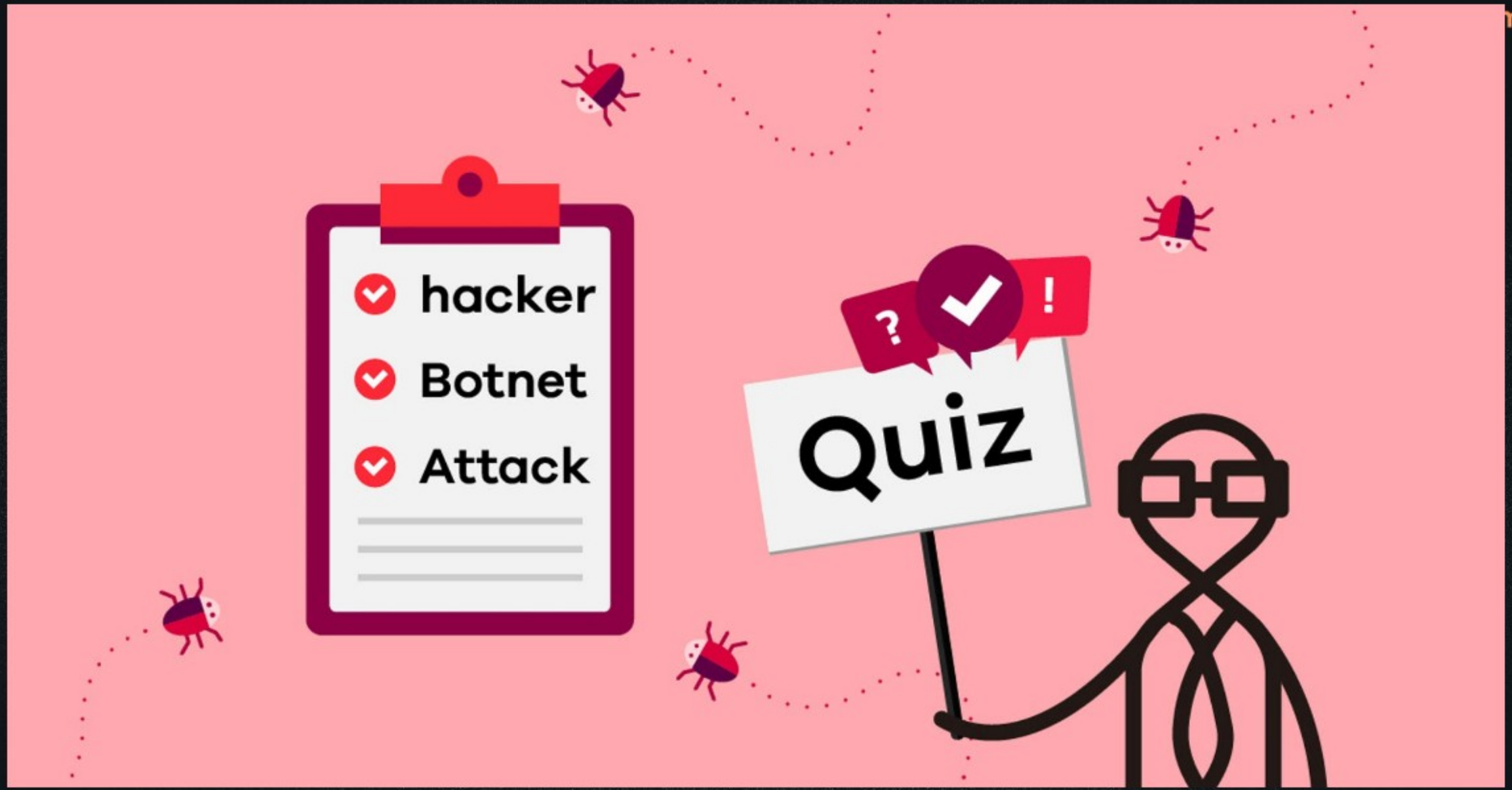
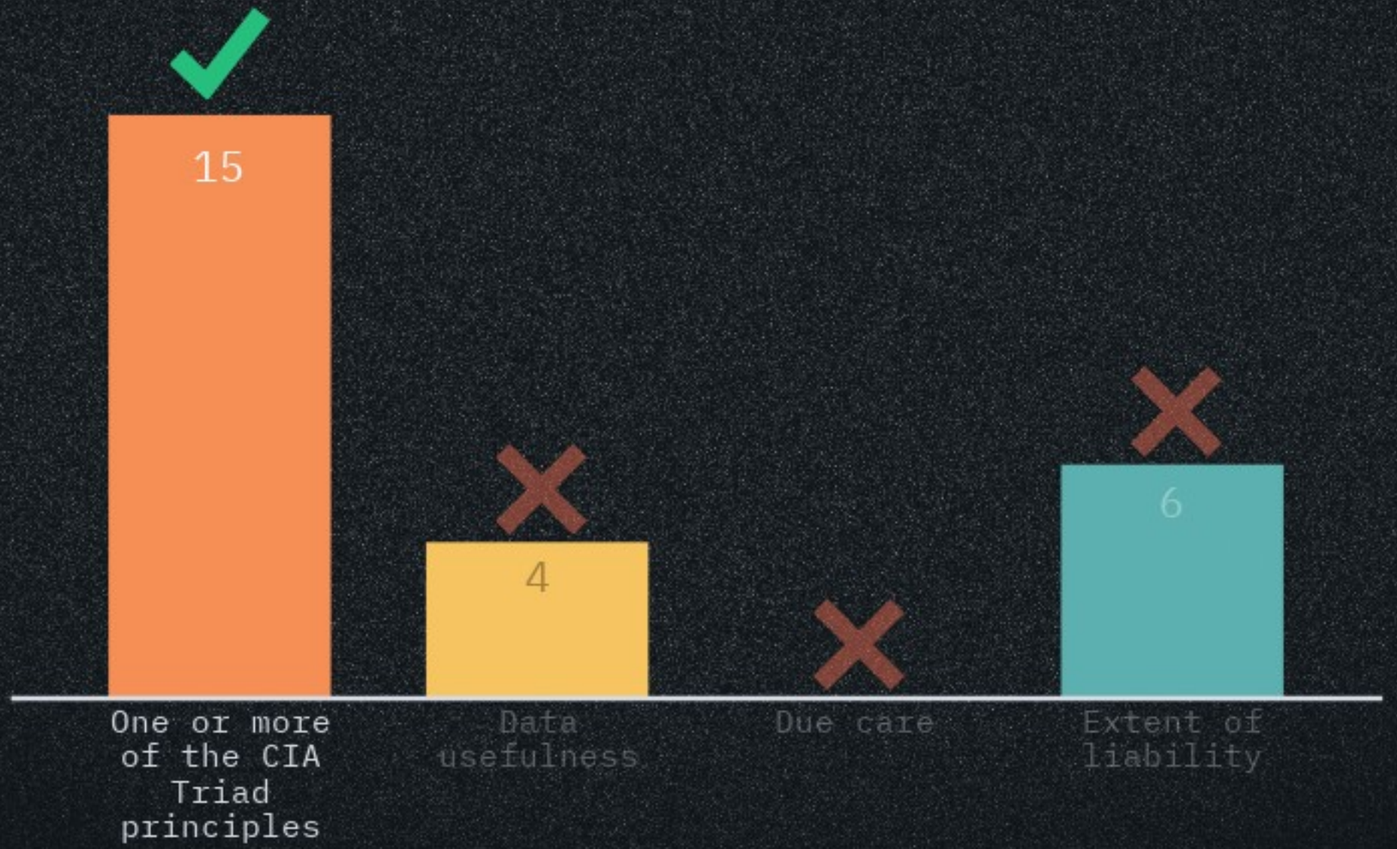

hacker
Botnet
Attack
Quiz

Vulnerabilities and risks are evaluated based on their threats against which of the following?

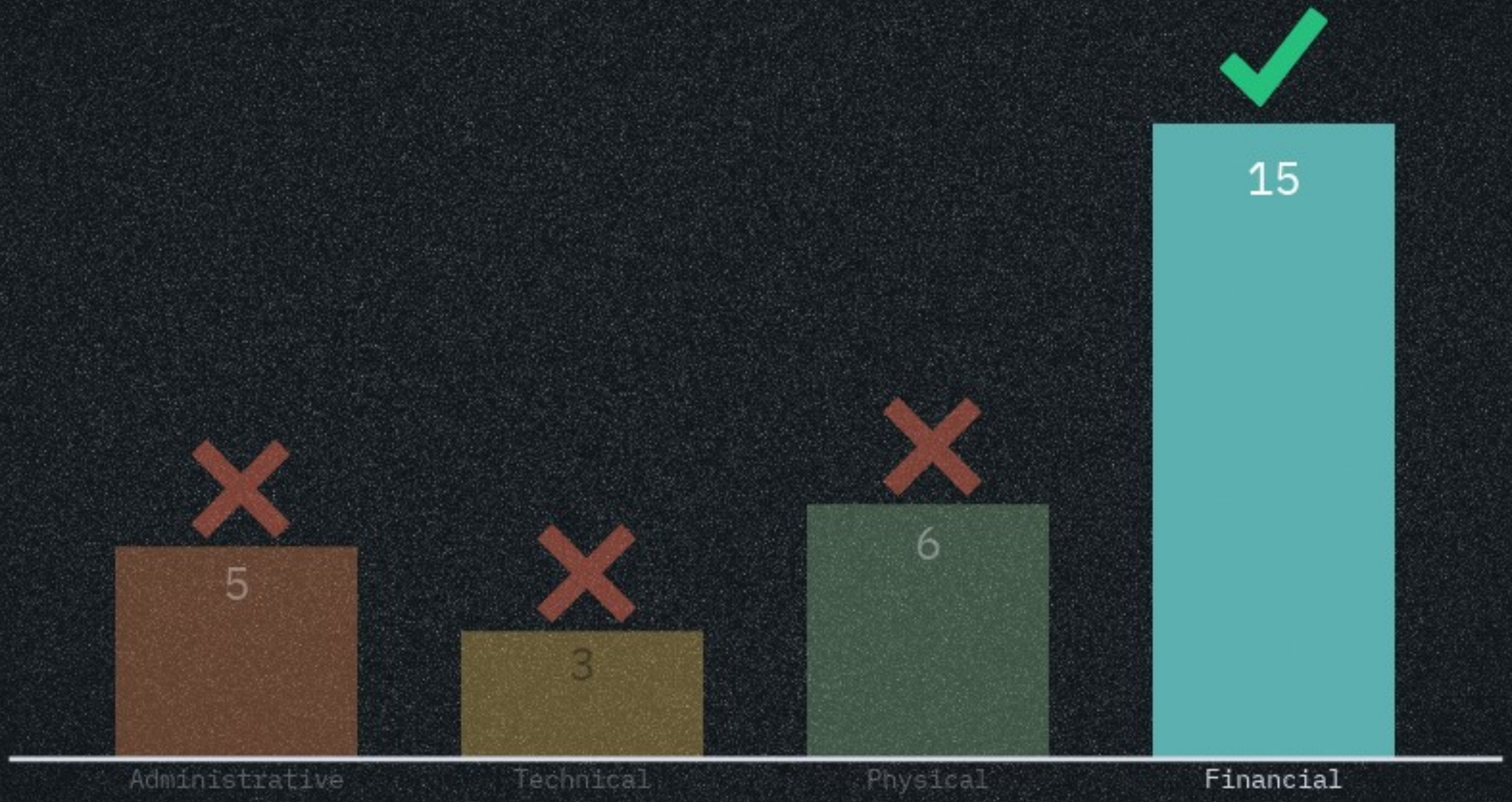


Mentimeter

25

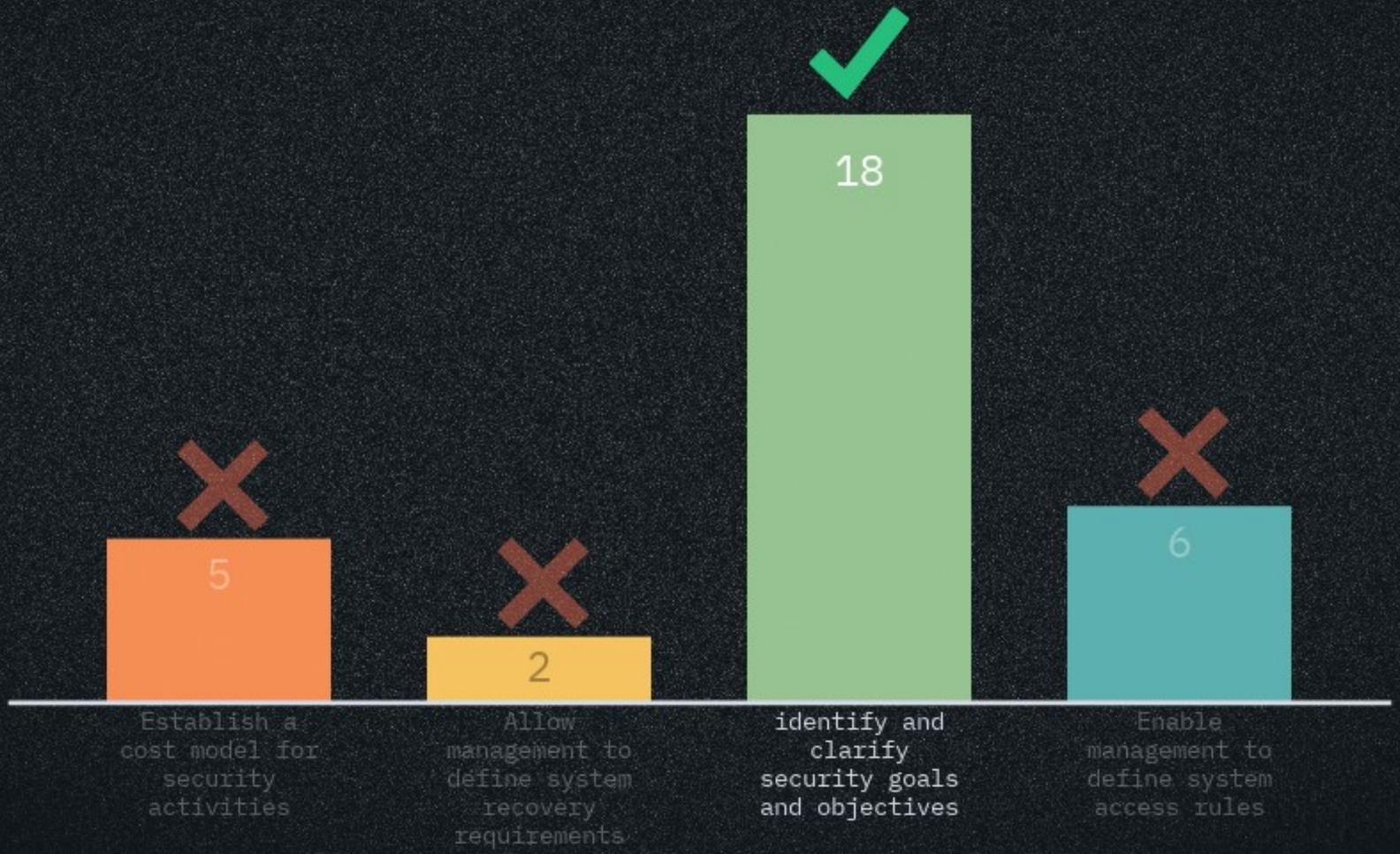
While designing a security framework, controls are placed to protect, which is NOT utilized to achieve management directives to protect company asset

