# INFO 6010 Lesson 11
# Security Operations Part 1
# Domain 7

Revision 2

Information Security Management & Network Security and Architecture

FANSHAWE

# Security Operations – Domain 7

- Operations department responsibilities
- Administrative management responsibilities
- **Physical security**
- Secure resource provisioning
- **Network and resource availability**
- Preventive and detective measures
- Incident management
- Investigations

PART 2

- Disaster recovery
- Liability
- Personal safety concerns

# Security Operations

- Operations security pertains to everything that takes place to keep networks, computer systems, applications, and environments up and running in a secure and protected manner
- It consists of ensuring that people, applications, and servers have the proper access privileges to only the resources they are entitled to and that oversight is implemented via monitoring, auditing, and reporting controls
- Operations take place after the network is developed and implemented

# Security Operations

- Includes the continual maintenance of an environment and the activities that should take place on a day-to-day or week-to- week basis
- These activities are routine in nature and enable the network and individual computer systems to continue running correctly and securely

# Operational Responsibility

- Operations security encompasses safeguards and countermeasures to protect resources, information, and the hardware on which the resources and information reside
- The goal of operations security is to reduce the possibility of damage that could result from unauthorized access or disclosure by limiting the opportunities of misuse

# Operational Responsibility

- The operations department usually has the objectives of preventing recurring problems, reducing hardware and software failures to an acceptable level, and reducing the impact of incidents or disruption
- Should investigate any unusual or unexplained occurrences, unscheduled initial program loads, deviations from standards, or other odd or abnormal conditions that take place on the network

# Security Operations

- **Due care and due diligence** are comparable to the "prudent person" concept
- A prudent person is seen as responsible, careful, cautious, and practical, and a company practicing due care and due diligence is seen the same
- The continual effort to make sure the correct policies, procedures, standards, and guidelines are in place and being followed is an important piece of the due care and due diligence efforts that companies need to perform

# Role of Operations Department

- The right steps need to be taken to achieve the necessary level of security, while balancing ease of use, compliance with regulatory requirements, and cost constraints
- It takes continued effort and discipline to retain the proper level of security
- Operations security is all about ensuring that people, applications, equipment, and the overall environment are properly and adequately secured

# Administrative Management

- One aspect of administrative management is dealing with personnel issues
- Includes separation of duties and job rotation
- Objective of separation of duties is to ensure that one person acting alone cannot compromise the company’s security in any way
- High-risk activities should be broken up into different parts and distributed to different individuals or departments

# Administrative Management

- Company does not need to put a dangerously high level of trust in certain individuals
- For fraud to take place, collusion would need to be committed, meaning more than one person would have to be involved in the fraudulent activity
- Separation of duties is a preventive measure that requires collusion to occur in order for someone to commit an act that is against policy

# Administrative Management

- Each role needs to have a completed and well-defined job description
- Security personnel should use these job descriptions when assigning access rights and permissions in order to ensure that individuals have access only to those resources needed to carry out their tasks
- Organizations should create a complete list of roles used within their environment, with each role's associated tasks and responsibilities

# Administrative Management

- Roles should then be used by data owners and security personnel when determining who should have access to specific resources and the type of access
- Separation of duties helps prevent mistakes and minimize conflicts of interest that can take place if one person is performing a task from beginning to end
- The user should not be able to modify her own security profile, add and remove users globally, or make critical access decisions pertaining to network resources

# Administrative Management

- **Job rotation** means that, over time, more than one person fulfills the tasks of one position within the company
- This enables the company to have more than one person who understands the tasks and responsibilities of a specific job title, which provides backup and redundancy if a person leaves the company or is absent
- Job rotation also helps identify fraudulent activities, and therefore can be considered a detective type of control

# Administrative Management

- **Least privilege** and **Need to know** are also administrative-type controls that should be implemented in an operations environment
- Least privilege means an individual should have just enough permissions and rights to fulfill her role in the company and no more
- If an individual has excessive permissions and rights – that give her access to information that exceeds her Need to Know – it could put the company at risk

# Administrative Management

- A user’s access rights may be a combination of
  - least-privilege attribute
  - user’s security clearance
  - user’s need to know
  - sensitivity level of the resource
  - mode in which the computer operates
- **Mandatory vacations** are another type of administrative control, it helps to identify fraudulent activities and enabling job rotation

# Security & Network Personnel

- The security administrator should not report to the network administrator, because their responsibilities have different focuses
- The network administrator is under pressure to ensure high availability and performance of the network and resources and to provide the users with the functionality they request

# Security & Network Personnel

- Security mechanisms commonly decrease performance in either processing or network transmission because there is more involved:
  - content filtering
  - virus scanning
  - intrusion detection prevention
  - anomaly detection

# Security Administrator

- The following tasks should be carried out by the security administrator, not the network administrator:
- Implement and maintain security devices and software
  - Despite some security vendors' claims that their products will provide effective security with “set it and forget it” deployments, security products require monitoring and maintenance in order to provide their full value
- Carry out security assessments
  - A security assessment identifies vulnerabilities in the systems, networks, software, and in-house developed products used by a business

# Security Administrator

- Create and maintain user profiles and implements and maintains access control mechanisms
  - The security administrator puts into practice the security policies of least privilege, and oversees accounts that exist, along with the permissions and rights they are assigned
- Set initial passwords for users
  - New accounts must be protected from attackers
  - The security administrator operates automated new password generators, or manually sets new passwords, and then distributes them to the authorized user

# Security Administrator

- Configure and maintain security labels in mandatory access control (MAC) environments
  - MAC environments, mostly found in government and military agencies, have security labels set on data objects and subjects
  - Access decisions are based on comparing the object’s classification and the subject’s clearance

  - (Review: what’s the “opposite” of MAC?)

