TECIS60632

Contribute to 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 contributing to analysing and evaluating of events of interest that may become incidents and escalating these to incident management teams as appropriate.

Performance criteria

You must be able to:

1. provide an initial response to reported information security incidents, in line with organisational standards
2. escalate information security issues to senior investigators in line with organisational incident escalation criteria
3. assist with interviews, information system analysis, documentation reviews and analysing protective monitoring systems during information security incident investigations
4. correctly follow the organisational procedures and standards relating to information security incident management activities
5. apply information security incident management tools in line with organisational standards
6. operate with integrity and confidentiality during information security incident investigation activities in line with organisational standards
7. seek appropriate advice and guidance as required during information security incident investigation activities
8. identify the need for detailed forensic examination as part of an information security incident investigation
9. document and report all findings from information security incident investigations in line with organisational standards

Knowledge and understanding

You need to know and understand:

1. what is meant by an information security incident
2. what is the purpose of incident management and its role within information security
3. when to call for detailed forensic examination as part of an investigation
4. how to report a security incident within their own work area
5. how the scale of an information security incident can impact the business and can instigate a business continuity response
6. how to record and preserve evidence such that it may be used to support formal proceedings
7. the main stages of incident management; e.g. identify, contain, cleanse, recovery, close
8. the processes, procedures, methods, tools and techniques relating to information security incident management activities and their deliverables
9. the external legislation and regulations, internal policies and internal and external standards that are relevant to information security incident management activities
10. the potential business impacts of security incidents upon
11. the need for confidentiality, Integrity, Availability and reputation in their area of work
12. how security incident management can mitigate the consequences of security incidents
13. the need to preserve evidence to support formal proceedings
14. the need for incident management activities to be carried out in accordance with any codes of conduct and organisational standards

TECIS60632

Contribute to 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	TECIS60632
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