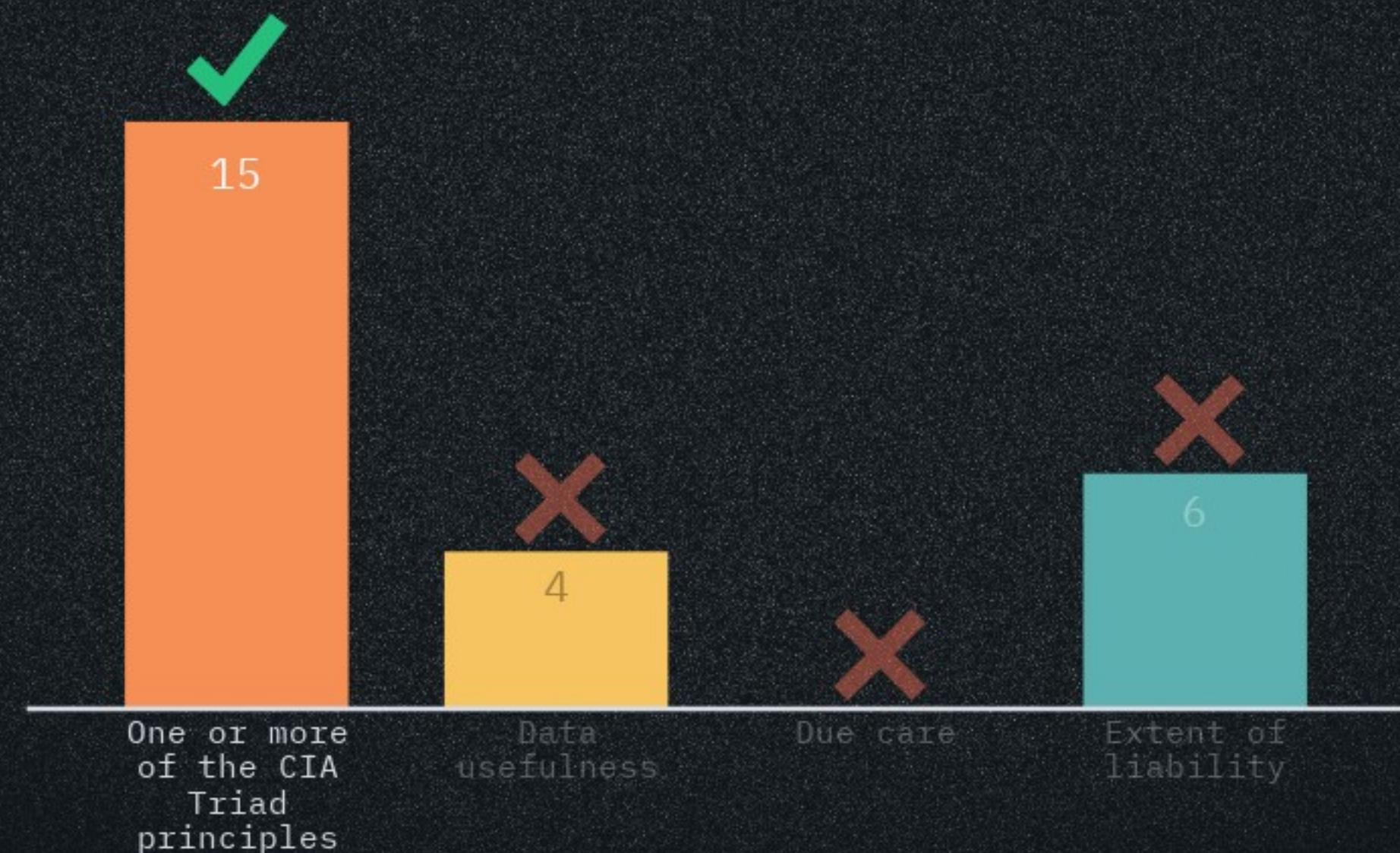


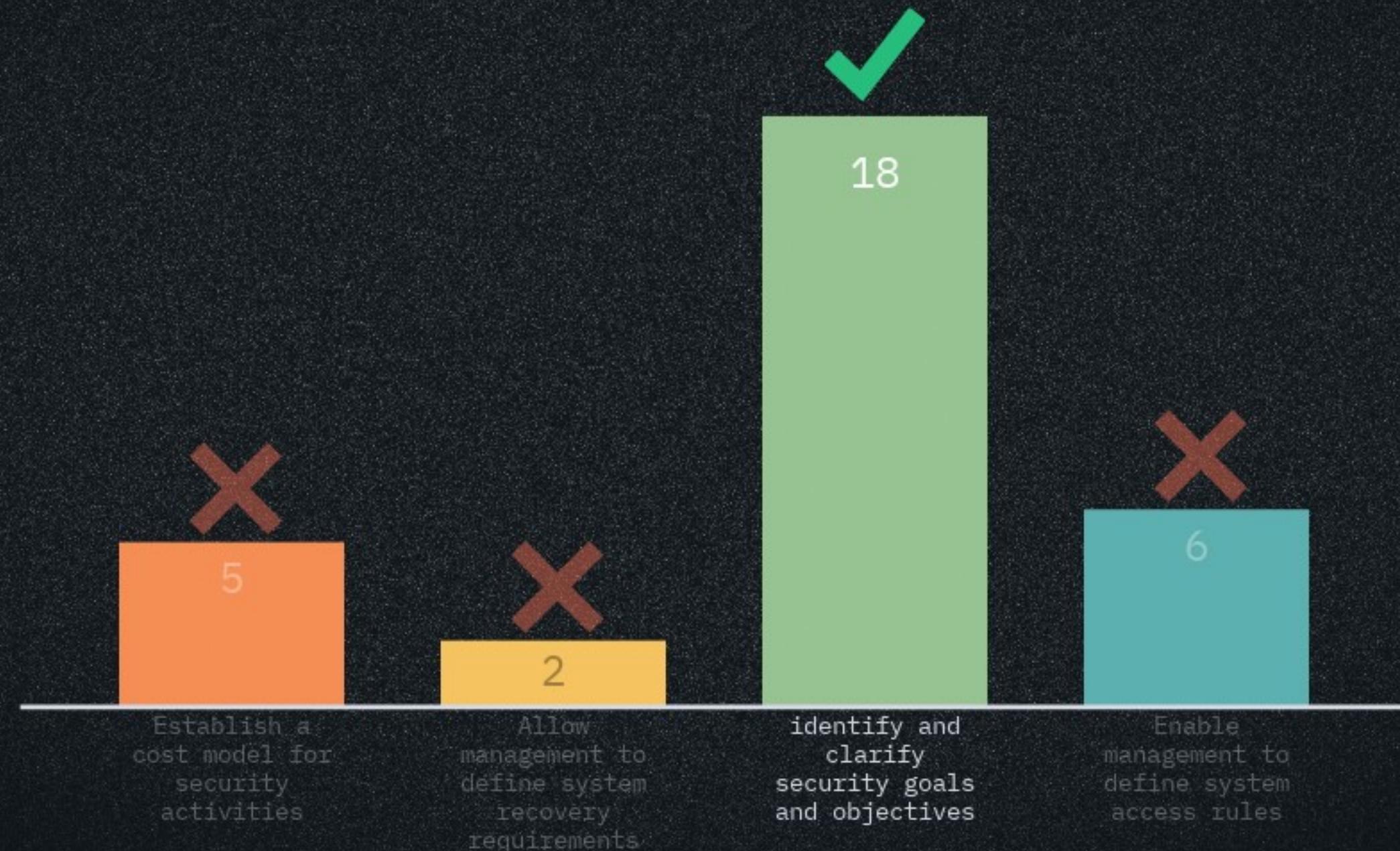
Vulnerabilities and risks are evaluated based on their threats against which of the following?



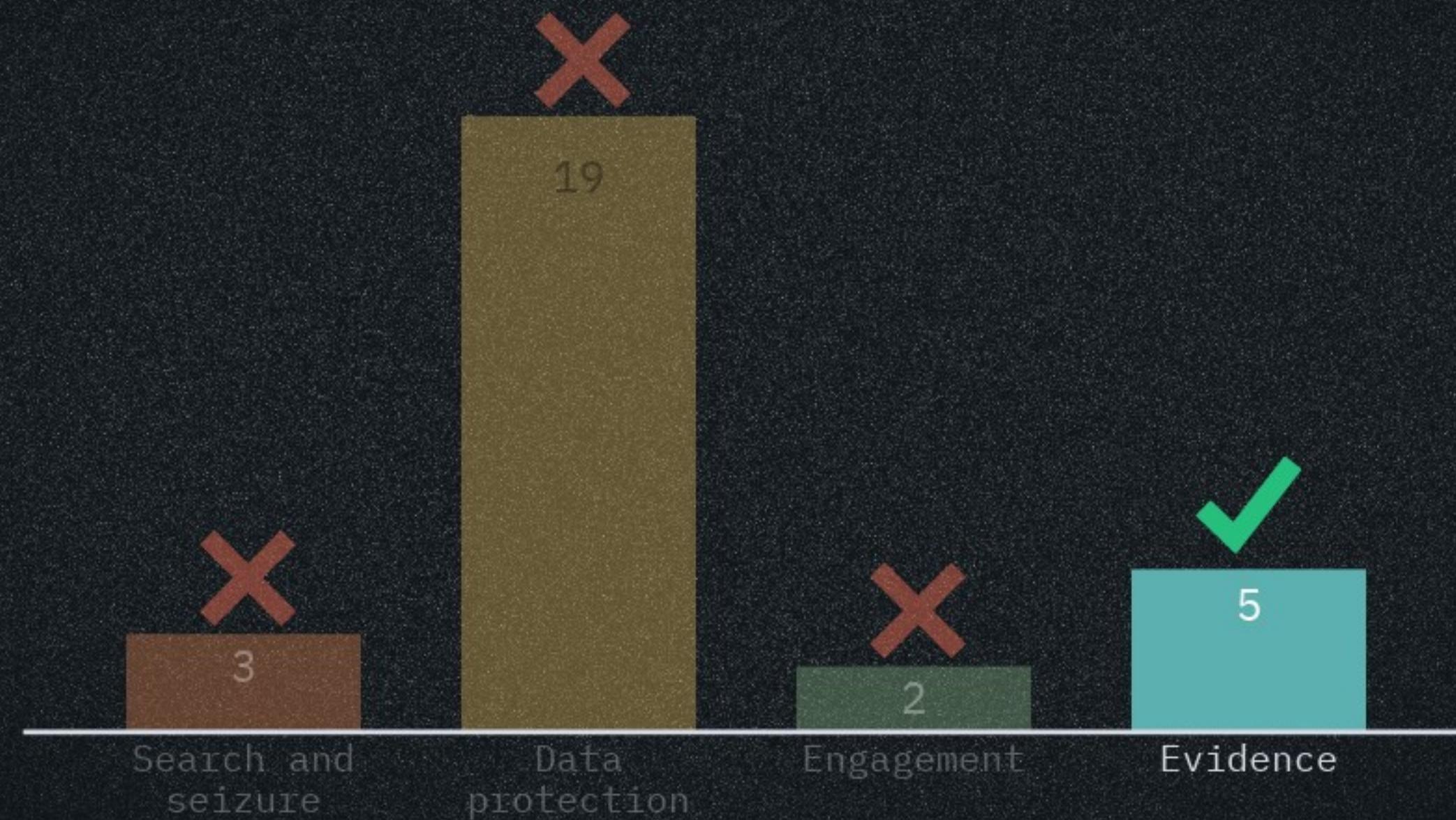
While designing a security framework, controls are placed to protect, which is NOT utilized to achieve management directives to protect company asset



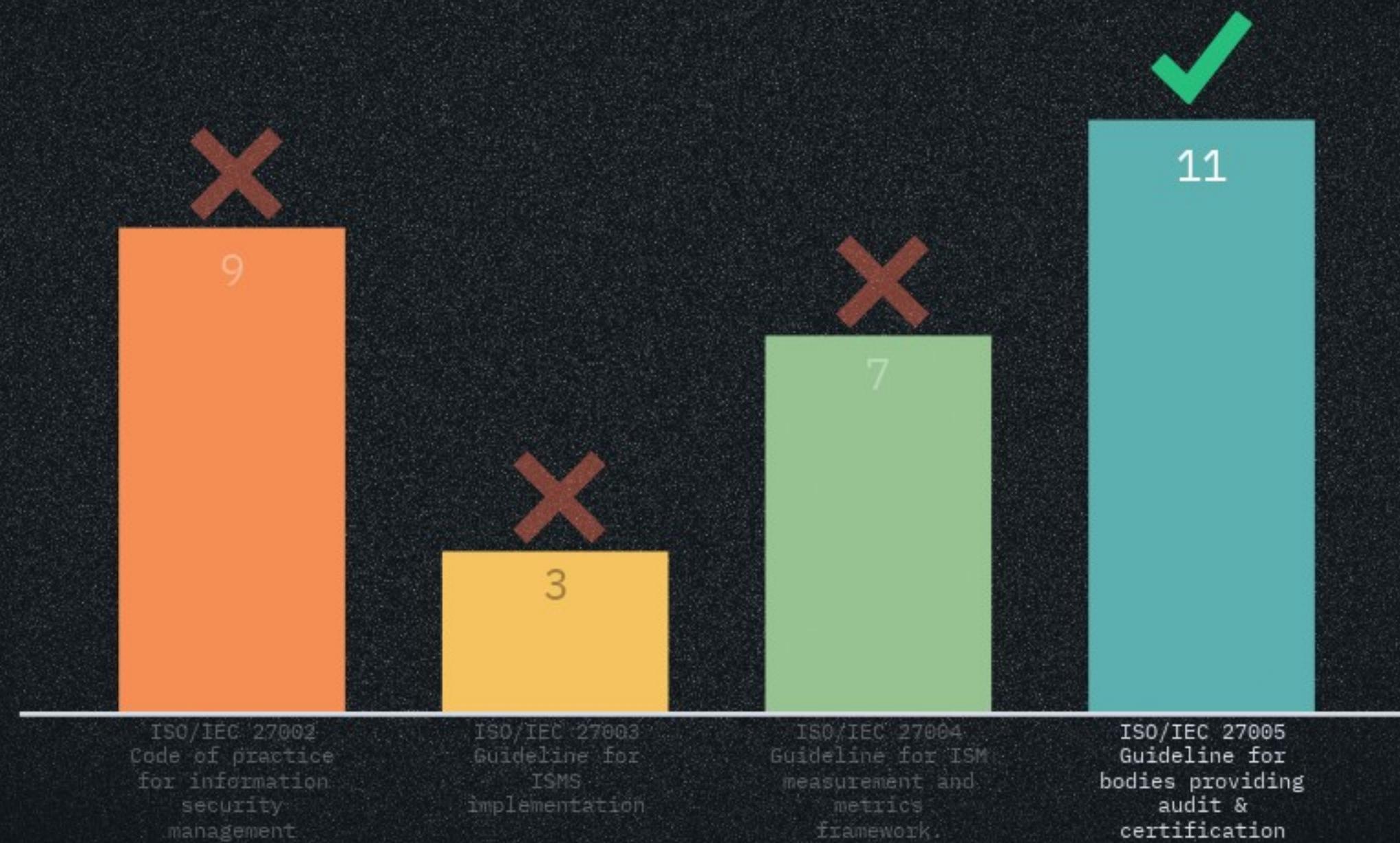
John have recently been appointed to develop a security policy for Gaming company, by doing so the company has ensured that it provides a way to



