TECIS600201

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 identify the cyber security threat landscape and recognise the vulnerabilities that allow cyber security breaches to occur which can threaten business stability. This includes the risk to business of compromises to the availability, integrity, confidentiality, authenticity and non-repudiation of business systems and associated data.

Effective cyber security resilience best 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 and is aimed at those whose main role would be enhanced through developing knowledge, understanding and skills in cyber security threats and vulnerabilities. Increasingly cyber security responsibilities are becoming embedded in a wide range of job roles across all sectors.

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 main cyber security threats posed to organisations to clearly demonstrate risk 2. evaluate the potential business risk of different cyber security threats to an organisation's data in terms of loss of confidentiality, integrity and availability 3. classify the common vulnerabilities that occur in computer networks, devices and systems 4. identify the different forms that social engineering can take and respond to these appropriately 5. work safely and securely at all times, complying with internal cyber security policies and procedures, external regulations and legislation 6. comply with organisational requirements regarding safe online behaviour when presented with un-verified links, open wireless networks and social networking sites

Knowledge and understanding

You need to know and understand:

1. how the availability, integrity, confidentiality, authenticity and non-repudiation of data can be impacted as a result of a cyber security attack 2. the sources of threats and how they are identified and monitored 3. the potential impact and consequences of cyber security threats 4. the vulnerabilities of a system that may be open to threat actors, including people, devices, networks and databases 5. how cyber security threats can lead to business risk and service disruption 6. the process of threat analysis and how this is managed 7. the role of threat intelligence and threat modelling to protecting organisational security 8. the need for verification of identity when performing certain data manipulation and financial transactions 9. how malware can spread in an organisation and attack a computer network 10. the social engineering threats to organisations, the techniques applied by social engineers, and how this can lead to a breach in security 11. the business risks and security implications of cloud computing arising from the increased exposure of data through shared data storage and access 12. industry standard risk frameworks and how to apply them 13. the range of unsafe behaviours that individuals can engage in that may compromise computer security (including: disclosing passwords, installing unauthorised software, failing to encrypt sensitive communications and disabling security software)

TECIS600201

Identify cyber security threats and vulnerabilities

Developed by	e-skills
Version Number	1
Date Approved	29 Apr 2020
Indicative Review Date	30 Mar 2023
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd
Original URN	TECIS600201
Relevant Occupations	ICT for Users
Suite	IT(Cyber Security)
Keywords	Information security, cyber security