# Security Administrator

- Review audit logs
  - While some of the strongest security protections come from preventive controls (such as firewalls that block unauthorized network activity), detective controls such as reviewing audit logs are also required
  - The security administrator’s review of audit logs detects bad things as they occur and, hopefully, before they cause real damage

# Accountability

- Users' access to resources must be limited and properly controlled to ensure that excessive privileges do not provide the opportunity to cause damage to a company and its resources
- Users' access attempts and activities while using a resource need to be properly audited, and logged
- The individual user ID needs to be included in the audit logs to enforce individual responsibility
- Monitoring audit logs helps determine if a violation has actually occurred or if system and software reconfiguration is needed to better capture only the activities that fall outside of established boundaries

# Accountability

- When monitoring, administrators need to ask certain questions that pertain to the users, their actions, and the current level of security and access:
- Are users accessing information and performing tasks that are not necessary for their job description?
- The answer would indicate whether users' rights and permissions need to be reevaluated and possibly modified

# Accountability

- Are repetitive mistakes being made?
- The answer would indicate whether users need to have further training
- Do too many users have rights and privileges to sensitive or restricted data or resources?
- The answer would indicate whether access rights to the data and resources need to be reevaluated, whether the number of individuals accessing them needs to be reduced, and/or whether the extent of their access rights should be modified

# Clipping Levels

- Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious
- The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised
- This baseline is referred to as a clipping level
- The goal of using clipping levels, auditing, and monitoring is to discover problems before major damage occurs and, at times, to be alerted if a possible attack is underway within the network

# Physical Security

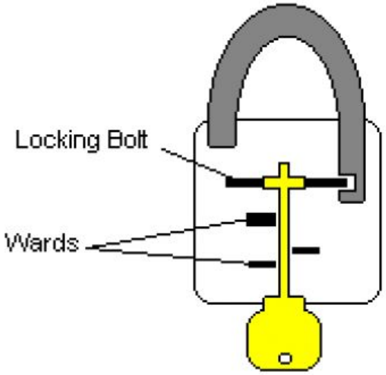
- Physical security should be implemented by using a layered approach.
- Physical security plans depend on the level of protection required for assets and resources
  - Depends on the acceptable level of risk
  - Derived from laws and regulations
    - Identify threats against assets
    - Identify types of attacks
    - Identify and understand business impact of threats
    - Identify types of countermeasures

# Facility Access Control

- Access control must be enforced through physical and technical controls.
- Physical access controls use mechanisms to identify individuals attempting to enter a facility or area.
- Only authorised individuals get in, unauthorised are barred and an audit trail of these actions is maintained.

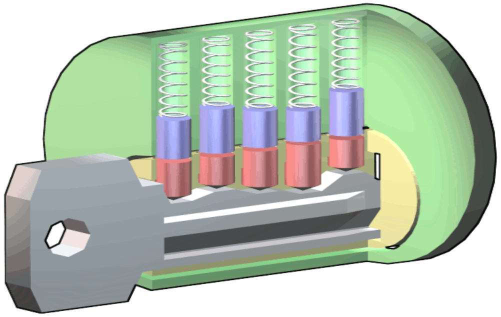
# Mechanical Locks

- Warded Mechanical Lock
  - Basic padlock
  - Spring loaded bolt with a notch cut in it
  - Key fits in the notch and slide the bolt from locked to unlocked position



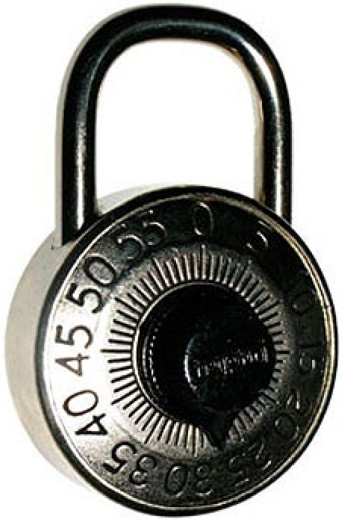
# Mechanical Locks

- Tumbler
  - Key fits into a cylinder which raises the lock metal pieces to the correct height positions so the bolt can slide from the locked to the unlocked position
  - Once all the metal pieces are at the correct height the internal bolt can be turned



# Mechanical Locks

- Combination
  - Do not require key (which can be lost)
  - Requires correct combination of numbers
  - Have internal wheels which must line up before bolt is unlocked



# Cipher Locks

- Cipher Locks
  - Do not require key (which can be lost)
  - Locks are keyless and use keypads or swipe cards
  - Combination can be changed
  - Some cipher locks support multiple user combinations

# Perimeter Security

- Regardless of which lock is used proper maintenance and procedure should be followed
  - Keys should be assigned by facility management
  - Key assignment should be documented
  - Procedures required for how keys are assigned, inventoried and destroyed
  - Most facilities have master and sub master keys allowing access with single key
    - These keys should be guarded

# Circumventing Locks

- Lock Raking
  - Lock pick is pushed to back of lock and pulled out quickly applying upward pressure
  - This method makes many pins fall into place
- Lock Bumping
  - A tactic an intruder can use to force the pins in a tumbler lock to their open position by using special key called a bump key

# External Boundary Protection Mechanisms

FANSHAWE

# Perimeter Fencing

- Fencing is first line of defense
  - Effective physical barrier
  - Works as a psychological deterrent (company is serious about security)
  - Can provide crowd control and access to entrances
  - Fencing must be maintained (rusty fence says we don’t care about security)
  - When choosing fencing you should consider ‘Gauge’ (threat type)
  - Risk analysis should determine fencing thickness

# Perimeter Fencing

- Fencing 3 or 4 feet high deter casual trespassers
- Fencing 6 to 7 feet are too high to climb easily
- Fencing 8 feet high with barbed wire will deter the most determined intruder
- Critical areas should have fencing at least 8 feet high
- Fence should be taut and not sag
- Fence posts should be deep with concrete footing
- Gauge is the thickness of the wire. The lower the gauge the larger the wire diameter
  - 11 Gauge = 0.0907 inch diameter
  - 9 Gauge = 0.1144 inch diameter
  - 6 Gauge = 0.162 inch diameter

# Perimeter Fencing

- The mesh sizing is the minimum clear distance between the wires
  - More difficult to climb or cut smaller mesh sizes
  - Extremely High Security = 3/8 inch mesh 11 Gauge
  - Very High Security = 1 inch mesh 9 Gauge
  - High Security = 1 inch mesh 11 Gauge
  - Greater Security = 2 inch mesh 6 Gauge
  - Normal Individual Security = 2 inch mesh 9 Gauge

