Finding Security & Privacy Risks

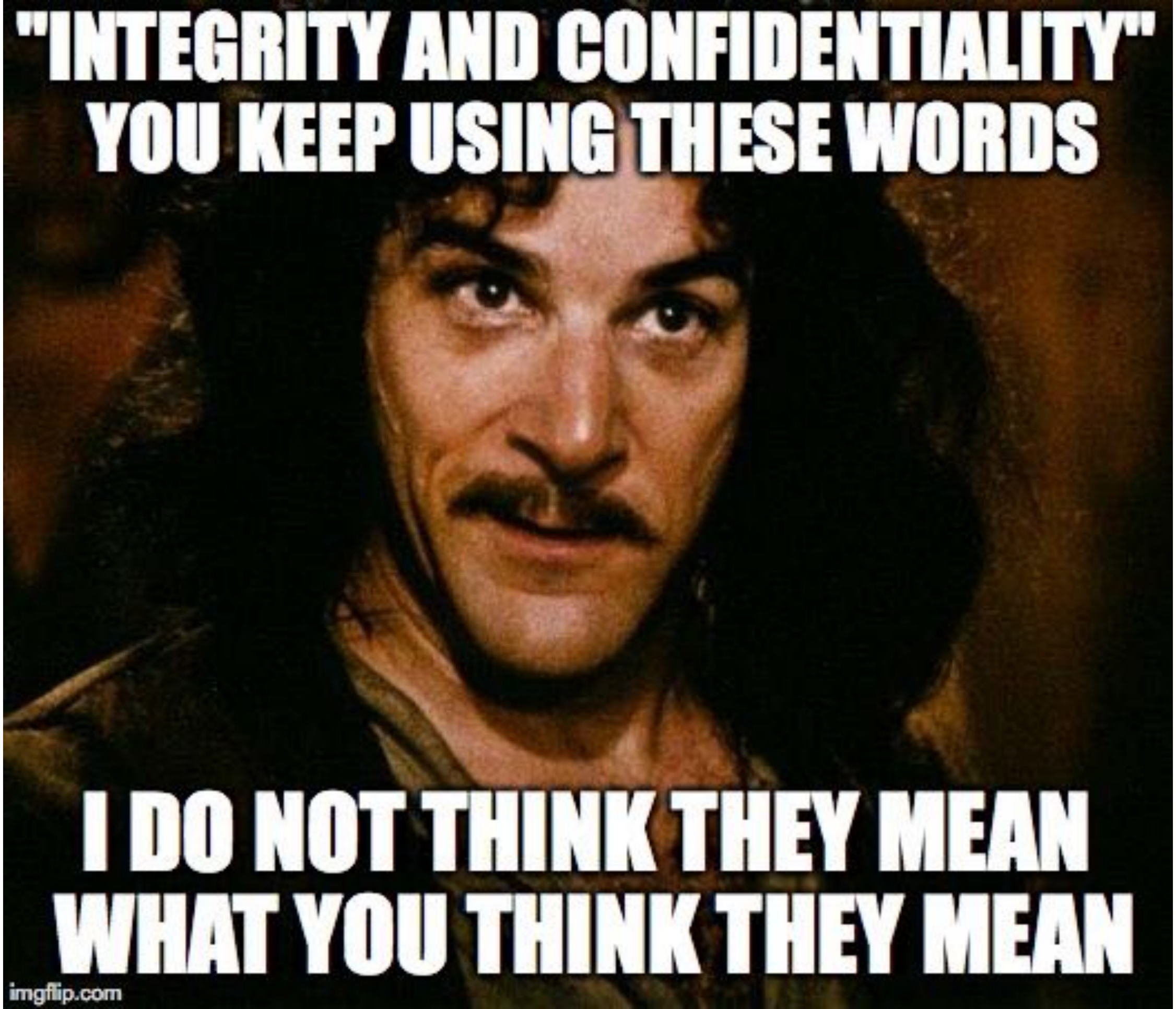
Shamal Faily
sfaily@bournemouth.ac.uk
https://cybersecurity.bournemouth.ac.uk

Story so far

- Identified personal data
- Identified and categorised privacy risks
- Is this enough to demonstrate GDPR compliance?