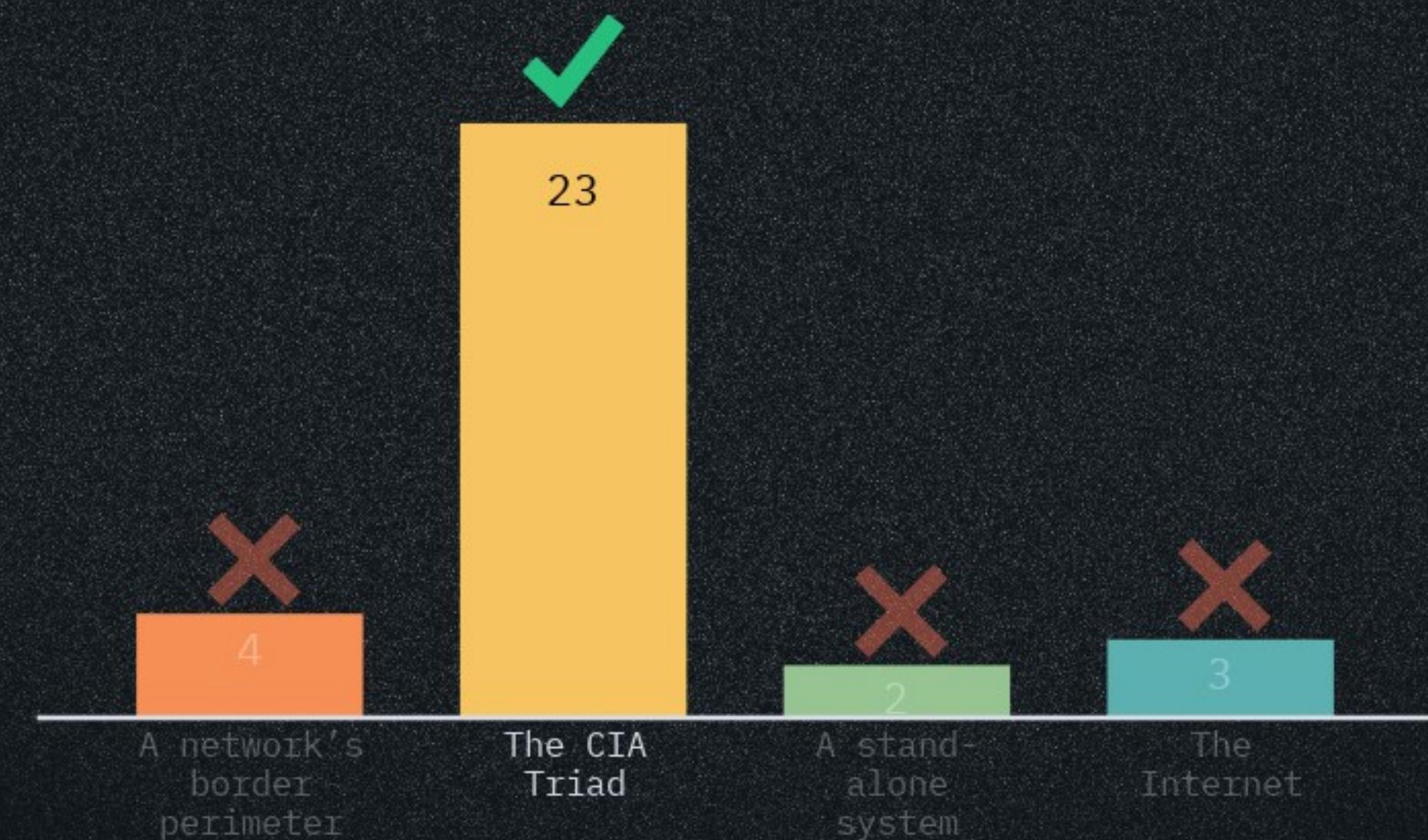
Sam is part of a legal team investigating an attack that compromised a web-server. From legal prospective which is the most critical item listed below



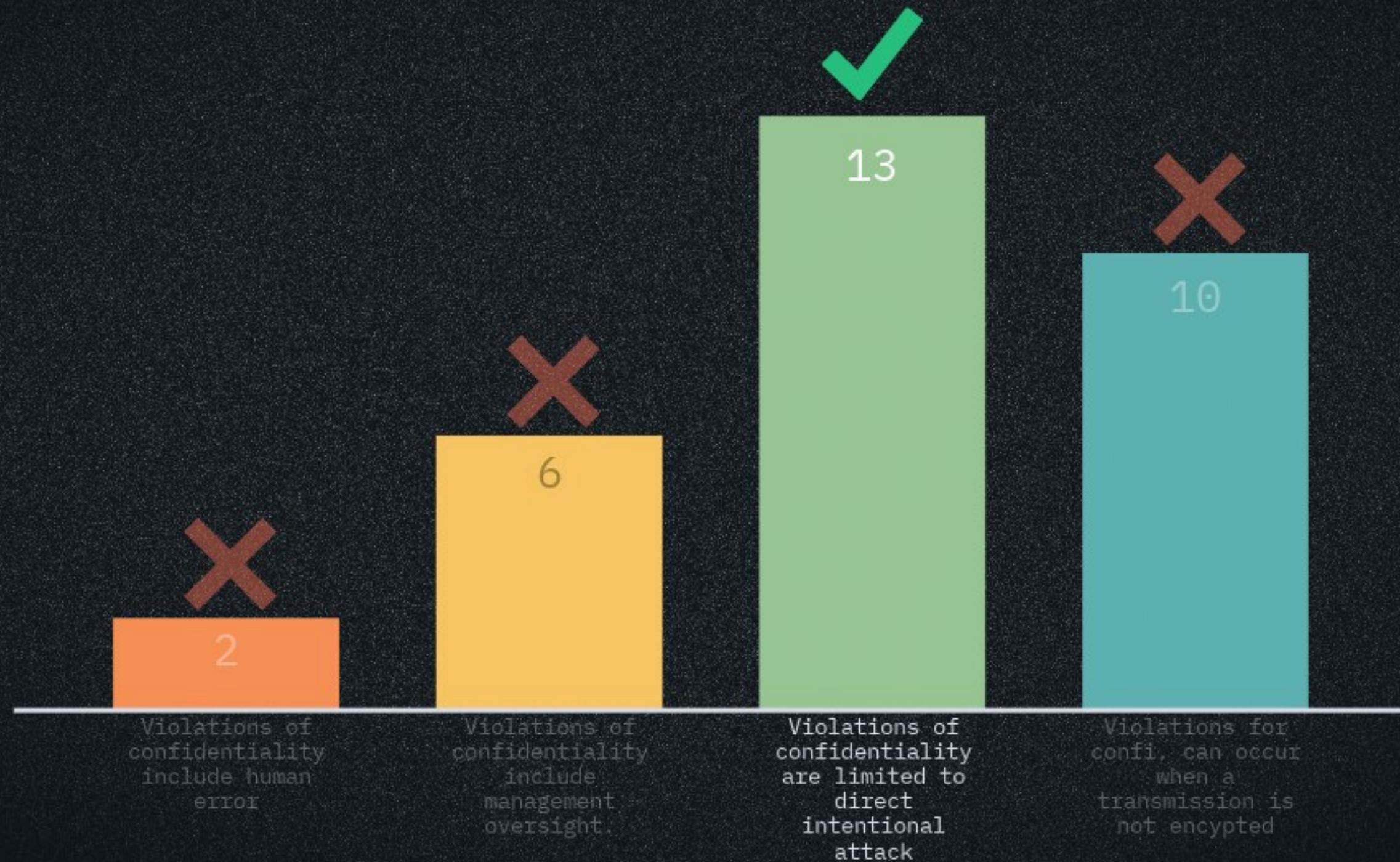
Which of the following provides an incorrect mapping of the individual standards that make up the family of ISO/IEC 2700 standards



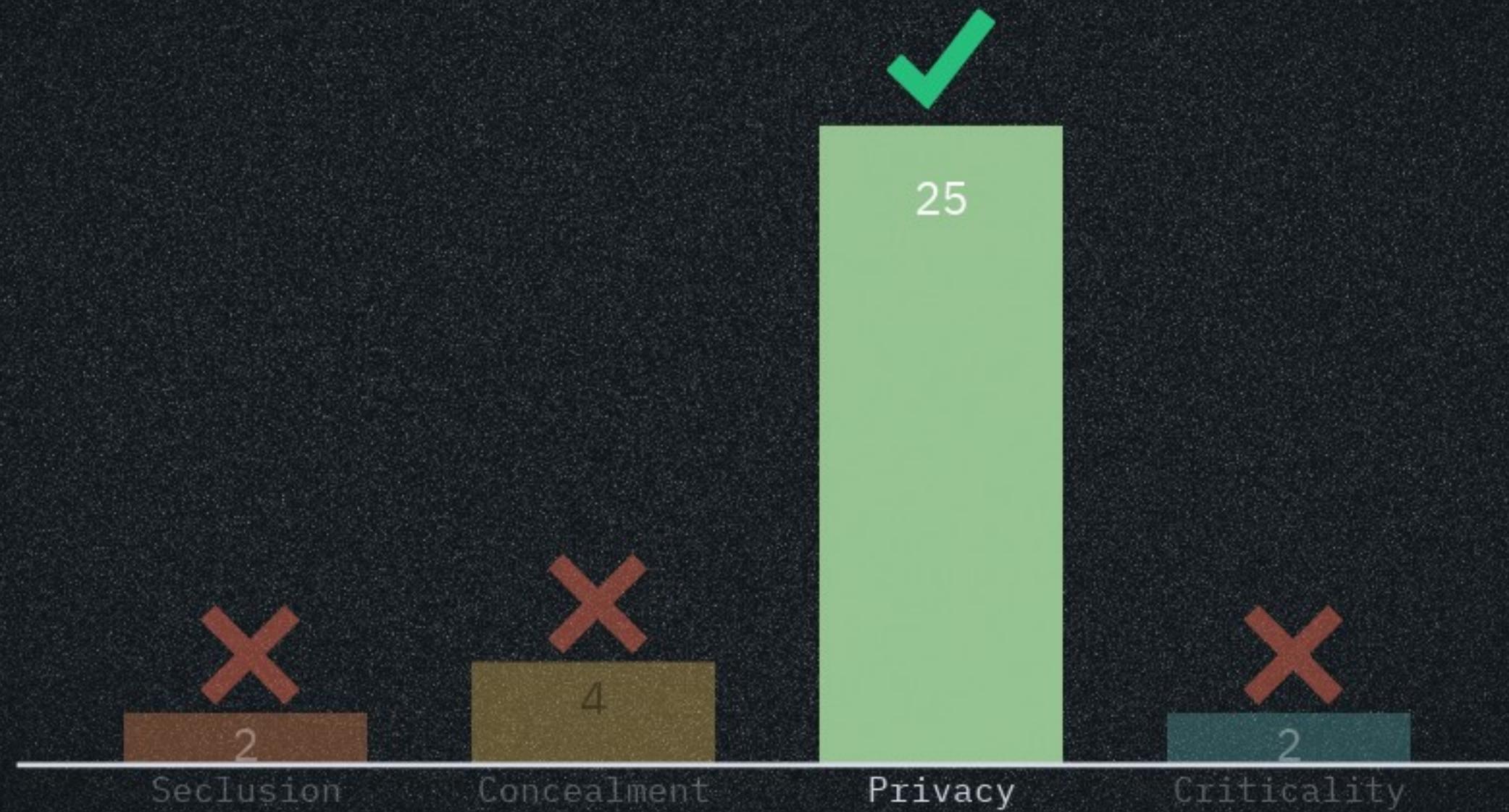
Which of the following contains the primary goals and objectives of security?