# Perimeter Gates

- Each gate has its own implementation and maintenance guidelines
- Classification is developed by Underwriters Laboratory (UL)
  - **Class I** – Residential Use
  - **Class II** – Commercial Use with general public access (public parking)
  - **Class III** – Industrial Use with limited public access (warehouse)
  - **Class IV** – Restricted Use monitored through CCTV camera or Security Guard

# Perimeter Security

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

# Perimeter Lighting

- Unlit or poorly lit areas attract intruders
- Each light should illuminate its own zone
- There should be overlap between illuminated zones
- Proper lighting is required when using surveillance equipment such as cameras
- Lighting must provide proper contrast between dark, dirty or darkly painted surfaces

# Perimeter Lighting

- Lighting should be installed in potential intruder areas
- Lighting should be directed away from security
  - Guards should be in the shadows
- Lighting should be directed at gates, entrances
- Continuous Lighting
  - Array of lights that provides illumination across a wide area (parking Lots)
- Responsive Area Illumination
  - intrusion detection system turns on lights in a specific area

# CCTV

- Closed Circuit TV
- Works best with security guards or other monitoring mechanisms.
- CCTV typically sends video to digital recording devices which stores video footage to an internal hard drive for review or retrieval at a later time.
- Before purchasing CCTV you must consider the following;
  - The purpose of CCTV
  - The field of view required
  - Amount of Illumination required
  - Integration with other Security Controls

# Perimeter Security

- Most CCTV utilize (CCD's) Charged Coupled Devices
  - Electrical circuit that receives light from the lens and converts it to electrical signals which is then displayed on the monitor
  - Allows for excellent optical detail and precise representation

# Perimeter Security

- CCTV utilize 2 different lens types
- Fixed Focal Point
- Zoom (varifocal)
- Focal length defines the effectiveness in viewing objects
  - The focal length value relates to angle of view
  - Long focal lenses provide a narrower view
  - Monitor Large Area = Smaller Focal Length
  - Normal focal length approximates the field of view of the human eye

# Perimeter Security

- Depth of Field
  - Depth of Field Increases as the size of lens opening decreases
  - Normal focal length approximates the field of view of the human eye
- Proper mounting required
  - Fixed mount vs. PTZ capable (Pan,Tilt, Zoom)

# Perimeter Security

- CCTV cameras iris
  - Control the amount of light entering the lens
  - Manual iris has ring around CCTV lens that is manually turned and controlled
  - Best used in fixed lighting areas
    - Iris cannot adjust to light changes
    - Auto-Iris should be used in areas with changing light conditions
- Lux
  - Metric used to represent illumination strength

# Intrusion Detection

- Intrusion Detection System are used to sense changes in environment
- Detect unauthorized entry
- IDS can monitor doors, windows, devices or removable coverings
- When a change is detected IDS activates an alarm.
- IDS uses the following to detect changes in environment:
  - Beams of Light
  - Sounds and Vibrations
  - Motion
  - Different types of fields
    - Microwave, ultrasonic, electrostatic
  - Electrical circuit

# Intrusion Detection

- 2 main types of IDS’s
- Electromechanical Systems & Volumetric Systems
- Electromechanical Systems:
  - Magnetic Switches, Metallic Foil, Pressure Plates)
  - Work by detecting a break in a circuit

# Intrusion Detection

- **Volumetric Systems**
  - Photoelectric System (Photometric)
  - (PIR) Passive Infrared System
  - Acoustical Detection System
    Wave Pattern Motion Detectors
  - Proximity Detector
  - Capacitance Detector
- **Photoelectric System**
  - Detects the change in a light beam
  - Can only be used in a windowless room
  - Uses visible or non visible light directed at a receiver or hidden mirror
  - If light is interrupted alarm is activated

# Intrusion Detection

- Passive Infrared System
  - Identified changes in heat waves
  - If ambient air temperature rises an alarm is activated
- Acoustical Detection System
  - Microphones installed on walls, floors or ceilings
  - Detect any sound during a forced entry
  - Cannot be used in noisy areas
- Vibration Systems
  - Detects seismic changes
  - Such as exterior walls, vaults (financial institutions)
- Wave Pattern Motion Detectors
  - Generates a wave pattern that is sent over an area and reflected back to the receiver
  - If pattern returned is disturbed an alarm is activated

# Intrusion Detection

- Vibration Systems
  - Detects seismic changes
  - Such as exterior walls, vaults (financial institutions)
- Wave Pattern Motion Detectors
  - Generates a wave pattern that is sent over an area and reflected back to the receiver
  - If pattern returned is disturbed an alarm is activated
- Proximity Detector (Capacitance Detector)
  - Generate a measurable magnetic field
  - If field is disrupted an alarm is activated

# Intrusion Detection

- Proximity Detector (Capacitance Detector)
  - Generate a measurable magnetic field
  - If field is disrupted an alarm is activated

- Intrusion Detection System
  - Expensive
  - Require Human Response
  - Require backup power
  - Can be linked to alarm system
  - Require a fail safe ‘activated’ configuration
  - Must detect and resist tampering

# Intrusion Detection

- **Patrol Force and Guards**
  - One of the best security mechanisms
  - More flexible then any other security mechanism
  - Provides good response and is a great deterrence
  - However it is expensive and people sometimes are unreliable
  - Proper bonding and background checks should be completed when choosing a guard
  - Guards should have clear tasks
  - Guard should be fully licensed and trained

# Intrusion Detection

- **Security Dogs**
  - Have proven to be highly useful in detecting intruders
  - Hearing and eyesight outperform those of humans
  - Their loyalty and intelligence can be used for protection
  - Security dogs should go through intense training
  - Dogs cannot know between authorized and unauthorized person
  - Dogs can supplement a security guard

# Auditing Physical Access

- Physical access control systems can use software auditing features to produce audit trails or access logs pertaining to access attempts. The following information should be logged and reviewed:
  - The date and time of the access attempt
  - The entry point at which access was attempted
  - The user ID employed when access was attempted
  - Any unsuccessful access attempts, especially if during unauthorized hours
- As with audit logs produced by computers, access logs are useless unless someone actually reviews them.

# Secure Resource Provisioning

- *Provisioning* is the set of all activities required to provide one or more new information services to a user or group of users ("new" meaning previously not available to that user or group).
- At the heart of provisioning is the imperative to provide these services in a secure manner, i.e. the services themselves must be secure.
- Users or systems utilize these services must access them in a secure manner and in accordance with their own authorizations and the application of the principle of least privilege.

