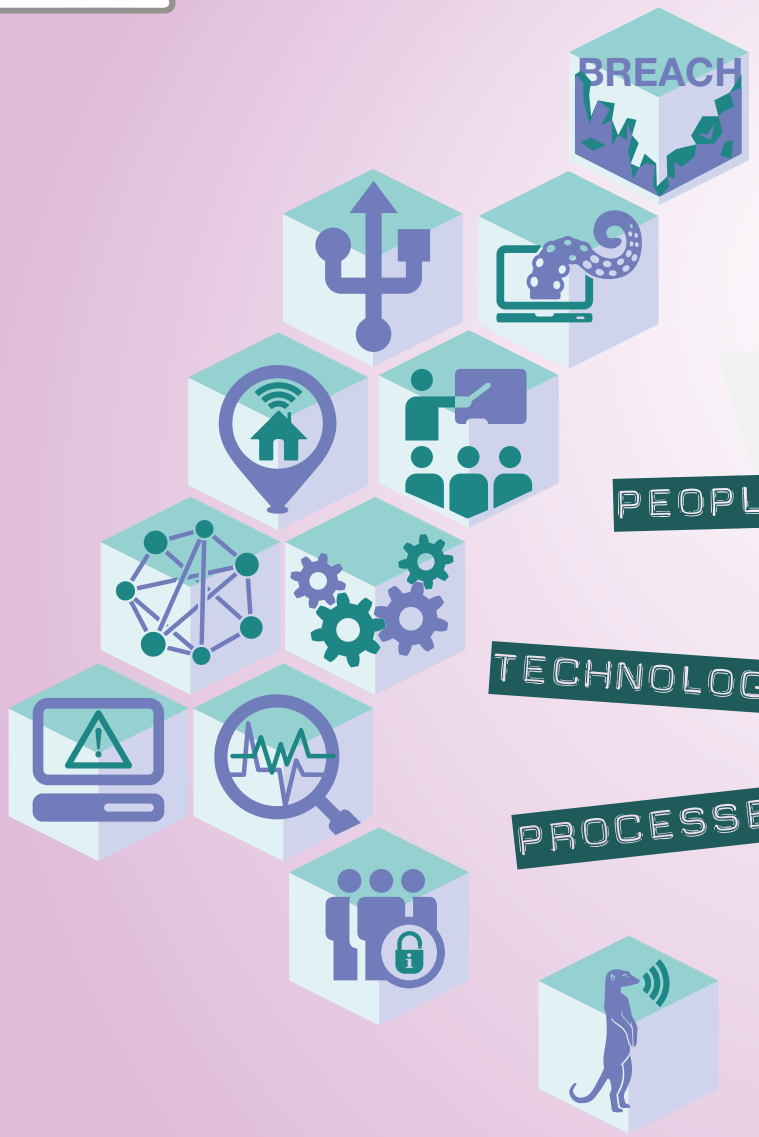
Risk Assessment



Your management will carry out a risk assessment to decide what needs to be done in your workplace to keep the risk of security breaches and data loss low.

Firstly, they'll look at where your organisation might be vulnerable and what the hazards are - these will depend on what your organisation does and on the information it uses.

Risks to the security of information come from three areas – people, technology and processes. Each of these areas needs to be considered in the risk assessment.

People: People in a workplace can be a weak link when it comes to information security. Everyone needs training. It's important that everyone who works in your organisation understands their role in keeping the organisation's information safe, knows what to do and follows proper procedure to make sure that no security breach is their fault.

Technology: As the use of technology increases, so does cyber crime. It's important to establish an overall cyber security strategy which is regularly reviewed.

Processes: Applications, architecture and infrastructure components must be installed and configured correctly. Components must be recorded and monitored and updated when necessary. Security controls and mechanisms must be implemented.

The risk assessment is used to create effective policies and procedures – which ALL employees must know and follow. Good employee awareness is one of the best and most effective ways of preventing security breaches.