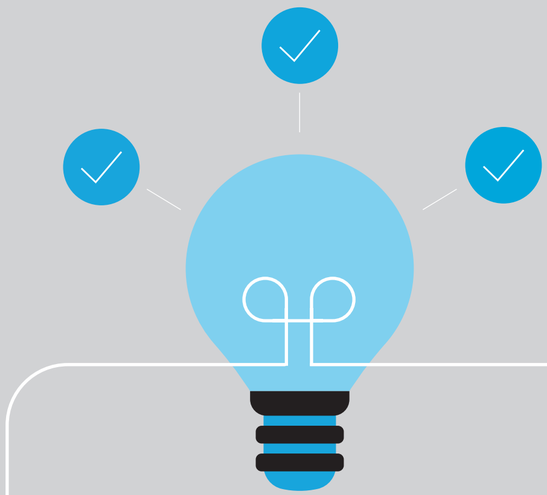
Responding to a cyber-incident

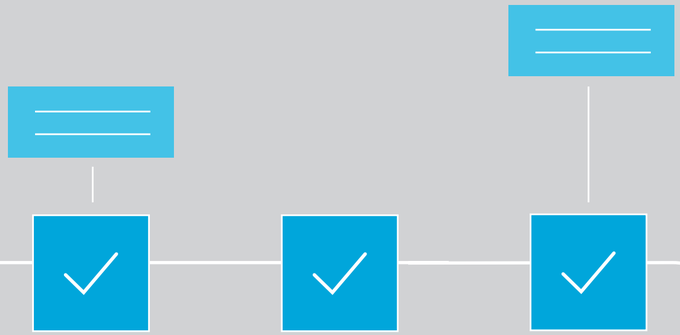


Understand

- Key information assets and where they are stored
- Applicable cybersecurity laws (e.g. GDPR, DPA)
- Likely attack vectors and points of vulnerability

Prepare

- Implement technical and organisational measures to safeguard the business and its assets
- Develop a robust governance framework with clear policies and procedures and assign oversight responsibility



Test, test, test

- Systems and security
- Processes and procedures

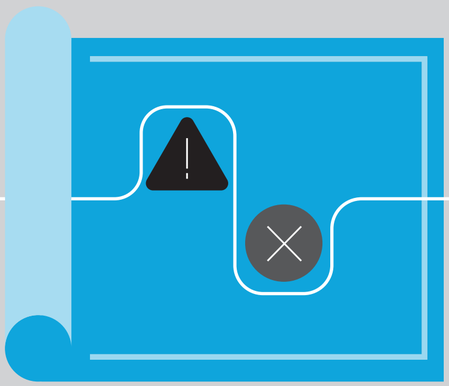
Audit and improve

Investigate incidents and conduct root cause analysis

- Review incident response and identify potential weaknesses
- Implement technical and organisational improvements
- Regularly ensure systems, policies and procedures are fit for purpose and audit for compliance

Communicate

- Agree and execute appropriate strategy with incident response team
- Assess whether to notify regulators, law enforcement, insurers and other third parties
- Communicate with affected individuals, if appropriate



Be proactive and reactive

- Use automated systems to identify incidents and take immediate action
- Prioritise incident response to resolve issues expediently
- Alert incident response team
- Engage other key stakeholders early in the response cycle