ROBERT GORDON UNIVERSITY ABERDEEN

MODULE DESCRIPTOR

Module Title

Social and Human Factors in Cyber Security

Reference	CM3134	Version	1
Created	February 2022	SCQF Level	SCQF 9
Approved	July 2016	SCQF Points	15
Amended	March 2021	ECTS Points	7.5

Aims of Module

To provide students with the ability to independently and as a team member identify, analyse, discuss and report key social and human factors in Cyber Security for both individuals and society. Students will also be provided with an opportunity to explore the human and design implications of Cyber Security. This includes key topics such as risk, trust, and user research for security.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Identify important social and human factor issues that impact professional behaviour linked to Cyber Security.
2	Research and analyse material and real-world situations that relate to social and human factor issues linked to Cyber Security.
3	Systematically debate, discuss and report the outcomes of investigations.
4	Provide advice and recommendations about how to tackle social and human factor issues linked to Cyber Security.

Indicative Module Content

Social and Human Factor challenges in Cyber Security; Critical reasoning and ethical frameworks; Risks and risk perception; Privacy; Intellectual Property; Computer Crime; User research and personas; Design for human values; Trust; Introduction to Social goal modelling.

Module Delivery

This module is delivered through lectures, tutorials and assessed practical work with formative feedback.

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4

Description: A written coursework to assess the understanding of social and human factor issues related to Cyber Security for a selected case study.

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of C1. An overall minimum grade D is required to pass the module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	None.
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1 MANJIKIAN, M. 2018. Cybersecurity Ethics: An Introduction. Taylor & Francis

2 TAVANI, H. T., 2013. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. 4th ed. Wiley.

3 FRIEDMAN, B., HENDRY, D. G. 2019. Value Sensitive Design: Shaping Technology with Moral Imagination. MIT Press