Mentimeter

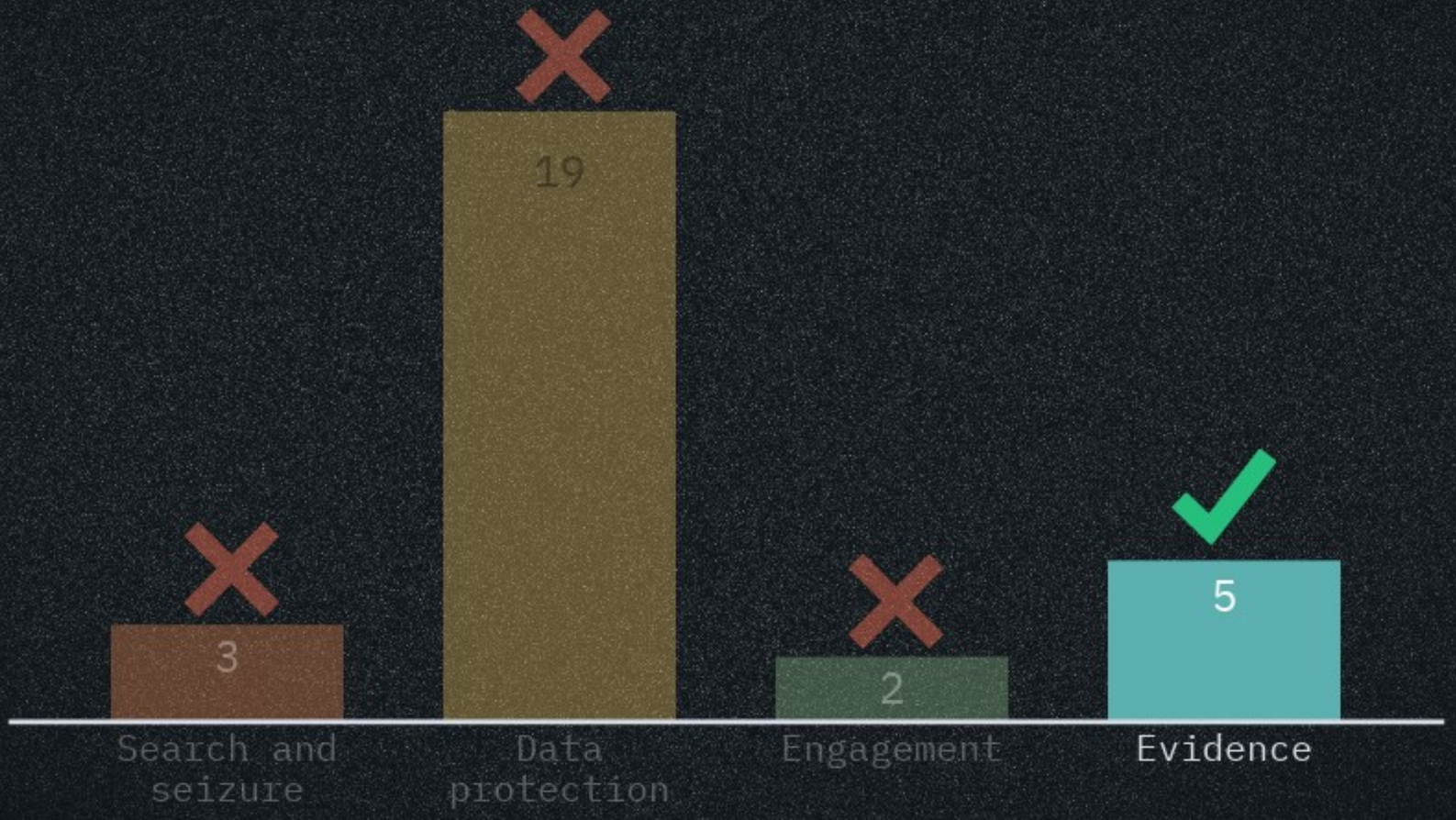


29

John have recently been appointed to develop a security policy for Gaming company, by doing so the company has ensured that it provides a way to



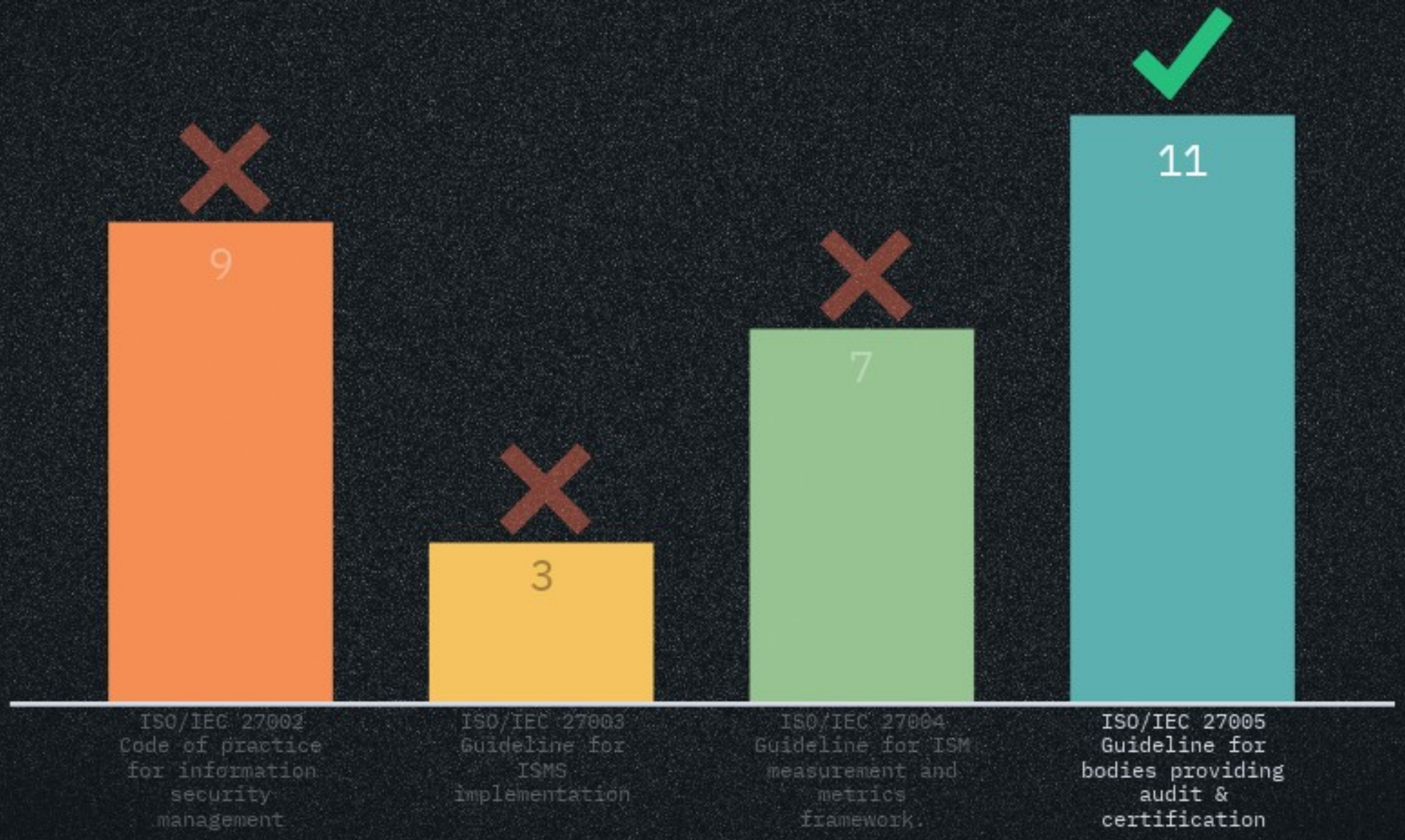
Sam is part of a legal team investigating an attack that compromised a web-server. From legal prespective which is the most critical item listed below



29

Which of the following provides an incorrect mapping of the individual standards that make up the family of ISO/IEC 2700 standards

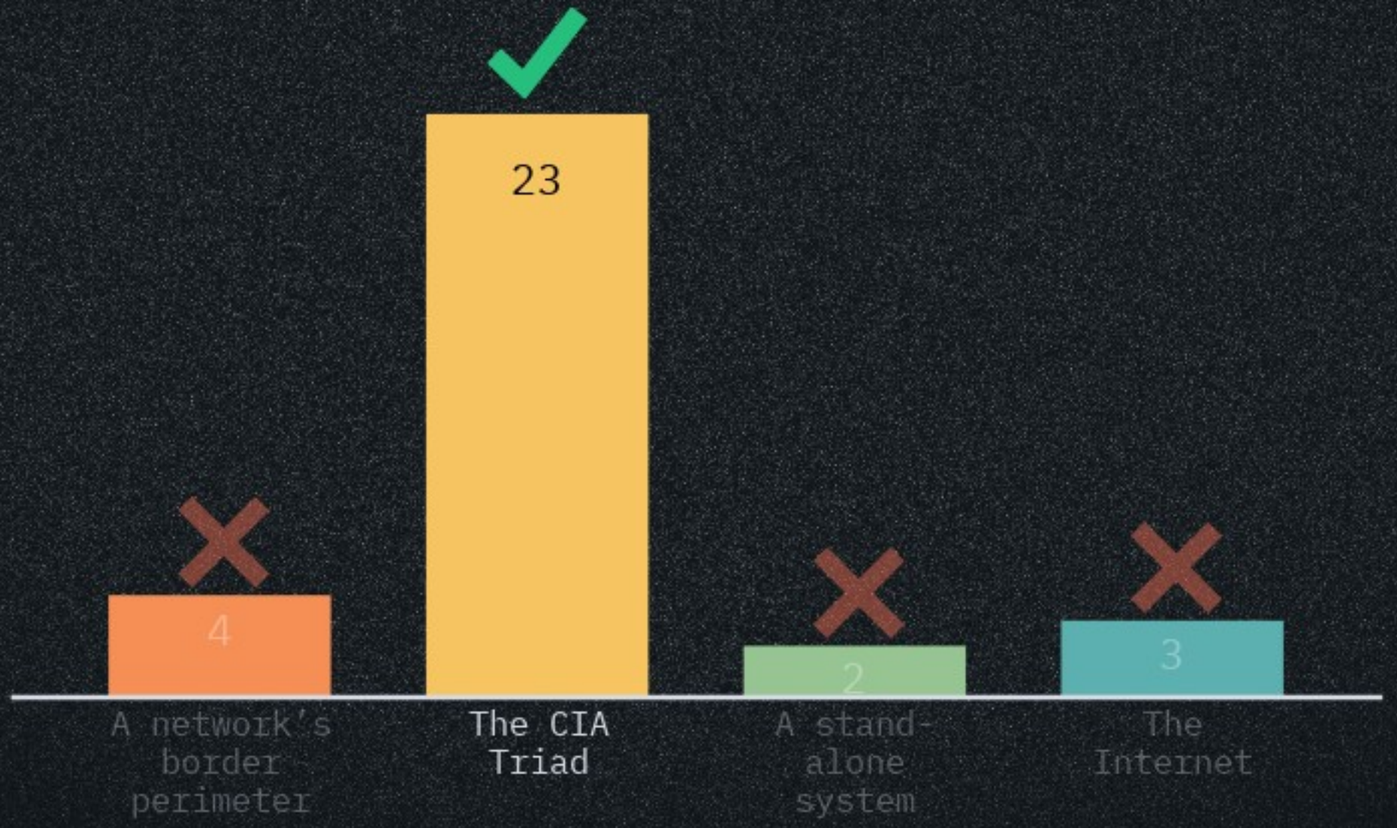
Mentimeter



30

Which of the following contains the primary goals and objectives of security?

