Data and Network Protection Course Descriptor

Course Title	Data and Network Protection	Faculty	EDGE Innovation Unit (London)
Course code	NCHNAP6138	Course Leader	Dr Yu-Chun Pan
Credit points	15	Teaching Period	This course will typically be delivered over a 6-week period.
FHEQ level	6	Date approved	September 2022
Core/Optional	Core for Cyber Security Specialist Specialism		
Prerequisites			

Course Summary

The threat to data security and networks is a major concern of all business and organisations. The increasing sophistication of threat agents and their ability to access data and compromise networks has potentially devastating effects. The course explores the principles, concepts and methods that underpin data and network protection. From data and network protection governance, policy and procedures to the advanced tools and techniques employed in the monitoring, analysis and identification of threats, the course provides insight into the safeguarding of data and networks. It considers the key elements of a robust data and network protection strategy and critically considers the recovery strategies that mitigate risk.

Course Aims

- To provide learners with the principles, concepts and techniques that underpin data and network protection.
- To provide learners with detailed insight into data and network protection processes and solutions.
- To enable learners to analyse data and network protection and develop robust responses to threats.

Learning Outcomes

On successful completion of the course, learners will be able to:

Knowledge and Understanding

K1c   Demonstrate knowledge and critical understanding of the principles, concepts and processes that underpin data and network protection.

K2c   Demonstrate knowledge and critical understanding of threats to data and network protection.

K3c   Demonstrate knowledge and critical understanding of data and network protection strategies and how to mitigate risk.

Subject Specific Skills

S1c   Apply critical analysis to accurately interpret the expectations of governance, policy, and processes for data and network protection.

S2c   Identify potential weak points in data and network protection within organisations and recommend improvements or solutions.

S3c   Critically and systematically develop and test conceptual network and data recovery plans.

Transferable and Professional Skills

T1ci   Apply critical analysis and professional communication skills to articulate complex issues.

T1cii   Utilise an advanced level of technical proficiency of written English, while effectively applying scholarly terminology, to critically evaluate, analyse and make judgements and apply these appropriately to a range of diverse contexts.

T2c   Apply analytical and critical thinking skills to complex technological problems and their solution.

T3c   Apply understanding of business contexts and develop arguments to support technological solutions and innovation.

Teaching And Learning

This is an e-learning course, taught throughout the year.

Teaching and learning strategies for this course will include:

- Online learning
- Online discussion groups
- Online assessment

Course information and supplementary materials will be available on the College's Virtual Learning Environment (VLE).

Learners are required to attend and participate in all the formal and timetabled sessions for this course. Learners are also expected to manage their self-directed learning and independent study in support of the course.

The course learning and teaching hours will be structured as follows:

- Off-the-job learning and teaching (6 days x 7 hours) = 42 hours
- On-the-job learning (12 days x 7 hours) = 84 hours (e.g. 2 days per week for 6 weeks)
- Private study (4 hours per week) = 24 hours

Total = 150 hours

Workplace assignments (see below) will be completed as part of on-the-job learning.

Assessment

Formative

Learners will be formatively assessed during the course by means of set assignments. These will not count towards the final degree but will provide students with developmental feedback.

Summative

Assessment will be in two forms:

AE	Assessment Type	Weighting	Online submission	Duration	Length
1	Set Exercises	60%	Yes	Requiring on average 20 – 30 hours to complete	-
2	Written Assignment (workplace case study)	40%	Yes	-	1500 words

Feedback

Learners will receive formal feedback in a variety of ways: written (via email or VLE correspondence) and indirectly through online discussion groups. Learners will also attend a formal meeting with their Academic Mentor (and for apprentices, including their Line Manager). These bi or tri-partite reviews will monitor and evaluate the learner's progress.

Feedback is provided on summative assessed assignments and through generic internal examiners' reports, both of which are posted on the VLE.

Indicative Reading

Note: Comprehensive and current reading lists for courses are produced annually in the Course Guide or other documentation provided to learners; the indicative reading list provided below is used as part of the approval/modification process only.

Books

- Magnusson, A. (2020) *Practical Vulnerability Management*: No Starch Press.
- McNab, C. (2016) *Network Security Assessment, 3rd Edition*: O'Reilly Media, Inc.
- Wang, J. and Kissel, Z.A. (2015) *Introduction to Network Security: Theory and Practice*, 2nd Edition: Wiley, Singapore.

Journals

Learners are encouraged to read material from relevant journals on data and network protection as directed by their course leader.

Electronic Resources

Learners are encouraged to consult relevant websites on data and network protection.

Indicative Topics

Learners will study the following topics:

- Data and Network Protection
- Data Legislation and Regulations
- Network Security Threats and Solutions

Title: NCHNAP6138 Data and Network Protection

Approved by: Academic Board

Location: Academic Handbook/Programme specifications and Handbooks/ Undergraduate Apprenticeship Programmes/BSc (Hons) Digital & Technology Solutions Programme Specification/Course Descriptors

Version number	Date approved	Date published	Owner	Proposed next review date	Modification (As per AQF4) & category number
1.0	September 20	September 2022	Dr Yu-Chun Pan	September 2027	