# Insider Threats
## *"The enemy within"*

Inveniamviamautfaciam

# “What is it?”

• It is: “Damage done to an organization by a trusted person who has or had access to a trusted area of the organizations infrastructure”

• Facing it is difficult and requires a change in mindset and how things work.

• Ignoring it will not will just make it worse

• It is the most common type of security threat

• Every single type of organization is at risk

• It is not purely technology related

Invenia amvia amautfacia m

# "Explain the Threat"

- Internal threats to an organisation are;
  - *Delete/Remove*
  - *Change/Alter*
  - *Copy/Duplicate*
  - *A combination of the above*

- Assets must be guaranteed in three areas:
  - *Confidentiality*: Secret data must stay secret.
  - *Integrity*: Data must be correct.
  - *Availability*: Data must be available.

- Threats to these three key properties must be protected against.

- These threats are embodied in:
  - *Disgruntled staff*
  - *Coerced/Pressurised Staff*
  - *Planted Staff*
  - *Unintentional damage + Unintentional access*

Inveniamviamaut facciam

# “What exposes me to the threat?”

- *Policies*
  - -In all organizations there is a point at which staff must be trusted.
  - -A lapse here means you have less recourse in enforcement

- *Logical*
  - -Logical controls exist to prevent unauthorised access
  - -Also to create accountability for the actions authorised people undertake
  - -Without proper audit trails, no-one can really say who did what to what
  - -This limits the detection of insider threat and the prosecution thereof.

- *Physical*
  - -A malicious insider has access in order to do work
  - -This is where physical controls come into play
  - -Organizations must know what data is leaving/entering on a physical level
  - -Failure here means, quite literally, that your data can walk out the door.

Inveniamviamautfaciam

# "The insiders"

- *Disgruntled Staff*
  - -Feel they have been wronged in some way
  - -They want to do something to "get their own back".
  - -This threat generally aims at deleting/destruction with no hiding

- *Coerced/Pressurised Staff*
  - -Something outside of work has now placed pressure on the staff
  - -Could be blackmail, debt, bribery, threats, urgent need for money
  - -These people do not want to be noticed

- *Planted Staff*
  - -Generally involved with industrial espionage
  - -Planted staff have all the qualities you want
  - -They will be very careful to not draw attention

- *Unintentional Damage*
  - -There are no no malicious or harmful goals in mind
  - -But they have the ability to perform certain actions
  - -When they make a mistake they end up doing a lot of damage
  - -Expanding internal network so it is externally accessible

Invenia mvia mautfacia m

# “Why should I worry?”

- Do you trust every member of staff 100%, 100% of the time?
- Why do you trust your staff? What have they done to earn that trust?
- Why when you hire a person do you now suddenly trust them?
- Even trustworthy people can do something wrong under stress/pressure
- Someone could unintentionally cause damage due to a lack of controls
- An attacker accessing to your trusted network bypasses most logical defences
- The knowledge and skill required to commit an attack is drastically reduced
- Insider threats are easy and extremely damaging
- Insiders are also familiar with the processes and procedures

Inveniamviamautfaciam

# "What can be done to protect against it?"

- Prevention is ideal but detection is a must.

- Work out an acceptable level of loss

- Access to the organizations resources is what makes insider attacks a threat

- *Education / Awareness*
  - Weakest point is its staff
  - Educate your staff, raise their awareness

- *Defense in Depth*
  - Do not place all its security needs on one system or setup
  - Have multiple levels of security within the organization

- *Backups/Archiving*
  - Recovery and detection must be quick and effective
  - A comprehensive backup plan for critical resources

- *Least Privilege*
  - Anyone should only have the access needed to do their job
  - This means the access to excess resources.
  - Access is very important in any insider threat model and attack

Invenia m via ama u t fac ia m

**Thank you for your attention**

Inveniamviamautfaciam