Integrity & Confidentiality

- You must show you have *appropriate* security measures to protect the data you hold.
- You need evidence that your security measures are appropriate.


"INTEGRITY AND CONFIDENTIALITY"
YOU KEEP USING THESE WORDS
I DO NOT THINK THEY MEAN
WHAT YOU THINK THEY MEAN
imgflip.com

Information Security

- Preservation of *confidentiality*, *integrity* and *availability* of information; in addition, other properties, such as *authenticity*, *accountability*, n*on-repudiation*, and *reliability* can also be involved.

ISO. ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management. ISO/IEC, 2007.

Confidentiality

- The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
- Associated with other properties
  - Hiding link between individuals and operations (Unlinkability)
  - Who individuals are (Anonymity)

https://www.flickr.com/photos/sophotow/16559284088

ISO. ISO/IEC 13335-1:2004: Information Technology – Security Techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. ISO/IEC, 2004.

Integrity

- The property of safeguarding the accuracy and completeness of assets

- Often a prerequisite for other properties

  - Modifying Operating System to circumvent Confidentiality and Availability

```
sysadmin@caillou:~$ gpg --fingerprint EBA34B1C
pub   4096R/EBA34B1C 2014-05-08
      Key fingerprint = 0B14 9192 9806 5962 5470  0155 FD72 0AD9 EBA3 4B1C
uid                  Micah Lee <micah@micahflee.com>
uid                  Micah Lee <micah@firstlook.org>
uid                  Micah Lee <micah.lee@firstlook.org>
uid                  Micah Lee <micah.lee@theintercept.com>
uid                  Micah Lee <micah@pressfreedomfoundation.org>
sub   4096R/64B1D8D1 2014-05-08
```

https://www.flickr.com/photos/xmodulo/15360894427

ISO. ISO/IEC 13335-1:2004: Information Technology – Security Techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. ISO/IEC, 2004.

Availability

- The property of being accessible and usable upon demand by an authorised entity

- A lack of mechanisms for this property
  - Overly restricted/expensive mechanisms can *reduce* availability

