses Tape drives
- Tape storage is low-cost storage option but is slow compared to disk storage
- Fits in environments where very large write-mostly storage applications , appropriate performance and reliability is required
- Data is stripped in parallel to multiple tape drives with or without redundant parity drive. This provides high capacity at low cost

Storage Area Network (SAN)

- Consists of numerous storage devices linked together connected through a high speed private network and storage specific switches
- SAN provide redundancy, fault tolerance, reliability, backup and allows interaction as one virtual entity
- Not commonly used in small or medium sized companies.
- Tape drives, optical junkboxes, and disk arrays may also be attached to and referenced through SAN

Clustering

- It is a fault-tolerant technology similar to redundant serves, except that each device takes part in processing services that are requested
- It provides availability, scalability, load balancing, redundancy and failover.
- Clustering is a logical outgrowth of redundant servers
- In a cluster a master controller has control over allocation of resources and users to cluster node.

Grid computing

- Load-balanced parallel means of massive computing implemented with loosely coupled systems that may join or leave the grid randomly
- Nodes do not trust each other and no central controller is available
- Grid computing cannot be used for applications that require tight interactions and coordinated scheduling among multiple workload units.
- Sensitive data should not be processed over a grid and this is not the proper technology for time-sensitive applications.

Backup – Hierarchical Storage Management

- HSM provides continuous online backup functionality
- It combines hard disk technology with the cheaper and slower optical or tape juke-boxes
- It dynamically manages the storage and recovery of files, which are copied to storage media devices that vary in speed and cost
- This was created to save money and time

Contingency Planning

- Contingency planning defines what should take place during and after an incident.
- It addresses how to deal with small incidents that do not quality as disasters.
- There should be three instances of the contingency planning document: one at the premises, a copy in the same site but in a fireproof safe, an another copy in the offsite location
- It should not be trusted until they are tested

Intrusion Detection Systems

- Major aspect of IDS are
  - False Positive – detecting intrusions when none happened
  - False Negative – Missing intrusions as benign
- Important step to reduce errors is to baseline the system
- Baselining refers to process of establishing the normal pattern of behaviour for a given network or system
- White-list and black-lists can be used to improve the efficacy of IDS

Patch Management

- Centralized Patch Management is considered the best practice for security operations
- The common approaches are
  - Agent Based
    - An update agent is installed in every device
  - Agentless
    - One or more device remotely connects to each host for patch update and compliance
  - Passive
    - Passively monitor network traffic to infer the patch levels on each networked service. This is the least effective approach

Honeypot

- Honeyclients
  - Synthetic applications meant to allow an attacker to conduct client-side attacks
  - Very important in honey family, because most of the successful attacks are client-side
  - Different flavours are there
    - Highly Interactive – requires humans to operate them
    - Low interaction – their behaviour is completely automated

Incident Management Process

- 7 Phases of Incident Management Process
  - Detect
  - Respond
  - Mitigate
  - Report
  - Recover
  - Remediate
  - Learn
- Incident management includes both proactive and reactive processes.

Incident Response Teams

- 3 different types of incident response teams
  - Virtual team
    - Made up of experts who have other duties.
    - This introduces slower response times and the members have to leave their current roles to address incidents
  - Permanent team
    - Dedicated only for incident response
    - Costly but response is faster
  - Hybrid team
    - Consists of both permanent and virtual staff

Incident Response Teams

- The team should have the following
  - Contact of outside agencies
  - Roles and responsibilities
  - Call tree
  - List of forensic experts to call
  - Steps to secure and preserve evidence
  - List of items to be included in management report
  - Description of how systems should be treated

Incident Handling

- IH should be closely related to Disaster Recovery
- Primary goal is to contain and mitigate any damage caused by an incident and to prevent any further damage
- IH should also be closely linked with company security policy and awareness program
- The Incident reporting process should be centralized, easy to accomplish, convenient and welcomed

Incident Management stages

- Detection
  - Most important step in responding to an incident
  - Properly tuned detection mechanisms will help in identification of incidents
- Response
  - Early stage of response is to figure out what information is needed to restore security
  - The goals are to figure out who did it, how they did it, when they did it and why
  - Biggest challenge for response teams is the dynamic nature of logs.
  - The response team members should have variety of skills

Incident Management stages

- Mitigation
  - Goal is to prevent or reduce any further damage from the incident
  - Proper mitigation strategy buys time for investigation and determination of root cause
  - Mitigation strategy should be based on the category of the attack, the assets affected by the incident and the criticality of those assets.
  - The strategies can be proactive or reactive
- Reporting
  - Reporting occurs during the life cycle of the incident at various stages and various levels
- Recovery
  - Returning all systems and information to known-good state
  - It is very important to gather all evidences before recovering the systems and information

