Chapter 11

Implementing policies to mitigate risks

horizontal line

# Personnel managing policies

**Acceptable use policy**

AUP defines proper system usage when using company systems.

**Mandatory vacations**

They can detect fraudulent activity while the employee is away, as another person will be covering.

**Separation of duties**

It prevents any single person or entity being able to complete all the functions of a critical or sensitive process. This reduces fraud.

**Job rotation**

Employees rotate through different roles in order to learn different processes. This ensures that employees cannot continue with fraudulent activity.

**Clean desk policy**

Keeping desk clean and free of papers; this reduces the threat of data exfiltration by people in the office.

**Background check**

Gives info on an employee which can identify risky employees

**NDA**

Ensures that data cannot be leaked or sold.

**Exit interviews**

Useful for gaining information on what to improve, and reminding them of NDAs they signed. It is also to confiscate sensitive material, such as cards or docs. User accounts are also disabled.

**Onboarding**

The process of granting access after hiring. When an employee leaves, it is important to revoke access

**Policy violations and adverse actions**

Policy violations are documented and acted upon accordingly

**Social media**

Social media can be used to obtain info on employees, which can then be used for cognitive password resets of accounts. It can also be used to impersonate a friend or someone they know.

**Banner ads and malware ads**

Some ads can contain flash applets with malicious code

**Social networking and P2P**

P2P pps can consume bandwidth, and also slow down other systems on the network. They can also lead to data exfiltration. This can be prevented by blocking access in firewalls.

**Agreement types**

* ISA: Interconnection security agreement, specifies technical and security requirements in a company
* SLA: Service level agreement, Agreement between a company and vendor which stipulates performance expectations, and max downtime levels
* MOU/MOA: Memorandum of understanding/agreement, Used to support the goal of an ISA, as it defines the responsibilities of each party when working towards a common goal.
* BPA: Business partners agreement, identifies shares of profits or losses each partner will take. Helps settle conflicts

**Protecting data**

**Data sensitivity and labelling**

Ensures users know what data they are handling via labels such as confidential etc.

This can help protect proprietary data which is related to things like patents

**Data destruction and media sanitisation**

When computers reach end of life, it is important to sanitise them of data before disposing of them.

Purging: Indicates all sensitive data has been removed from device

File shredding: Overwrites the space where the file is located with 0s and 1s

Wiping: Process of completely removing all data from a disk

Erasing and overwriting: Physically destroying

Burning:

Paper shredding

Pulping: Additional step after shredding, to reduce it to mash

Degaussing: Electromagnet, renders data on tape unreadable

Pulverising: physically destroying media

**Data retention policies**

Identifies how long data is retained

**PII and PHI**

Personal health info and PII must be protected, and they must identify procedures for handling and retaining PII in data policies.

**Legal and compliance issues**

* HIPAA: Health insurance portability and accountability, mandates that all organisations protect PHI
* GLBA: Requires financial services to provide customers with a privacy note
* SOX: Requires that execs take responsibility for ensuring accuracy of financial reports
* GDPR: Data protection for EU

**Data roles and responsibilities**

* **Owner**: responsible for data labelling and handling, and ensuring security controls are implemented
* **Steward/custodian**: Handles routine tasks to protect data, such as regular backups and proper labelling
* **Privacy officer**: Ensures company is complying with relevant data laws.

**Responding to incidents**

Incident response policies help personnel identify and respond to incidents. This can also cause a policy review and update.

**Incident response plan**

Formal plan that personnel can use when responding to an incident. Includes:

* Definitions of incident types
* Cyber-incident response team: Have the knowledge and skills to respond to an incident
* Roles and responsibilities: Identify specific roles for the IR team
* Escalation: Gets the necessary personnel involved
* Reporting requirements: Outlines who needs to be notified and when
* Exercises: Test the response of all members in a team

**IR process**

1. Preparation: Guidance to personnel, as well as establishing procedures
2. Identification
3. Containment: Incident is isolated and contained
4. Eradication: Removing components form the attack
5. Recovery: returning all processes to normal, inc backups etc
6. Lessons learned: Review procedures and policies to improve

**Basic forensic procedures**

Help collect and analyse information, and prevent any modification of it

**Order of volatility**

Refers to order in which you should start collecting data; you should collect it from most volatile to least volatile. The order, from most volatile to least volatile, is:

1. Data in cache
2. Data in RAM
3. Paging file, an extension of RAM
4. Data on local disk drives
5. Logs stored on remote systems
6. Archive media

**Data acquisition and preservation of evidence**

Ensures that data is not modified

Capture system image: Forensic image of disk is taken bit by bit and analysed.

Hashes: Hash is taken of data, and then write-protected. Later, another has is taken and compared. If they are the same, then data has not been modified.

**Network traffic and logs**

Packet analysers can identify mac addresses of offending computers, and IPs can be traced with the ISP. Network logs can identify what happened and form where.

**CCTV**

Video footage with timestamps can help

**Screenshots**

**Witness interviews**

Witnesses can provide first hand accounts of what happened and when it happened

**Chain of custody**

Process that provides assurance that data has been handled properly, and documents control and possession of data by personnel

**Legal hold**

Refers to a court order to maintain different types of data for evidence

**Data recovery**

Lost data, and data has been deleted is still recoverable through several tools.

**Logging for intelligence gathering**

An active logging strategy can help an organisation gather significant info on attackers. It should increase the amount of logging regularly, and have filters so they only see the data they need. They should be able to view all logs

**Track man hours and expenses**

Man-hours and expenses incurred by an IR team should be logged to improve accuracy of cost values used in a quantitative risk assessment.

**Training**

**Role-based awareness training**

* Data owner: Need to understand their responsibilities when it comes to protecting data
* System admin: Trained on the security of the system
* System owner: Responsible for ensuring that system admins have all the necessary skills
* User: Need to understand common threats
* Privileged user: Need training on classification and handling of data
* Exec user: need high level briefings , and info on everything
* IR team: Detailed info on how to respond to incidents

**ACRONYMS**

**Agreement types**

ISA: Interconnection security agreement, specifies tech and sec requirements

SLA: Service level agreement, agreement between company and vendor which stipulates performance expectations

MOU/MOA: Memorandum of understanding/agreement, used to support goal outlines in ISA

BPA: Business partners agreement, outlines shares of profits or losses each partner takes. Helps settle conflicts.

**Legal and compliance issues**

HIPAA: Health insurance portability and accountability, mandates that all organizations protect PII

GLBA: Requires financial companies to provide customers with a privacy note.

SOX: Requires that execs take responsibility for financial report accuracy