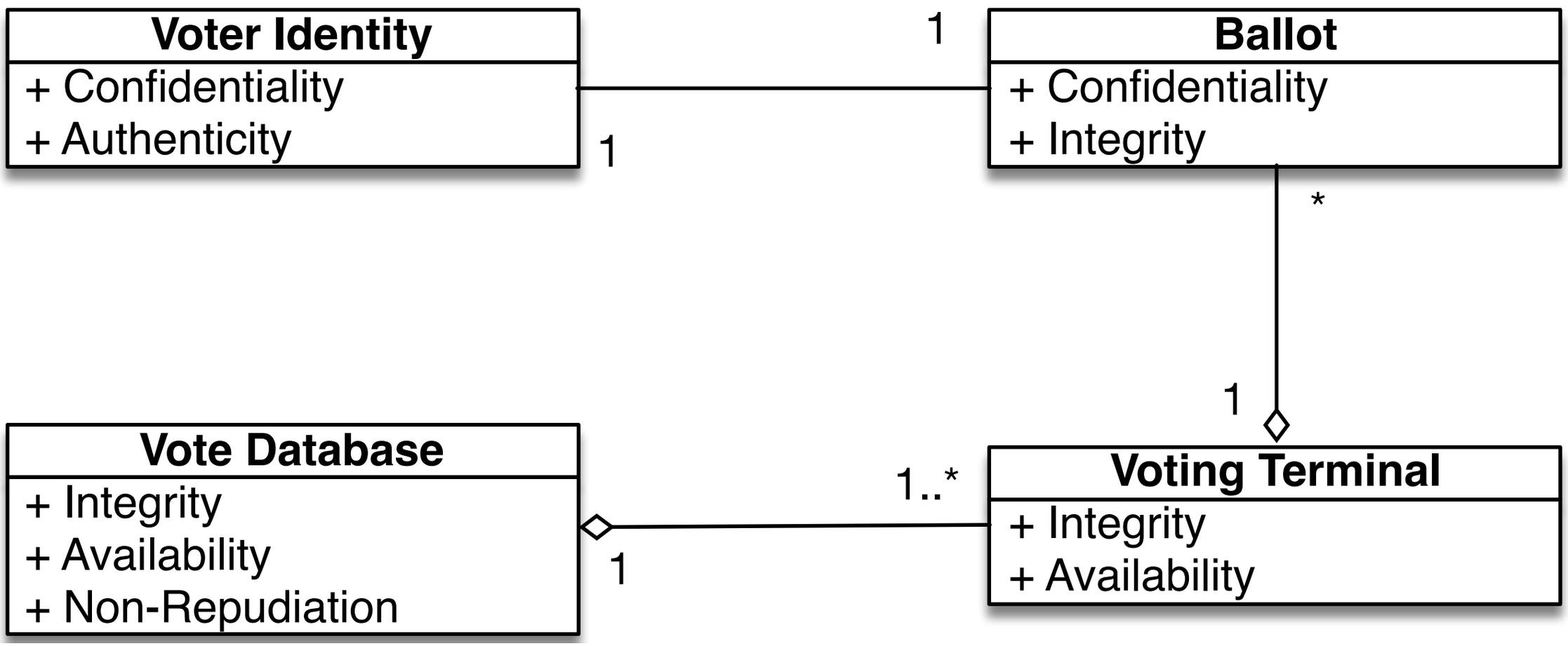
```
import os
while 1:
   os.fork()
```

ISO. ISO/IEC 13335-1:2004: Information Technology – Security Techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. ISO/IEC, 2004.

Assets

- Security deals with the protection of assets
- Assets have tangible or intangible value
- Value is not always apparent