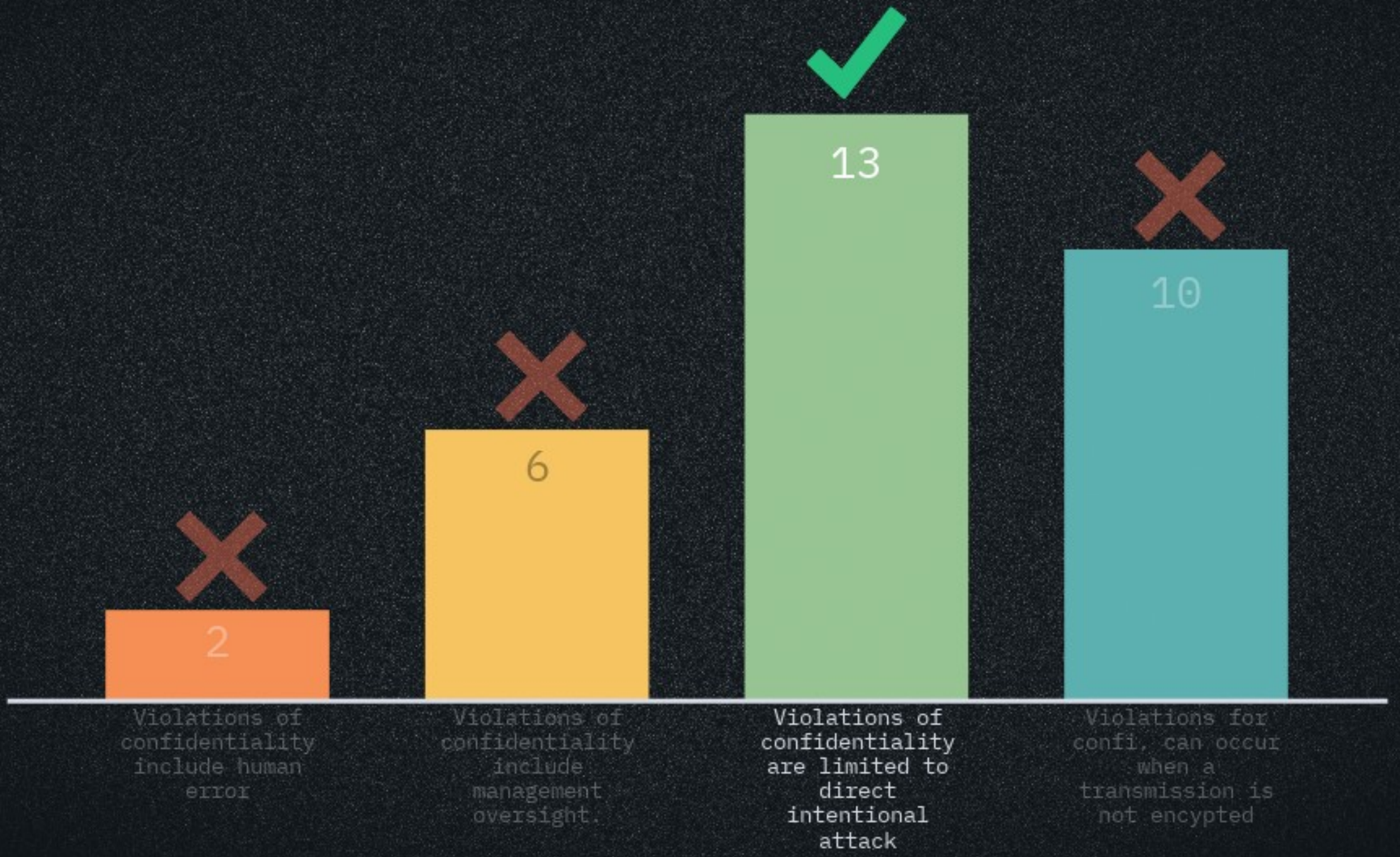
Mentimeter



32

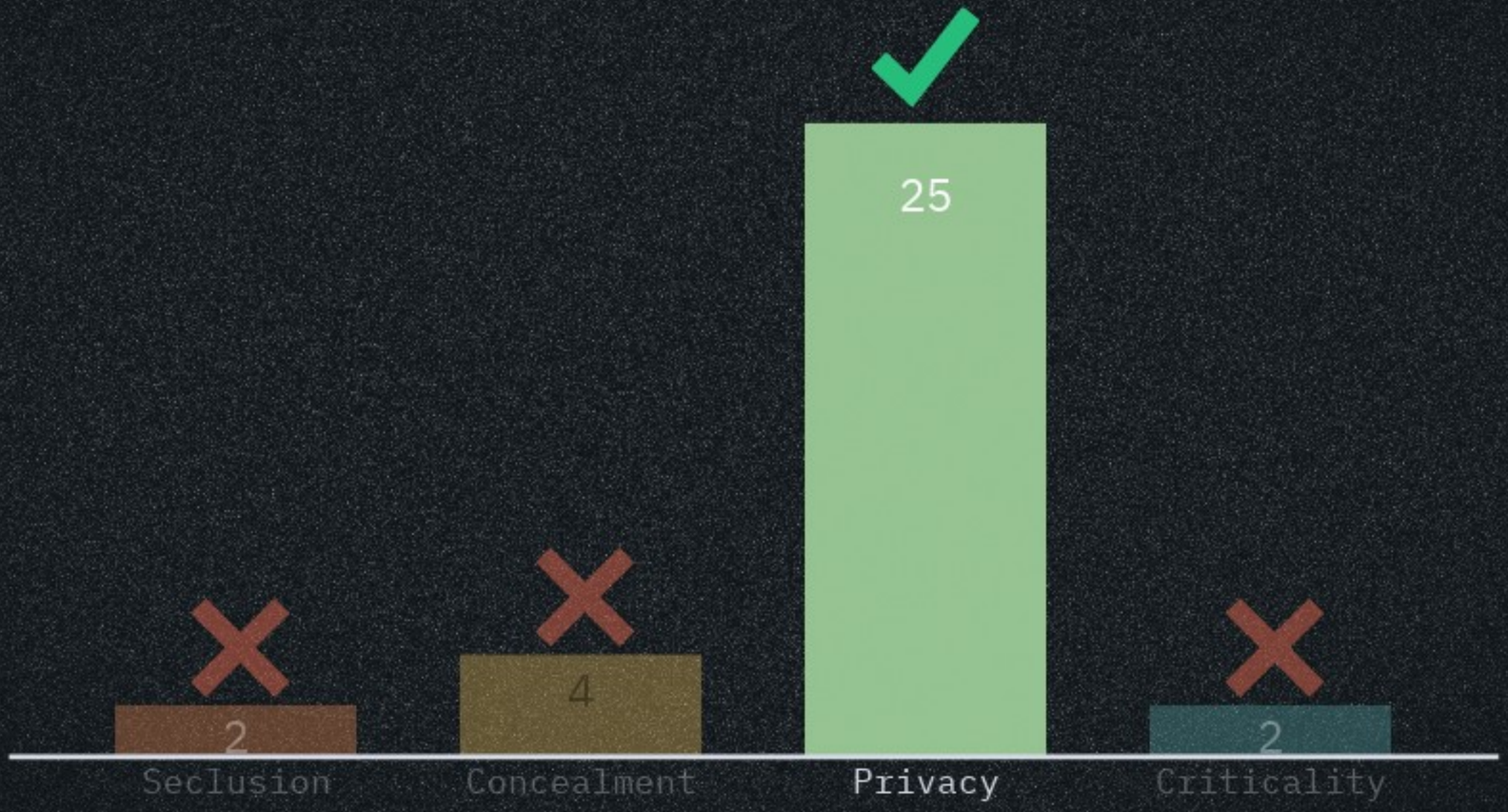
Which of the following is not true?

Mentimeter



31

Refers to keeping information confidential that is personally identifiable or whichmight cause harm, embarrassment, disgrace to someone if revealed

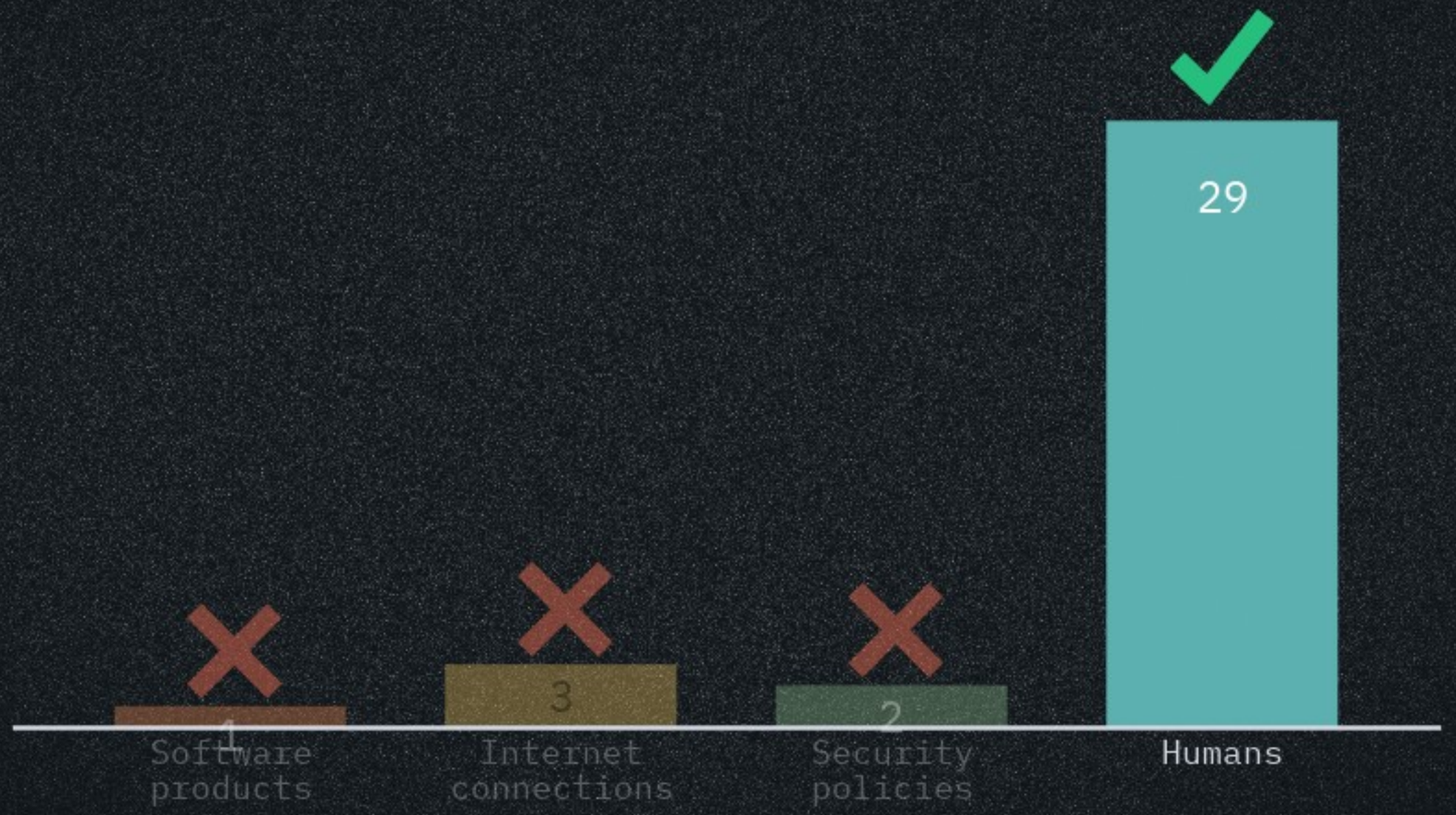


All but which of the following items requires awareness for all individuals affected?

Mentimeter

32

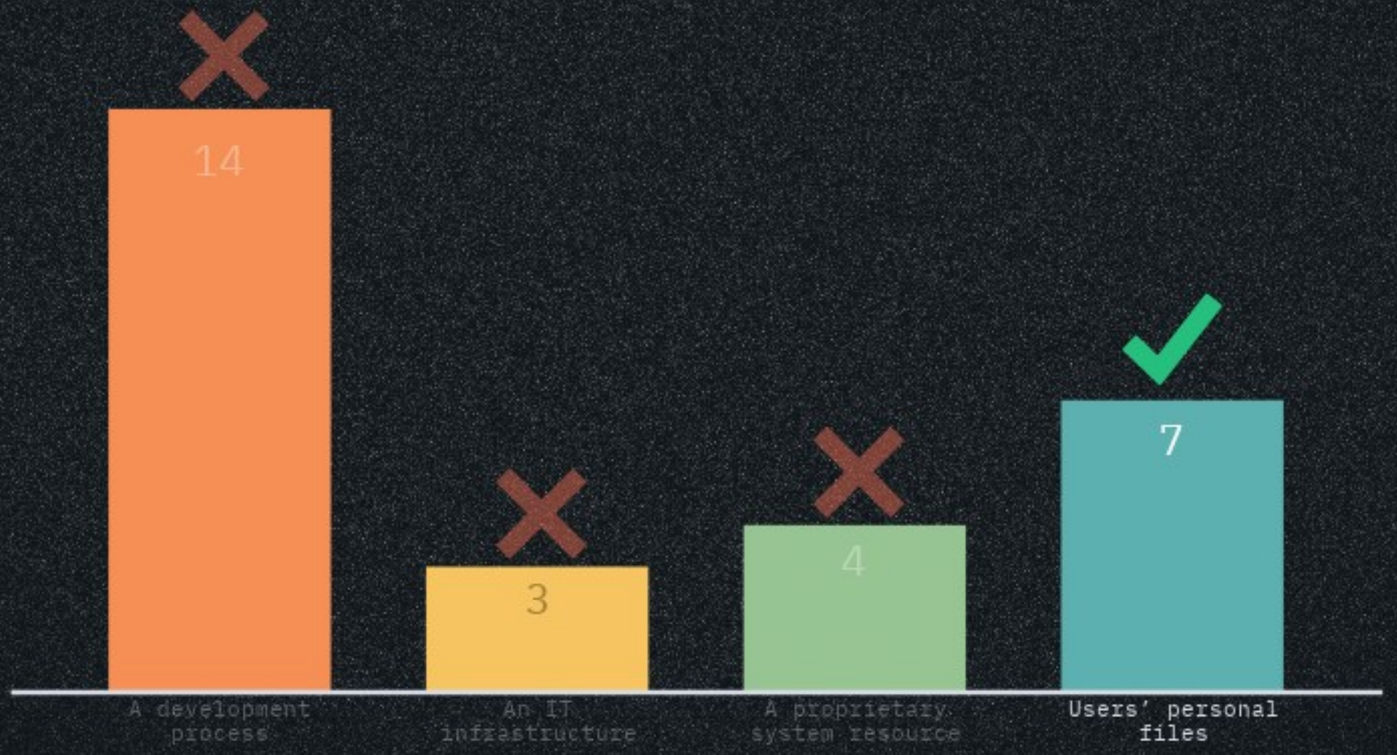
Which of the following is the weakest element in any security solution?



35

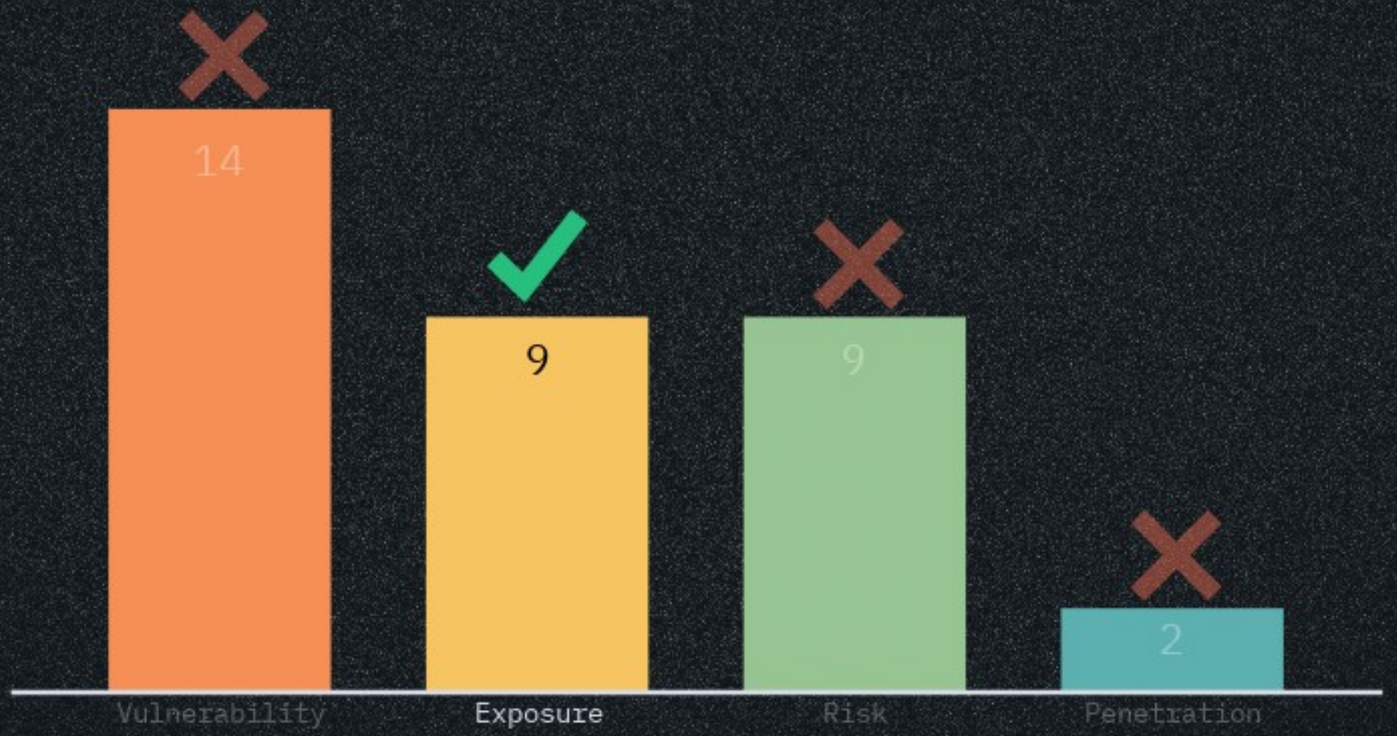
Which of the following would generally not be considered an asset in a risk analysis?

