# MODULE SPECIFICATION

| Part 1: Information | | | |
|---|---|---|---|
| Module Title | Practical Security | | |
| Module Code | UFCFBN-30-3 | Level | Level 6 |
| For implementation from | 2020-21 | | |
| UWE Credit Rating | 30 | ECTS Credit Rating | 15 |
| Faculty | Faculty of Environment & Technology | Field | Computer Science and Creative Technologies |
| Department | FET Dept of Computer Sci & Creative Tech | | |
| Module type: | Standard | | |
| Pre-requisites | None | | |
| Excluded Combinations | None | | |
| Co- requisites | None | | |
| Module Entry requirements | None | | |

**Part 2: Description**

**Overview**: This module will cover the implementation, maintenance and support of the security controls that protect an organisation's systems and data assets from threats and hazards. It gives consideration to current security technologies and practices and their governance in relation to organisational policies and standards to provide continued protection. Broadly speaking, it covers material relevant to the role of a cyber security analyst including understanding network infrastructure, software and data to identify where threat and hazard can occur, periodic vulnerability assessments, security incidents response and resolution.

**Educational Aims:** This unit will apply a range of teaching techniques using both research and practical activities to reinforce the understanding of cyber security within a business or organisation.

**Outline Syllabus:** Common attack techniques (e.g. phishing, social engineering, malware, network interception, blended techniques, denial of service and theft) and how to how to mitigate them

Perform a risk assessment

Analyse and perform a penetration testing suggesting different ways to treat risk and apply management

strategies

Cyber security culture (e.g. positive and negative impacts)

Security threats and vulnerabilities to planned and installed information systems or services (e.g. risk assessment, mitigation, remediation)

Security case against recognised security threats, and recommend mitigation, security controls and appropriate processes

User access policy for an information system for a business' system (e.g. user privileges, access accounts)

Business impact analysis in response to a security incident and follow a disaster recovery plan to meet elements of a business continuity policy

Cyber security audit activities, demonstrating security control effectiveness

Organisational security policies and standards to implement security processes in line with policies and standards

Security requirements for a business (e.g. including functional and non-functional security requirements)

The types of security (e.g. confidentiality, authentication, non-repudiation, service integrity)

Security big picture (network security, host OS security, physical security)

Analysis of network domain

Identification of information's assets

**Teaching and Learning Methods:** Introductory lectures are supported by seminars, case studies, visits and practical workshops. In addition this module will be supported by interactive forums and learning tools.

Independent learning includes hours engaged with essential reading, case study preparation, assignment preparation and completion.
Study time will be organised each week with a series of both essential and further readings and preparation for practical workshops.

Scheduled learning will typically include lectures, seminars, supervision, external visits and an interactive forum.

All students are expected to attend a series of tutorials.

| **Part 3: Assessment** |
| --- |
| This module is assessed by a combination of techniques: Presentation (30 Minutes) and a 3,000 word report.<br><br>Component A – Presentation<br>Students will be required to present a 30-minute presentation that will require knowledge of the common types of attacks that could take place on any given system and the impacts these could cause both financially and socially. They will need to be able to identify and assess the risk to a system and create a full risk assessment based on a system network. This also involves areas such as physical security and organisational security.<br><br>Students will need to be able to identify how to apply penetration to a system and recognise the benefits and the results that it can bring. They will also need to be able to explain how penetration testing helps to provide information assurance. |

Students should be able to evaluate the cyber security culture in a business and understand how this could be a positive or negative culture depending on how it is implemented within a business.

Component B – Written Report and Practical Elements (3000 Words)
Students will be required to analyse and evaluate any security threats and vulnerabilities to planned and installed information on a current system. They should also be able to analyse both functional and non-functional security requirements. Through this evaluation, identification of how these risks will be stopped and mitigated through a risk assessment. The risk assessment should be able to lead on to what controls should be implemented into a system and the impact this will have.

Students will need to be able to create a user access policy that will take into account current standards (e.g. ISO27001, Cyber security essentials) to identify where access should be allowed and the risks that could be associated with the allocation of these rights.

Students will need to perform an impact analysis on a business network and follow a disaster recovery plan to ensure a business can continue normal operations. During this process, they will need to ensure that new and existing policies are applied to the network to ensure it is operating under the correct policies.

Students will be required to perform a range of cyber security audits to systems and analyse the networks effectiveness, making recommendations of where improvements could be made if required and showing how current security protocols ensure information assurance.

Opportunities for formative assessment exist for the assessment strategy used. Verbal feedback and written feedback is given to all students providing a personal platform for improvement.

| First Sit Components | **Final Assessment** | **Element weighting** | **Description** |
|---|---|---|---|
| Presentation - Component A | ✓ | 50 % | Oral Assessment (30 Minutes) |
| Report - Component B | | 50 % | Written Report (3000 Words) |
| **Resit Components** | **Final Assessment** | **Element weighting** | **Description** |
| Presentation - Component A | ✓ | 50 % | Oral assessment (30 minutes) |
| Report - Component B | | 50 % | Written report (3000 words) |

**Part 4: Teaching and Learning Methods**

Learning Outcomes

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

| **Module Learning Outcomes** | **Reference** |
|---|---|
| Identify and demonstrate a critical understanding of the types of security and the security big picture. | MO1 |
| Identify the main types of common attack techniques. | MO2 |
| Recognise and assess risk including performing a risk assessment. | MO3 |
| Apply and justify penetration testing techniques effectively and understand how it contributes to assurance. | MO4 |
| Identify, justify and apply different approaches to risk treatment and management in practice. | MO5 |
| Critically appraise the importance of ‘cyber security culture’ in an organisation, and how it may contribute to security risk. | MO6 |

| | | |
|---|---|---|
| | Analyse and evaluate security threats and vulnerabilities to planned and installed information systems or services and identify how these can be mitigated. | MO8 |
| | Perform security risk assessments for a range of information systems and propose solutions. | MO9 |
| | Develop a security case against recognised security threats, and recommend mitigation, security controls and appropriate processes. | MO10 |
| | Define and justify a user access policy for an information system given knowledge of the system architecture, security requirements and threat/risk environment. | MO11 |
| | Perform a business impact analysis in response to a security incident and follow a disaster recovery plan to meet elements of a given business continuity policy. | MO12 |
| | Conduct a range of cyber security audit activities to demonstrate security control effectiveness. | MO13 |
| | Research and investigate common and emerging attack techniques and recommend how to defend against them. | MO14 |
| | Identify and follow organisational security policies and standards and implement security processes in line with policies and standards. | MO15 |
| | Analyse security requirements including functional and non-functional security requirements that may be presented in a security case. | MO16 |

| | | |
|---|---|---|
| Contact Hours | **Independent Study Hours:** | |
| | Independent study/self-guided study | 228 |
| | **Total Independent Study Hours:** | 228 |
| | **Scheduled Learning and Teaching Hours:** | |
| | Face-to-face learning | 72 |
| | **Total Scheduled Learning and Teaching Hours:** | 72 |
| | **Hours to be allocated** | 300 |
| | **Allocated Hours** | 300 |
| Reading List | *The reading list for this module can be accessed via the following link:*<br><br>https://rl.talis.com/3/uwe/lists/816B7A89-D61D-2FE2-D676-D63D33CA1EBD.html | |

| **Part 5: Contributes Towards** |
|---|
| This module contributes towards the following programmes of study: |