# Asset Management

- Asset management is easily understood as “knowing what the company owns.”
- This may be called inventory management but in Operations Security it is so much more
- A prerequisite for knowing if hardware (including systems and networks) and software are in a secure configuration is knowing what hardware and software are present in the environment
- Asset management includes knowing and keeping up-to-date this complete inventory of hardware (systems and networks) and software

# Asset Management

- It is necessary to know the complete manifest of components within each hardware system, operating system, hardware network device, network device operating system, and software application in the environment
- Asset management means knowing everything—hardware, firmware, operating system, language runtime environments, applications, and individual libraries—in the overall environment

# Configuration Management

- Every company should have a policy indicating how changes take place within a facility, who can make the changes, how the changes are approved, and how the changes are documented and communicated to other employees
- Without these policies in place, people can make changes that others do not know about and that have not been approved, which can result in a confusing mess at the lowest end of the impact scale, and a complete breakdown of operations at the high end
- The changes can happen to network configurations, system parameters, applications, and settings when adding new technologies, application configurations, or devices, or when modifying the facility’s environmental systems
- Changes must be effective and orderly, because time and money can be wasted by continually making changes that do not meet an ultimate goal

# Change Control

- A well-structured change management process should be put into place to aid staff members through many different types of changes to the environment
- This process should be laid out in the change control policy.

1. Request for a change to take place
   - Requests should be presented to an individual or group that is responsible for approving changes and overseeing the activities of changes that take place within an environment
2. Approval of the change
   - The individual requesting the change must justify the reasons and clearly show the benefits and possible pitfalls of the change
   - Sometimes the requester is asked to conduct more research and provide more information before the change is approved

# Change Control

3. Documentation of the change
   - Once the change is approved, it should be entered into a change log
   - The log should be updated as the process continues toward completion
4. Tested and presented
   - The change must be fully tested to uncover any unforeseen results
   - Depending on the severity of the change and the company’s organization, the change and implementation may need to be presented to a change control committee
   - This helps show different sides to the purpose and outcome of the change and the possible ramifications.

# Change Control

5. Implementation
   - Once the change is fully tested and approved, a schedule should be developed that outlines the projected phases of the change being implemented and the necessary milestones
   - These steps should be fully documented and progress should be monitored.
6. Report change to management
   - A full report summarizing the change should be submitted to management
   - This report can be submitted on a periodic basis to keep management up-to-date and ensure continual support

# Change Control

- It is critical that the operations department create approved back-out plans before implementing changes to systems or the network
- It is very common for changes to cause problems that were not properly identified before the implementation process began

# Change Control Documentation

- Failing to document changes to systems and networks is only asking for trouble, because no one will remember what was done to that one server in the DMZ six months ago or how the main router was fixed when it was acting up last year
- Changes to software configurations and network devices take place pretty often in most environments, and keeping all of these details properly organized is impossible, unless someone maintains a log of this type of activity
- If no one properly documents the incident and what was done to fix the issue, the company may be doomed to repeat the same scramble six months to a year down the road

# Break Time

FANSHAWE

# Trusted Recovery

- When an operating system or application crashes or freezes, it should not put the system in any type of insecure state
- The usual reason for a system crash in the first place is that it encountered something it perceived as insecure or did not understand and decided it was safer to freeze, shut down, or reboot than to perform the current activity
- An operating system's response to a type of failure can be classified as one of the following:
  - System reboot
  - Emergency system restart
  - System cold start

# Trusted Recovery

- A **system reboot** takes place after the system shuts itself down in a controlled manner in response to a kernel (trusted computing base) failure
- If the system finds inconsistent object data structures or if there is not enough space in some critical tables, a system reboot may take place
- This releases resources and returns the system to a more stable and safer state

# Trusted Recovery

- An **emergency system restart** takes place after a system failure happens in an uncontrolled manner
- This could be a kernel or media failure caused by lower-privileged user processes attempting to access memory segments that are restricted
- The system sees this as an insecure activity that it cannot properly recover from without rebooting
- The system thus goes into a maintenance mode and recovers from the actions taken. Then it is brought back up in a consistent and stable state

# Trusted Recovery

- A **system cold start** takes place when an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system to a more consistent state
- The system, kernel, and user objects may remain in an inconsistent state while the system attempts to recover itself, and intervention may be required by the user or administrator to restore the system
- It is important to ensure that the system does not enter an insecure state when it is affected by any of these types of problems, and that it shuts down and recovers properly to a secure and stable state

# Trusted Recovery

- **Security Concerns (Secure Recovery)**
- Bootup sequence (C:, A:, D:) should not be available to reconfigure
  - To ensure that systems recover to a secure state, the design of the system must prevent an attacker from changing the bootup sequence of the system
- Writing actions to system logs should not be able to be bypassed.
  - Through separation of duties and access controls, system logs and system state files must be preserved against attempts by users/attackers to hide their actions or change the state to which the system will next restart
- If any system configuration file can be changed by an unauthorized user, and then the user can find a way to cause the system to restart, the new—possibly insecure—configuration will take effect

# Trusted Recovery

- System forced shutdown should not be allowed
  - To reduce the possibility of an unauthorized configuration change taking effect, and to reduce the possibility of denial of service through an inappropriate shutdown, only administrators should have the ability to instruct critical systems to shut down
  - Output should not be able to be rerouted
  - Diagnostic output from a system can contain sensitive information
  - The diagnostic log files, including console output, must be protected by access controls from being read by anyone other than authorized administrators
  - Unauthorized users must not be able to redirect the destination of diagnostic logs and console output

# Input and Output Controls

- What is input into an application has a direct correlation to what that application outputs. Thus, input needs to be monitored for errors and suspicious activity.
- Applications need to be programmed to only accept certain types of values input into them and to do some type of logic checking about the received input values.
- I/O issues that can cause problems if not dealt with properly are:
  - Data entered into a system should be in the correct format and validated to ensure that it is not malicious.
  - Transactions should be *atomic*, meaning that they cannot be interrupted between the input being provided and the generation of the output. (Atomicity protects against a class of attacks called time-of-check/time-of-use, or TOCTOU.)
  - Transactions must be timestamped and logged.
  - Safeguards should be implemented to ensure output reaches the proper destinations securely:
  - Cryptographic hashes or message authentication codes (which are digitally signed hashes) should be used to ensure the integrity of critical files.
  - The output should be clearly labeled to indicate the sensitivity or classification of the data.
  - Once output is created, it must have the proper access controls implemented, no matter what its format (paper, digital, tape).
  - If a report has no information (nothing to report), it should contain “no output.”