Incident Management stages

- Remediation
  - Based on the investigation decide the permanent solutions to prevent occurrence of similar incident
  - Identification of Indicators of Attack (IoA) that can be used to detect similar incidents in future
  - Also gathering the Indicators of Compromise (IoC) which will tell if the attack has been successful and security is compromised
- Learning
  - Review the incident, how it was handled, carry post-mortem analysis
  - This phase can help make adjustments to response strategies

Disaster Recovery

- Key Points
- RTO – Recovery Time Objective
  - The maximum time within which a business process must be restored to an acceptable service level after a disaster
  - RTO value should be lesser than MTD
  - RTO deals with getting the infrastructure and systems back up and running
- MTD represents the time after which the business cannot recover
- Work Recovery Time (WRT)
  - Remainder of the overall MTD value after RTO has passed
  - WRT deals with restoring data, testing process, and then making the production process live

Disaster Recovery

- RPO – Recovery Point Objective
  - It is the acceptable amount of data loss measured in time.
  - Represents the earliest point in time to which data must be recovered
  - The higher the value of data, the lower the RPO value
- The actual RTO, MTD, RPO values are derived from the Business impact assessment (BIA)

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

Facility Recovery

- Three main types of disruptions
  - Nondisaster
    - Disruption in a service that has significant but limited impact on the conduct of business operations
  - Disaster
    - An event that causes the entire facility to be unusable for a day or longer
  - Catastrophe
    - Major disruptions that destroys the facility altogether
- Recovery Alternatives
  - Redundant site
  - Outsourcing
  - Rented offsite
  - Reciprocal agreement

Leased or Rented Offsite Facilities

Hot Site

- Fully configured and ready to operate in few hours
- Only missing resources will be data and people
- Best for companies that require immediate availability
- Many providers support annual testing
- It is the most expensive of all options
- May not be suitable for companies that operate custom/proprietary hardware and software

Warm Site

- Leased or rented facility partially configured with some equipment such as HVAC, infrastructure components but not actual computers
- Most widely used model
- Less expensive than host site and can be up and running within a reasonably acceptable time period.
- Better choice for companies that operate custom/proprietary hardware and software
- Much of the equipment must be purchased, delivered and configured at warm site
- Annual testing is usually not available
- Can provide long term solution than hotsite
- Tapes should be brought back to original site for testing

Cold Site

- Facility that supplies the basic environment, electrical wiring, air-condition and flooring
- No systems or software will be available
- Cheapest of the options available
- It may take days or weeks to bring up the facility
- Cold sites are often used as backup for call centers, manufacturing plants
- All the Infrastructure equipment's need to be shipped and configured.

Reciprocal Agreements

- Alternate site approach between companies that work in similar field or has similar technology
- Cheaper way than other options, but not always the best choice
- It will only provide short term solution
- The mixing of operations may introduce lot of security risks
- Careful testing needs to be conducted to determine if one company can support the other during disaster
- These agreements are not enforceable

Redundant Sites

- Mirror sites that are equipped and configured exactly like the primary site
- The business processing capability between the two can be completely synchronized
- Both the sites are owned by the company and hence has inherent advantages
- It is the most expensive backup facility

Rolling Hot Site

- Mobile hot site behind a large truck or a trailer converted into a data processing or working area
- It is a portable and self-contained data facility
- Another similar solution is prefabricated building

Backup Strategies

Full Backup

- All data is backed up and saved
- During full backup the archive bit is cleared and set to 0
- Recovery is just one step process; but the backup and recovery process could take a long time

Differential Backup

- Backup the files that have been modified since the last full backup
- This process does not change the archive bit value
- When data needs to be restored, the full backup is laid down first, then the most recent differential backup is put on top of the full backup
- Takes more time in backing up phase but takes less time to restore

Incremental Backup

- Backups all files that have been modified since the last full or incremental backup
- This process clears the archive bit and set to 0
- Takes less time to backup than differential backup but takes more time for restoration

Backup Strategy

- If an organization wants the backup and restoration processes to be simplistic and straightforward, it can use Full backup
- It is very important to not mix the differential and incremental backup.
- It is very important that the backup data is restored and tested at regular frequencies