Mentimeter

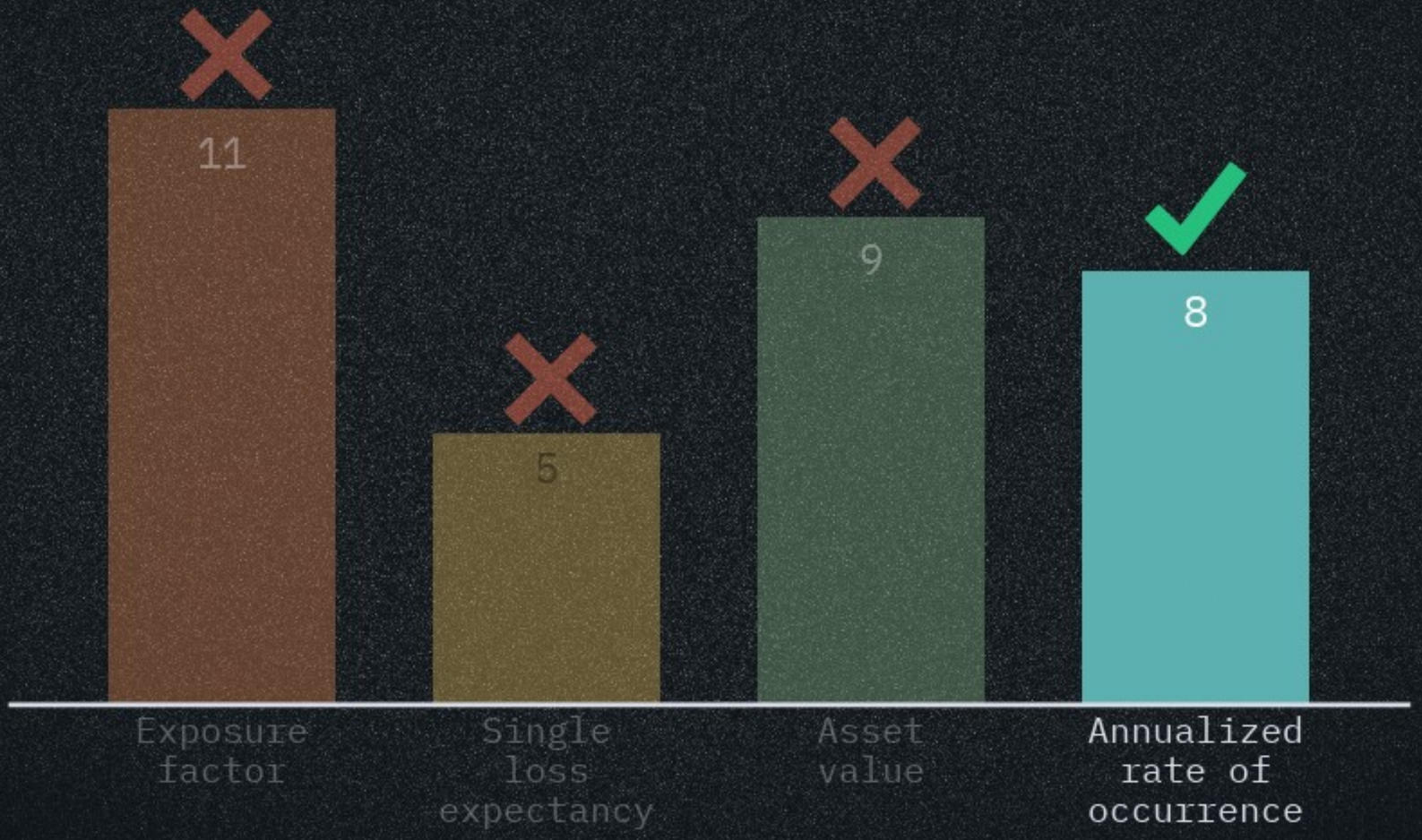


28

When a safeguard or a countermeasure is not present or is not sufficient, what remains?



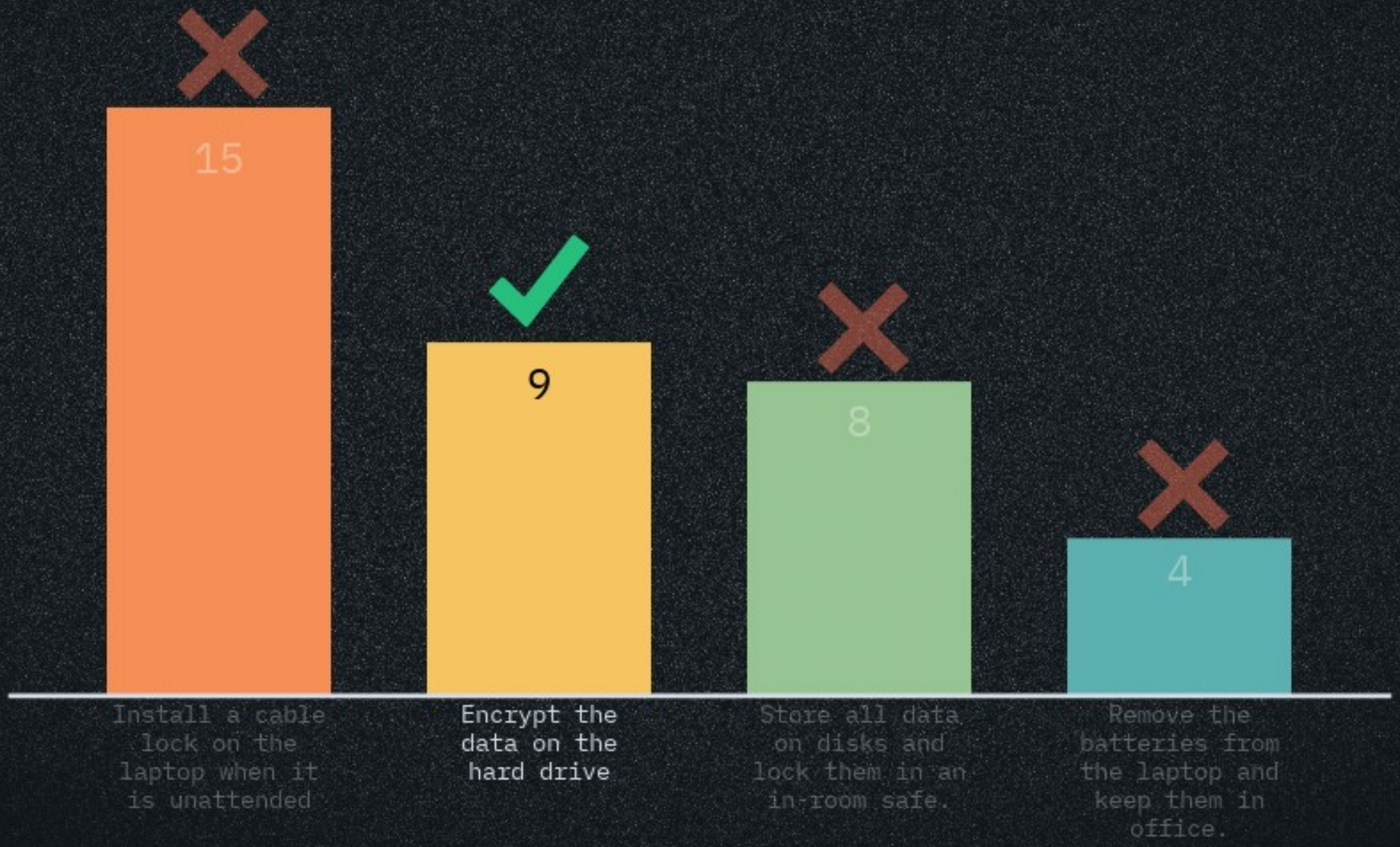
You've performed a basic quantitative risk analysis to select a countermeasure. When the calculations again, which of thefollowing factors will change



Mentimeter

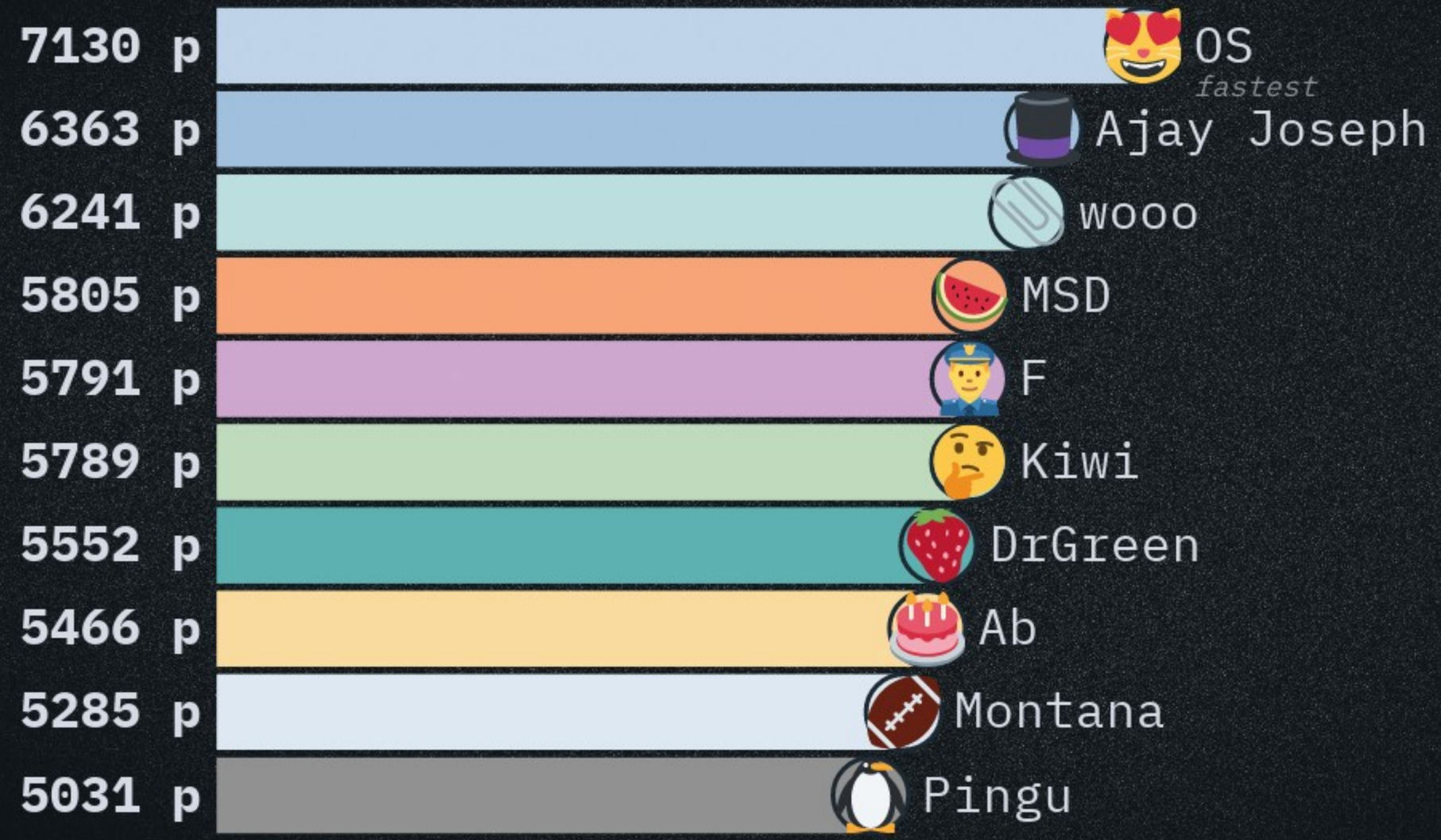
33

An IT cpmpany have had muiltple incidents of laptop being stolen. Forcing company to amend their security policy. The countermeasure chosen was



Leaderboard

Mentimeter



41

Class Test

- 12 Novemeber between 1:40 - 4:00 pm
- Location - C2.04 and C2.05
- Everything we covered till week 6

3 2 2

For an organisation list all the vulnerabilities you can think of.