# System Hardening

- Unauthorized physical access to a security-sensitive item, renders it virtually impossible to secure.
- Physical components of networks through which information flows must be secured:
  - Wiring closets should be locked.
  - Network switches and hubs, when it is not practical to place them in locked wiring closets, should be inside locked cabinets.
  - Network ports in public places (for example, kiosk computers and even telephones) should be made physically inaccessible.
- Physical security alone is not enough,  technical ,easures must also be employed.
- Unnecessary software or services should be removed.

# Remote Access Security

- To gain the benefits of remote access without taking on unacceptable risks, remote administration needs to take place securely.  The following are just a few of the guidelines to use.
- Commands and data should not take place in clear text (that is, should be encrypted)
  - For example, SSH should be used, not Telnet
- Truly critical systems should be administered locally instead of remotely
- Only a small number of administrators should be able to carry out this remote functionality
- Strong authentication should be in place for any administration activities
  - Think: One-time Passwords, or Public/Private key pairs

# Network and Resource Availability

FANSHAWE

# Network & Resource Availability

- Network and resource availability often is not fully appreciated until it is gone
- Administrators and engineers need to implement effective backup and redundant systems to make sure that when something happens (and something will happen) users’ productivity will not be drastically affected
  - Redundant hardware ready for “hot swapping” keeps information highly available by having multiple copies of information (mirroring) or enough extra information available to reconstruct information in case of partial loss (parity, error correction)
  - Fault-tolerant technologies keep information available against not only individual storage device faults but even against whole system failures

# Mean Time Between Failures

- MTBF is the estimated lifespan of a piece of equipment
- MTBF is calculated by the vendor of the equipment or a third party
- The reason for using this value is to know approximately when a particular device will need to be replaced
- Based on historical data or scientifically estimated by vendors

# Mean Time to Repair

- Mean Time To Repair (MTTR) is the amount of time it will be expected to take to get a device fixed and back into production
- For a hard drive in a redundant array, the MTTR is the amount of time between the actual failure and the time when, after noticing the failure, someone has replaced the failed drive and the redundant array has completed rewriting the information on the new drive
  - The MTTR may pertain to fixing a component or the device, or replacing the device, or perhaps refers to a vendor’s SLA
  - If the MTTR is too high for a critical device, then redundancy should be used

# Single Point of Failure

- A single point of failure poses a lot of potential risk to a network, because if the device fails, a segment or even the entire network is negatively affected
- Devices that could represent single points of failure are firewalls, routers, network access servers, T1 lines, switches, bridges, hubs, and authentication servers
- Multiple paths should exist between routers in case one router goes down, and dynamic routing protocols should be used so each router will be informed when a change to the network takes place
- Redundant array of inexpensive disks (RAID) provides fault tolerance for hard drives and can improve system performance

# RAID

- Redundant array of inexpensive disks (RAID) is a technology used for redundancy and/or performance improvement
  - Combines several physical disks and aggregates them into logical arrays
  - When data are saved, the information is written across all drives
  - A RAID appears as a single drive to applications and other devices
  - When data are written across all drives, the technique of striping
- The most common RAID levels used today are levels 0, 1, 5, 6 and 10

# RAID

| RAID Level | Activity | Name |
|---|---|---|
| 0 | Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only. | Striping |
| 1 | Mirroring of drives. Data are written to two drives at once. If one drive fails, the other drive has the exact same data available. | Mirroring |
| 5 | Data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure. | Interleave parity |
| 6 | Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives. | Second parity data (or double parity) |
| 10 | Data are simultaneously mirrored and striped across several drives and can support multiple drive failures. | Striping and mirroring |

# MAID

- **MAID – Massive Array of Inactive Disks**
- Used for medium scale storage requirements
  - Hundreds of terabytes
- Niche requirement where mostly write operations are required and infrequent use of some disks in the array
- The disk arrays remain inactive and powered down
- The disk controller powers on the appropriate disk in the array array when an application request is received. The data is transferred and then the disks are powered down
- Save on energy consumption and working life of the disks

# RAIT

- **RAIT – Redundant Array of Independent Tapes**
- Tape storage is the least expensive cost of operation and is good for storage of large amounts of data.
- Tape however is slow to retrieve the stored data compared to other systems
- Similar to RAID 1 in that data is striped over the array of tapes in parallel with no redundant parity drive

# Storage Area Networks

- Drawing from the Local Area Network (LAN), Wide Area Network (WAN), and Metropolitan Area Network (MAN) nomenclature, a Storage Area Network (SAN) consists of large amounts of storage devices linked together by a high-speed private network and storage-specific switches
- This creates a “fabric” that allows users to attach to and interact in a transparent mode
- When a user makes a request for a file, he does not need to know which server or tape drive to go to—the SAN software finds it and magically provides it to the user
- SANs provide redundancy, fault tolerance, reliability, and backups, and allow the users and administrators to interact with the SAN as one virtual entity

# Clustering

- Clustering is a fault-tolerant server technology that is similar to redundant servers, except each server takes part in providing services that are requested
- A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system
  - Clustering provides for availability and scalability
  - It groups physically different systems and combines them logically, which provides immunity to faults and improves performance
  - Clusters work as an intelligent unit to balance traffic, and users who access the cluster do not know they may be accessing different systems at different times
  - To the users, all servers within the cluster are seen as one unit
  - Clusters may also be referred to as server farms

# Grid Computing

- Similar to clustering but no central controller
- Computing nodes are arranged in an informal grid
- Nodes can join and leave the grid at random
- Each node can work on a computation when it is currently inactive
- Should not be used for sensitive data because no control is available at remote computing node
- Not good for time sensitive applications