Electronic Backup Solutions

- Disk duplexing
  - More than one disk controller is in use. If one controller fails the other is ready and available
- Disk Shadowing
  - Data is dynamically created and maintained on two or more identical disks.
  - Used to ensure the availability of data and to provide a fault-tolerant solution by duplicating hardware and maintaining more than one copy of the information
  - It provides online backup storage
  - It can boost read operation performance
  - It is an expensive solution because two or more hard drives are used to hold the exact same data
  - Companies choose this model if fault tolerance is required

Electronic Backup Solutions

- Electronic Vaulting
  - Makes copies of files as they are created/modified and periodically transmits them to an offsite backup site
  - Method of transferring bulk information to offsite facilities for backup
  - The transmission happens in batches (does not happen in real time)
- Remote Journaling
  - Method of transmitting data offsite usually by moving the journal or transaction logs to the offsite facility **not the actual files**
  - These logs contains the delta that has taken place on the original files
  - Journaling is efficient for database recovery, where only the reapplication of a series of changes to individual records is required to resynchronize the database.
  - Takes place in real-time and only transmits the file deltas

Electronic Backup Solutions

- Data repositories commonly have replication capabilities, so that when changes take place to one repository, they are replicated to all of the other repositories.
- Replication can be asynchronous or synchronous
- Asynchronous – Primary and secondary data volumes are out of sync. Synchronization takes place in seconds, minutes, hours, days, depending upon the technology in use
- Synchronous – primary and secondary repositories are always in sync

High Availability

- Combination of technologies and process that work together to ensure that some specific thing is always up and running
- Redundancy, failover, fault tolerance capabilities increase the reliability of a system or network
- High reliability allows for high availability

Insurance

- The decision to go for insurance or not should be based on the BIA
- The goal is to ensure the insurance coverage fills in the gaps of what the current preventive countermeasures cannot protect against
- Cyber Insurance
  - New type of coverage that insures losses caused by DoS, Malware, hacking, etc.
- Business Interruption Insurance
  - If the company is out of business for a certain length of time, insurance company will provide for expenses.

Restoration and Recovery

- Restoration team is responsible for getting the alternate site into a working and functioning facility
- Salvage team is responsible for getting the primary facility
  - Backup data from the alternate site and restore it within the new facility
  - Carefully terminate contingency operation
  - Securely transport equipment and personnel to the new facility
- The least critical functions should be moved back to primary facility first. This helps evaluate the operational ready state of the facility before the we move the mission critical applications

BCP Types

Plan type	Description
Business Resumption Plan	Focuses on recreating the necessary business process instead of focusing on IT Component. It is process oriented instead of procedural-oriented
Continuity of Operations Plan (COOP)	Establishes senior management and a headquarters after a disaster. Outlines roles and authorities, orders of succession
IT Contingency Plan	Plan for systems, networks and major application recovery procedures after disruptions.
Crisis Communication Plan	Includes internal and external communication structure and roles. Identifies specific individuals who will communicate with external entities
Cyber Incident response plan	Focuses on malware, hackers, intrusions, attacks and other security issues.
Disaster Recovery plan	Focuses on how to recover various IT mechanisms after a disaster.
Occupant emergency Plan	Establishes personnel safety and evacuation procedures

Computer Forensics

- Digital Evidence
  - It has a very short lifetime and must be collected first
  - Most fragile and volatile information must be collected first
- Best Procedure
  - Remove the system from the network, dump the contents of the memory, power down the system, and make a sound image of the attacked system and perform forensic analysis on this copy
- Dumping the memory contents is the crucial step
- Documentation is the most critical component in an investigation process

Motive, Opportunity and Means

- Motive
  - Who and why of a crime
  - May be induced by either internal or external conditions
  - Understanding the motive of a crime is an important piece in figuring out who would engage in such an activity
- Opportunity
  - Where and When of a crime
  - Opportunities usually arise when certain vulnerabilities or weakness are present
- Means
  - Pertains to the abilities a criminal would need to be successful