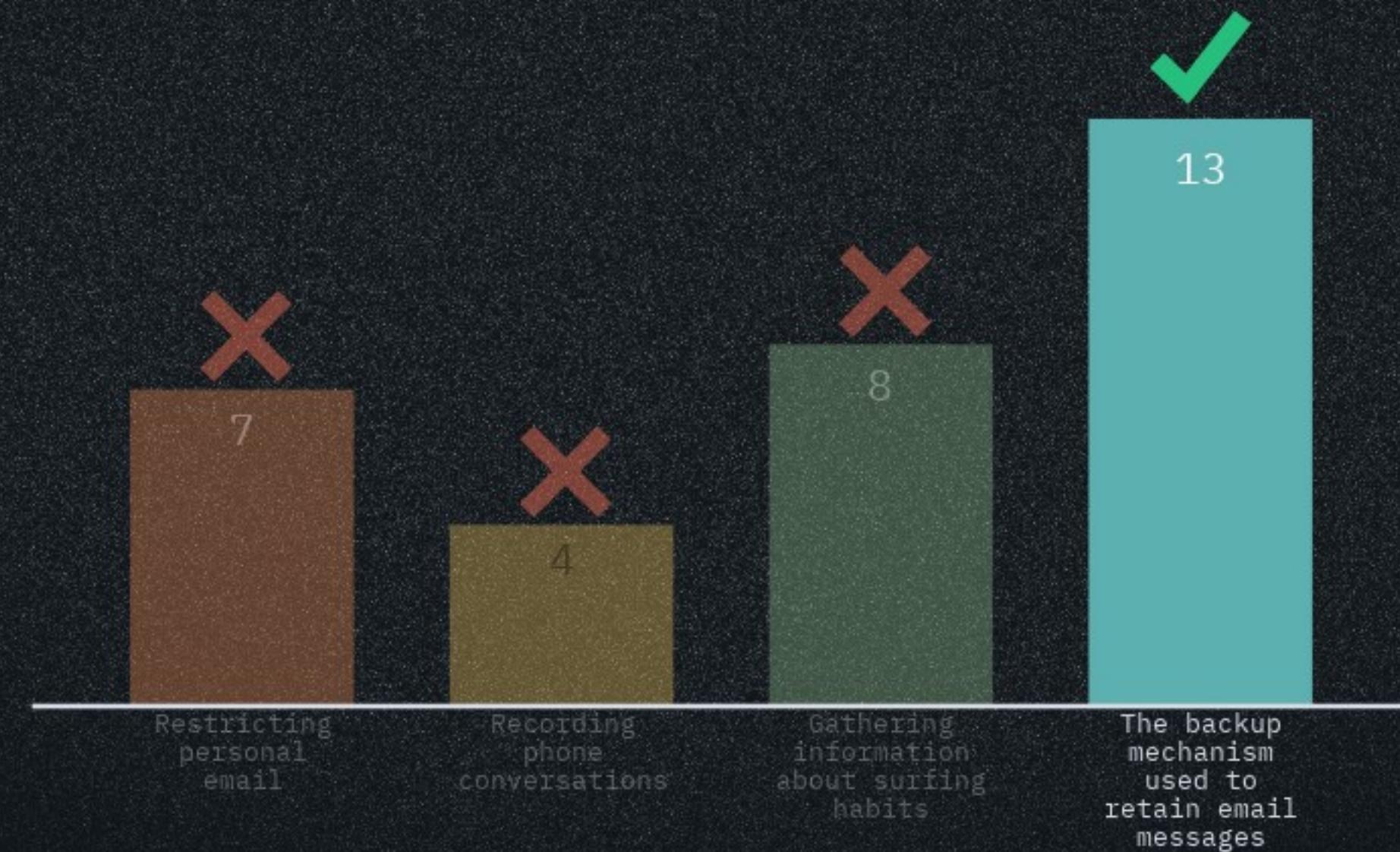
Which of the following is not true?



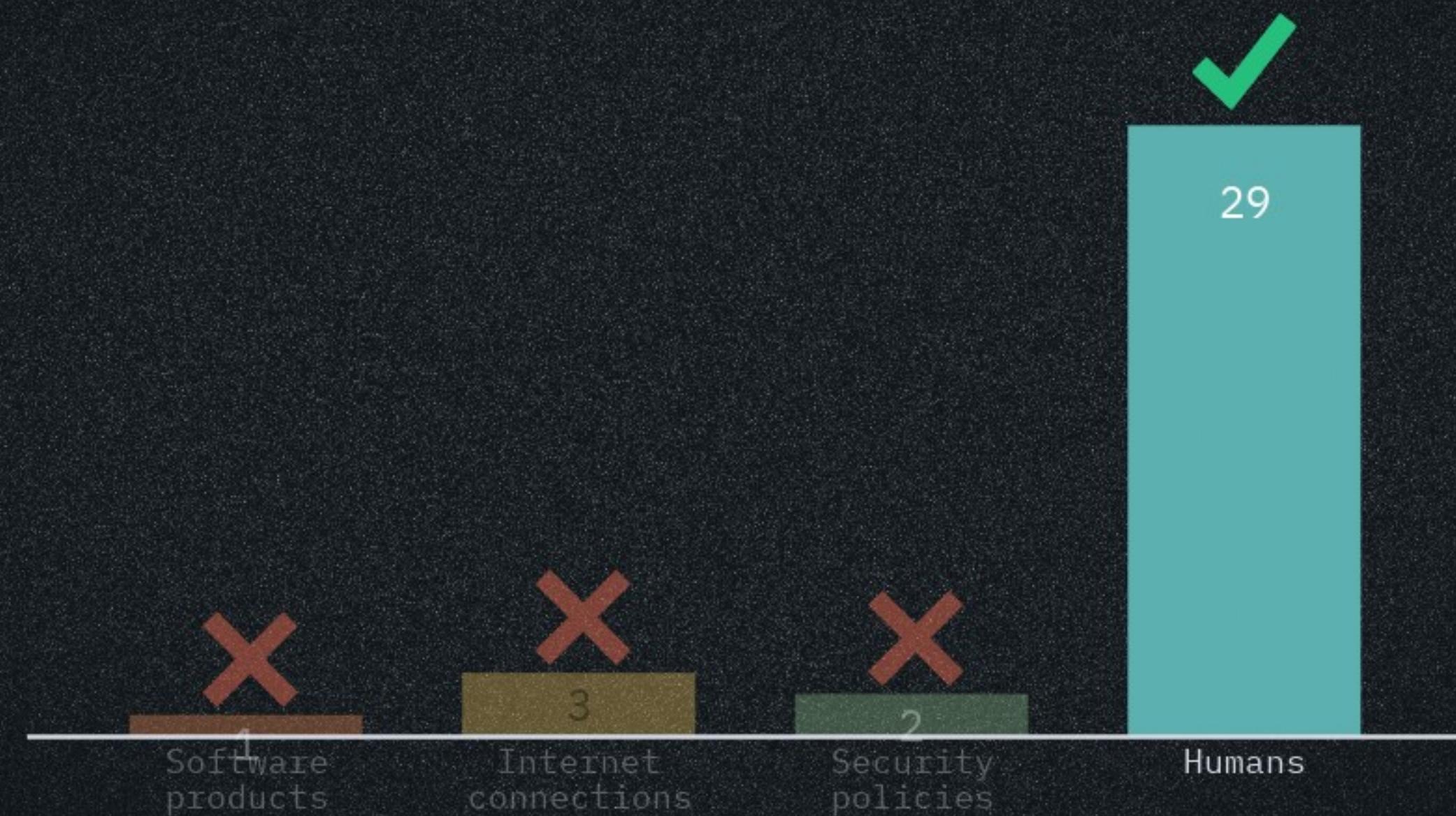
Refers to keeping information confidential that is personally identifiable or which might cause harm, embarrassment, disgrace to someone if revealed



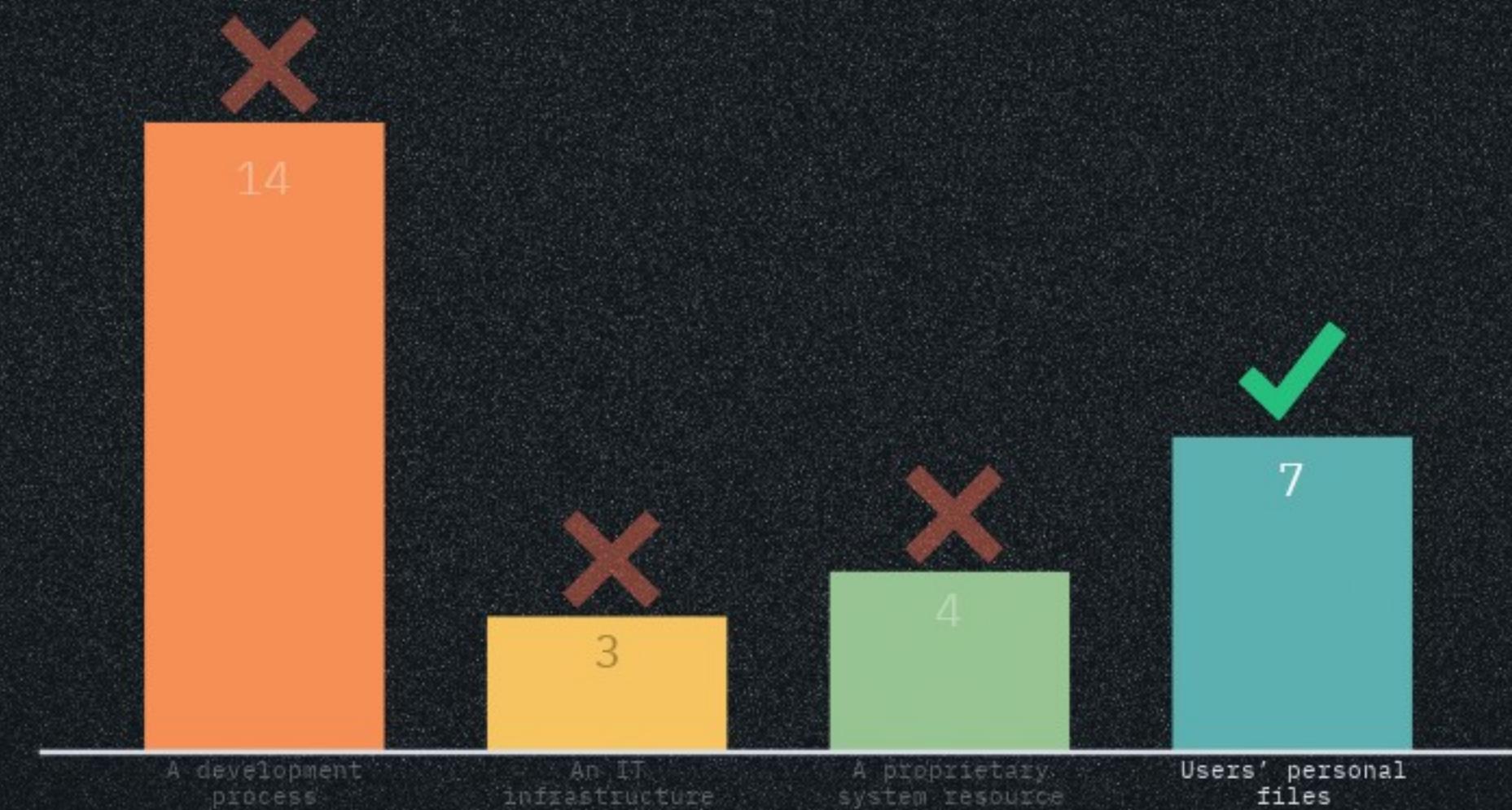
All but which of the following items requires awareness for all individuals affected?



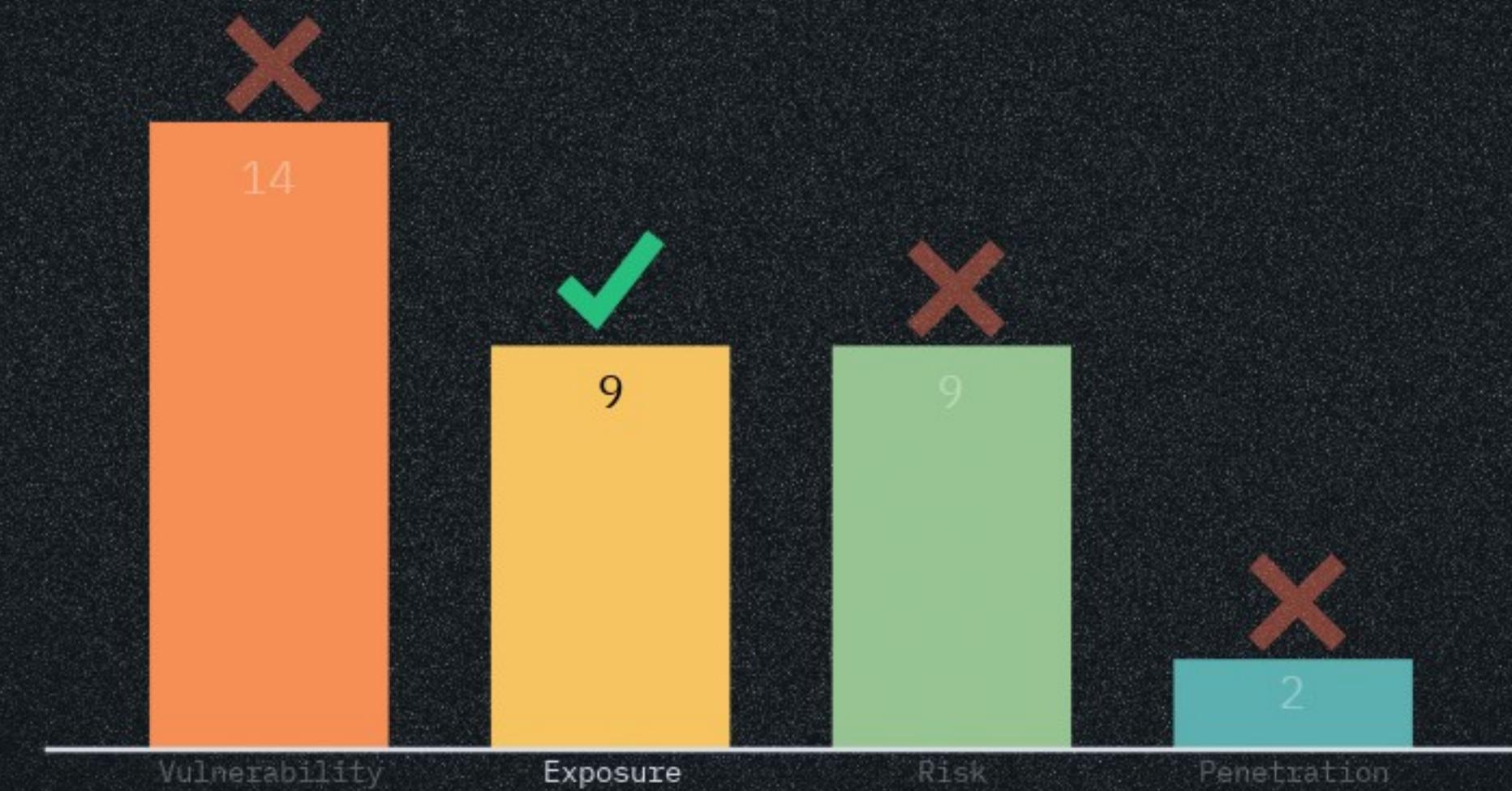
Which of the following is the weakest element in any security solution?