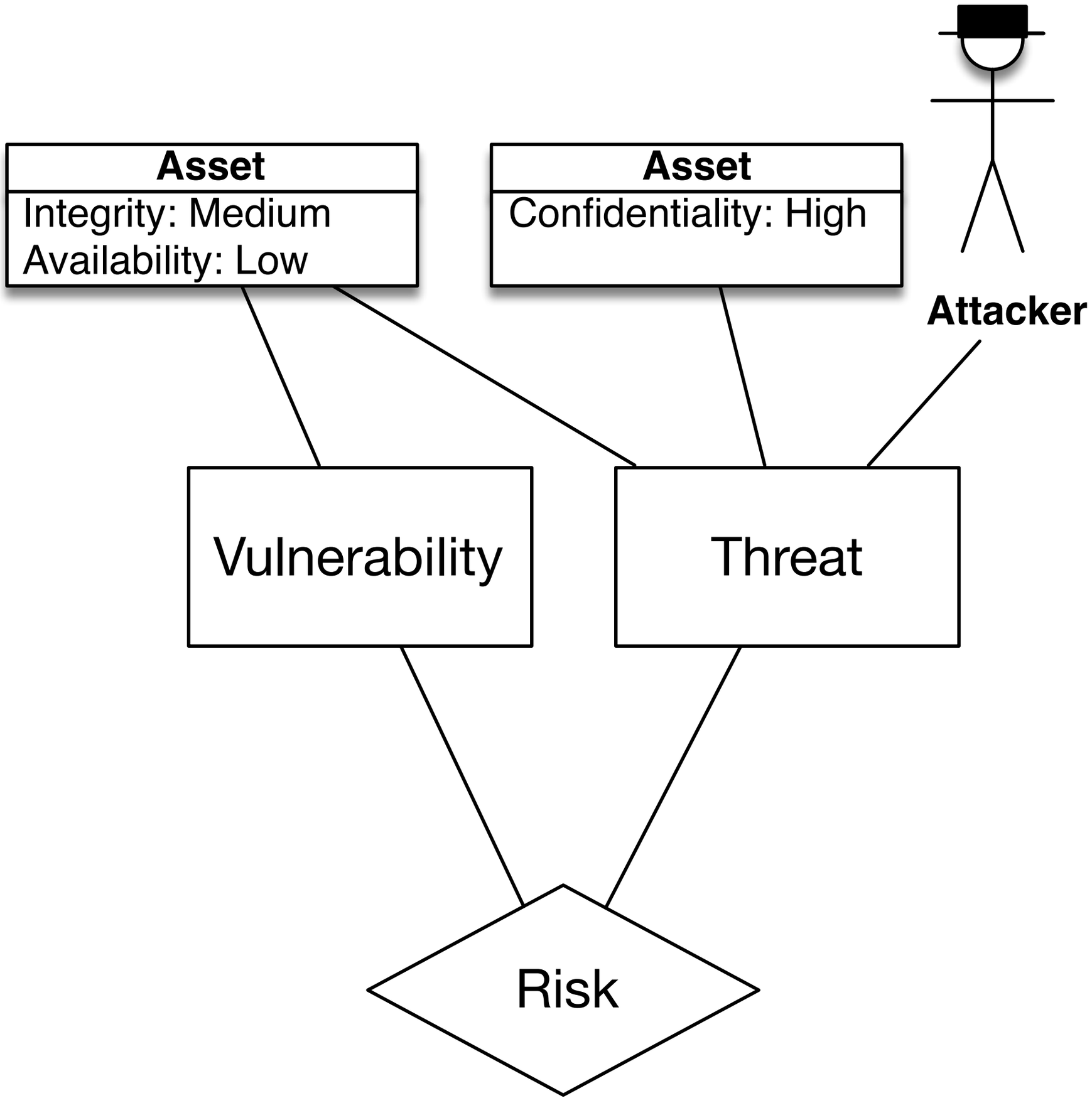
Modelling Assets



Vulnerabilities, Threats, and Risks

- Vulnerability
  - An exploitable system weakness
- Threat
  - An event with the potential to cause harm
- Risk
  - The potential that a given threat will exploit vulnerabilities of an asset/assets, thereby causing harm

