| | |
|---|---|
| **Unit Title** | Cyber Security for Creative Industries (blended) |
| **FHEQ Level** | Level 5 |
| **Unit Code** | ECLC20202 |
| **Credit Value** | 15 |
| **Unit Type** | Elective |

| **Learning Hours (Blended)** | | | |
|---|---|---|---|
| **Staff – Student Contact Hours** | | **Independent Study Hours** | |
| Classes | 37.5 | Independent study | 80 |
| Supervised access to Ravensbourne resources | | Preparation for assessment | 32.5 |
| **Total** | | 150 | |

## Unit Description

Creative industries heavily rely on computing devices, computer-based networks, cloud computing, cloud storage and equipment which is normally connected with the internet. This leaves them exposed to cyber threats resulting in potential data loss or network disruptions. The computing devices maybe protected directly by the IT department but Operational Technology (OT) at times is overlooked for potential threats. Broadcasting in particular is regarded as part of the critical infrastructure of any country and its protection requires multi-layered and multi-disciplinary approach.

This unit is designed to provide you with basic understanding and knowledge about potential cyber security risks, how to mitigate and minimize them and what could be remedial actions.

Most of the production, storage and distribution, graphics, animation and game development work, alongside video recording, editing and streaming are all performed on digital devices which are prone to cyber-attacks hence it is essential for all users to learn about cyber security fundamentals.

Effective protection of content and digital assets relies on various techniques and a range of standards which are developed by the industry along with regular recommendations.

Cyber Security needs to be considered at every stage of digital deployment. From analysing user requirements, development of software and deployment of databases up to the connectivity with the internet and cloud, every element of the communication and storage should be secured from hackers.

The Five Principles underpin the Mindsets and Skillsets Manifesto and are the foundation upon which all course curriculum frameworks and unit specifications are based. The relevant Principles as stated below have been mapped against the Learning Outcomes relevant to each course unit and at each level (see Programme Specifications for full

description of the Five Principles):

1. Cultivate / Where the individual thrives.
2. Collaborate / Where disciplines evolve.
3. Integrate / Where education engages industry.
4. Advocate / Where purpose meets practice.
5. Originate / creativity meets technology.

## Unit Indicative Content

### Cyber Security

### Industry-wide Knowledge

- Risk assessment and regulations
- Impact of cybercrime
- Information and Cyber Security
- Network Security Protocols
- Attack types and vectors
- Policies and Procedures
- Penetration Testing
- Malware & Attack Technologies
- Block Chain
- Operating System Security
- Forensics
- Hardware and Software Security
- Network Security
- Possible security measures
- Password policies
- Physical Security
- Anti-Virus, Firewalls

### CyBOK knowledge areas

- Malware & Attack Technologies

## Unit Aims

1. To examine Cyber Security principles, protocols and standards

2. To evaluate potential risks throughout the work flow (hardware, network and content) including mobile and cloud technologies.
3. To identify various authentication methods and apply them to secure systems
4. To conduct a risk assessment of the environment and outline phases of incident response
5. To evaluate current Malware and attack technologies and suggest preventive measures
6. To be able to evaluate the importance of policies, procedures and compliance .

## Unit Learning Outcomes

LO 1 Research/Inspiration

Analyse and interpret information gathering techniques using a wide range of sources, providing visual, contextual and industry case-study research as appropriate.

Related Principle: ORIGINATE

LO 5 Presentation /Storytelling for Influence
Select and employ effective methods of presentation and communication of projects in considering the audience/client and the purpose of the work, whether in visual, oral or written form.

Related Principle: ADVOCATE

LO 6 Critical and creative mindsets Analyse conceptions of diverse practice and use this to inform a course of action
Related Principle: ORIGINATE

## Learning and Teaching Methods

This unit will be delivered using a combination of:

- Lectures / Seminars
- Online activities
- Self-directed independent study
- Peer learning, group discussion, guest speakers

| Assessment methods and tasks | |
|---|---|
| **Assessment tasks** | **Weighting (%)** *(one grade or multi-grade unit)* |
| Portfolio | 60% |
| Group poster presentation | 40% |

## Indicative Assessment Criteria

Identify potential risks associated with your personal and professional work. (LO1)

Identify various authentication methods and apply them to secure systems (Lo1)

**For a given case study or scenario:**

Evaluate potential risks throughout the work flow (hardware, network and content) including mobile and cloud technologies. (LO6)

Conduct a risk assessment of the environment and outline phases of incident response (LO6)

Evaluate current Malware and attack technologies and suggest preventive measures (LO5)

Critically evaluate the role of a security policies, compliance and regulations for protecting information assets. (LO5)

## Essential Reading list

The Cyber Security Body of Knowledge. (2019). 1st ed. The National Cyber Security Centre.

Easttom, C. (2016). Computer Security Fundamentals, Third Edition. 3rd ed. Pearson.

**Recommended Reading List**

Taylor, Andy, et al. Information Security Management Principles. BCS, 2013.

Beasley, J. and Nilkaew, P. (2018). Networking essentials. Pearson. (ISBN 9780789758743)

Meyers, M. and Weissman, J. (2018). Mike Meyers CompTIA Network+ Guide to Managing and Troubleshooting Networks Lab Manual, Fifth Edition (Exam N10-007). ßMcGraw-Hill Education;.

Gupta, B., Perez, G., Agrawal, D. and Gupta, D. (2020). *Handbook of Computer Networks and Cyber Security*. Cham: Springer.
http://isacacuracao.com/wp-content/uploads/2019/01/CSXFundamentals_2Day_04172018.pdf

Further reading and resources will be identified in your Project Brief.