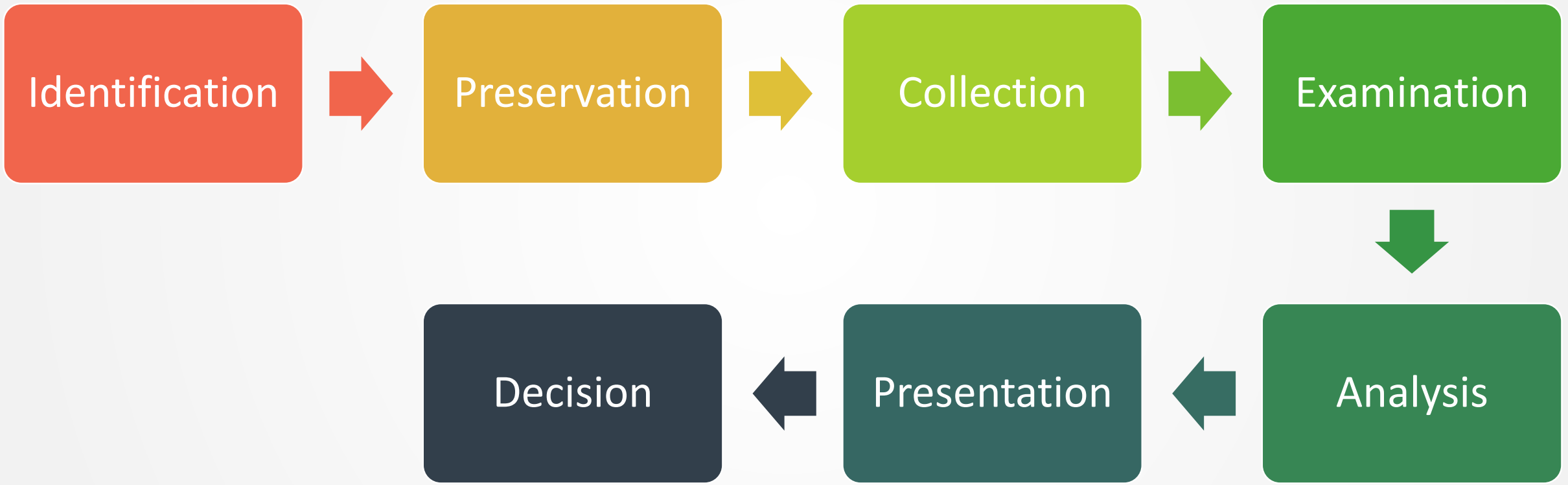
Computer Criminal Behaviour

- Psychological crime scene analysis (profiling) can also be conducted using the criminal's MO and signature behaviours.
- Profiling provides insight into the thought process of the attacker and can be used to identify the attacker or at the very least, the tool used to conduct the crime
- Locard's Exchange principle states the criminal leaves something behind at the crime scene and takes something with them.

Investigative Assessment Types

- Network Analysis
  - Traffic analysis
  - Log analysis
  - Path tracing
- Media Analysis
  - Disk Imaging
  - Timeline analysis
  - Registry analysis
  - Slack space analysis
  - Shadow volume analysis
- Software Analysis
  - Reverse engineering
  - Malicious code review
  - Exploit review
- Hardware/Embedded device review
  - Dedicated appliance attack points
  - Firmware and dedicated memory inspections
  - Embedded operating systems, virtualized software, hypervisor analysis

Forensic Investigation Process



Controlling the crime scene

- Steps that should take place to protect the crime scene
  - Only allow authorized individuals to work on the crime scene
  - Document who is there in the crime scene
  - Document who were the last individuals to interact with the systems
  - If the crime scene does become contaminated, document it

Forensic process best practices

- The original image must be a bit-level copy, sector by sector, to capture deleted files, slack spaces and unallocated clusters
- The original image is called the primary image which must be stored in a library
- Investigator should only work from a copy of the primary image called the secondary image
- These should be timestamped to show when the evidence is collected
- Before collecting the images to a new media it is important to ensure the destination is sanitized

Chain of Custody

- A history that shows how evidence was collected, analysed, transported, and preserved in order to be presented in court
- Chain of custody should follow evidence through its entire life cycle
- When copies of data need to be made, the copies must be able to be independently verified and must be tamperproof
- Chain of custody evidence dictates that all evidence be labelled with information indicating who secured and validated it
- Magnetic disk surfaces should not be marked on
- The most common reason for improper evidence collection are lack of an established incident response team, lack of an established incident response process, poorly written policy or a broken chain of custody
- Dead forensics – when the investigation is done on static data in lab
- Live forensics – when the investigation is done in field and includes volatile data