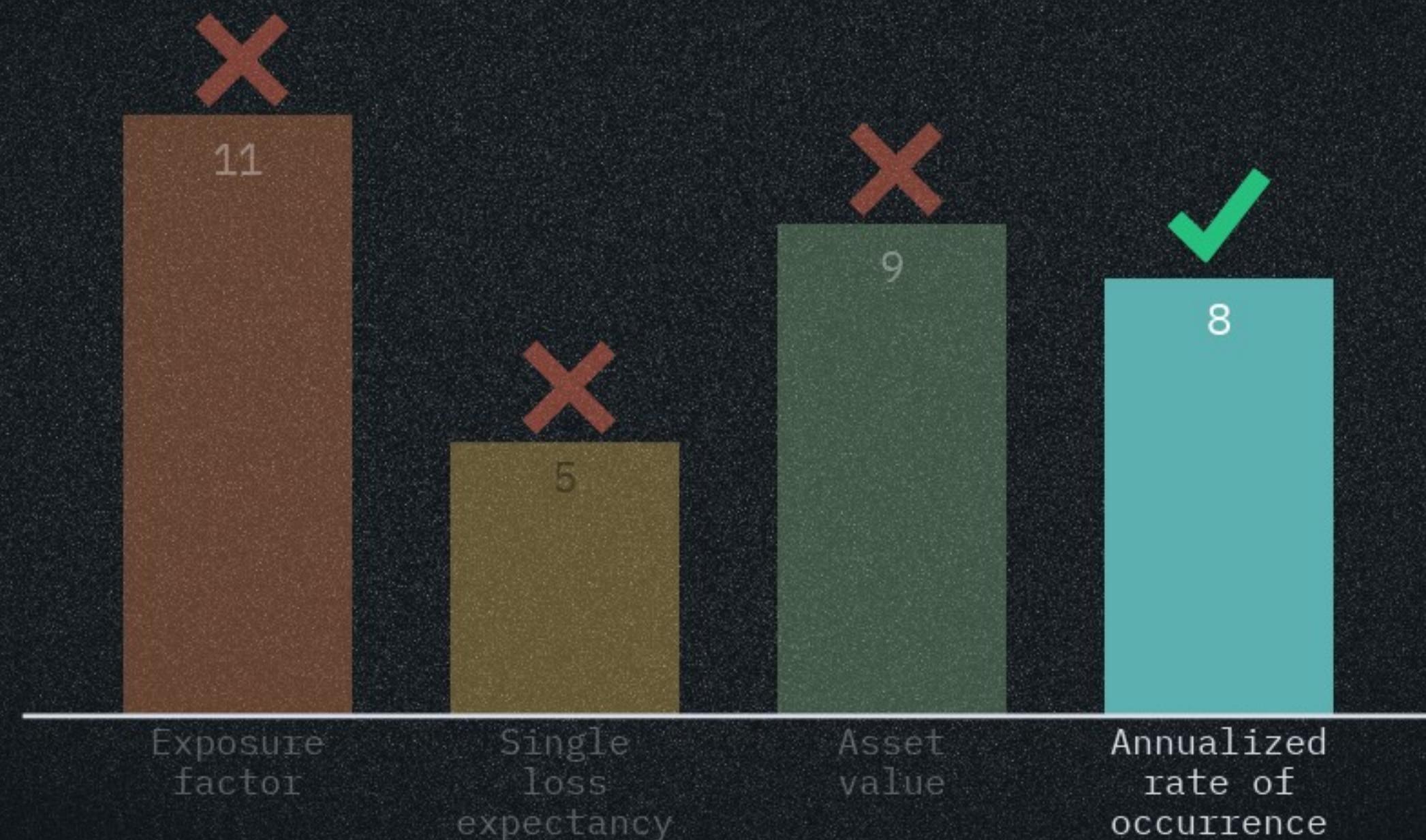
Which of the following would generally not be considered an asset in a risk analysis?



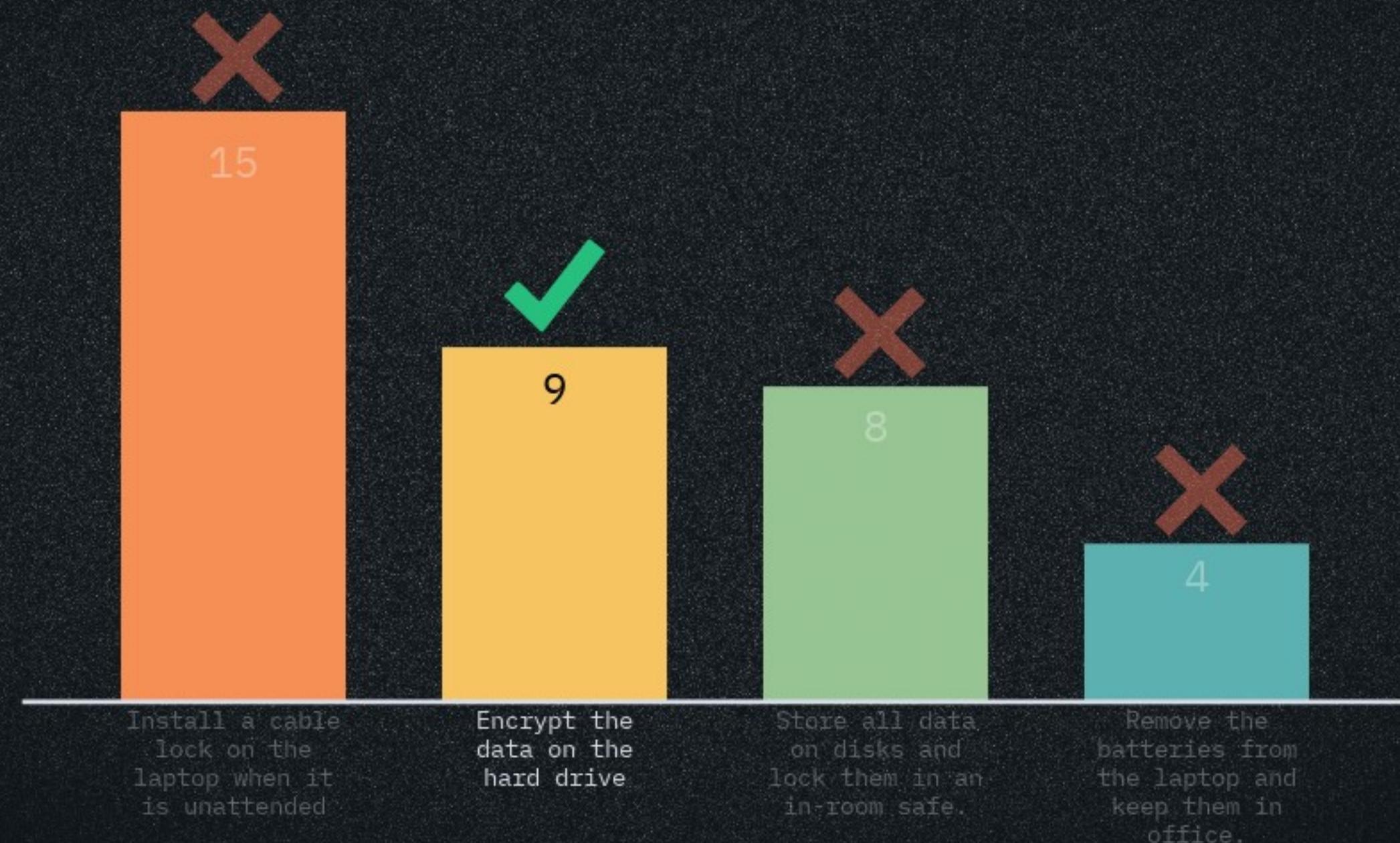
When a safeguard or a countermeasure is not present or is not sufficient, what remains?



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



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



Leaderboard



Class Test

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



LOCAL TIME
7:16:11ATTACKS TODAY
220,707

(X) NEW ATTACK FROM UNITED STATES TO THAILAND
(X) NEW ATTACK FROM THAILAND TO UNITED STATES
(X) NEW ATTACK FROM JAPAN TO THAILAND
(X) NEW ATTACK FROM JAPAN TO MEXICO

FIREYE CYBER THREAT MAP

ATTACKERS
TOP COUNTRIES
PAST 30 DAYS



[VIEW FULL SCREEN](#)

Powered by FireEye Labs
TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)

FINANCIAL SERVICES
SERVICES/CONSULTING
TELECOM
MANUFACTURING
INSURANCE

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

ransomware

trojan

hacker

ddos

dos

ransom ware

cracking

viruses

data

sniffing

social engineering

mim soso

spoofing

back door

backdoor access

data breach

phishing email

bribe

money

data theft

data tampering

sql injection

none

meme

hacking

worms

lots of money

personal information

data theft

mim attack

phising

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

The word cloud is centered around the word "data" in a large, bold orange font. Surrounding it are various other words related to data security and hacking, such as "private information", "personal information", "money", "password", "database", "username", "resources", "data leakage", "trade secrets", "damage rep of buisness", "intellectual property", "xss", "availability", "card details", "trade secrete", "information", "compromising the data", and "credential details". The words are in different colors (orange, green, blue, purple) and sizes, creating a dense cloud effect.

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 reactive measure once a product has been deployed



Identifying threats

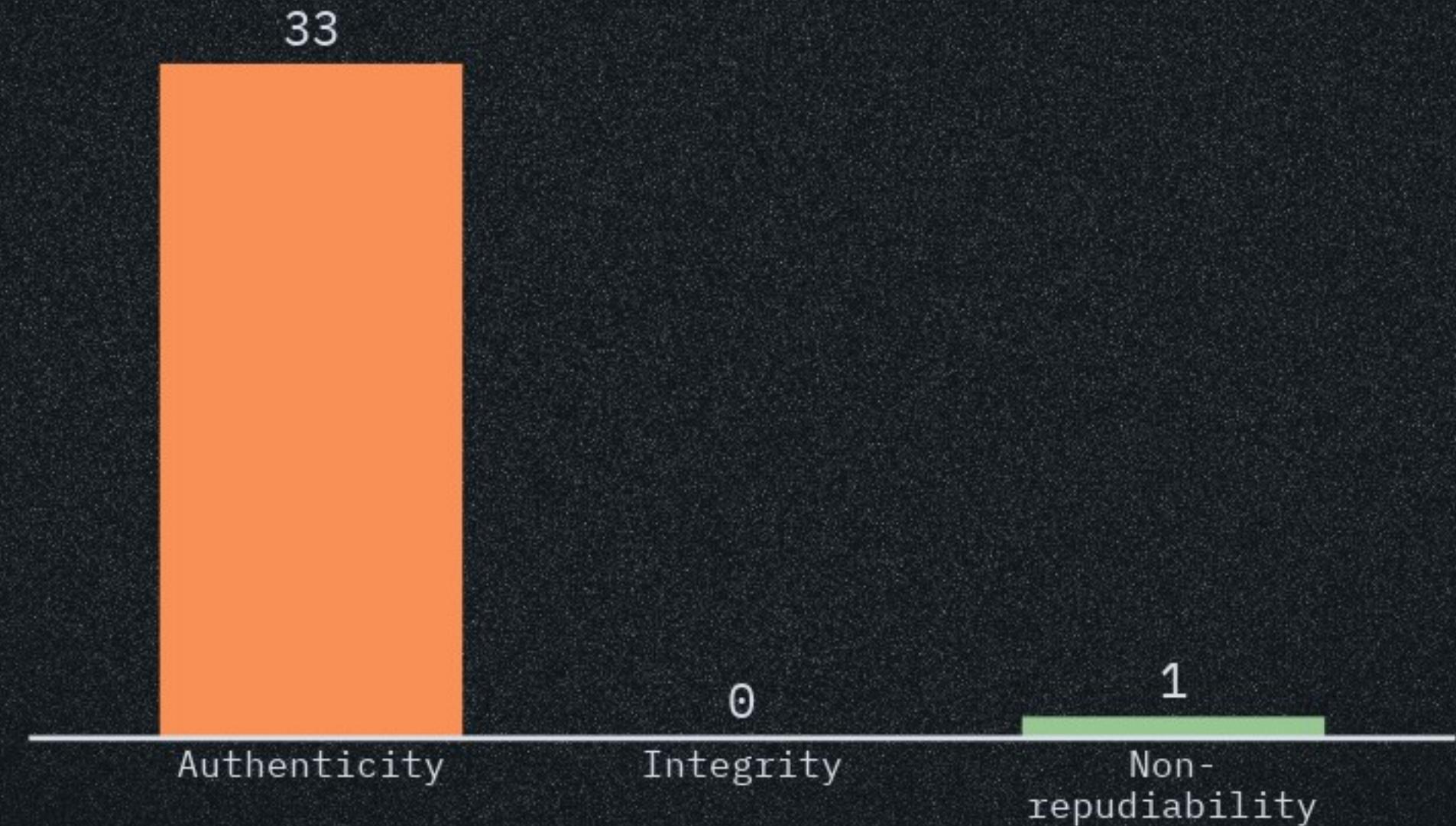
- Focused on Assets- This method uses asset valuation results and attempts to identify threats to the valuable assets
- Focused on Attackers- Some organizations are able to identify potential attackers and can identify the threats they represent based on the goal
- Focused on Software- If an organization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