List top three attacks that can be carried out using the vulnerabilities mentioned earlier

27

In your opinion, by using the attack to exploit a vulnerability what is the hacker trying to access/steal/compromise

Threat modelling

- Threat modeling is a structured approach to identifying potential threats that could exploit vulnerabilities.
- A threat modeling approach looks at who would most likely want to attack us
- How could they successfully do this?
- Threat modeling can be performed as a proactive measure during design and development or as a reactivemeasure once a product has been deployed

Identifing threats

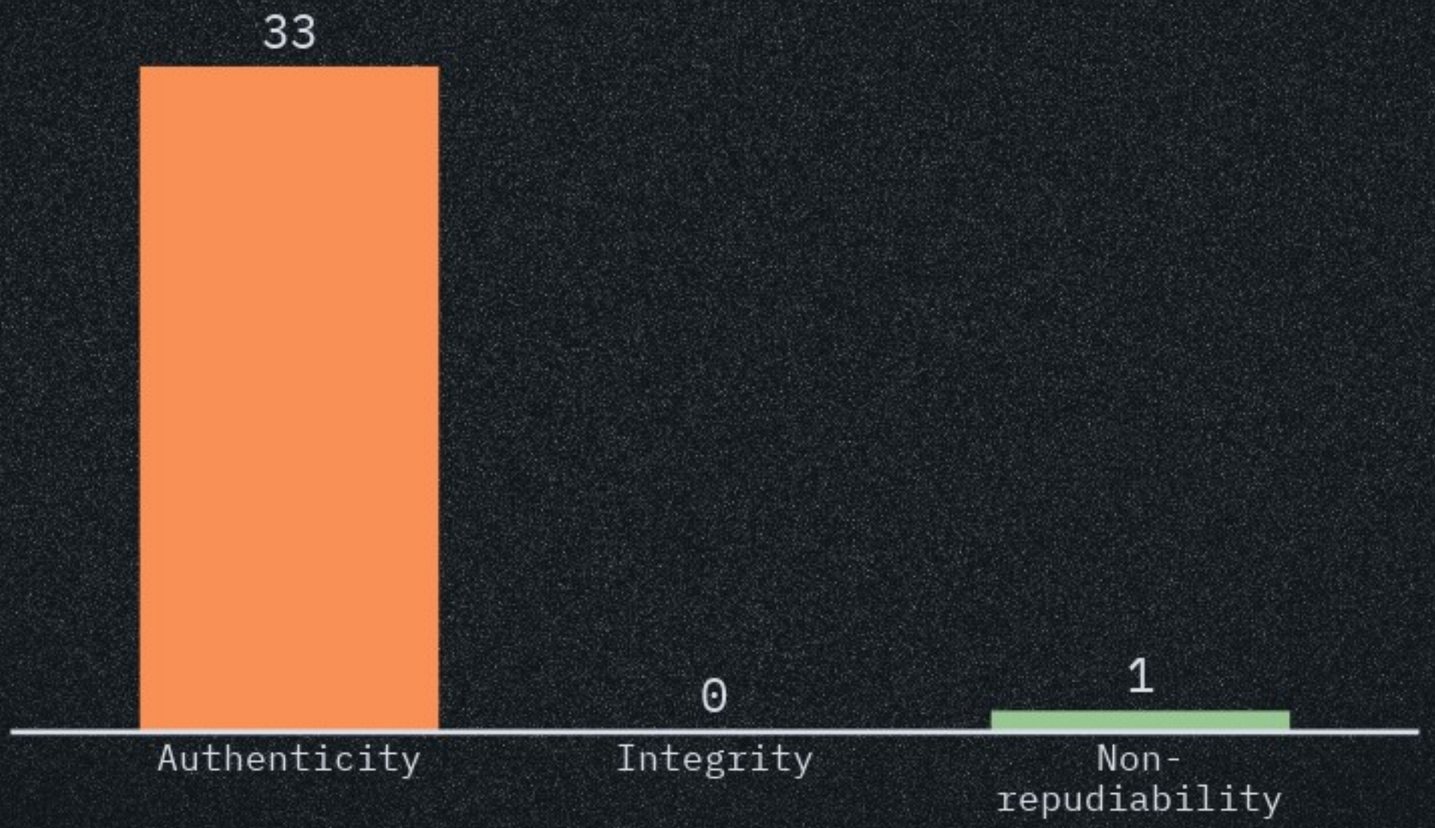
- Focused on Assets- This method uses asset valuation results and attempts to identify threats to thevaluable assets
- Focused on Attackers- Some organizations are able to identify potential attackers and can identify the threats they represent based on the goal
- Focused on Software-If an organization develops software, it can consider potential threats against thesoftware.

STRIDE

- Developed by Microsoft as part of threat modelling procedure in 1999.
- Helps to prompt questions e.g. what would happen if ...?
- Helps reduce chance of failing to identify a risk

Mentimeter

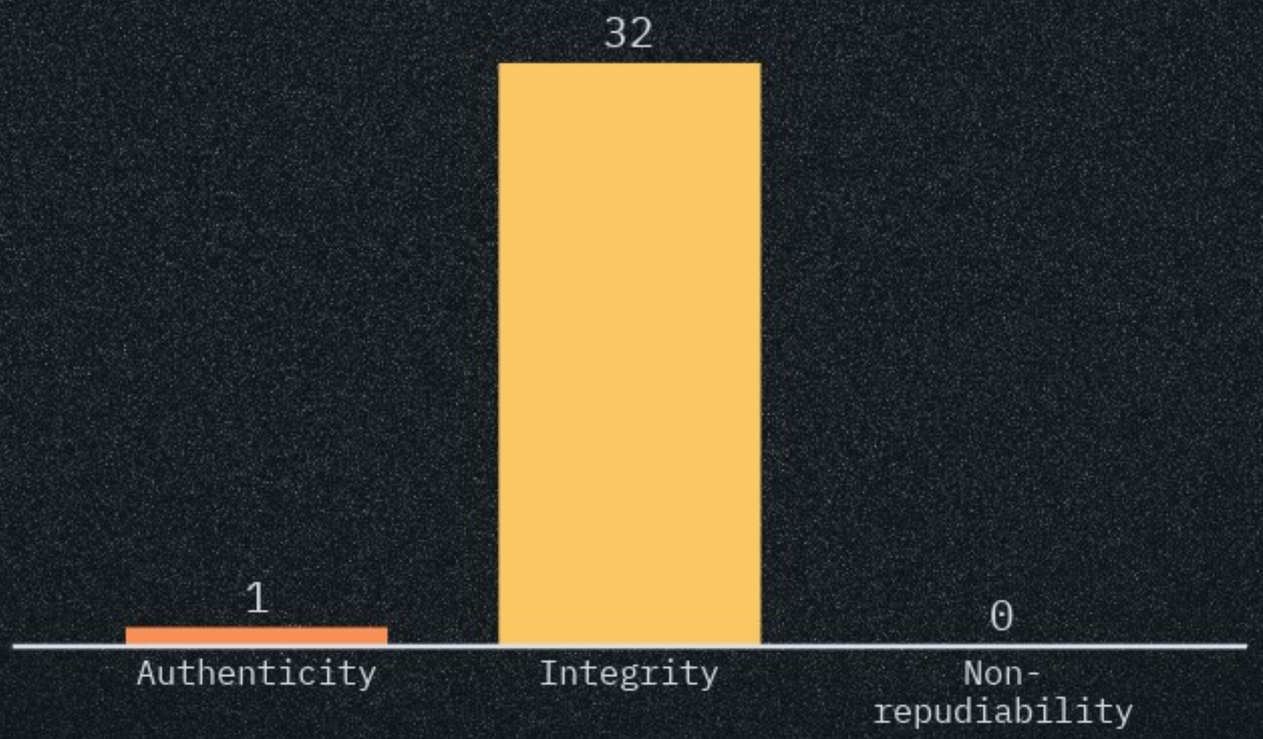
Spoofing - a situation in which a person or program successfully identifies as another by falsifying data. Which security property is violated



34

Tampering - modification of data or code, which security property is violated

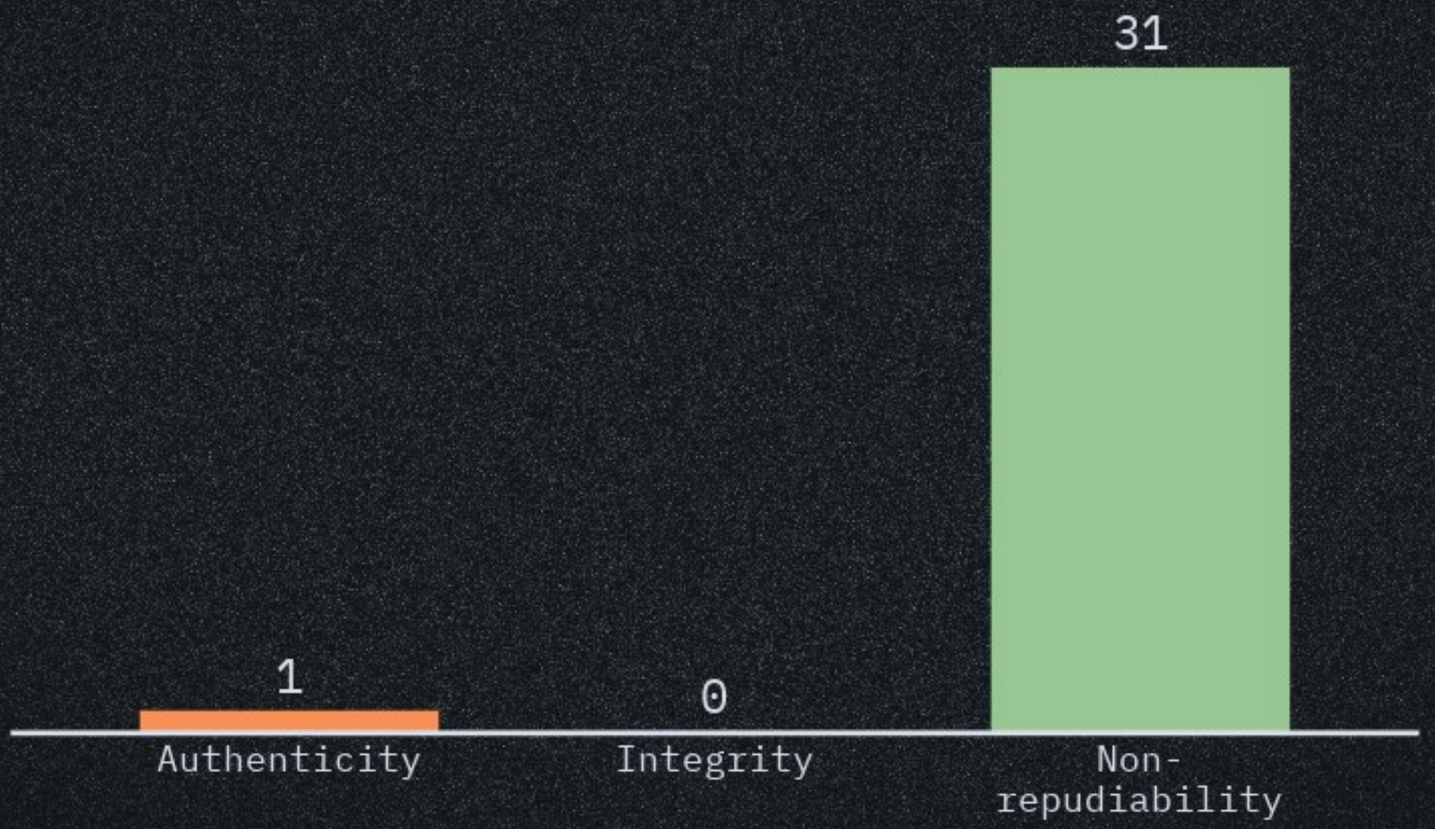
Mentimeter



33

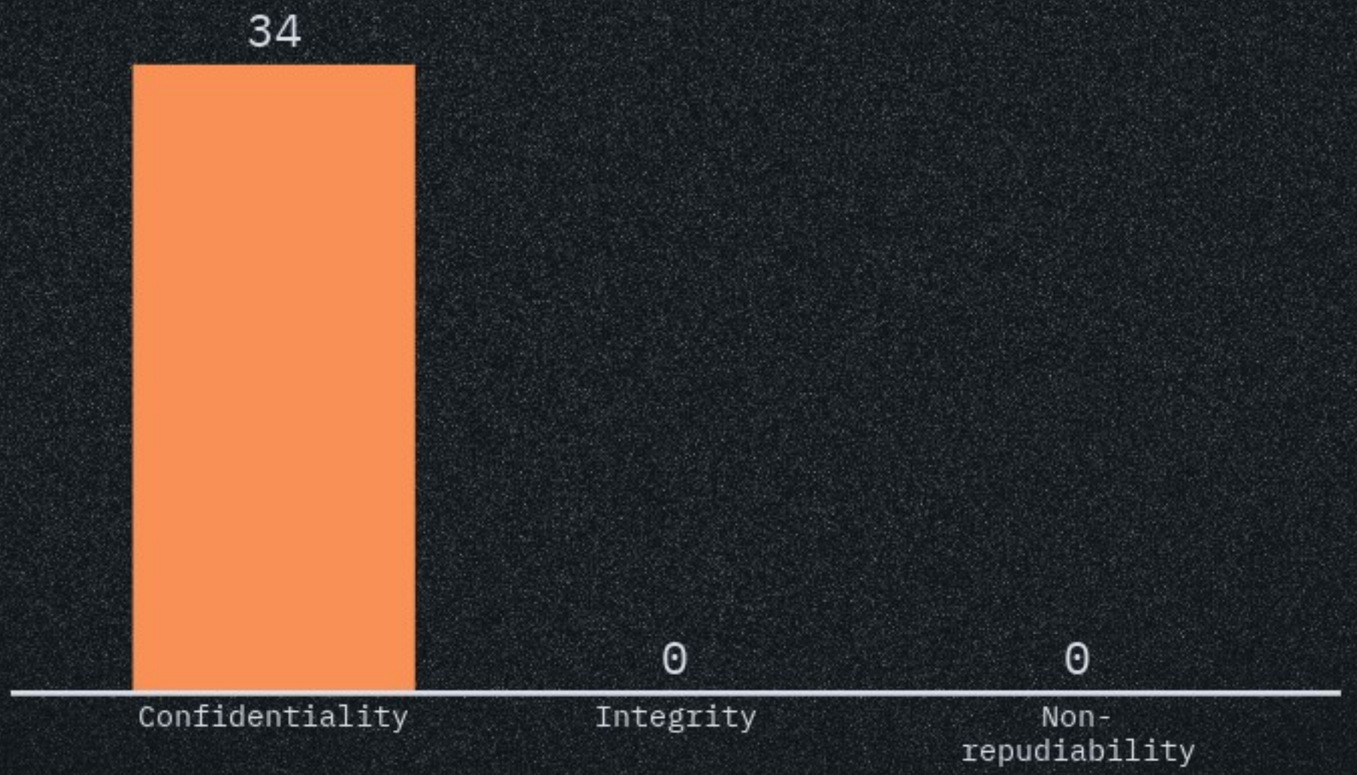
Repudiation This is a threat where an attacker deletes or changes a transaction or login information in an attempt to refute that they ever took place