# Backups

- Backing up software and having backup hardware devices are two large parts of network availability
- You need to be able to restore data if a hard drive fails, a disaster takes place, or some type of software corruption occurs
- A policy should be developed that indicates what gets backed up, how often it gets backed up, and how these processes should occur
- The integrity of these backups needs to be checked to ensure they are happening as expected

# Hierarchical Storage Management

- **Hierarchical Storage Management (HSM)**
- HSM (Hierarchical Storage Management) provides continuous online backup functionality
- It combines hard disk technology with the cheaper and slower optical or tape jukeboxes
- The HSM system dynamically manages the storage and recovery of files, which are copied to storage media devices that vary in speed and cost
- The faster media holds the data that are accessed more often, and the seldom-used files are stored on the slower devices, or near-line devices

# Contingency Planning

- When an incident strikes, more is required than simply knowing how to restore data from backups
- Detailed procedures that outline the activities to keep the critical systems available and ensure that operations and processing are not interrupted
- Actions that are required to take place for emergency response, continuity of operations, and dealing with major outages must be documented and readily available to the operations staff
- Contingency plans should not be trusted until they have been tested
- Organizations should carry out exercises to ensure that the staff fully understands their responsibilities and how to carry them out

# Preventing and Detecting

**1.** Understand the risk. Risk can never be zero so direct resources towards mitigating the most dangerous ones.

**2.** Use the right controls.  The relationship between risks and controls is many to many, since a given risk can have multiple controls assigned to it and a given control can be used to mitigate multiple risks. The number of risks mitigated by one control provides an indicator of the value of that control to the organization. Multiple controls mitigating a risk may be less efficient, but may provide resiliency.

**3**. Use the controls correctly. Placement and correct configuration are critical.

**4.** Manage your configuration as it will become obsolete at some point in the future.

**5.** *Assess your operation.* Constantly look at the defensive plan, comparing it with the latest threat and risk assessments, are all the risk being properly mitigating? Test the controls using cases derived from risk assessments. A good penetration test can both verify and validate the controls.

# Intrusion Detection & Prevention Systems

- The difference between an IDS and an IPS is that an IDS will only detect and report suspected intrusions, while an IPS will detect, report, and stop suspected intrusions.
- The types of intrusions given the highest priority should be those that have the potential to realize the risks identified in the risk management plan.

**Whitelisting and Blacklisting**

- A *whitelist* is a set of known-good resources such as IP addresses, domain names, or applications.
- A *blacklist* is a set of known-bad resources.

# Antimalware & Vulnerability Management

- Antimalware or antivirus software is designed to detect and neutralize malicious software, including viruses, worms, and Trojan horses.
- Most commercially antivirus software is rule based, it works by identifying a distinctive attribute of the malware, extracting that as its signature, and then updating all software systems with it.
- ***Vulnerability management*** is the cyclical process of identifying vulnerabilities, determining the risks posed to the organization, and applying security controls that bring those risks to acceptable levels.

# Patch Management

- Patch management is “the process for identifying, acquiring, installing, and verifying patches for products and systems.”
- *Patches* are software updates intended to remove a vulnerability or defect in the software, or to provide new features or functionality for it.
- Unmanaged Patching – periodic checking and application of patches if any are available is simple but risky because:
  - Admin credentials required – violates least privilege.
  - Configuration management – status of every application difficult to verify.
  - Bandwidth utilization -  independent downloads lead to network congestion.
  - Service availability - Servers are almost never configured to automatically update themselves because this could lead to unscheduled outages that have a negative effect on the organization.

# Centralized Patch Management

- Centralized patch management is considered a best practice for security operations.
- The most common approaches are:
  - **Agent based:** an update agent is installed on each device. This agent communicates with one or more update servers and compares available patches with software and versions on the local host, updating as needed.
  - **Agentless:** one or more hosts that remotely connect to each device on the network using admin credentials and check the remote device for needed updates.
  - **Passive:** monitor network traffic to infer the patch levels on each networked application or service. While minimally intrusive to the end devices, least effective as not always be possible to uniquely identify software versions through their network traffic artifacts.

# Honeypots and Honeynets

- Honeypot: a server that is left open or appears to have been sloppily locked down, allowing an attacker relatively easy access. The intent is for the server to look like an easy target so that the attacker spends his time in the honeypot instead of in a live network. In short, the honeypot diverts the attacker away from the live network.
- Honeynet:  is a group of virtual servers contained within a single physical server, and the servers within this network are honeypots. The honeynet mimics the functionality of a live network.

# Security Information & Event Management

- A security information and event management (SIEM) system is a software platform that aggregates security information and security events and presents them in a single, consistent, and cohesive manner.
- SIEMs collect data from a variety of sensors, perform pattern matching and correlation of events, generate alerts, and provide dashboards that allow analysts to see the state of the network. Examples are: Splunk (commercial) and Elastic Stack (open-source).

# Incident management Process

FANSHAWE

# The Incident Management Process

Many computer crimes go unreported

- This makes it harder to know the real statistics of how many attacks happen

We commonly use the terms “event” and “incident” interchangeably

- An **event** is a negative occurrence that can be observed, verified, and documented
- An **incident** is a series of events that negatively affects the company and/or impacts its security posture

Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error

# Incident Response

- When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whoever has been delegated to investigate these types of situations
- All companies should have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place
- This policy should be managed by the legal department

# Incident Response

- All organizations should develop an incident response team, as mandated by the incident response policy, to respond to the large array of possible security incidents
- Purpose of having an incident response team is to ensure that there is a group of people who are properly skilled, who follow a standard set of procedures, and who are singled out and called upon when this type of event takes place

# Incident Response

- There are 3 different types of incident response teams:
- Virtual team
  - Made up of experts who have other duties and assignments within the organization
  - This type of team introduces a slower response time, and members must neglect their regular duties when an incidents occur
- Permanent team
  - Dedicated strictly to incident response can be cost prohibitive to smaller organizations
- Hybrid
  - Certain core members are permanently assigned to the team whereas others are called in as needed

# Incident Response

- The incident response team should have the following basic items available:
  - Contact info for outside agencies and resources
  - Outline of roles and responsibilities
  - A call tree to contact these roles and outside entities
  - A list of computer or forensics experts to contact
  - Steps on how to secure and preserve evidence
  - A list of items that should be included on a report for management and potentially the courts
  - A description of how the different systems should be treated in this type of situation (For example, the systems should be removed from both the Internet and the network and powered down)