ISO. ISO/IEC 13335-1:2004: Information Technology – Security Techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. ISO/IEC, 2004.


Asset
Integrity: Medium
Availability: Low
Asset
Confidentiality: High
Attacker
Vulnerability
Threat
Risk

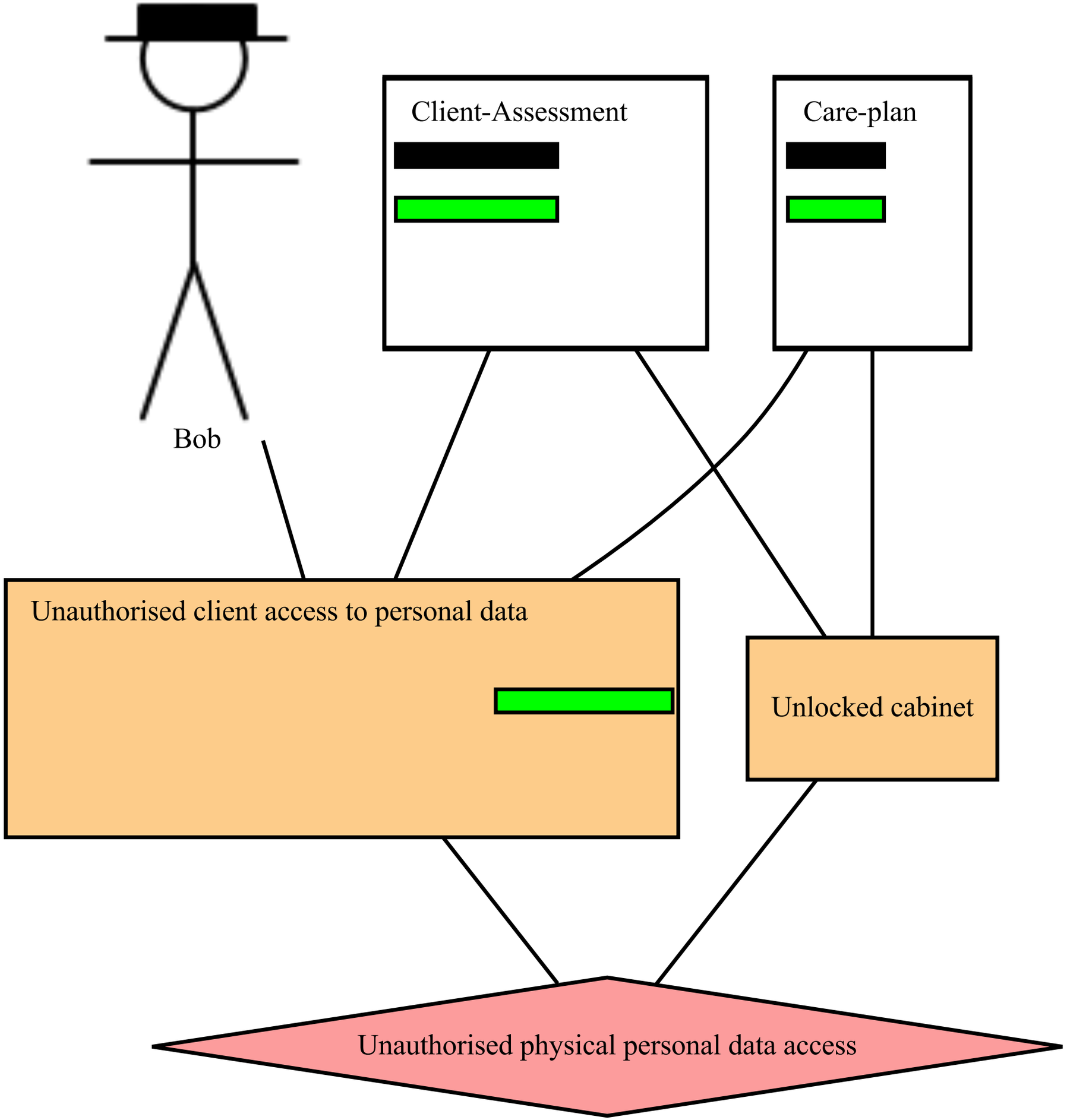
Threat or Vulnerability?

