Sec+ 501 Get Certified Topic 11 – Implementing Policies to Mitigate Risks

CH 11 – EXPLORING SECURITY POLICIES

- Security Policy:
  - Written documents that lay out a security plan within a company to reduce and manage risk.
  - Helps prevent incidents, data loss and theft when implemented with procedures.
  - Can be a large single document or divided into several smaller documents depending on the needs of the company
- SOP – Standard Operating Procedure
  - Step to step instructions employees can use to perform common tasks or routine operations
- **Remember this:**
  - **Written security policies are administrative controls that identify a security plan. Personnel create plans and procedures to implement security controls and enforce the security policies.**
- AUP – Acceptable Use Policy
  - Defines Proper System Usage or rules of behaviour for employees when using IT systems
  - Describes purpose of computer systems/networks, how users can access them and responsibilities of users when they access the systems
  - E.G: Monitoring websites and data sent out via email
  - AUP may include privacy statements informing users what computer activities that they may consider private and often includes definitions + examples of unacceptable use
- Mandatory Vacation
  - Mandatory vacation policies require employees to take time away from their job. These policies help to deter fraud and discover malicious activities while employee is away.
- Separation of duties
  - Separation of duties prevents any single person or entity from controlling all functions of a critical or sensitive process by dividing tasks between employees. This helps prevent

potential fraud, such as if a single person prints and signs checks.
    - E.G: Accounting, if one person signs and prints of accounting statements, they could easily embezzle money out of the business if not checked. Segregation of duties separates roles to make sure integrity of bills are not compromised
- Job rotation
    - Job rotation policies require employees to change roles on a regular basis. Employees might change roles temporarily, such as for 3-4 weeks or permanently. This helps ensure employees can't continue with fraudulent activity indefinitely.
- Clean Desk Policy
    - Directs users to Keep areas organized and free of papers
    - Goal: Reduce threats of security incidents by ensuring protection of sensitive data
    - Items left on desks that should be cleared include:
        - Keys, Cellphones , Access Cards, sensitive documents/papers, logged on computer, printouts, passwords on post-it notes, file cabinets left open, PII documents/items etc.
    - E.G: Don't leave password on post-it note as an infiltrator might be able to access computer via shoulder surfing
- **Remember this:**
    - **A clean desk policy requires users to organize their areas to reduce risk of possible data theft. Reminds users to secure sensitive data and may include a statement about not writing down passwords**
- Background check
    - Checks potential employee history with intention of discovering anything about person that might make him a less ideal fit for a job
- NDA – Non disclosure agreement
    - Agreement between 2 entities to ensure proprietary data is not disclosed to unauthorized entities.

        - E.G: Collaboration of project where 2 parties share proprietary data to each other and distribution of data is limited.
- Exit Interview –
    - Conducted with departing employees before they leave an organization.
    - E.G:
        - What did you like/dislike about your job here?
        - Can you tell me what prompted you to leave this position?
        - What skills did you learn?
        - What was your working relationship with your supervisor and peers? Etc.
    - User accounts should be disabled. Collect staff equipment such as tablets, smartphones, badges, proximity cards etc.
- Onboarding –
    - Process of granting individuals access to an organization's computing resources after being hired.
        - E.G: Providing user account with least privilege
    - Offboarding is opposite of onboarding, revoking access
- Policy violations and adverse actions
    - Supervisor may: Choose to document as written counselling and place warning in employee's HR folder
    - Fire the man/woman with letter of notice, reason
- Other general security policies
    - Implement personnel management policies that affect other areas of an employee's life
        - E.G: Behaviour on social media and use of email
- **Remember this:**
    - **Social media sites allow people to share personal comments with a wide group of people. However, improper use of social networking sites can result in inadvertent information disclosure. Attackers can also use information available on these sites to launch attacks against users or in a cognitive password attack to change a user's password. Training helps users understand the risks.**

