PRINCIPLES OF SECURITY

Lesson Date	@March 5, 2024
Status	Complete

CIA TRIAD — Information security model used to create security policy

1. C for confidentiality: Data is only accessible to authorized people
2. I for integrity: Data cannot be altered by unauthorized people
3. A for availability: Data is available

PRINCIPLES OF PRIVILEGES

Levels of access given to individuals are based on 2 factors :

1. Individual’s role in the organization
2. sensitivity of the information being stored in the system

2 key concepts used to assign and manage the access rights of individuals:

1. PIM [Privileged Identity Management] —- used to translate a user’s role within an organization into an access role on a system
2. PAM [Privileged Access Management] —- manage the privileges a system’s access role has

MORE SECURITY MODELS

1. Bell LaPadula Model

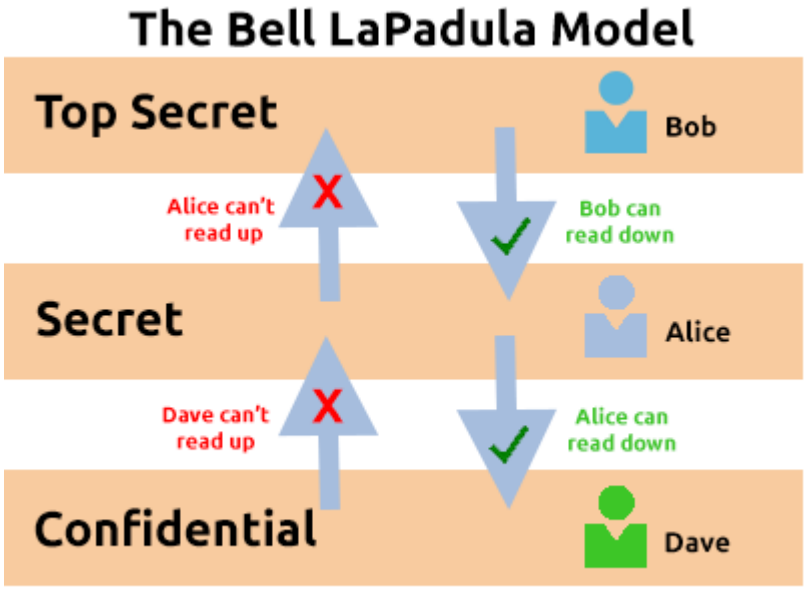
- popular within military and governmental organizations
- used to achieve confidentiality
- uses the rule "**can't** read up, can read down"

ADVANTAGES

- proven to be successful
- policies can be replicated to real-life organization hierarchies
- simple to implement

DISADVANTAGES

- model relies on a large amount of trust within the organization



2. Biba Model

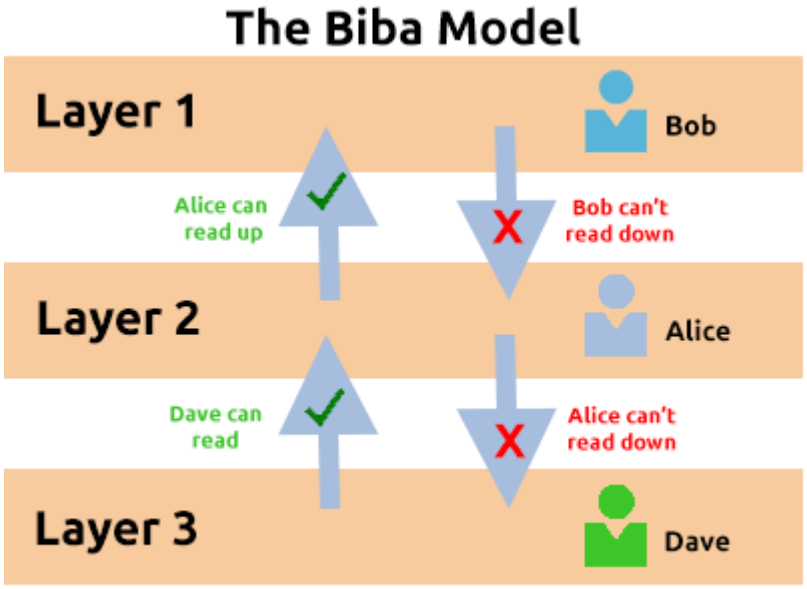
- used to achieve integrity
- The Biba model is used in organisations or situations where integrity is more important than confidentiality. For example, in software development, developers may only have access to the code that is necessary for their job. They may not need access to critical pieces of information such as databases, etc.
- uses the rule "**can** read up, can't read down"

ADVANTAGES

- simple to implement
- resolves the limitations of the Bell-LaPadula model by addressing both data confidentiality and integrity

DISADVANTAGES

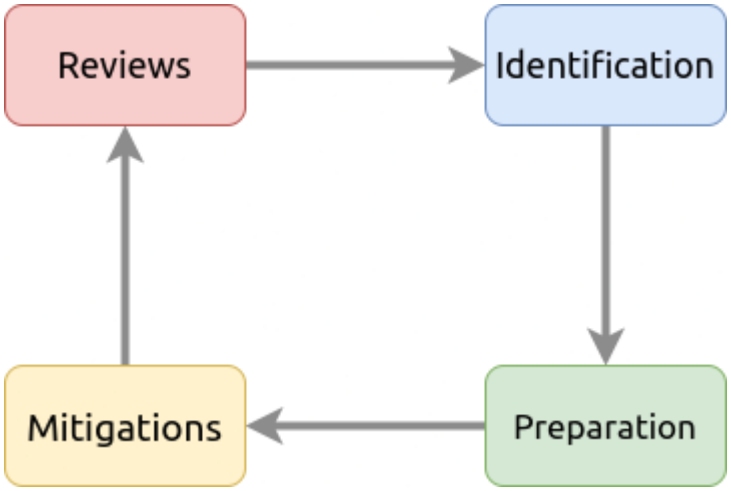
- often results in delays within a business
- THings can easily be overlooked when applying security controls



THREAT MODELLING AND INCIDENT RESPONSE

Threat Modelling

- Process of reviewing, improving and testing the security protocols in place in an organization's IT infrastructure and services
- similar to risk assessment
- components are: PREPARATION, IDENTIFICATION, MITIGATIONS, REVIEW



- an effective threat model consists of :

1. threat intelligence
2. asset identification
3. mitigation capabilities
4. risk assessment

Two important frameworks— **STRIDE** and **PASTA**

Authored by Microsoft security researchers in 1999

> ⚠ STRIDE = Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privileges

> ⚠ PASTA = Process for Attack Simulation and Threat Analysis

Incident Response

- breach of security is called INCIDENT
- Actions taken to resolve the threat are known as Incident Response(IR)
- Incidents are classified using a rating of urgency and impact.

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

- an incident is responded to by a Computer Security Incident Response Team (CSIRT)

Phases in IR

Action	Description
Preparation	Do we have the resources and plans in place to deal with the security incident?
Identification	Has the threat and the threat actor been correctly identified in order for us to respond to?
Containment	Can the threat/security incident be contained to prevent other systems or users from being impacted?
Eradication	Remove the active threat.
Recovery	Perform a full review of the impacted systems to return to business as usual operations.
Lessons Learned	What can be learnt from the incident? I.e. if it was due to a phishing email, employees should be trained better to detect phishing emails.