Mentimeter



32

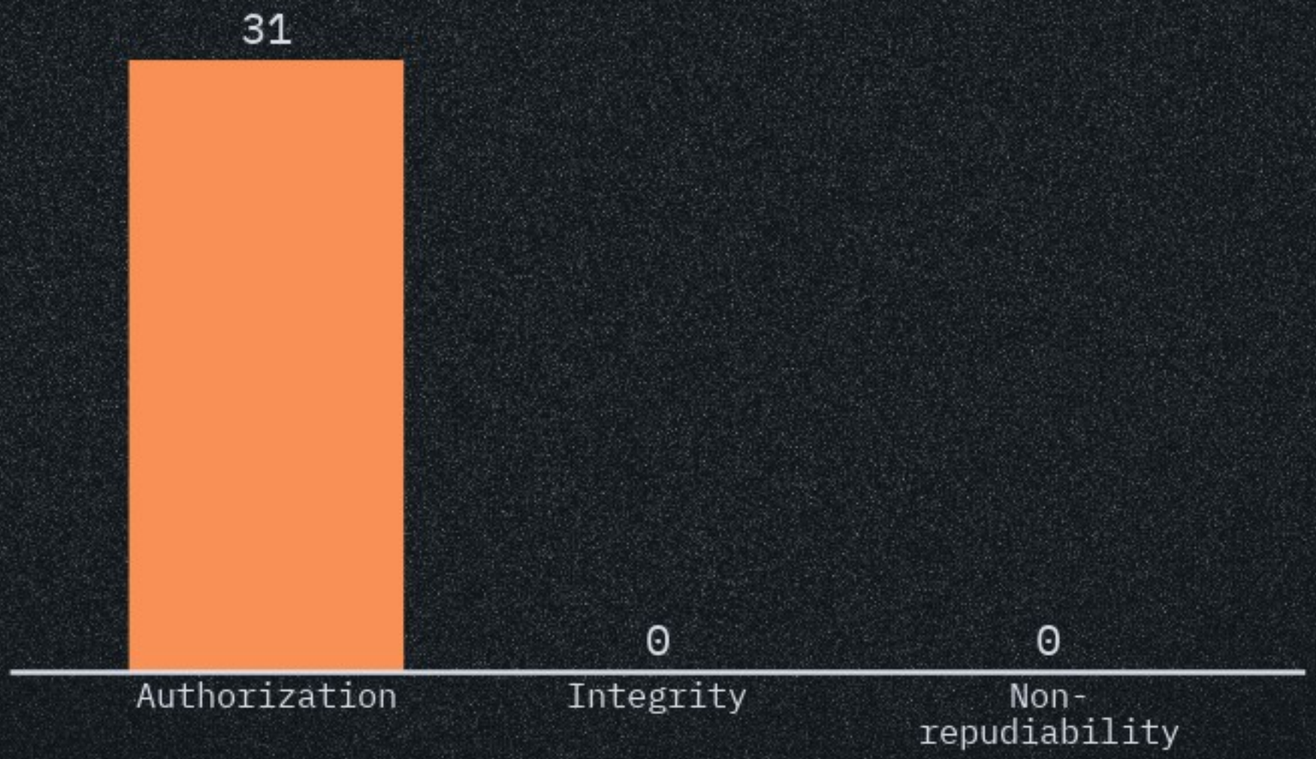
Information disclosure- Exposing information to someone who is not authorised to, which security property is violated



34

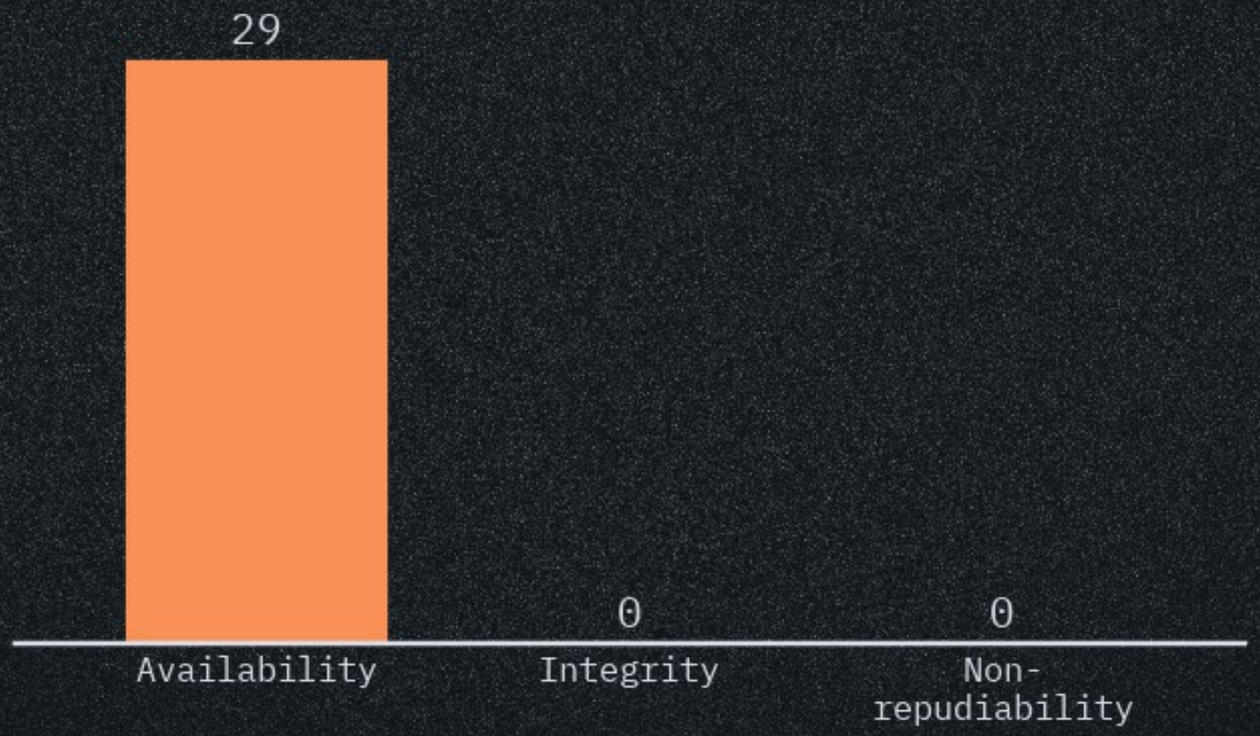
Elevation of Privilege- gain capabilities without proper authentication, which security property is violated

Mentimeter



31

Denial of Service- deny or degrade service to a user, which security property is violated

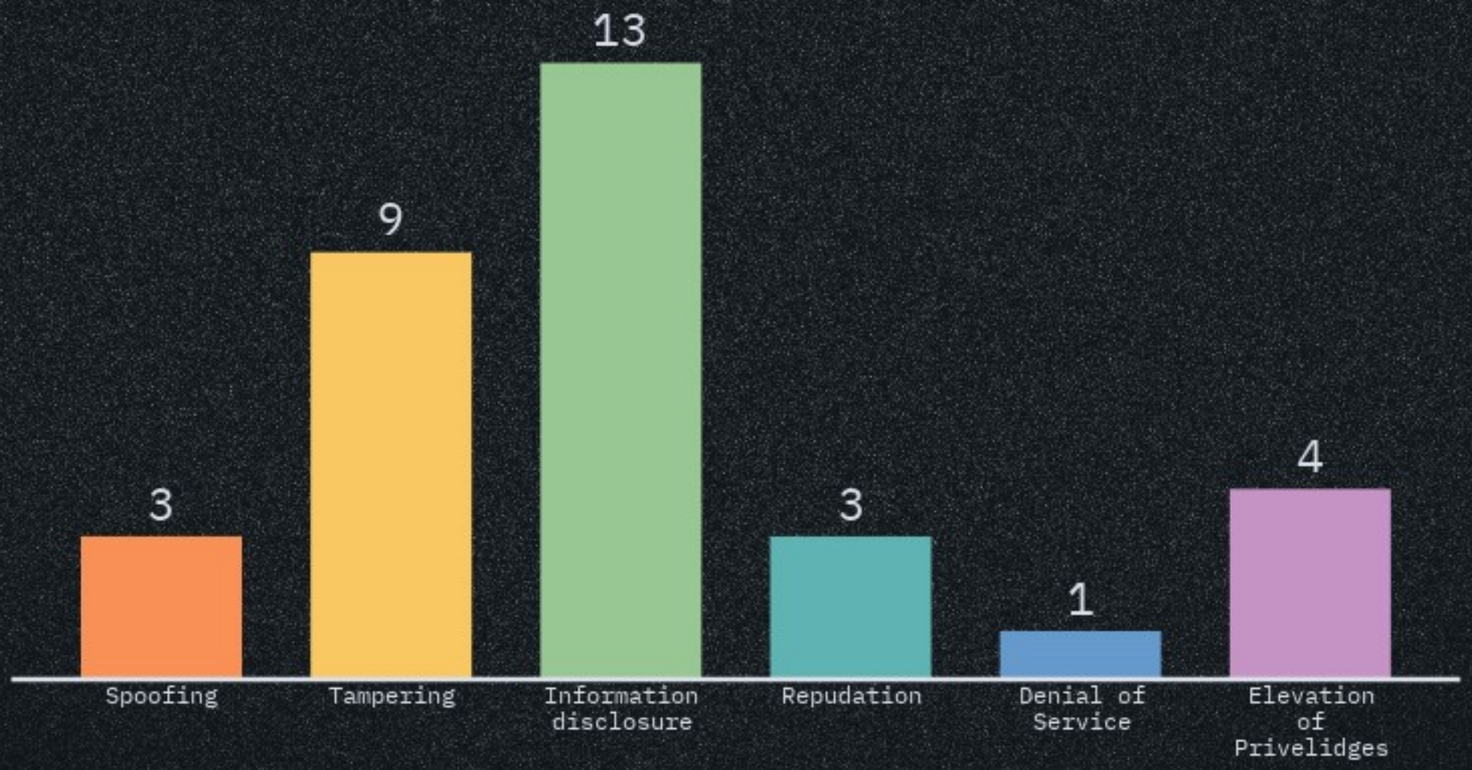


29

What all attacks can be carried out targetting the data over an unsecured network?

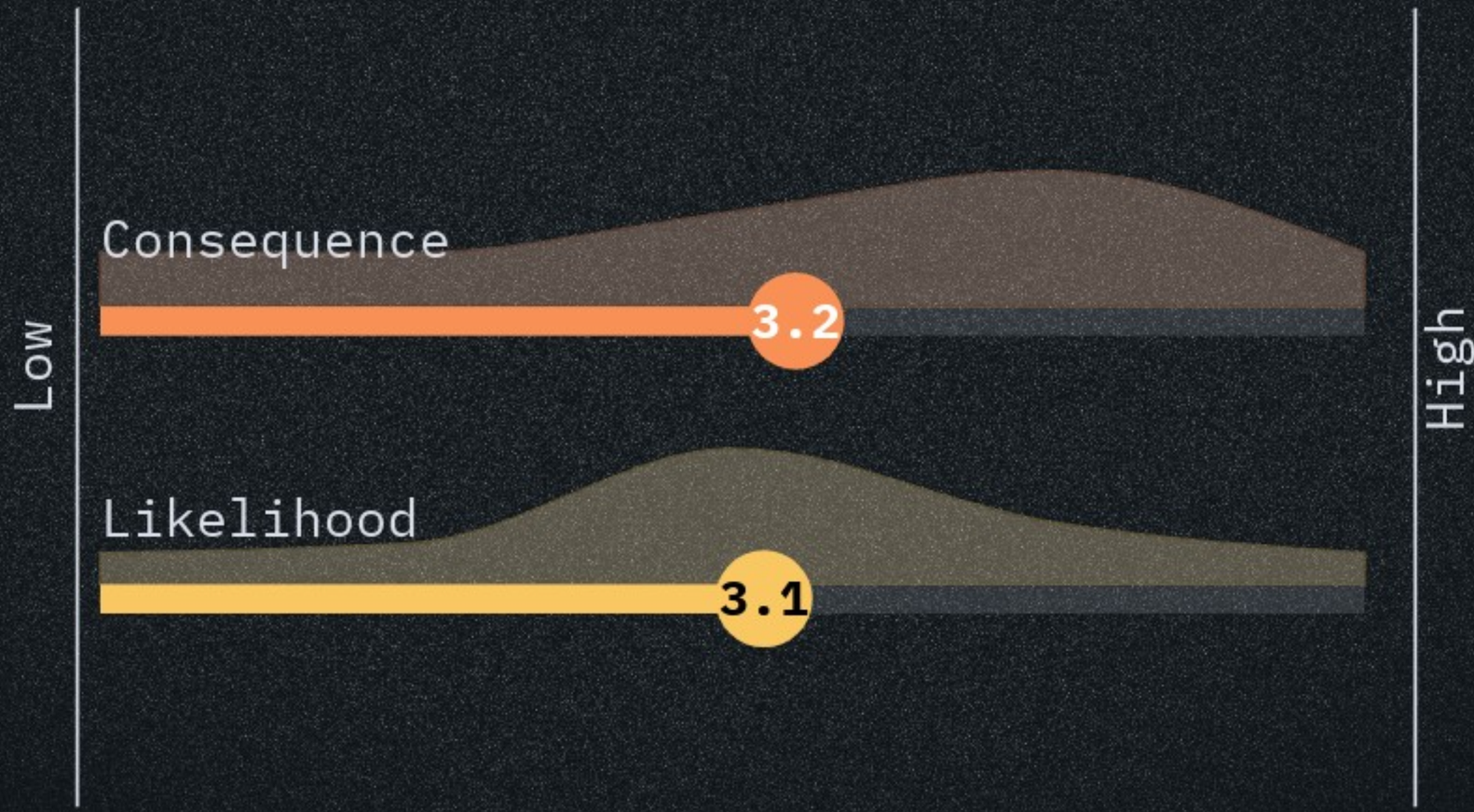
For data in transit on an unsecured network an attacker can carry out an attack that can effect the data