- Banner Ads and Malvertisement
  - Attackers deliver malware through malicious banner ads for several years. These advertisements look like regular ads but contain malicious code. Many are flash applets and others redirect users to another server
  - Usually used on social media and mainstream sites
    - 1. Via buying ads
    - 2. Attacking web site and inserting ads onto the website
- Social Networking and P2P
  - P2P: Peer-to-peer file sharing allows users to share files, video and data over the internet.
  - Organisations usually restrict P2P due to consuming network bandwidth and slowing down other systems on network.
  - Main reason is Data Leakage
    - Unintentionally shares files.
  - Block P2P via firewall
- **Remember this:**
  - **Data leakage occurs when users install P2P software and unintentionally share files. Organizations often block P2P software at the firewall.**
- Agreement Types:
  - ISA – Interconnection security agreement
    - Specifies technical and security requirements for planning, establishing, maintain and disconnecting a secure connection between 2 or more entities.
      - E.G: Stipulating certain types of encryption for all data in transit
  - SLA – Service Level agreement
    - Agreement between company and vendor stipulating performance expectations such as minimum uptime and maximum downtime levels.
    - Used in contracting services from service providers such as ISP's and CSP's. Include monetary penalties if broken
  - MOU/MOA – Memorandum of understanding/agreement
    - Expresses understanding between 2 or more parties indicating intention to work together towards a common goal

        - Doesn't include monetary penalties
    - BPA – Business partners agreement
        - Written agreement detailing relationship between business partners and obligations towards partnership.
        - E.G: Profits/Losses each partner will take, responsibilities to each other, leaving partnership factors etc.
        - Helps settle conflicts when arisen
- **Remember this:**
    - **A memorandum of understanding or memorandum of agreement (MOU/MOA) defines responsibilities of each party but is not as strict as a service level agreement (SLA) or interconnection security agreement (ISA). If parties will be handling sensitive data, they should include an ISA to ensure strict guidelines are in place to protect data while in transit. MOU/MOA often support ISA.**

PROTECTING DATA

- Information Classification
    - Top secret, secret, confidential, unclassified – sensitivity of government documents
    - Proprietary, private, Confidential, public – Private companies
    - Public data – available to everyone
    - Confidential data – Information organization intends to keep secret among a certain group of people.
    - Proprietary data – data related to an ownership
        - E.G: Patents or trade secrets
    - Private data – Information about an individual that should remain private
        - E.G: PII and PHI (Personal Health Information)
- Data Labelling – Ensures data are handled and processed.
    - R&D – Research and Development
        - Should be classified and labelled
- **Remember this:**
    - **Data classifications and data labelling help ensure personnel apply proper security controls to protect information.**

- Data Destruction and Media Sanitization
  - When computers reach end of their life cycles, organizations donate, recycle or destroy/throw them away.
  - Must ensure data isn't included to people outside organization if unauthorized people receive it.
  - Sanitization ensures personnel remove all usable data from system.
    - Purging – All sensitive data has been removed from device
    - File shredding – Overwriting space where file is located with 1's and 0's.
    - Wiping – Removing all remnants of data on a disk.
    - Erasing and Overwriting
      - SSDs (Solid State Drives) require special processes for sanitization. Traditional drive tools aren't as effective so smash/physically destroy them.
    - Burning
      - Burn materials in an incinerator
    - Paper shredding
    - Pulping
      - Additional step after shredding paper. Reduce paper to mash/puree.
    - Degaussing
      - Degausser is a powerful electronic magnet. Passing a disk through a degaussing field renders data on tape/magnetic disk unreadable.
    - Pulverising
      - Physical destruction of media such as with a hammer
    - Cluster Tip Wiping
      - Special process removing random data stored at end of a file. Useful when you want to keep a file but remove random data. Files are stored in clusters of about 4KB.
- Data retention Policy –
  - **Identifies how long data is retained and sometimes specifies where it is stored**

