# Identify cyber security threats and vulnerabilities

## Overview

This standard covers the competences needed for non-cyber security specialists to contribute towards the cyber security resilience of an organisation. This includes the ability to recognise the cyber security threat landscape and identify the cyber security environments which can threaten business stability.

Effective cyber security resilience occurs when not only cyber security professionals, but also the wider workforce are aware of the threats and vulnerabilities that exist, both within and outside of an organisation - this standard is for individuals whose main work role is not that of a cyber security professional i.e. those who follow, maintain and enhance cyber resilience practices and procedures whilst undertaking their own specialised tasks or functions.

The underpinning knowledge required to meet this standard will provide an understanding of the threats and vulnerabilities that can impact an organisation, an awareness of how they may evolve and their potential impacts.

## Performance criteria

*You must be able to:*

1. Identify the cyber security threats posed to organisations, including the risk to company data in terms of loss of confidentiality, integrity and availability
2. Recognise the common vulnerabilities in digital networks, devices and systems employed within the workplace
3. Determine the forms that social engineering may take and how to respond appropriately
4. Work safely and securely at all times, complying with internal cyber security policies and procedures as well as external regulations and legislation
5. Comply with organisational requirements regarding good online behaviour in areas such as; un-verified links, open wireless networks and social networking sites

## Knowledge and understanding

*You need to know and understand:*

1. That cyber security threats may occur as attack events that negatively impact the availability, integrity or confidentiality of IT systems and associated data
2. The importance of threat intelligence and threat modelling to protecting organisational security
3. The nature and characteristics of threats and vulnerabilities
4. How viruses spread in an organisation and attack a digital network
5. The social engineering threats to organisations, the techniques applied by social engineers, how this can lead to a breach in security and how to respond to them
6. The vulnerabilities of a system that may be open to threat actors, including people, devices, networks and databases
7. How the security implications of cloud computing relate to the increased exposure of data resulting from this form of shared data storage and access
8. That unsafe network activities relate to the behaviours that individuals can engage in that may compromise network security, including: sharing passwords with co-workers, installing unauthorised software, failing to encrypt sensitive communications and disabling security software
9. How vulnerabilities can be identified
10. The potential impact of cyber security threats being realised

# Identify cyber security threats and vulnerabilities

| | |
|---|---|
| **Developed by** | ODAG |
| **Version Number** | 1 |
| **Date Approved** | March 2020 |
| **Indicative Review Date** | March 2023 |
| **Validity** | Current |
| **Status** | Original |
| **Originating Organisation** | ODAG Consultants Ltd |
| **Original URN** | TECIS60021 |
| **Relevant Occupations** | ICT for users |
| **Suite** | IT Users |
| **Keywords** | Information security, cyber security |