STRIDE

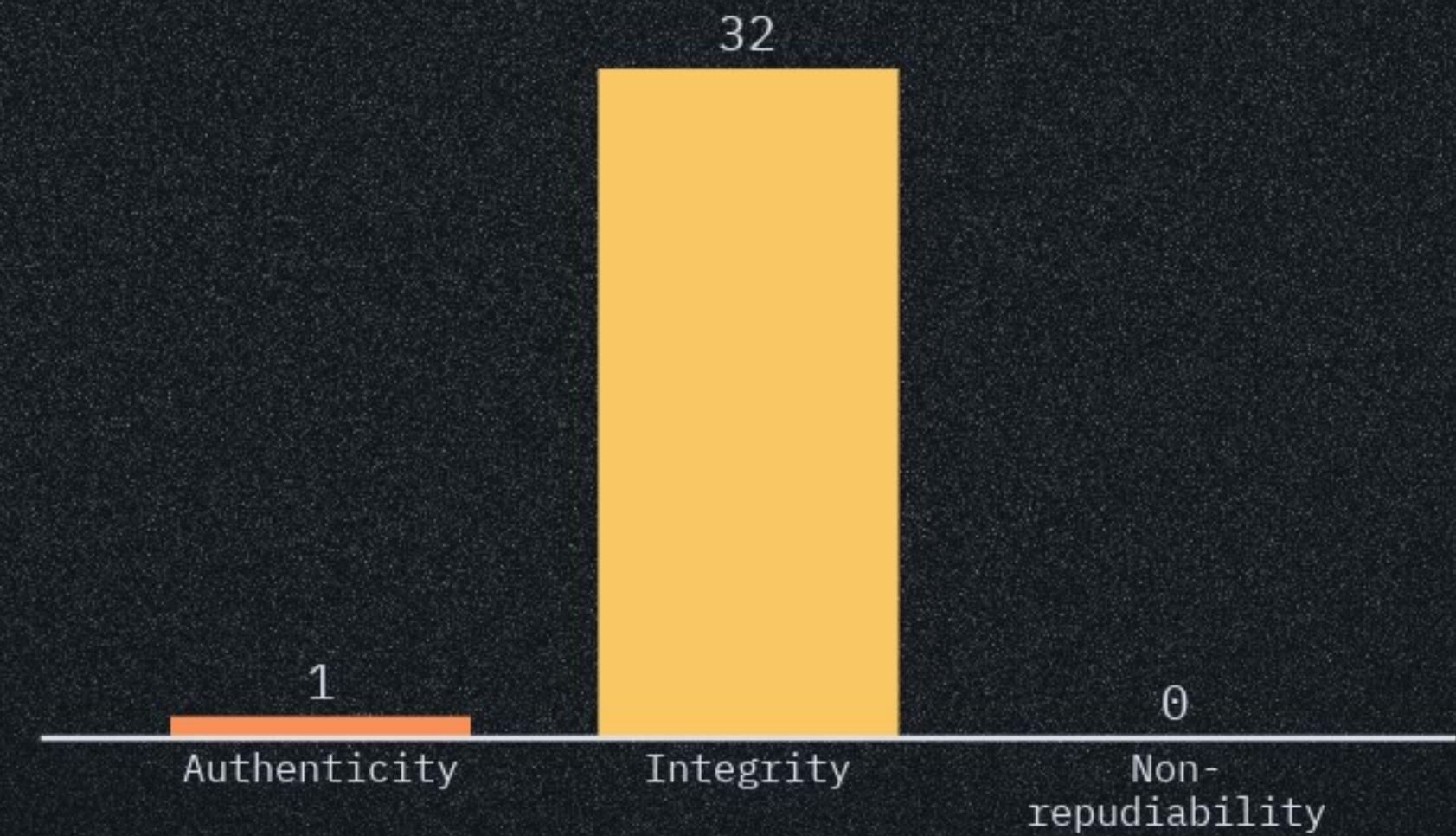
- Developed by Microsoft as part of threat modelling procedure in 1999.
- Helps to prompt questions e.g. what would happen if ...?
- Helps reduce chance of failing to identify a risk



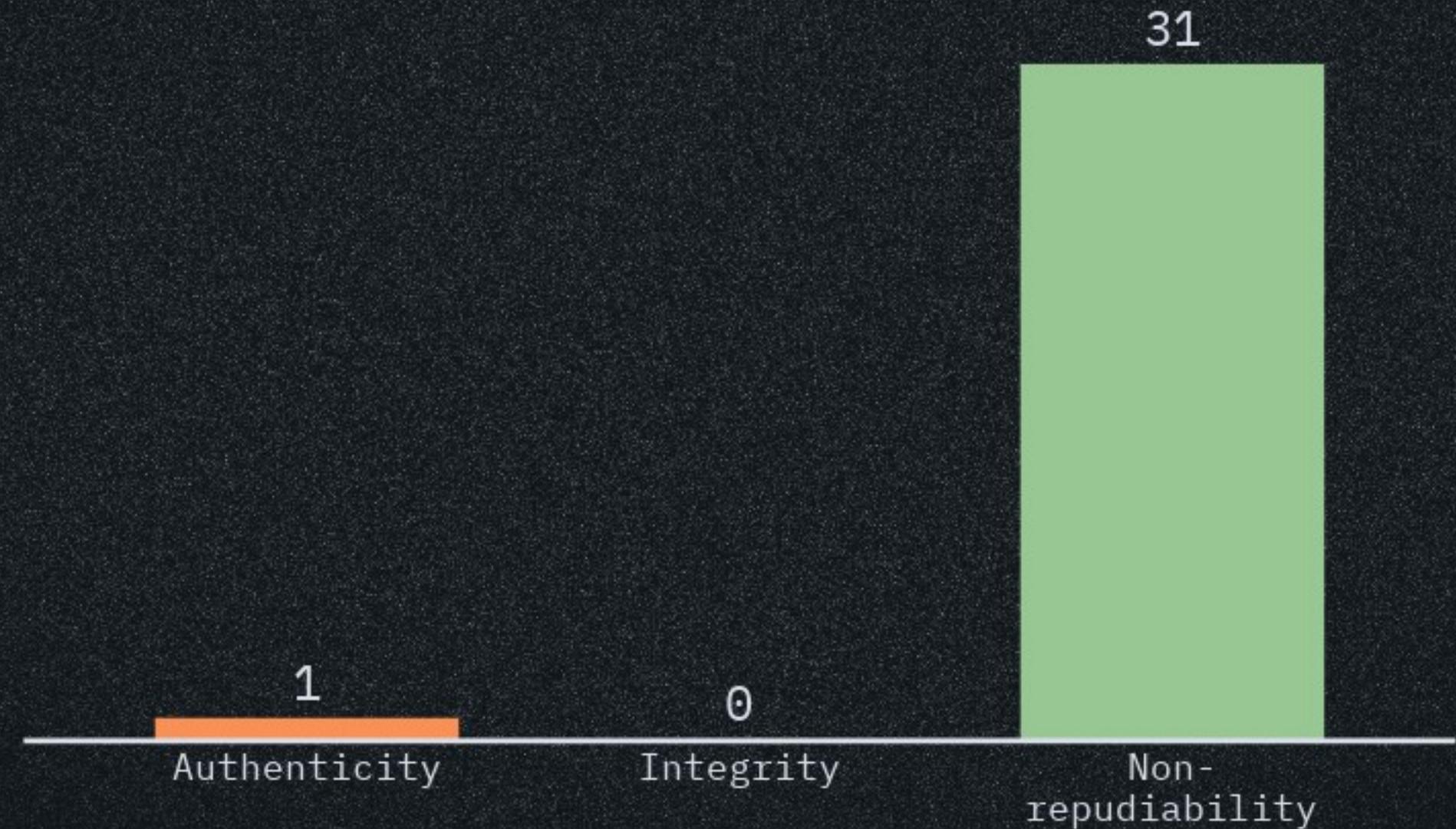
Spoofing - a situation in which a person or program successfully identifies as another by falsifying data. Which security property is violated



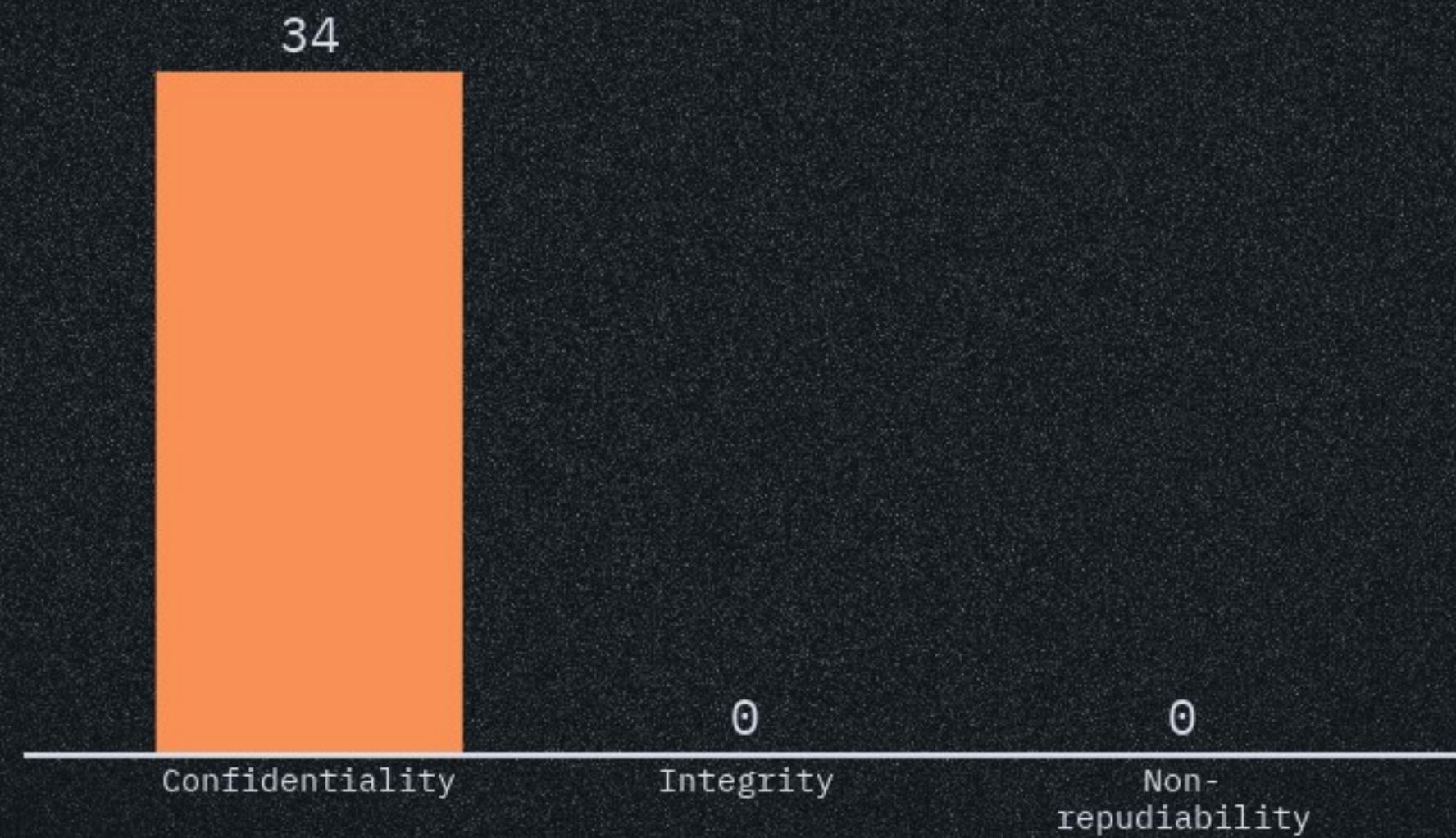
Tampering - modification of data or code, which security property is violated