  - Reduces amount of resources such as hard drive space or backup tapes required to retain data.
  - Reduces Legal liabilities
- PII and PHI
  - PII – Personal Identifiable Information
  - PHI – Personal Health Information
- **Remember this:**
  - **PII includes information such as a full name, birth date, biometric data and identify numbers such as a SSN. PHI is PII that includes medical or health information. Organizations have an obligation to protect PII and PHI and often identify procedures for handling and retaining PII in data policies.**
- Legal and Compliance Issues:
  - HIPAA – Health Insurance Portability and Accountability Act of 1996
    - Mandates organizations protect PHI such as health of an individual held by doctors, hospitals etc.
  - GLBA – Gramm-Leach Bililey Act
    - Financial Services Modernization Act and includes a Financial Privacy Rule
    - Rule: Financial institutions must provide consumers with a privacy notice explaining what information they collect and what information is used
  - SOX – Sarbanes Oxley Act
    - Executives within an organization take individual responsibility for accuracy of financial reports. Includes specifics on auditing and identifies penalties for noncompliance
    - Was passed after several accounting scandals
  - GDPR – General Data Protection Regulation
    - EU regulation mandating protection of privacy data for individuals within EU
- Data Roles and responsibilities
  - Owner – overall responsibility of data
    - E.G: CEO or department head
    - Responsible for classification of data, security controls are implemented and data is labelled correctly

- Steward/Custodian –
  - Handles routine tasks to prevent data
    - E.G: Backup tape classification and storage times
- Privacy Officer
  - Executive position within an organization.
  - Ensures organization is complying with relevant laws such as HIPAA, SOX etc.

- **Remember this:**
  - **Key data roles within an organization are responsible for protecting data. Owner has overall responsibility for protection of data. Steward or custodian handles routine tasks to protect data. Privacy officer is an executive responsible for ensuring organization complies with relevant laws**
- **Remember this:**
  - **An incident response policy defines a security incident and incident response procedures. Incident response procedures start with a preparation to prepare for and prevent incidents. Preparation helps prevent incidents such as malware infections. Personnel review the policy periodically and in response to lessons learned after incidents.**
    - E.G: One hacker broke into a government system which had a welcome message. After this, government used warning banners telling users that only authorized personnel should be accessing system.
- IRP – Incidence response plan
  - Provides more detail than an incident response policy. Provides organizations a formal coordinated plan personnel can use when responding to an incident.
    - Definitions of Incidence Types
      - Helps employees identify difference between an event and an actual incident.
      - Incidents include attacks from botnets, malware from email, data breach, ransomware etc. and categorise them into specific sections
    - Cyber-incident response teams

        - Compromised of employees with expertise in different areas.
        - CIRT – Cyber-incident response team, or security incident response team. Each team has knowledge/skills to respond to an incident and usually have extensive training such as collecting, validating, identifying evidence etc.
    - Roles and Responsibilities
        - Specific roles for an incident response team with their responsibilities.
    - Escalation
        - Escalation of an incident to inform supervisors of malware infections and resolving it as an example. If critical servers are under attack from a DDoS escalation can require all members to get involved.
    - Reporting Requirements
        - Depends on severity of incident
    - Exercises
        - To test response of all members of the team
        - E.G: Testing admins ability to rebuild a server after a simulated attack.
- Incident Response Process
    - 1. Preparation
    - 2. Identification
    - 3. Containment
    - 4. Eradication
    - 5. Recovery
    - 6. Lessons learned
- **Remember this:**
    - **First step in incident response process is preparation. After identifying an incident, personnel attempt to contain or isolate the problem. This is often as simple as disconnecting a computer from a network. Eradication attempts to remove all malicious components from an attack and recovery returns a system to normal operation. Reviewing lessons**

learned allows a personnel to analyse the incident and response with a goal of preventing a future occurrence.