Evidence – Admissible in court

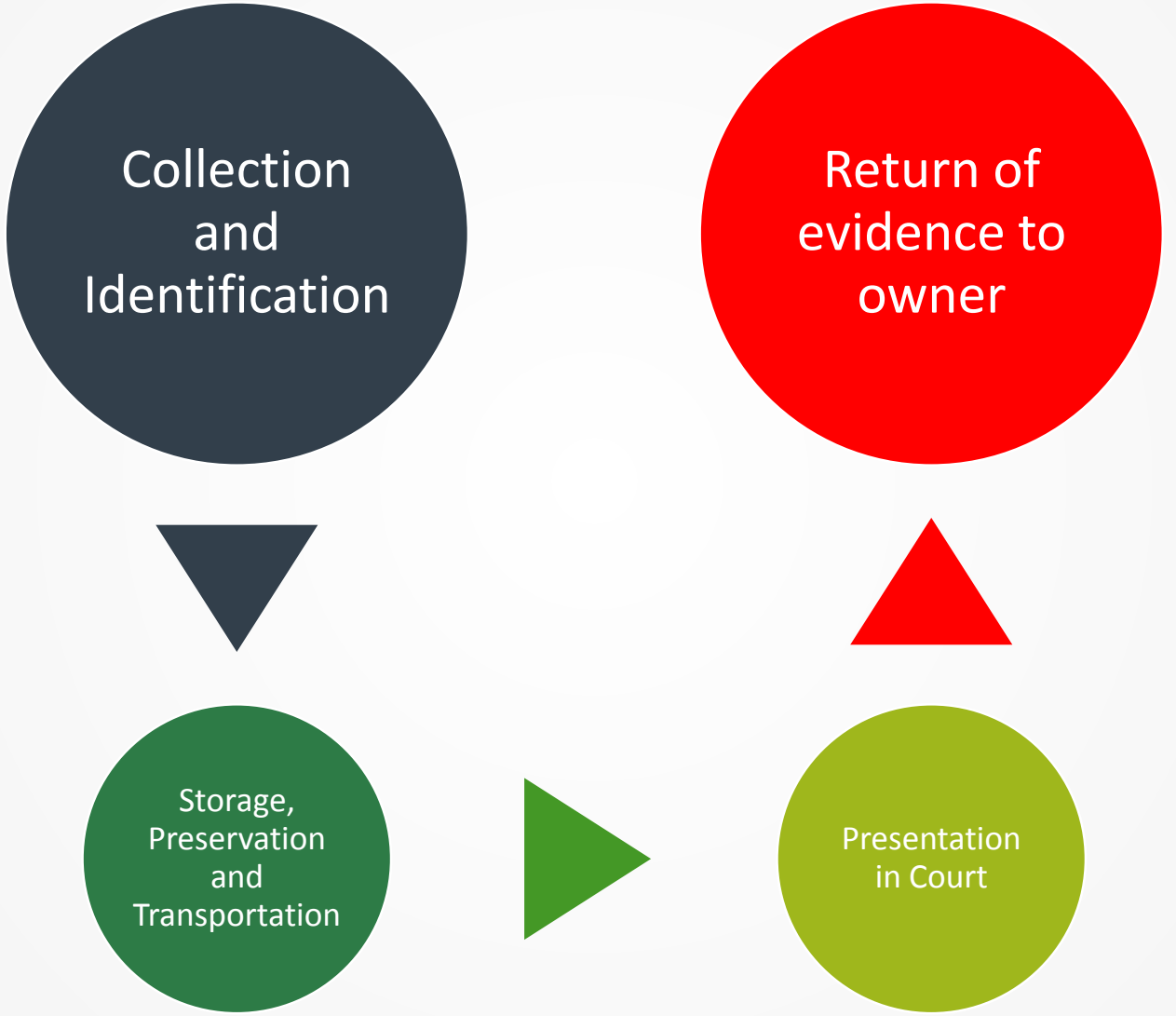
- Computer-related documents are considered hearsay – meaning they are second-hand evidence
- Hearsay evidence is not normally admissible in court unless it has first-hand evidence that can be used to prove the evidence accuracy
- The value of evidence depends on the genuineness and competence of the source
- Business records exception rule:
  - Under this rule, a court could admit any records of a business
    - That were made in the regular course of business
    - That the business has a regular practice to make such records
    - That were made at or near the time of the recorded event
    - That contain information transmitted by a person with knowledge of the information within the document

Evidence – Admissible in court

- The evidence should be relevant, complete, sufficient and reliable to the case at hand

Relevant	Must have reasonable and sensible relationship to the findings
Complete	It must present the whole truth of the issue
Sufficient (believable)	It must be persuasive enough to convince a reasonable person of the validity of the evidence
Reliable	It must be consistent with the facts; must be factual and not circumstantial

Evidence Lifecycle



Liability Scenarios

- To prove negligence in court, the plaintiff must establish that the defendant had a legally recognized obligation to protect the plaintiff from an unreasonable risk
- Proximate cause – is an act or omission that naturally and directly produces a consequence. It is the superficial or obvious cause for an occurrence

CyIntegriti

UNCOMPLICATE SECURITY