# Incident Response

- When a suspected crime is reported, the incident response team should follow a set of predetermined steps to ensure uniformity in their approach and make sure no steps are skipped
  - **First**, the incident response team should investigate the report and determine that an actual crime has been committed
  - Senior management should be informed immediately
  - If an employee is involved human resources must be called right away
  - Document the starting time of the crime, along with the company employees and resources involved
- At this point, the company must decide if it wants to conduct its own forensics investigation or call in external experts

# Incident Response

- A clearly defined incident-handling process is:
  - More cost-effective
  - Enables recovery to happen more quickly
  - Provides a uniform approach
- Incident handling should be closely related to disaster recovery planning and should be part of the company’s disaster recovery plan
- Without an effective incident-handling program, individuals who have the best intentions can sometimes make the situation worse by damaging evidence, damaging systems, or spreading malicious code

# Incident Response

- Incident handling should be closely linked to the company’s security training and awareness program
- Employees need to know how to report an incident
- The incident response policy should also dictate how employees should interact with external entities, such as the media, government, and law enforcement

# Incident Response

- Given the sensitive nature of public disclosure, communications should be handled by communications, human resources, or other appropriately trained individuals who are authorized to publicly discuss incidents
- Public disclosure of an event can lead to two possible outcomes. If not handled correctly, it can compound the negative impact of an incident
- If public disclosure is handled well, it can provide the organization with an opportunity to win back public trust

# The Cyber Kill Chain

The kill chain can be used as a management tool to help continuously improve network defense. There are seven stages in the model, including:

- **Reconnaissance:** Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
- **Weaponization:** Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
- **Delivery:** Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)
- **Exploitation:** Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
- **Installation:** Malware weapon installs access point (e.g., "backdoor") usable by intruder.
- **Command and Control:** Malware enables intruder to have "hands on the keyboard" persistent access to target network.
- **Actions on Objective:** Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.

# The Incident Management Process

Defensive courses of action can be taken against these phases:

- Detection: determine whether there is a problem or not.
- Response: prevent information disclosure and unauthorized access
- Mitigation: stop or contain the damage.
- Reporting: initial report as part of continuous documentation.
- Recovery: return all systems to a good known state.
- Remediation: ensure that the attack can never be successful again.
- Treat the systems and facilities as potential crime scenes.

# Incident Response

## Cops or No Cops?

- Management needs to make the decision as to whether law enforcement should be called
- The following are some of the issues to understand if law enforcement is brought in:
  - Company loses control over investigation once law enforcement is involved
  - Secrecy of compromise is not promised; it could become part of public record
  - Effects on reputation need to be considered (the ramifications of this information reaching customers, shareholders, and so on)
  - Evidence will be collected and may not be available for a long period of time. It may take a year or so to get into court

# Investigations

## Computer Forensics & Evidence Collection

- **The International Organization on Computer Evidence (IOCE)** was created to develop international principles dealing with how digital evidence is to be collected and handled so various courts will recognize and use the evidence in the same manner
- In the USA the **Scientific Working Group on Digital Evidence (SWDGE)** aims to ensure consistency across the forensic community

# Scientific Working Group on Digital Evidence

- The principles developed by the SWGDE for the standardized recovery of computer-based evidence are governed by the following attributes:
  - Consistency with all legal systems
  - Allowance for the use of a common language
  - Durability
  - Ability to cross international and state boundaries
  - Ability to instill confidence in the integrity of evidence
  - Applicability to all forensic evidence
  - Applicability at every level, including that of individual, agency, and country

# Scientific Working Group on Digital Evidence

- The SWGDE principles:

**1.** When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

**2.** Upon the seizing of digital evidence, actions taken should not change that evidence.

**3.** When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

**4.** All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.

**5.** An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

**6.** Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

# Motive, Opportunity & Means

- **Motive**
  - The “who” and “why” of a crime. The motive may be induced by either internal or external conditions. A person may be driven by the excitement, challenge, and adrenaline rush of committing a crime, which would be an internal condition
- **Opportunity**
  - The “where” and “when” of a crime. Opportunities usually arise when certain vulnerabilities or weaknesses are present
  - If a company does not have a firewall or does not perform access control, auditing, and supervision, employees may have opportunities to embezzle funds and defraud the company
- **Means**
  - Pertains to the abilities a criminal would need to be successful

# Computer Criminal Behaviour

- Computer criminals have a specific modus operandi (MO), i.e.  criminals use a distinct method of operation to carry out their crime that can be used to help identify them.
- *Locard's exchange principle:* States that a criminal leaves something behind at the crime scene and takes something with them. This principle is the foundation of criminalistics. Even in an entirely digital crime scene, Locard's exchange principle can shed light on who the perpetrator(s) may be.

# Incident Investigations

- It is important that all security professionals understand how computer investigations should be carried out
  - Legal requirements for specific situations
  - Understanding the “chain of custody” for evidence
  - What type of evidence is admissible in court
  - Incident response procedures and escalation processes
- When a computer crime takes place, it is critical that the investigation steps are carried out properly to ensure that evidence will be admissible in court and that it can stand up under the cross-examination and scrutiny

# Types of Investigations

There are four general types of assessments performed by investigators.

**Network analysis**

- Traffic analysis
- Log analysis
- Path tracing

**Media analysis**

- Disk imaging
- Timeline analysis (modify, access, create times)
- Registry analysis
- Slack space analysis
- Shadow volume analysis

**Software analysis**

- Reverse engineering
- Malicious code review
- Exploit review

**Hardware/embedded device analysis**

- Dedicated appliance attack points
- Firmware and dedicated memory inspections
- Embedded operating systems, virtualized software, and hypervisor analysis

# Computer Forensics

- **Forensics** is a science and an art that requires specialized techniques for the recovery, authentication, and analysis of electronic data for the purposes of a criminal act
- People conducting the forensics investigation must be properly skilled in this trade and know what to look for
- If someone reboots the attacked system or inspects various files, this could corrupt viable evidence, change timestamps on key files, and erase footprints the criminal may have left

# Computer Forensics

- Most digital evidence has a short lifespan and must be collected quickly in order of volatility
- It is best to 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
- You should always perform forensic analysis on a cloned copy preserving original artifact.