- Basic Forensic Procedures
  - Forensic Evaluation – Helps organization collect and analyse data as evidence it can use in prosecution of a crime.
    - Usually proceed with assumption that data collected will be used as evidence in court
  - Forensic experts have specialized tools to capture data
    - E.G: FTK (Forensic Toolkit by Access Data)
- Order volatility
  - Order in which you should collect evidence.
  - Volatile – Not permanent. Should collect evidence starting with most volatile and moving to least volatile.
  - Order of volatility from most → least volatile:
    - Data in cache memory, including processor cache and hard drive cache →
    - Data in RAM, including system and network processes →
    - A paging file (swap file) on system disk drive →
    - Data stored on local disk drives →
    - Logs stored on remote systems →
    - Archive media
- **Remember this:**
  - **When collecting data for a forensic analysis, you should collect it form the most volatile to the least volatile. Order of volatility is cache memory, regular RAM, swap or paging file, hard drive data, logs stored on remote systems and archived media.**
- Other specific procedures to ensure evidence isn't modified:
  - 1. Capture specific image
    - Forensic image captures entire content of drive
    - One disk imaging tool used for forensics is the 'dd' command available in Linux
    - Captures entire contents of disk including system files, user files and files marked for deletion but not overwritten
    - Experts then create a copy and analyse the copy. Never modify the original.

    - 2. Take hashes
        - Provides proof that collected data has retained integrity and to make sure that imaging process has not modified data
- **Remember this:**
    - **A forensic image is a bit-by-bit copy of the data and does not modify the data during the capture. Experts capture an image of the data before analysis to preserve original and maintain its usability as evidence. Hashing provides integrity for captured images, including images of both memory and disk drives. You can take a hash of a drive before and after capturing an image to verify that the imaging process did not modify the drive contents.**
- 3. Network Traffic and Logs
    - Prove computer/s was involved in attack through MAC address and other techniques such as tracking ISP
- 4. Capture Video
- 5. Record Time offset
    - Identify exact dates and times when someone created, modified, last saved and last accessed a particular file.
- 6. Screenshot
- 7. Interview Witnesses
- 8. Chain of Custody
    - A process providing assurance that evidence has been controlled and handled properly after collection.
    - Forensic experts usually establish a chain of custody when they first collect evidence.
    - E.G: Provides a record of every person who was in possession of a physical asset collected as evidence.
    - If evidence isn't controlled, someone can modify, tamper and corrupt it. A chain of custody helps aid evidence collecting procedure.
- 9. Legal Hold
    - A court order to maintain different types of data as evidence.
        - E.G: Maintain digital and paper documents for past 3 years of evidence for a fraud case.
    - Data retention policies also apply here.

- **Remember this:**
  - **A chain of custody provides assurances that evidence has been controlled and handled properly after collection. It documents who handled the evidence and when they handled it. A legal hold is a court order to preserve data as evidence.**
- Recovery of Data
  - Restoring Data
  - Forensic tools can be used to recover unsanitized data and system files
- Active Logging for Intelligence Gathering
  - An active logging strategy increases amount of logged data collected on a routine basis.
  - Good for long-term analysis
- Track Man-Hours and expense
- Provide Training
  - Role based training is targeted to personnel based on their roles.
  - Goal: Minimize risk to an organization providing users training to better prepare themselves to avoid threats
    - Data Owners
    - System Administrators
    - System Owners
    - Users
    - Privileged User
    - Executive User
    - Incident Response team
- **Remember this:**
  - **Role-based training ensures employees receive appropriate training based on their roles in the organization. Common roles that require role-based training are data owners, system administrators, end users, privileged users and executive users.**
- Organizations should abide by certain standards such as the PCI DSS – Payment Card Industry Data Security Standard including 6 control objectives and 12 specific requirements to prevent fraud.
- Personal issues:

    - Insider threat, personal email, policy violation, social engineering and social media.
- When policy violations are detected, management acts based on organization's policies. This can include termination or verbal counselling.