TECIS60652

Manage information security incident investigation and management activities

Overview

When information security incidents occur, organisations must respond quickly and effectively to protect themselves from attack and limit the damage and scope of attacks. In order to do this they need to establish incident response teams and define the policies and standards relating to developing, operating, and improving incident management capabilities.

This standard defines the competencies associated with developing the standards for detecting, investigating and managing security incidents and providing a full security investigation and management capability.

Performance criteria

You must be able to:

1. define and implement the policies, standards and procedures for detecting, investigating and managing information security incidents
2. lead the incident investigation and management team in line with organisational standards
3. manage the resourcing, training and development needs of the information security incident investigation and management team in line with organisational requirements
4. manage the response plans to information security incidents including producing the final report in line with organisational standards
5. coordinate the root cause analysis of incidents in line with organisational standards
6. assess the need for digital forensic activity, and escalate incidents to digital forensic teams as required
7. prepare incident reports and communicate with stakeholders to ensure all immediate risks are addressed
8. provide accurate updates on the status of information security incidents
9. undertake exercises to test, verify and improve information security incident response performance and update policies and procedures as required
10. communicate the ongoing capability of the incident investigation and management team in line with organisational requirements

Knowledge and understanding

You need to know and understand:

1. how to lead a team conducting information security incident investigations to identify and analyse incident information
2. how to conduct all phases of information security incident response and management
3. how to assess the capability of the information security incident response team
4. how to develop the policies and standard required for information security incident investigation and management
5. how to determine the scope of a potential security breach through incident investigation techniques
6. how to co-ordinating root cause analysis of information security incidents
7. how to report and present the findings of information security incident investigation to sponsors and stakeholders
8. that rapid response processes need to be followed for information security incidents
9. how to create and execute information security incident tests with increasing sophistication across all critical information systems to verify incident response performance
10. the importance of building strong relationships both internally and externally as part of the information security incident response team
11. the need to identify sources of information security incident investigation and management best practice and how to exploit these

TECIS60652

Manage information security incident investigation and management activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60652
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, incident management, incident investigation