Module Specification

Cyber Security Incident Management and Professionalism

Version: 2024-25, v1.0, 04 Feb 2022

Contents

Part 1: Information

Module title: Cyber Security Incident Management and Professionalism

Module code: UFCFNU-20-3

Level: Level 6

For implementation from: 2024-25

UWE credit rating: 20

ECTS credit rating: 10

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: None

Delivery locations: Gloucester Campus

Field:

Module type:

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Managing security incidents requires a rigorous approach and may have to be performed in real time. There are defined processes with key stages:

•Writing a plan

•Training

•Defining roles and responsibilities

•Establishing and testing a data recovery plan

•Identifying potential security incidents through monitoring and report all incidents.
•Assessing identified incidents to determine the appropriate next steps for mitigating the risk.
•Responding to the incident by containing, investigating, and resolving it
•Complying with legal and regulatory requirements
•Learning and documenting lessons
Students will be instructed and practice incident management. This includes the professional, legal and ethical responsibilities in dealing with an incident. Therefore this module requires apprentices to research and investigate the legal, ethical and regulatory requirements

Features: Not applicable

Educational aims: This module contributes to coverage of the professional, ethical and legal aspects of cyber security management.

Outline syllabus: You will cover:
•network monitoring and logging techniques and technologies
•how attack techniques and vulnerabilities manifest in network monitoring and logging systems
oe.g., analysis of a network log or the output of a network monitoring tool may reveal the likely means of an attack
•the relative merits of manual and automated techniques
•the relative merits of signature-based anomaly detection and algorithmic anomaly detection
•how statistical techniques might be applied in support of analysis of cyber security incidents
•integration and correlation of information from various sources
•cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation
•how to communicate with incident response team/process and/or customer or other external authority incident response team/process for incidents
•key features of the main laws applicable to England that are relevant to cyber security issues including legal requirements that affect individuals and organisations, e.g.:
oComputer Misuse Act, Data Protection Act, GDPR, Human Rights Act.

•the cyber security standards and regulations and their consequences for at least 2 sectors, e.g.:

ogovernment, finance, telecommunications, petrochemical/process control, critical infrastructure

ocompare and contrast the differences

•the implications of international laws and regulations that affect organisations, systems and users in the UK, movement of data and equipment across international borders and between jurisdictions, e.g.:

oDigital Millennium Act, ITAR, Safe Harbour

•legal issues relevant to cryptography, e.g.:

oUK, EU and US export control of cryptography, the Wassenaar Arrangement

•benefits and costs and the main motives for uptake of significant security standards such as:

oCommon Criteria, PCI-DSS, FIPS-140-2, Government (e.g. UK NCSC, cyber essentials) schemes

•applicability of laws and regulations to security testing of 3rd parties (‘ethical hacking’, ‘pen testing’)

•ethical responsibilities of a cyber security professional

•applicability of laws and regulation to intelligence collection and analysis, and the relationship to data protection, human rights and privacy

•the legal responsibilities of system users and how these are communicated effectively

•laws and regulations applicable to cyber security, personal and sensitive data, employee protection and monitoring, relevant to England and one other non-UK jurisdiction (eg USA - HIPAA)

oshould encompass what is prohibited (i.e., an offence), protections, legal risks and obligations

•social context

•analytical tools

•professional ethics

•intellectual property

•privacy

•professional communication

•sustainability

Part 3: Teaching and learning methods

Teaching and learning methods: This module pulls together many of many of the strands of Cyber Security previously studied. Where necessary, lectures will provide underpinning knowledge.

Students will work in groups an isolation chamber to manage a cyber security incident from detection through to the completion of the incident management documentation.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Work in a novel situation to detect and manage real security incidents, the response and all communications, including within the team and with 3rd parties.

MO2 Synthesise knowledge in order to organise testing & investigation work in accordance with legal & ethical requirements, identify and raise non-compliance issues.

MO3 Work within an employment team to develop & apply information security policy to implement legal or regulatory requirements.

Hours to be allocated: 200

Contact hours:

Independent study/self-guided study = 90 hours

Placement = 50 hours

Face-to-face learning = 60 hours

Total = 200

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/FA02EF10-151C-8740-1E45-AAA3D8A6CC63.html

Part 4: Assessment

Assessment strategy: Assessment of this module consists of two tasks. In the first, the students gain experience of managing a security incidence and they work in a group to manage and respond to a cyber security event. As they work through the incident, the group is expected to document their process and the communications both within the team and with 3rd parties. The group is assessed on the this documentation. The intention here is that the work closely mirrors that which would be carried out in a real situation.

In the second piece of work, the student is encouraged to consider their workplace cyber-readiness by taking what they have learned and applying to to their workplace. The student works individually on a report on their workplace security policies, identifying any shortfalls particularly in the area of legal and regulatory compliance.

At resit, students will be given a new incident which they will work on individually.

Assessment components:

Report - Component B (First Sit)
Description: Individual report on security policies within a given organisation.
Weighting: 40 %
Final assessment: No
Group work: No
Learning outcomes tested: MO2, MO3

Portfolio - Component A (First Sit)
Description: Portfolio documenting the process pursued and the communications that have taken place in managing a security incident.
Weighting: 60 %
Final assessment: Yes
Group work: Yes
Learning outcomes tested: MO1, MO2

Report - Component B (Resit)

Description: Reworked report

Weighting: 40 %

Final assessment: No

Group work: No

Learning outcomes tested: MO2, MO3

Portfolio - Component A (Resit)

Description: Reworked portfolio and demonsration

Weighting: 60 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [Sep][FT][GlosColl][3yrs] BSc (Hons) 2022-23

Cyber Security Technical Professional {Apprenticeship-GLOSCOLL} [GlosColl] BSc (Hons) 2022-23