# Forensics

- **The Forensics Investigation Process**
- To ensure that forensics activities are carried out in a standardized manner, it is necessary for the team to follow specific laid-out steps so nothing is missed and thus ensure the evidence is admissible
- Each team or company may commonly come up with their own steps, but all should be essentially accomplishing the same things:
  - Identification
  - Preservation
  - Collection
  - Examination
  - Analysis
  - Presentation
  - Decision

# Forensics

- During the examination and analysis process of a forensics investigation, it is critical that the investigator works from an image that contains all of the data from the original disk.
- It must be a bit-level copy, sector by sector, to capture deleted files, slack spaces, and unallocated clusters
- A file copy tool does not recover all data areas of the device necessary for examination

# Crime Scene

- It is important to control who comes in contact with the evidence of the crime to ensure its integrity. The following are just some of the steps that should take place to protect the crime scene:
  - Only allow authorized individuals access to the scene. These folks should have knowledge of basic crime scene analysis
    - In court, the integrity of the evidence may be in question if there are too many people milling around
  - Document who is at the crime scene
  - Document who were the last individuals to interact with the systems
  - If the crime scene does become contaminated, document it. The contamination may not negate the derived evidence, but it will make investigating the crime more challenging

# Crime Scene

- The original media should have two copies created:
  - A primary image (a control copy that is stored in a library)
  - A working image (used for analysis and evidence collection)
  - Before creating these images, the investigator must make sure the new media has been properly purged, meaning it does not contain any residual data
- These should be time stamped to show when the evidence was collected
- Investigator works from the duplicate image because it preserves the original evidence
  - Prevents inadvertent alteration of original evidence during examination, and allows recreation of the duplicate image if necessary

# Crime Scene

- Digital data are volatile and can be contained in the following:
  - Registers and cache
  - Process tables and ARP cache
  - Contents of system memory
  - Temporary file systems
  - Data on the disk

# Crime Scene

- Acquiring evidence on live systems and those using network storage further complicates matters because you cannot turn off the system in order to make a copy of the hard drive
- To ensure that the original image or data is not modified, it is important to create message digests (hash values) for files and directories before and after the analysis to prove the integrity of the original image

# Chain of Custody

- Evidence from these types of crimes can be very volatile and easily dismissed from court because of improper handling, it is important to follow very strict and organized procedures when collecting and tagging evidence
- Chain of custody should follow evidence through its entire life cycle, beginning with identification and ending with its destruction, permanent archiving, or return to owner
- Each piece of evidence should be marked in some way with the date, time, initials of the collector, and a case number if one has been assigned

# Chain of Custody

- Wires and cables should be labeled, and a photograph of the labeled system should be taken before it is actually disassembled
- Media should be write-protected
- Storage should be dust free and kept at room temperature without much humidity, and, of course, the media should not be stored close to any strong magnets or magnetic fields

# Chain of Custody

- The crime scene should be photographed, including behind the computer if the crime involved some type of physical break-in
- All storage media should be contained, even if it has been erased, because data still may be obtainable
- After everything is properly labeled, a chain of custody log should be made of each container and an overall log should be made capturing all events

# Evidence

- The next step is the analysis of the evidence. Forensic investigators use a scientific method that involves
- Determining the characteristics of the evidence, such as whether it’s admissible as primary or secondary evidence as well as its source, reliability, and permanence
- Comparing evidence from different sources to determine a chronology of events

# Evidence

- Event reconstruction, including the recovery of deleted files and other activity on the system
- This can take place in a controlled lab environment or, thanks to hardware write- blockers and forensic software, in the field
- The interpretation of the analysis should be presented to the appropriate party
- This could be a judge, lawyer, CEO, or board of directors

# Evidence

- Evidence has its own life cycle, and it is important that the individuals involved with the investigation understand the phases of the life cycle and properly follow them
  - The life cycle of evidence includes
  - Collection and identification
  - Storage, preservation, and transportation
  - Presentation in court
  - Return of the evidence to the victim or owner
- Several types of evidence can be used in a trial, such as written, oral, computer generated, and visual or audio
  - Not all evidence is equal in the eyes of the law, and some types of evidence have more clout, or weight, than others

# Best Evidence

- Best evidence is the primary evidence used in a trial because it provides the most reliability
- An example of something that would be categorized as best evidence is an original signed contract
- Oral evidence is not considered best evidence because there is no firsthand reliable proof that supports its validity, and it therefore does not have as good a standing as legal documents
- Oral evidence cannot be used to dispute a legal document, but it can be used to interpret the document.

# Secondary Evidence

- Secondary evidence is not viewed as reliable and strong in proving innocence or guilt (or liability in civil cases) when compared to best evidence
- Oral evidence, such as a witness’s testimony, and copies of original documents are placed in the secondary evidence category

# Direct Evidence

- Direct evidence can prove a fact all by itself and does not need backup information to refer to. When direct evidence is used, presumptions are not required
- One example of direct evidence is the testimony of a witness who saw a crime take place
- Oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up
- Direct evidence often is based on information gathered from a witness’s five senses

# Circumstantial Evidence

- Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact
- This type of fact is used so the judge or jury will logically assume the existence of a primary fact
- For example, if a suspect told a friend he was going to bring down eBay's web site, a case could not rest on that piece of evidence alone because it is circumstantial. However, this evidence can cause the jury to assume that because the suspect said he was going to do it, and hours later it happened, maybe he was the one who did the crime

# Corroborative Evidence

- Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own but is used as a supplementary tool to help prove a primary piece of evidence.

# Hearsay Evidence

- Hearsay evidence pertains to oral or written evidence presented in court that is second- hand and has no firsthand proof of accuracy or reliability
- If a witness testifies about something he heard someone else say, it is too far removed from fact and has too many variables that can cloud the truth

# Surveillance

- Two main types of surveillance are used when it comes to identifying computer crimes:
  - Physical surveillance
  - Computer surveillance
- Physical surveillance
  - Pertains to security cameras, security guards, and closed-circuit TV (CCTV), which may capture evidence
- Computer surveillance
  - Pertains to auditing events, which passively monitors events by using network sniffers, keyboard monitors, wiretaps, and line monitoring

# Homework

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

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

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

# Questions

- ?