TECIS60023

Respond to and recover from cyber security attack

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 respond to and recover from cyber security attacks by following organisational policies and procedures.

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 cyber security controls, tools and techniques needed in order to defend against threats.

Performance criteria

You must be able to:

1. Identify unauthorised access, or attempted access, to a system that breaches the system's security policy in order to affect its integrity or availability
2. Recognise the symptoms of a cyber security attack and how to escalate these in line with organisational procedures
3. Carry out appropriate tasks and responses to a cyber security attack in line with defined responsibilities and organisational policies and procedures
4. Recognise and report security breaches in a timely manner following organisational incident response management procedures
5. Document all stages of a response in order to evaluate whether the response was appropriate and effective
6. Confirm system and data integrity following a cyber security attack and disaster recovery action

Knowledge and understanding

You need to know and understand:

1. That the organisation's systems, networks and data are continually monitored and any identified anomalies and weaknesses should be acted upon
2. That the objective of cyber security resilience is to maintain the organisation's ability to deliver services and intended outcomes despite adverse cyber events
3. The consequences of different types of attack e.g. a ransomware attack and a denial of service attack have different consequences for employees and organisations
4. Digital services and data are designed to be resilient in the event of disaster and can be recovered within timescales agreed with senior management
5. That symptoms of cyber security attack include (but not be limited to): fake anti-virus messages, unwanted browser toolbars, redirected internet searches, frequent random pop-ups, fake e-mails or messages originating from an account, online password changes, unexpected software installations, unexplained mouse movements, anti-virus or anti-malware disablement and curtailment, loss of or corrupted data, unexplained withdrawals from bank accounts
6. The importance of reporting cyber security incidents in an organisation by appropriate means, including and notifying authorised staff of suspicious activity
7. The steps involved in responding to a cyber security attack
8. The organisational policies and procedures to enable the recovery or continuation of vital technology infrastructure, systems and data following a cyber security event (as well as natural or human-induced disasters)
9. That disaster recovery is part of business continuity and should be invoked after a cyber security attack to ensure all critical business functions are operational
10. The importance of backup and recovery in disaster recovery
11. The defined roles and responsibilities of authorised staff and the wider workforce for quickly discovering an incident and effectively containing the damage, eradicating the threat, and restoring the integrity of affected network and systems

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	TECIS60023
Relevant Occupations	ICT for users
Suite	IT Users
Keywords	Information security, cyber security