Mentimeter



33

Calculate risk for one of the threat identified

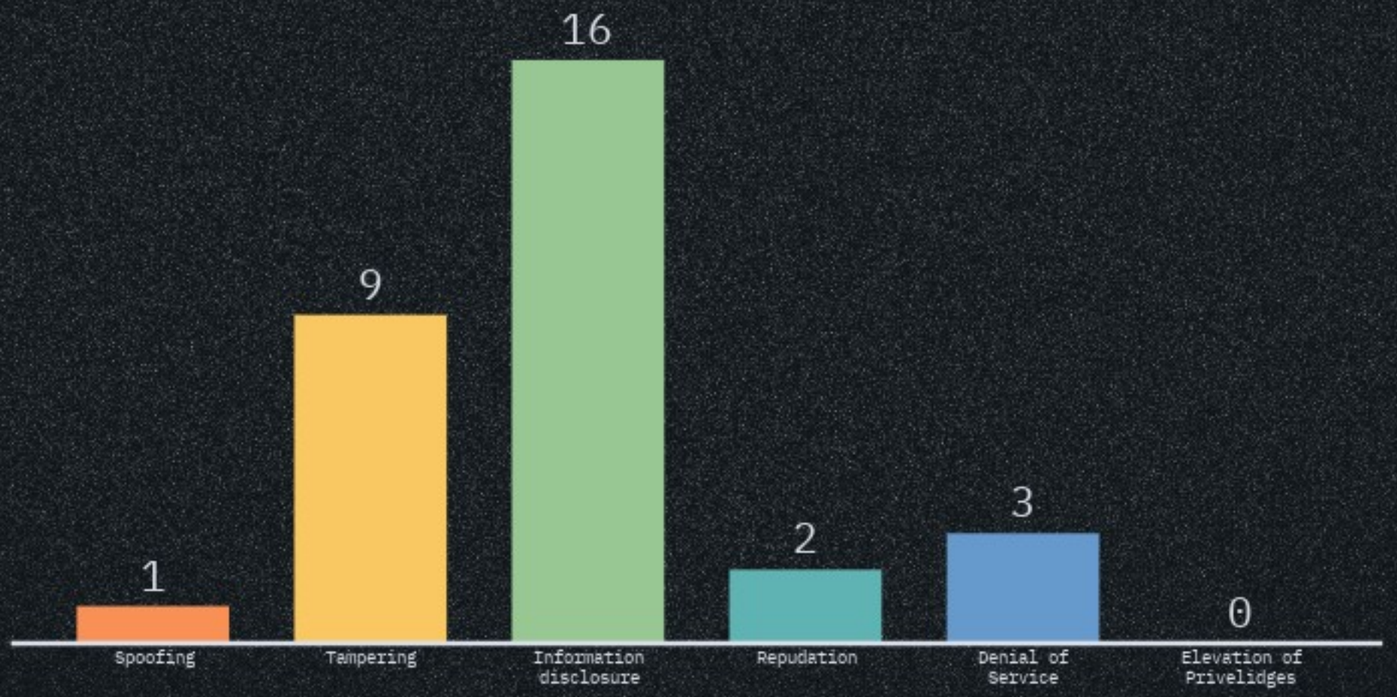


List all the attacks you can think of

39

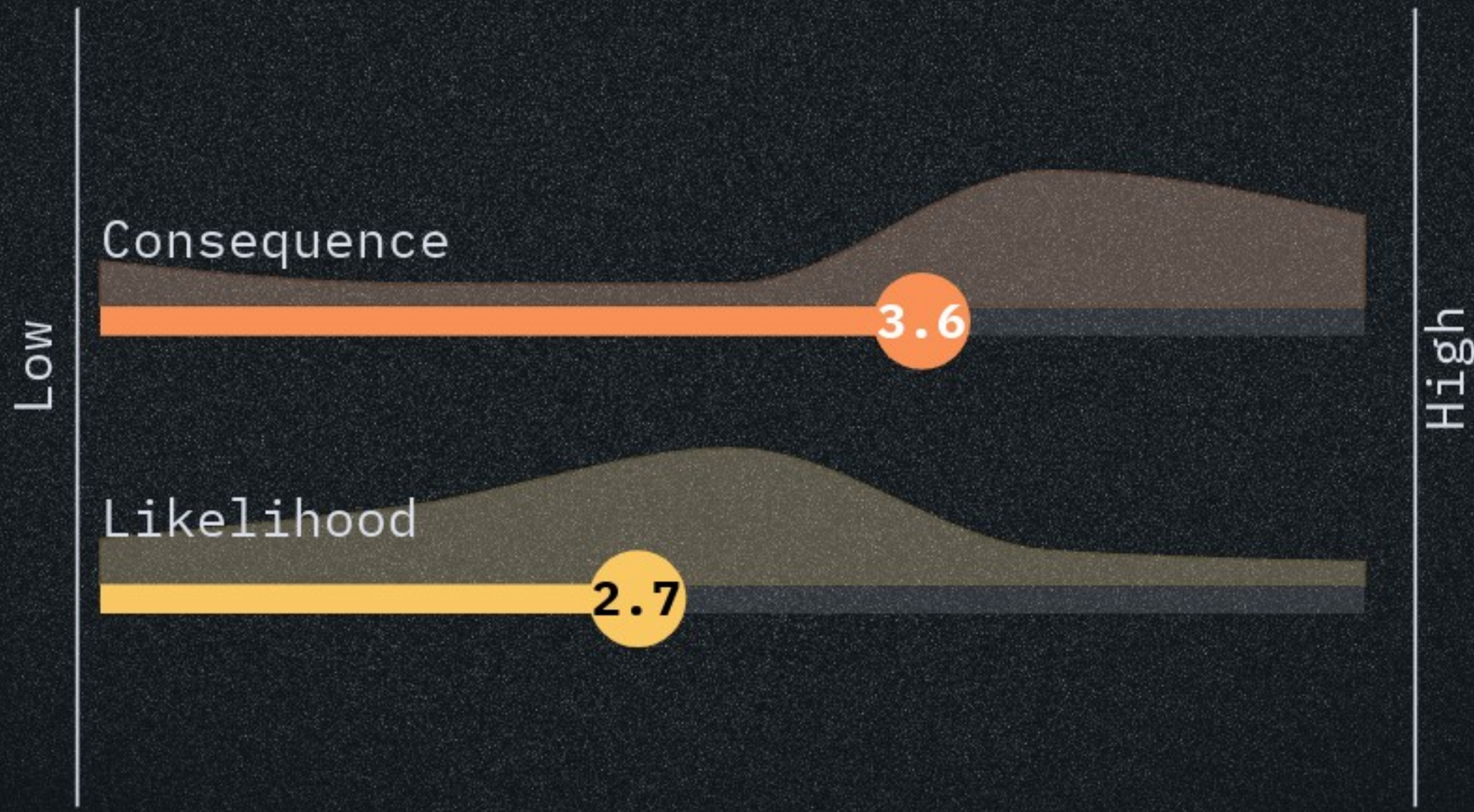
For data stored on a database, an attacker can carry out an attack that can effect the data

Mentimeter



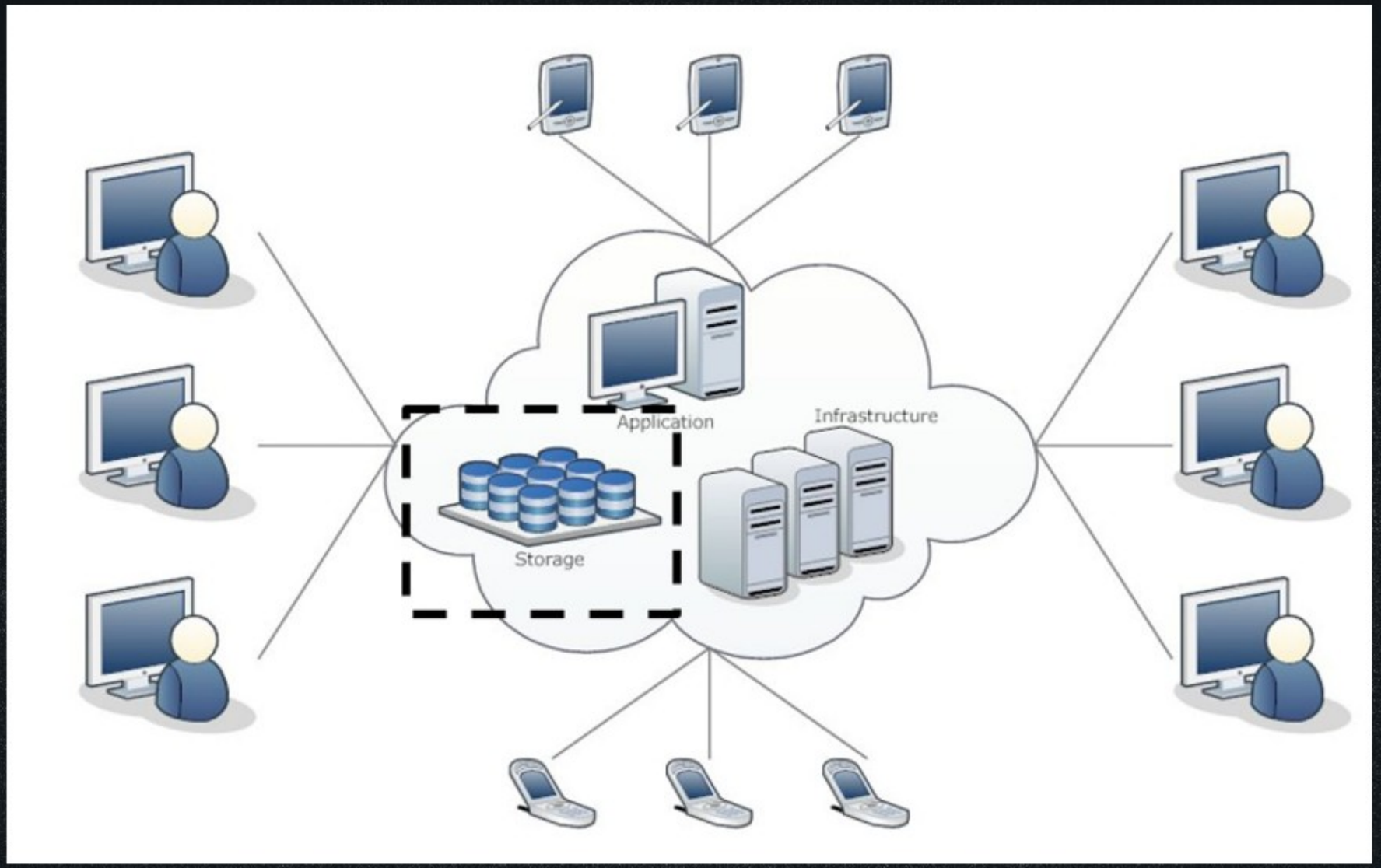
31

Calculate risk for one of the threat identified



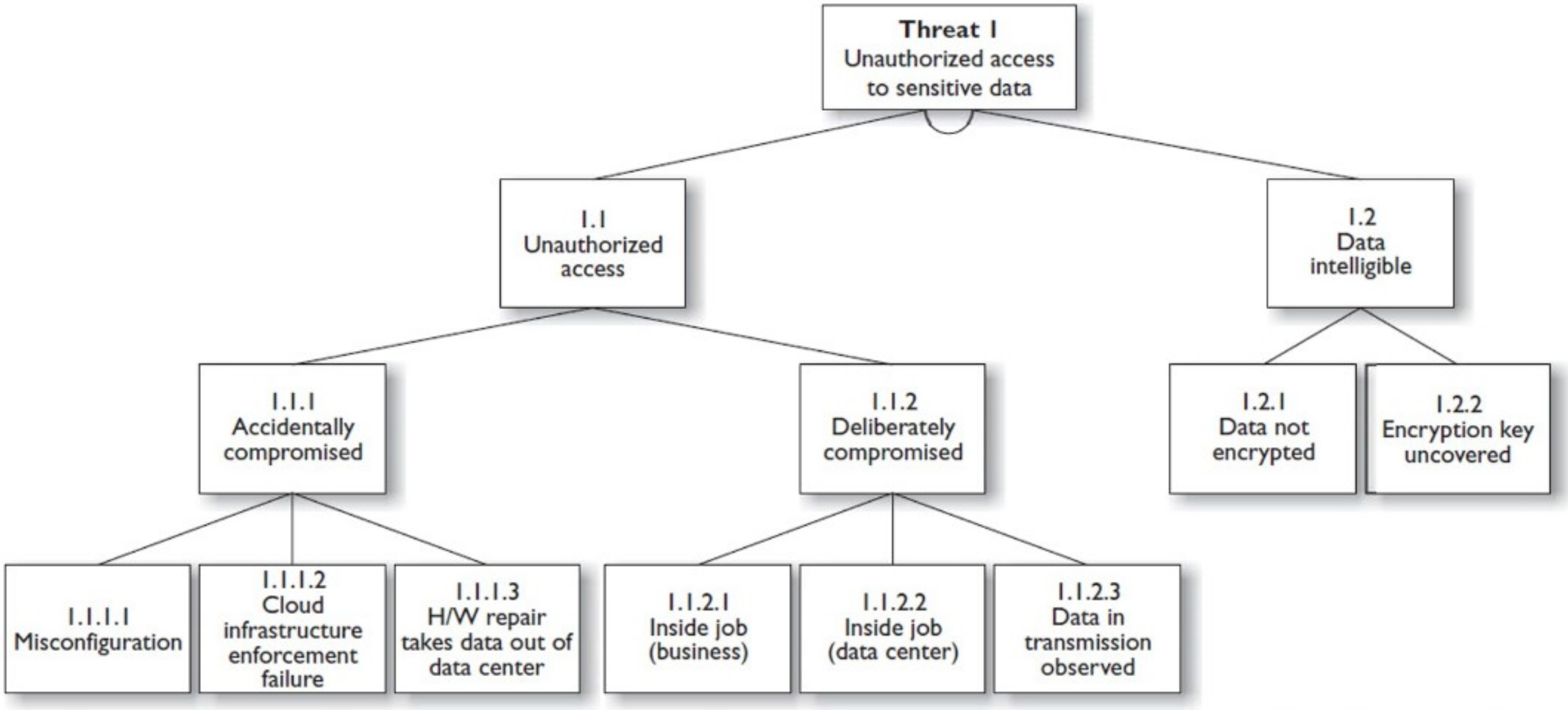
Attack Trees

- Are conceptual diagrams showing how an asset, or target, might be attacked.
- They have been used to describe threats on computer systems and possible attacks to realize those threats



A company is hosting services and data on cloud.

1 1 1 1 2



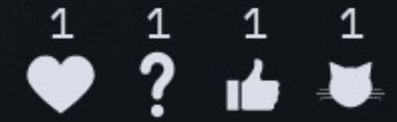
Attack Treet for Unauthorised Access to Sensitive data

DREAD

- DREAD methodology is used to rate, compare and prioritize the severity of risk presented by each threat that is classified using STRIDE.
- Damage – how bad would an attack be?
- Reproducibility – how easy is it to reproduce the attack?
- Exploitability – how much work is it to launch the attack?
- Affected users – how many people will be impacted?
- Discoverability – how easy is it to discover the threat?

Damage – how bad would an attack be?

- 1 = Nothing
- 2 = Compromised or affected individual user data.
- 3 = Compromised or affected every user data.



Reproducibility - how easy is it to reproduce the attack?

- 1 = Very hard or impossible, even for administrators of the application.
- 2 = One or two steps required, may need to be an authorized user.
- 3 = Just a malicious app, No need of authentication.

Exploitability - how much work is it to launch the attack?

- 1 = Advanced programming and deep knowledge, with custom or advancedattack tools.
- 2 = Malware exists on the Internet, or an exploit is easily performed, usingavailable attack tools
- 3 = Just a malware or native application

Affected users - how many people will be impacted?

- 1 = None
- 2 = Some users, but not all
- 3 = All users

Discoverability - how easy is it to discover the threat?

- 1 = Very hard to impossible; requires source code or administrative access.
- 2 = Can figure it out by guessing or by analyzing the application data flow.
- 3 = Details of faults like this are already in the public domain and can be easilydiscovered using a search engine.