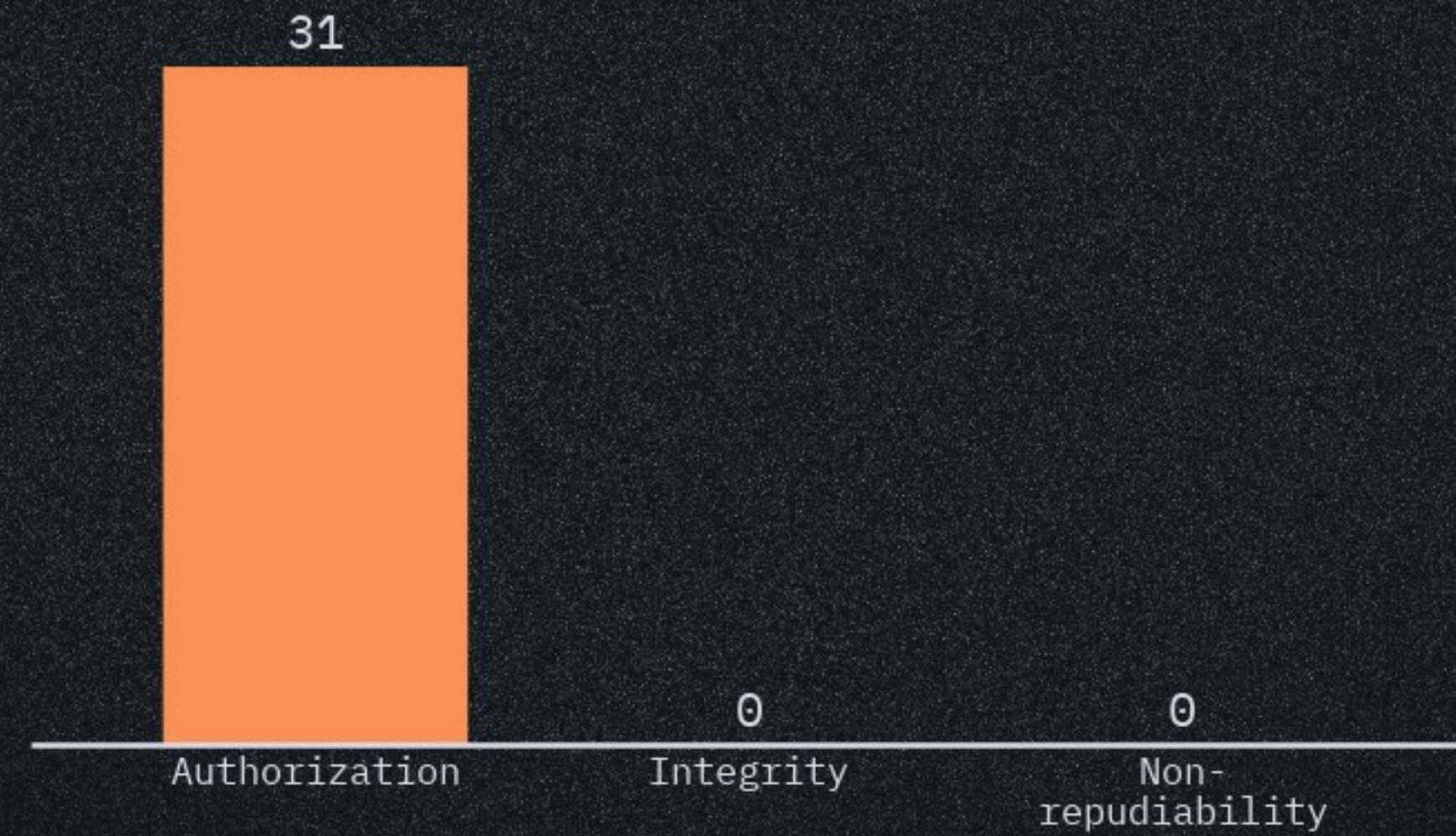
Repudiation This is a threat where an attacker deletes or changes a transaction or login information in an attempt to refute that they ever took place



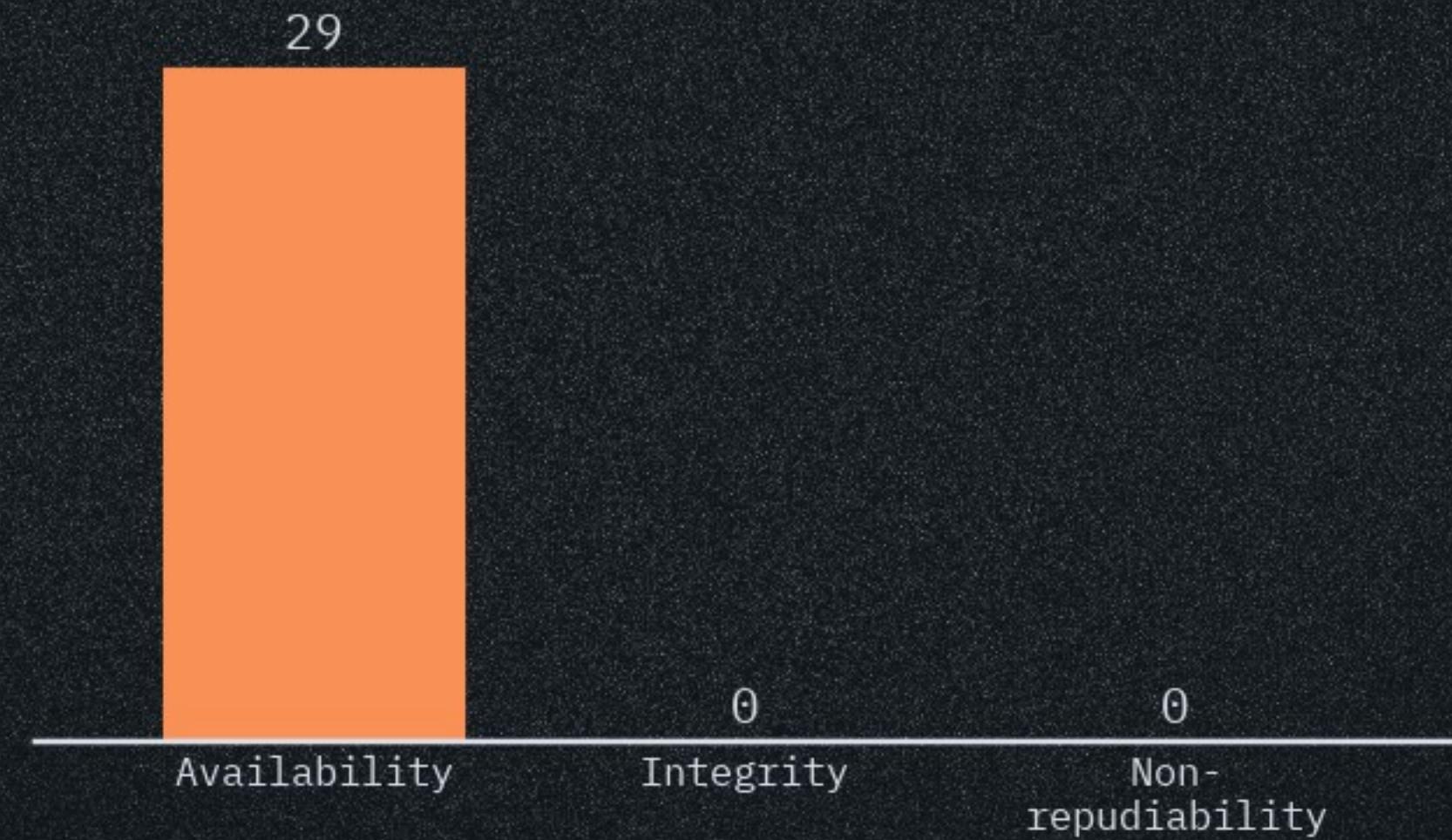
Information disclosure- Exposing information to someone who is not authorised to, which security property is violated



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



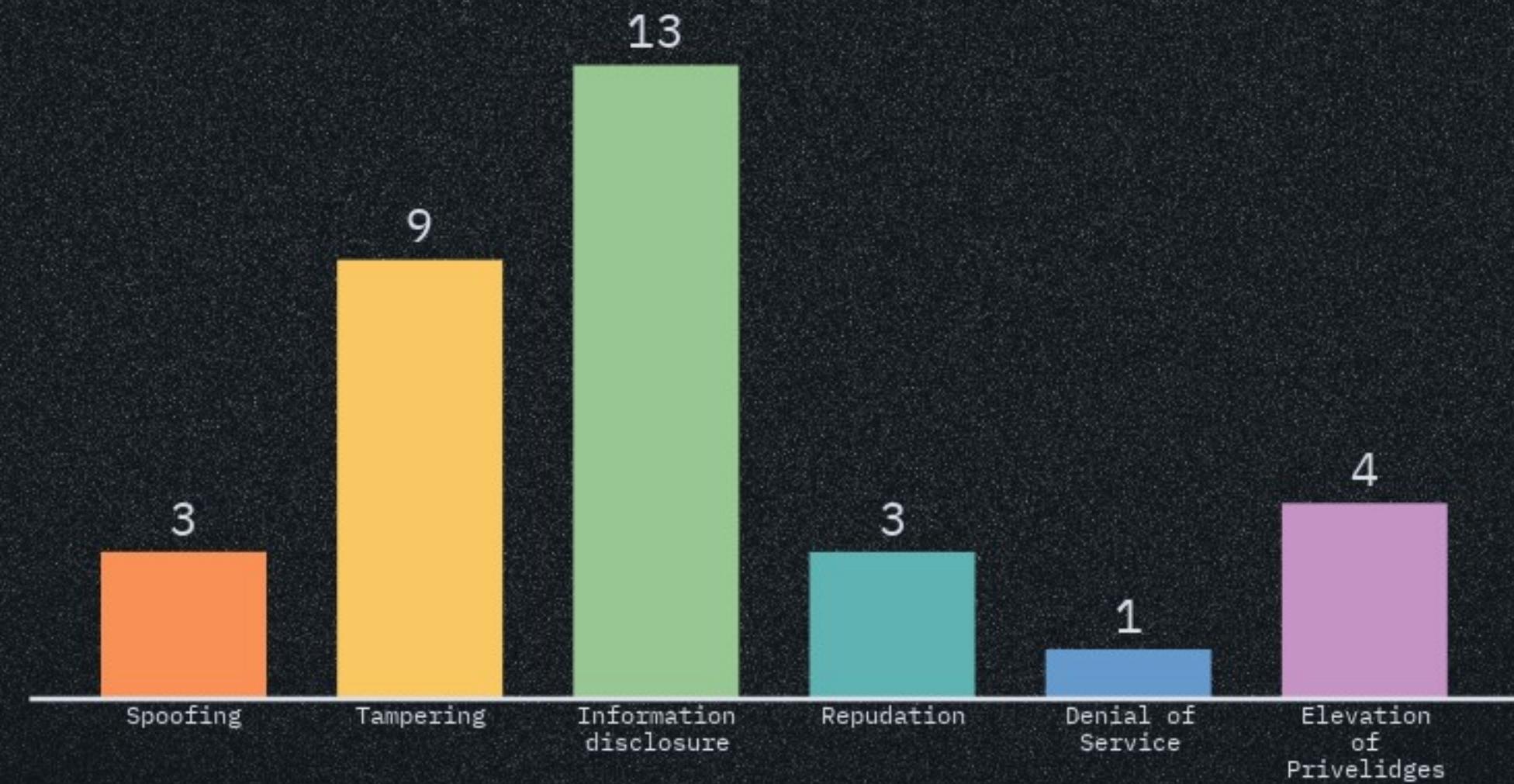
Denial of Service- deny or degrade service to a user, which security property is violated



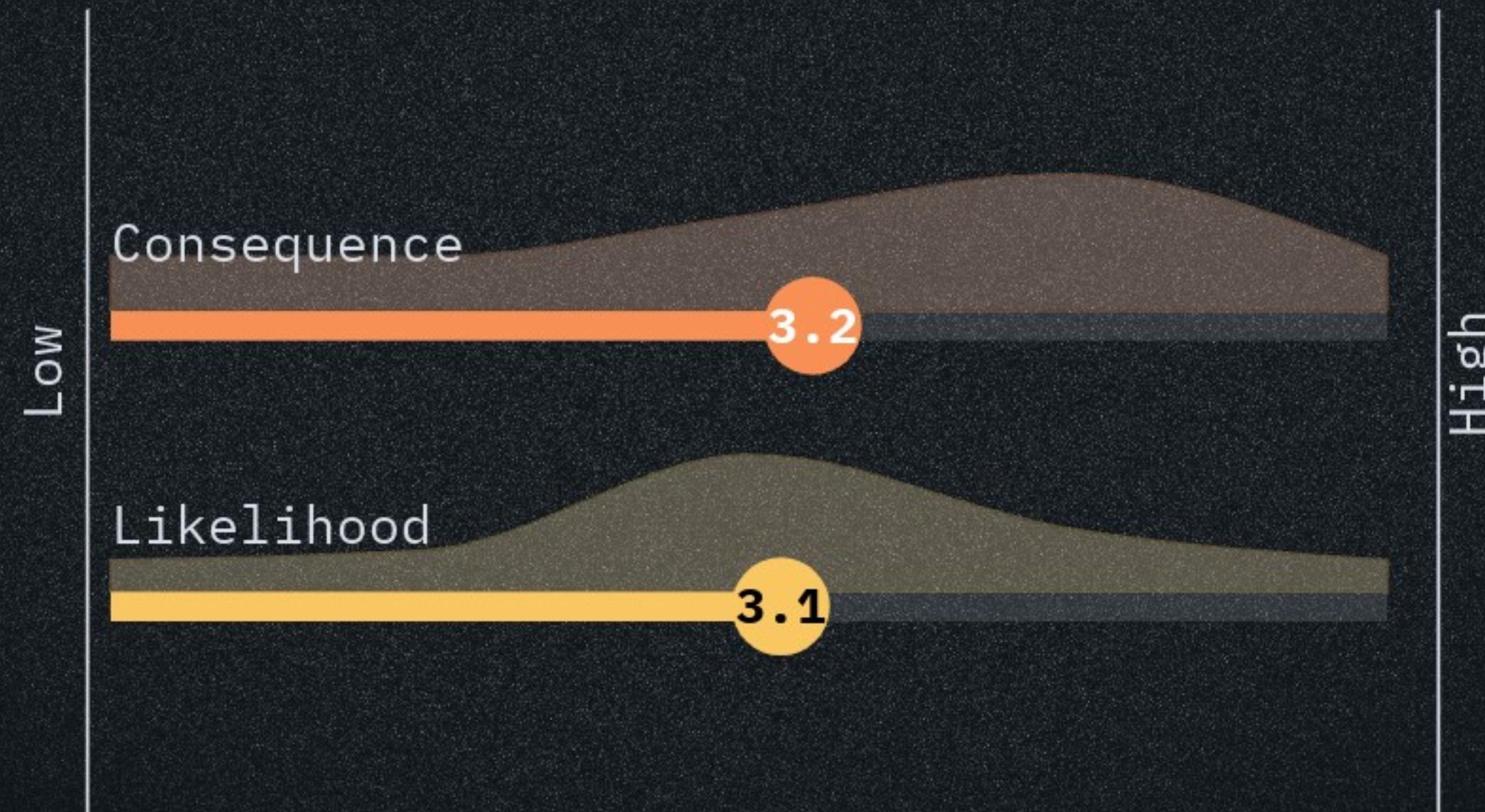
What all attacks can be carried out targetting the data over an unsecured network?