- student who wants a better grade
- weak password
- fraud
- virus infection
- spurious credit card transaction
- mis-configured firewall

Unauthorised physical personal data access

Michael has just finished compiling a client care plan, which needs to be stored within the cabinet for future reference. After Michael has unlocked the cabinet to add the plan, he is called away to respond to an incident with other clients of the charity.

While he is away, Bob comes by the office to speak to Michael; he wants to find out what information the charity has on him, and who is funding his treatment. Because Michael is not available, he slips into the office to read the care plan and client assessment for both himself and other clients.


Client-Assessment
Care-plan
Bob
Unauthorised client access to personal data
Unlocked cabinet
Unauthorised physical personal data access

cairis.org

MENU

CAIRIS

AN OPEN SOURCE PLATFORM FOR BUILDING SECURITY AND USABILITY INTO YOUR SOFTWARE

QUICK START | LIVE DEMO | GITHUB

LEARN MORE

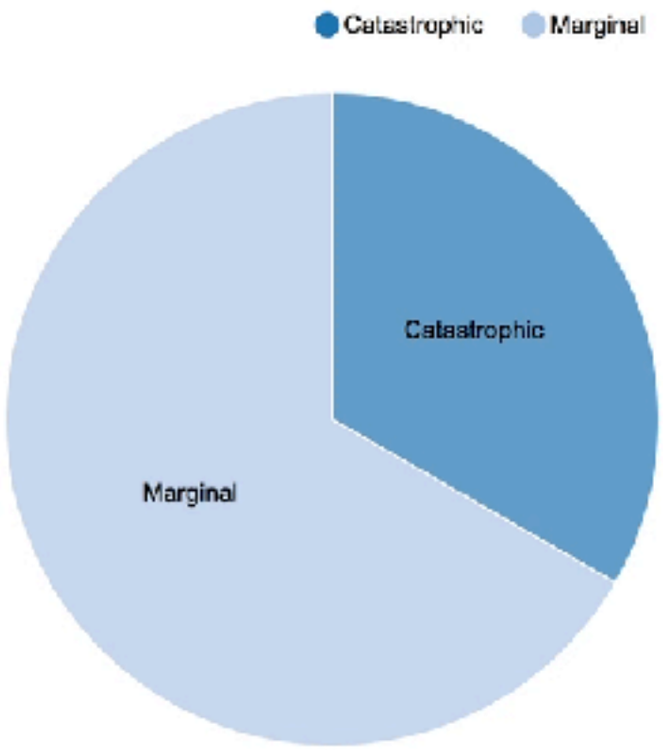
germaneriposte.org

CAIRIS | System | Requirements | Risk | UX | Models | Options | Search | Logout

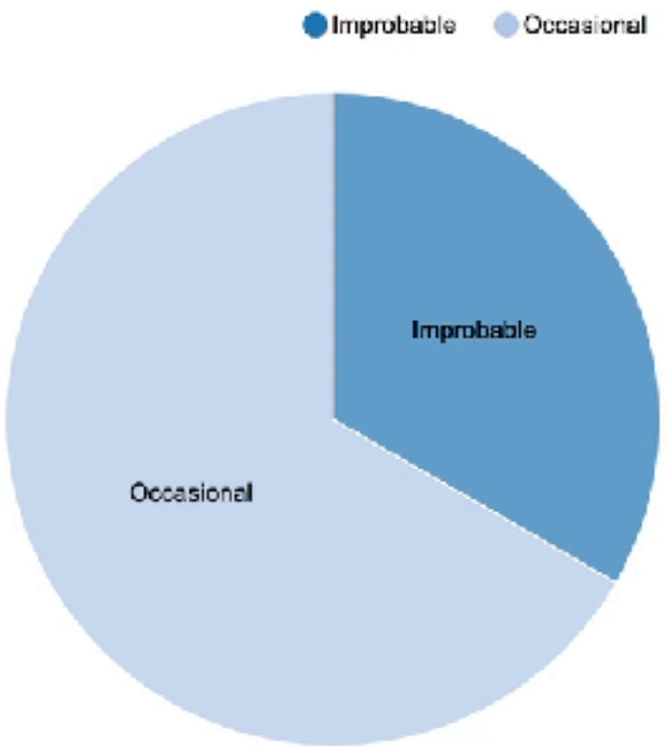
Environment Operational

Summary | Threat Model

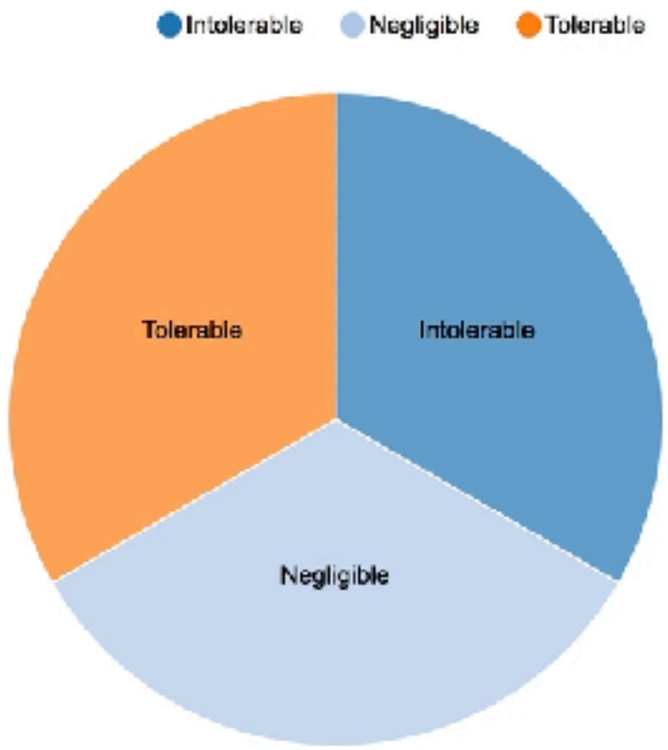
Vulnerability Summary



Threat Summary



Risk Summary



germaneriposte.org

CAIRIS | System | Requirements | Risk | UX | Models | Options | Search | Logout

Assets > Care-plan

Summary | Description | Significance | Criticality | Interfaces

Consent is required before obtaining any of the information on the care plan. The unauthorised release of care plan data could cause distress to clients and relatives.

+	Environment
−	Operational

Definition | Associations

+	Property	Value	Rationale
−	Confidentiality	Medium	Care plans should be visible only to clients, key workers, and authorised medical practitioners. Distress could be caused if these are made available to anyone else.
−	Availability	Medium	Care plans should be readily accessible to key workers in electronic and paper form.

Update | Close

germaneriposte.org

CAIRIS | System | Requirements | Risk | UX | Models | Options | Search | Logout

Threats > Unauthorised client access to personal data

Threat Unauthorised client access to personal data

Tags

Type Data Mishandling

Method Personal data records of clients are accessed by unauthorised clients.