Threats	D	R	E	A	D	Total	Rating
Threat 1	2	3	3	2	3	13	High
Threat 2	2	3	3	2	2	12	High
Threat 3	1	1	1	3	1	7	Low
Threat 4	2	2	2	2	3	11	Medium
Threat 5	2	3	2	3	3	13	High

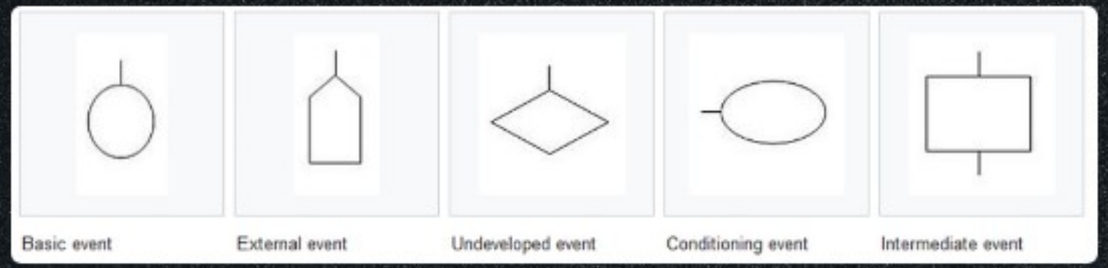
DREAD model for risk analysis

- 12-15 = High Risk
- 8-11= Medium Risk
- 5-8= Low Risk

Fault Tree Analysis

- A more useful approach to identifying failures that can take place within more complex environments and systems
- An undesired effect is taken as the root or top event of a tree of logic
- Each situation that has the potential to cause that effect is added to the tree as a series of logic expressions
- They are labeled with actual numbers pertaining to failure probabilities

Event Symbols

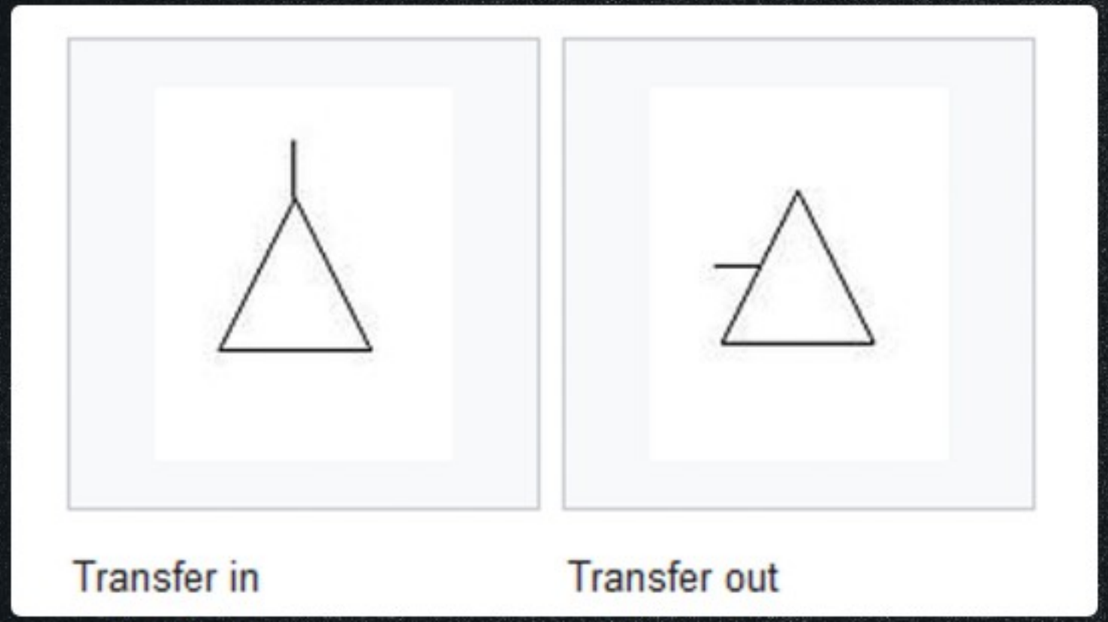


- Basic event - failure or error in a system component or element.
- External event - normally expected to occur (not of itself a fault)
- Undeveloped event - an event about which insufficient information is available, or which is of no consequence
- Conditioning event - conditions that restrict or affect logic gates
- An intermediate event- to provide more room to type the event description

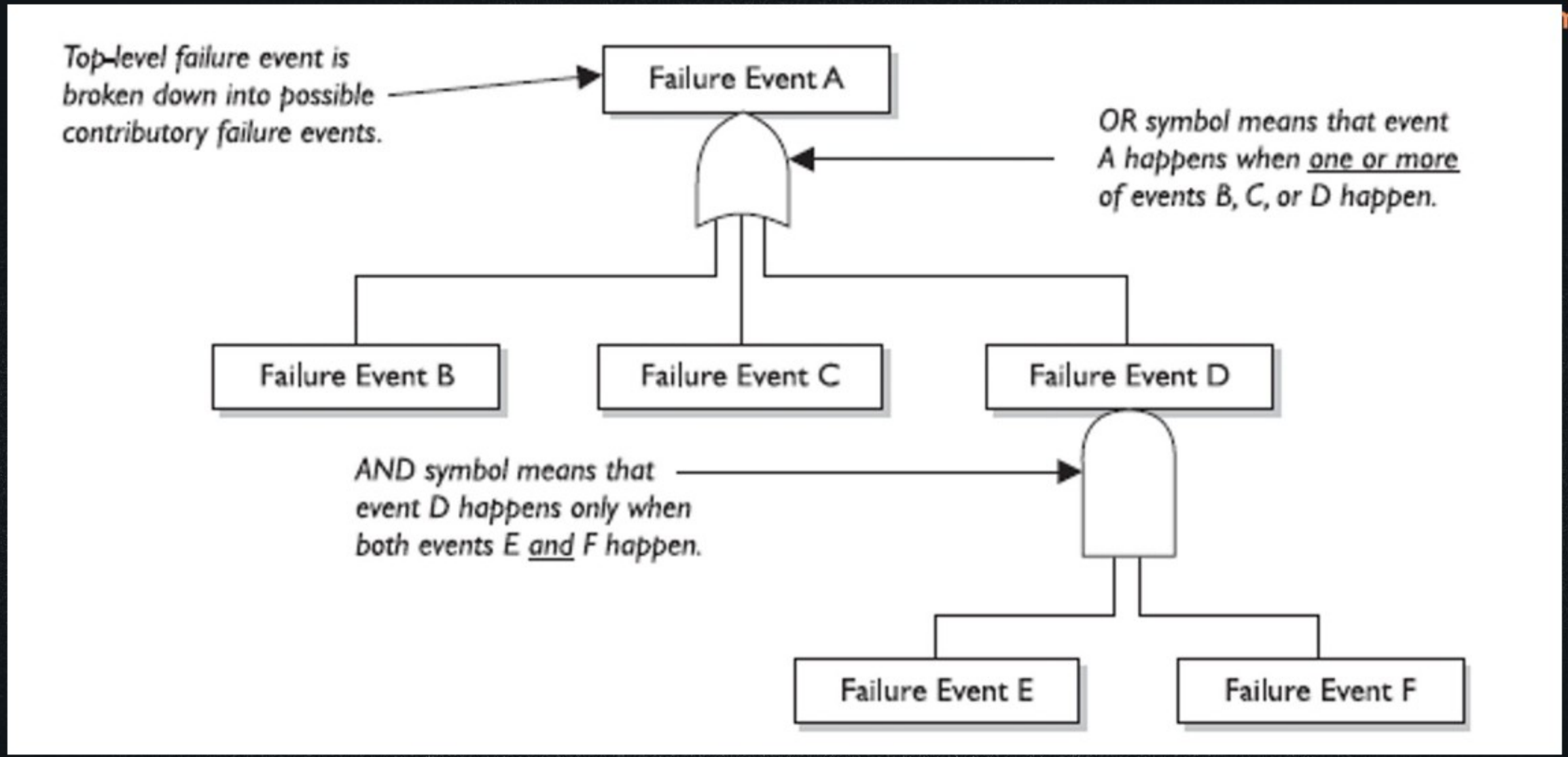
Gate Symbols

- OR gate - the output occurs if any input occurs
- AND gate - the output occurs only if all inputs occur
- Exclusive OR gate - the output occurs if exactly one input occurs.
- Priority AND gate - the output occurs if the inputs occur in a specific sequence specified by a conditioning event.
- Inhibit gate - the output occurs if the input occurs under an enabling condition specified by a conditioning event.

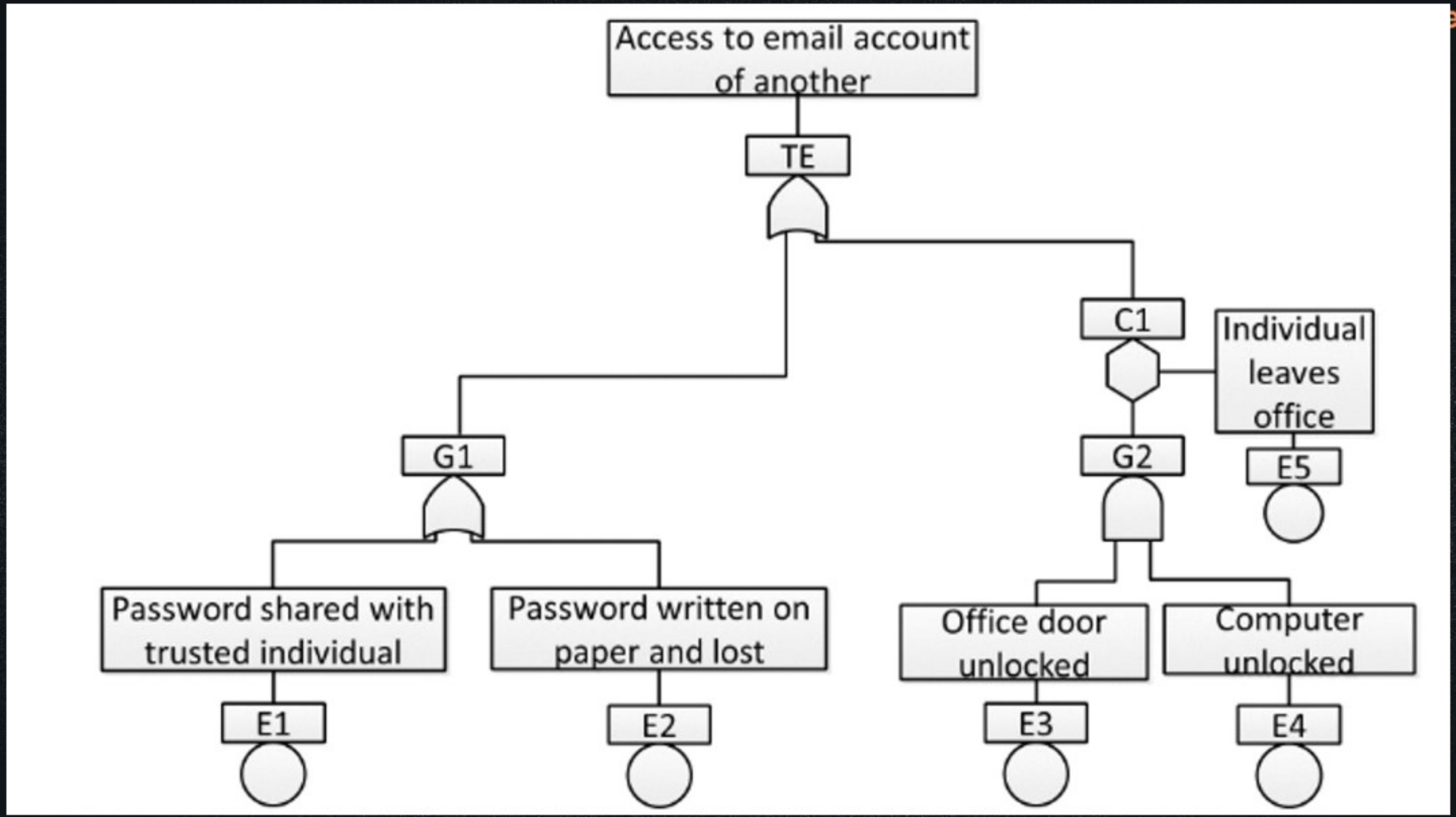
Transfer Symbols



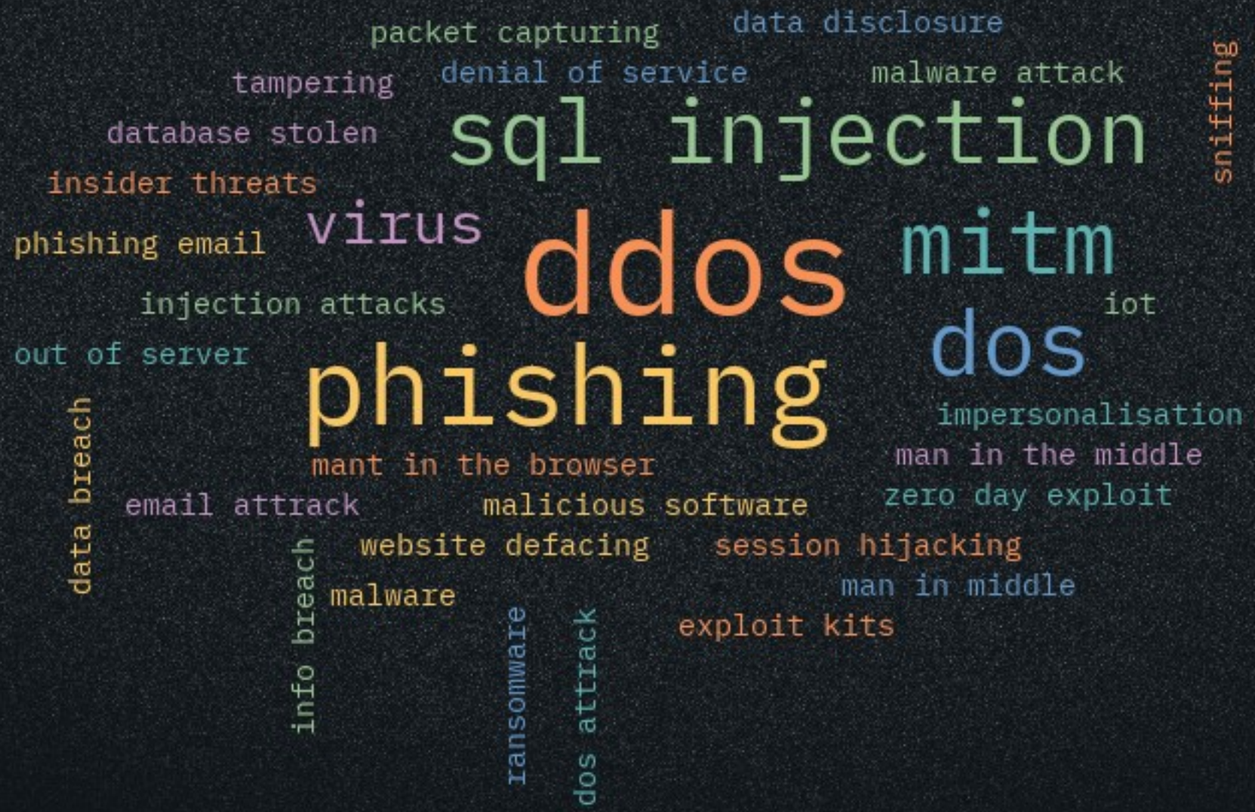
- Transfer symbols are usd to conect the inputs and outputs of realted fault trees.
- Transfer in- Transfer in the results from a subsystem
- Transfer out- Transfer results out to be used by differnt fault tree.



Fault tree and logic components


Access to email account of another
TE
G1
C1
Individual leaves office
G2
E5
Password shared with trusted individual
Password written on paper and lost
Office door unlocked
Computer unlocked
E1
E2
E3
E4

Name all possible cyber attacks a company with given network might be facing



26