A word cloud visualization centered around the word "phishing". Other prominent terms include "sql injection", "man in the middle", "ddos", "dos", "mitm", "tampering", "spoofing", "malware", "trojans", "internet connection", "impersonation", "phishing email", "cryptojacking", "web attacks", "authentication system", "repudiation", "denial of service", "packet capturing", "unauthorised access", "data breach", "data theft", "data loss", "virus", "idk", and "session hijacking". The words are rendered in various colors and sizes, with larger and more saturated colors appearing in the center and smaller, lighter colors towards the edges.

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



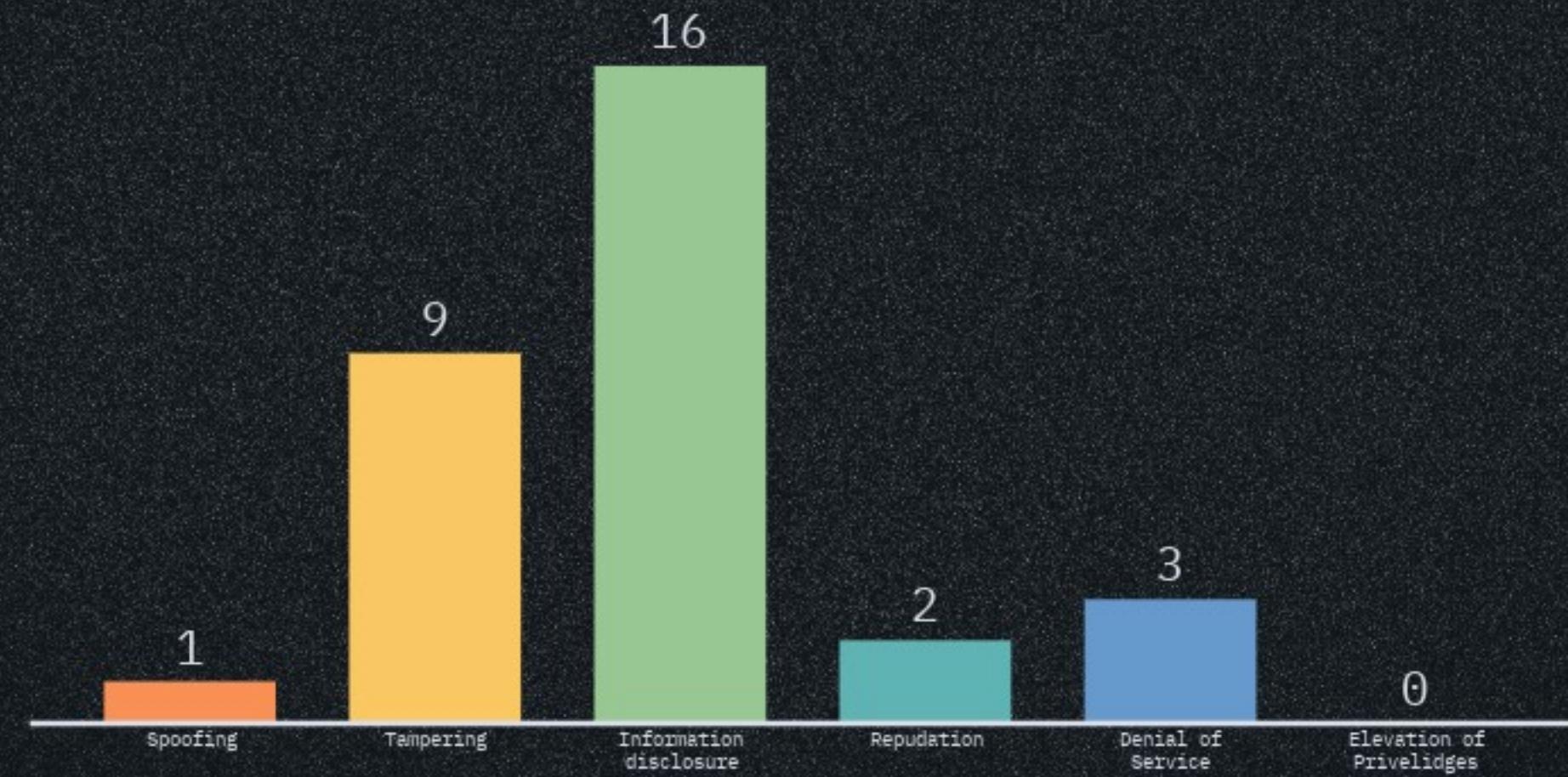
Calculate risk for one of the threat identified



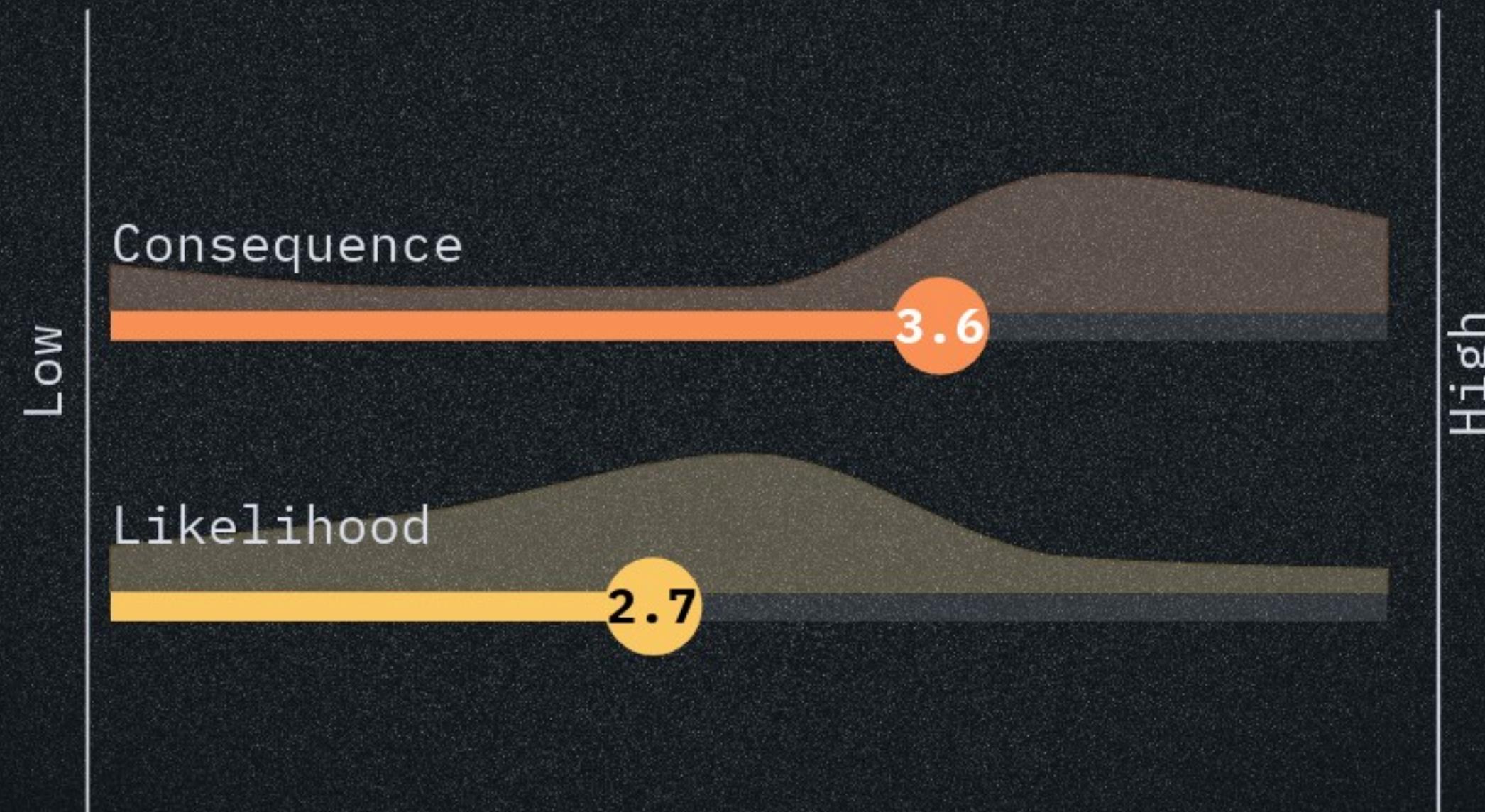
List all the attacks you can think of

A word cloud centered around the term "sql injection". Other prominent terms include "malware", "ddos", "data breach", "information disclosure", "denial of service", "cross site scripting", "ip theft", "data loss", "ransomware", "data tampering", "phishing", "mitm", "sql", "sql injection", "encoding", "data leak", "data tamper", "!#*&!\$", "state secrets", "elevation of privileges", "information exposure", "man in middle", "temping", "info disclosure", "formjacking", "injection attacks", "database breach", "malware injection", "data leakage", and "data lose".