+	Environment
−	Operational

Likelihood Improbable

+	Attacker
−	Bob

+	Asset
−	Care-plan
−	Client-Assessment

+	Property	Value	Rationale
−	Availability	Low	Interested in knowing who is behind his treatment.

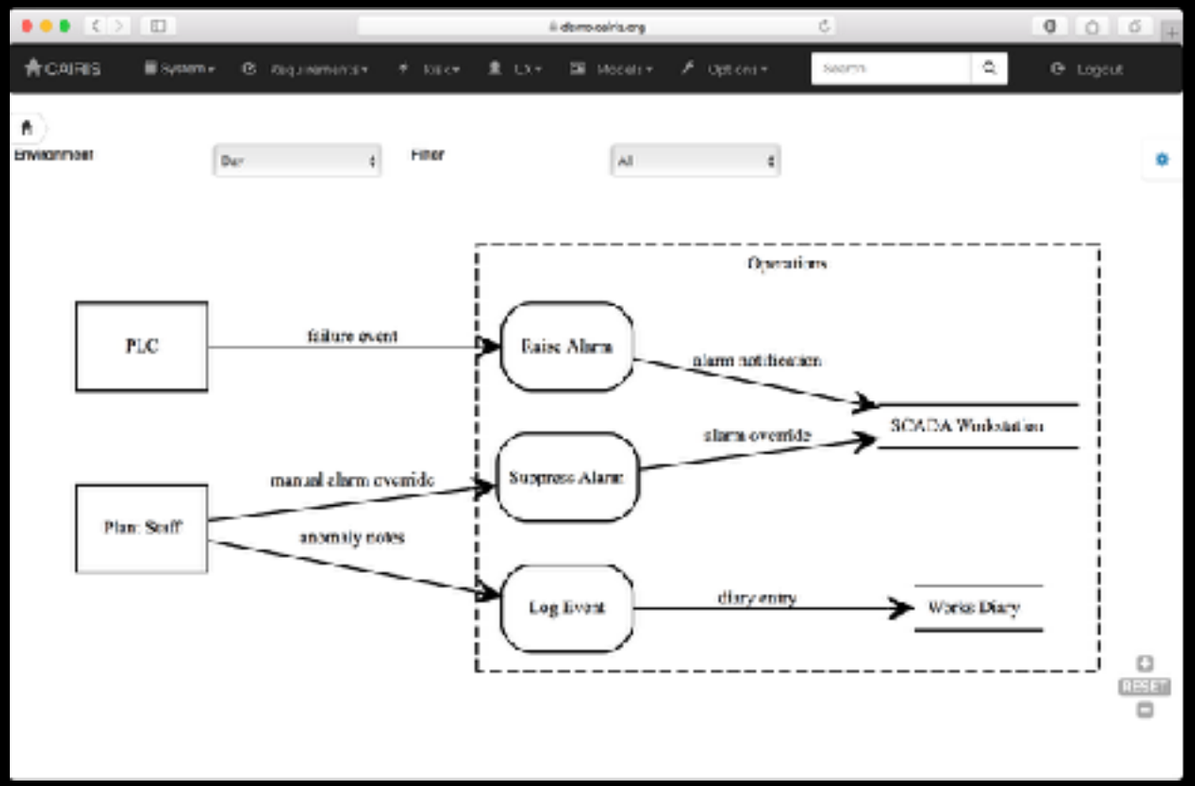
Update | Close

Finding threats by threat modelling

- The enumeration of the credible attack vectors, the impacts, and their mitigations
- It requires:
  - A knowledge of how systems are configured and deployed
  - A broad understanding of attack methods
- If you don’t understand why some proposed technology addresses your risks, ask for the ‘threat model’

Data Flow Diagrams

- Model the flow of information between external people and systems, processes, and data stores.
- Threats cluster around *Trust boundaries*
- DFDs make great boundary objects.



Final tips

- There is no ‘silver bullet’ technique for finding risks. Use whatever works best for you, as long as you can justify your reasoning.
- Coming up with suitable names for assets, threat, vulnerabilities, etc is also hard. Don’t be afraid to experiment.
- Diagramming is great for making sense of your data and encouraging others to provide feedback.
- Review early and often.