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

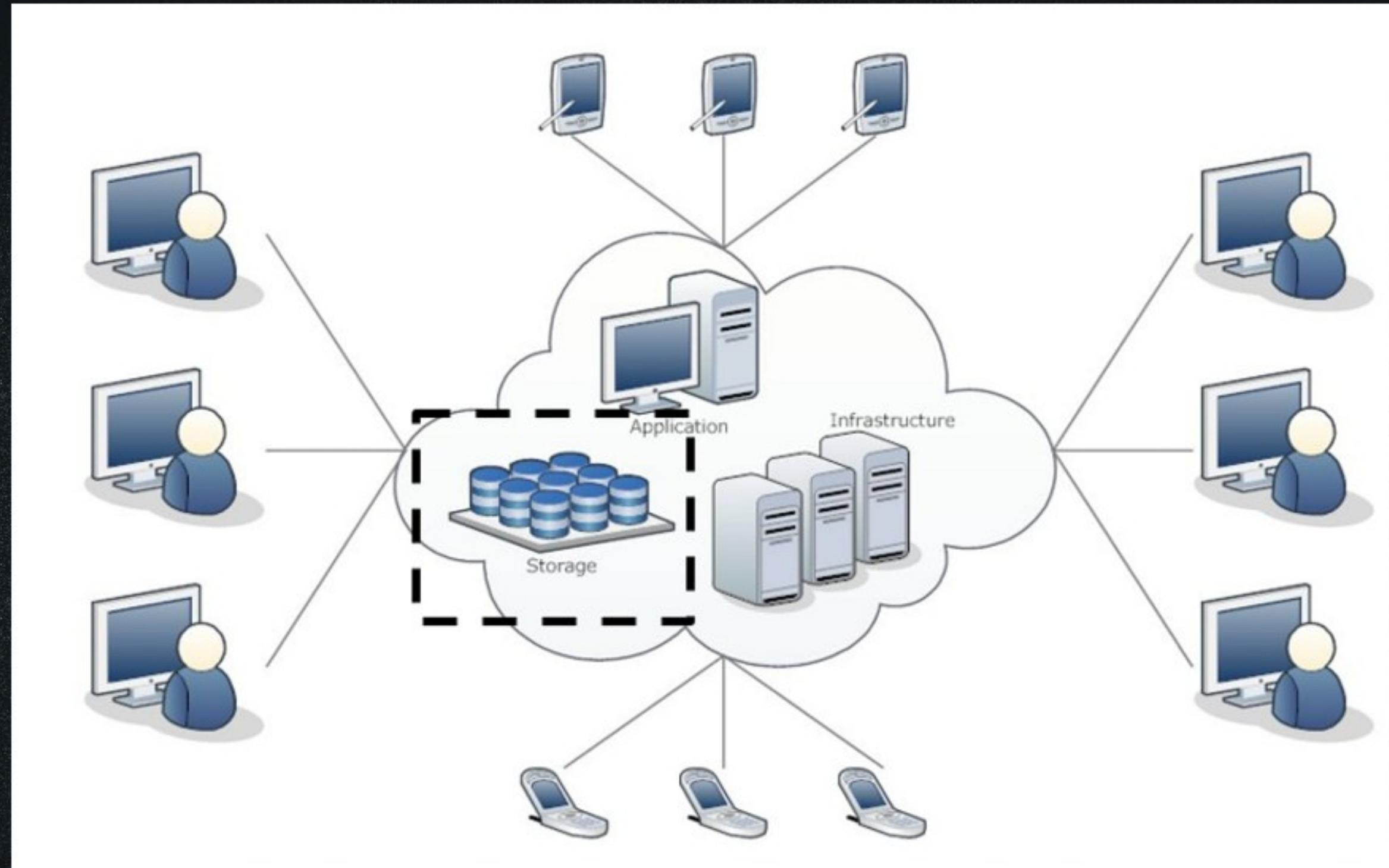


Calculate risk for one of the threat identified



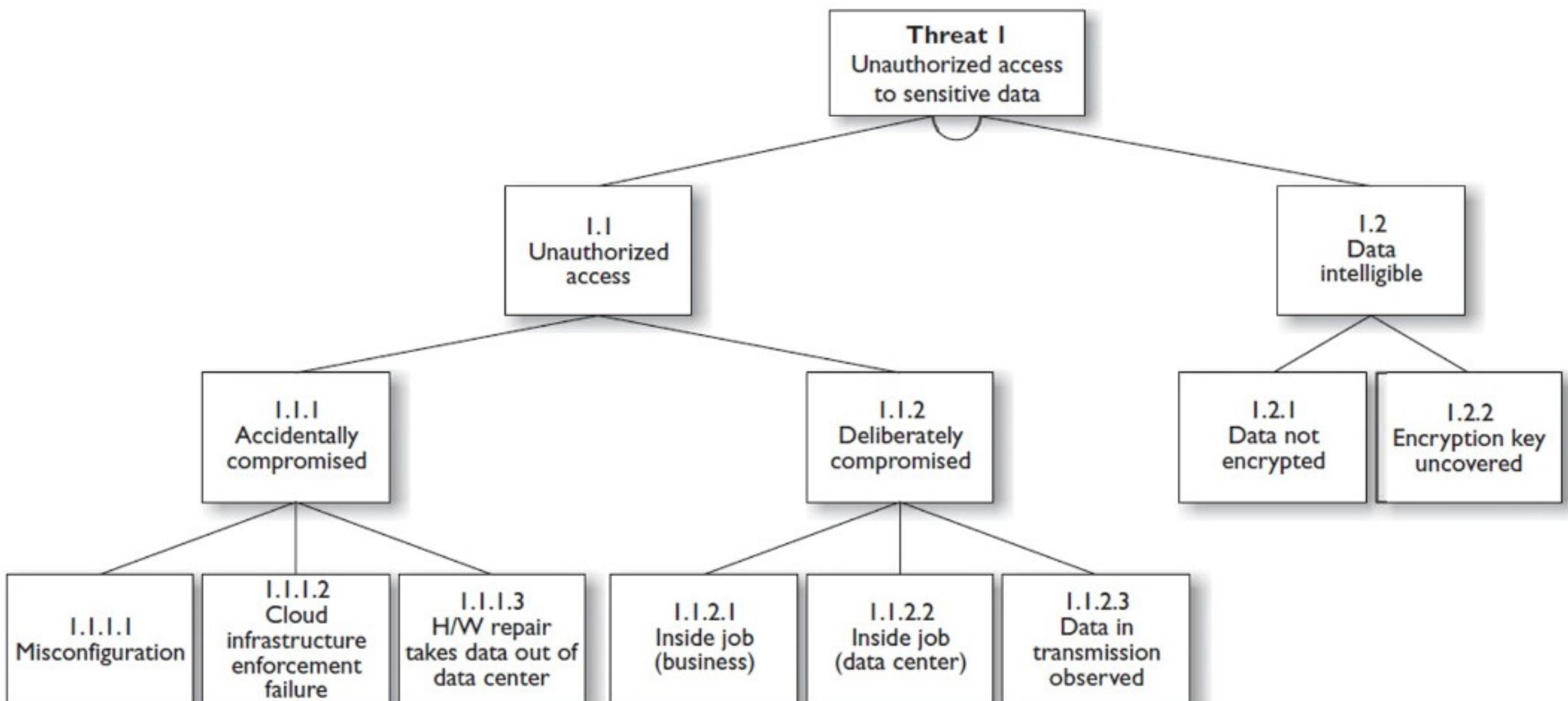
Attack Trees

- 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.





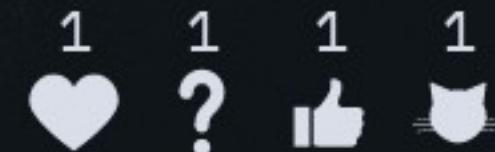
Attack Tree for Unauthorised Access to Sensitive data

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 advanced attack tools.
- 2 = Malware exists on the Internet, or an exploit is easily performed, using available 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 easily discovered using a search engine.

DREAD model for risk analysis

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

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



Fault Tree Analysis

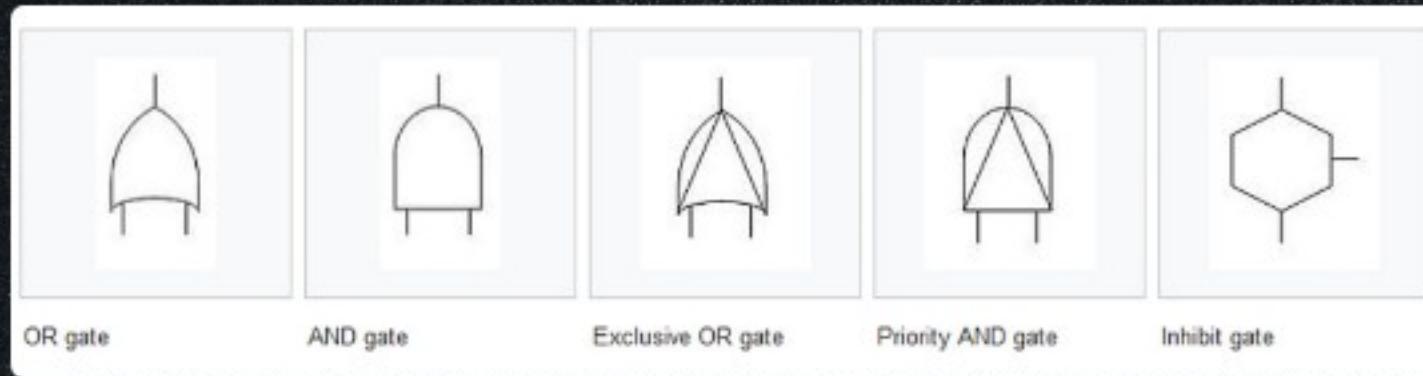
- A more useful approach to identifying failures that can take place within more complex environments and systems
- An undesired effect is taken as the root or top event of a tree of logic
- Each situation that has the potential to cause that effect is added to the tree as a series of logic expressions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



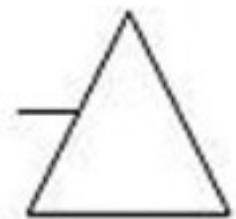
- OR gate - the output occurs if any input occurs
- AND gate - the output occurs only if all inputs occur
- Exclusive OR gate - the output occurs if exactly one input occurs.
- Priority AND gate - the output occurs if the inputs occur in a specific sequence specified by a conditioning event.
- Inhibit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

Transfer Symbols

- Transfer symbols are used to connect the inputs and outputs of related fault trees.
- Transfer in- Transfer in the results from a subsystem
- Transfer out- Transfer results out to be used by different fault tree.



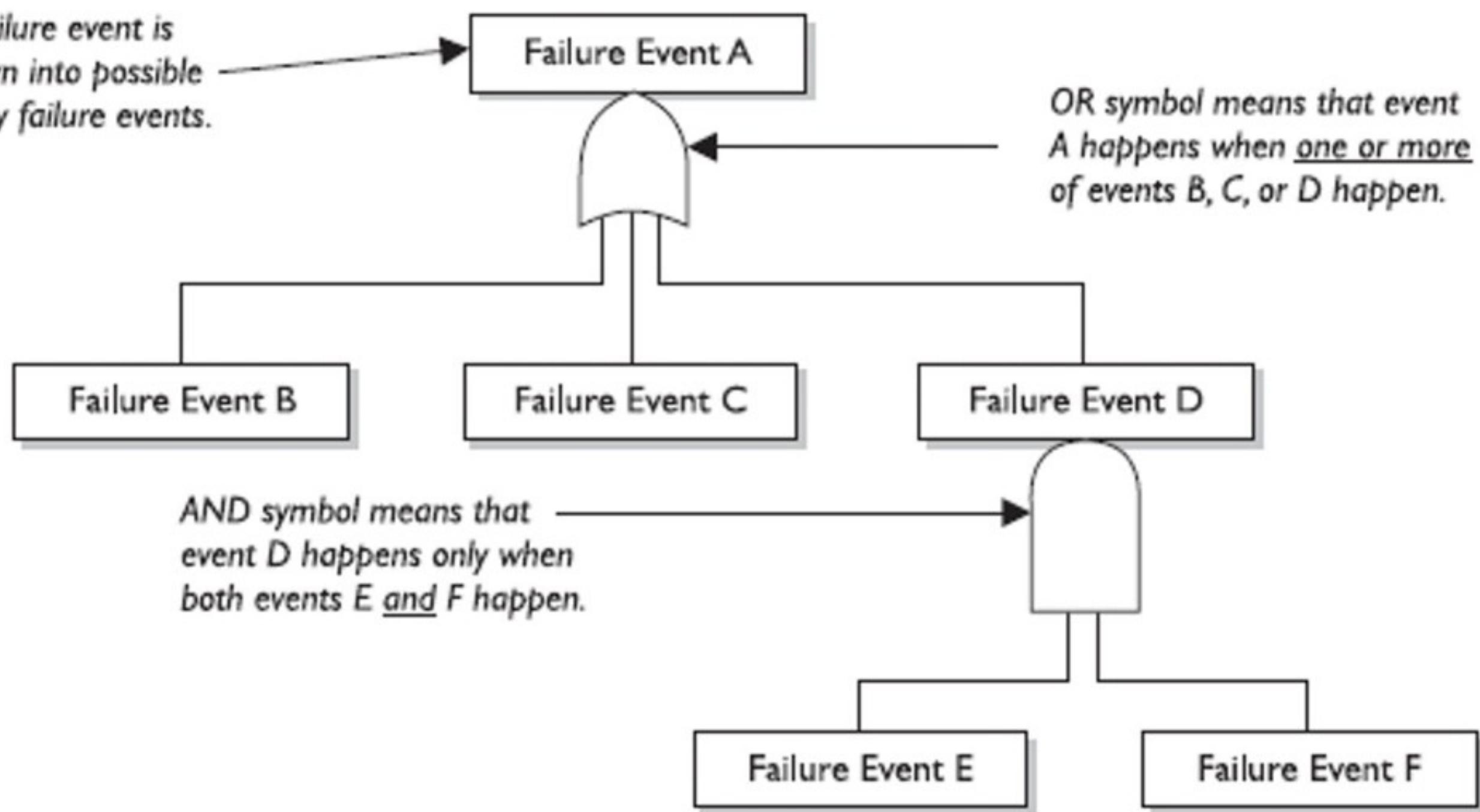
Transfer in



Transfer out

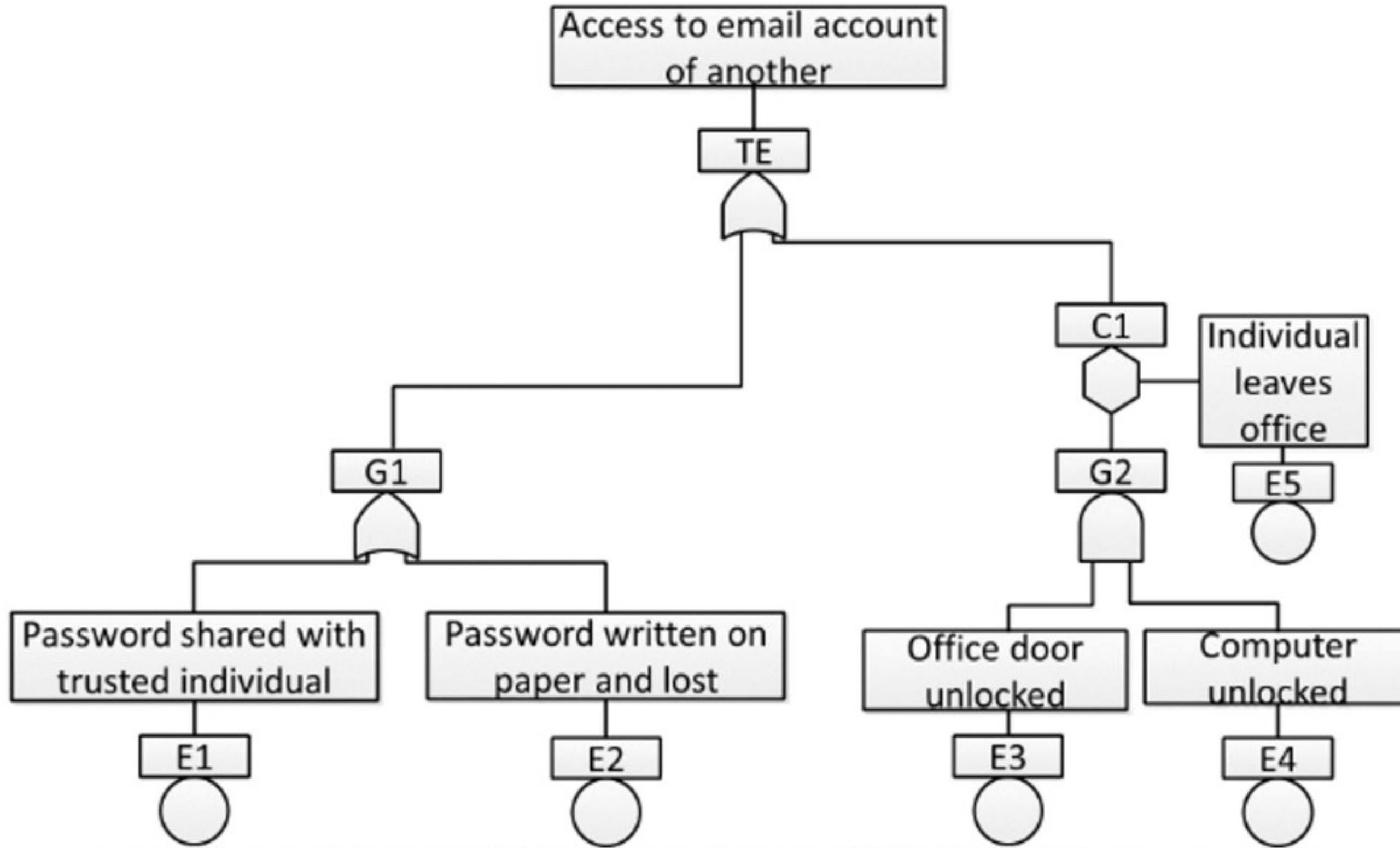


Top-level failure event is broken down into possible contributory failure events.



Fault tree and logic components





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

A word cloud visualization representing various cyber threats. The most prominent word is 'phishing' in large yellow text. Surrounding it are other terms related to cyber attacks, such as 'sql injection' (green), 'ddos' (orange), 'mitm' (teal), 'dos' (blue), 'virus' (purple), and 'ransomware' (pink). Other visible words include 'data breach', 'info breach', 'exploit kits', 'man in the middle', 'zero day exploit', 'malware', 'website defacing', 'session hijacking', 'man in the browser', 'email attack', 'out of server', 'injection attacks', 'phishing email', 'insider threats', 'database stolen', 'tampering', 'denial of service', 'sniffing', 'data disclosure', 'malware attack', 'internet of things (iot)', 'impersonalisation', and 'man in the middle'. The words are colored in a variety of pastel shades.