Computer Science and Creative Technologies

Coursework and Assessment Specification – (both components A and B)

Module Details

Module Code	CSF_UFCFXN-15-M
Module Title	Cyber Security Futures
Module Leader	Abdullahi Arabo
Module Tutors	Panos and Essam Ghadafi
Year	2019/2020
Component/Element Number	A and B
Total number of assessments for this module	2 – component A and B
Weighting	A 25 % and B 75%
Element Description	A – presentation of report B – report

Dates

Date issued to students	28 01 2020
Date to be returned to students	22 May 2020
Submission Date	02/04/2020 –report component (B) May/June Assessment period for component (A)
Submission Place	Online for component (B)
Submission Time	14:00 for component (B)
Submission Notes	For component (B) Submit a report online

Feedback

Feedback provision will be	Online for the final report (B) and where possible in class, face to face feedback for presentation (A)– during the assessment period

Contents

Section 1: Overview of Assessment

This assignment assesses the following module learning outcomes:

- Evaluate and critique the current trends and challenges in cyber security. (A, B)
- Report on evidenced speculation about likely future trends and their impact. (A, B)
- Communicate complex information clearly and effectively. (A, B)

The assignment brief describes both Component B and Component A assessment. Component B is worth 75% of the marks for the module, Component A is worth the remaining 25%.

Broadly speaking, component B of the assignment requires you to produce a 3000-word analysis of an issue relating to current and *emerging trends in cyber security*. Component A of the assessment requires the delivery of a 15-minute presentation including questions and answers to disseminate your findings and conclusions or roadmap for the future.

The assignment is described in more detail in section 2.

This is an *individual* assignment.

Working on this assignment will help you to develop your knowledge and understanding of current trends and development in cyber security threats and challenges, it will enable you to identify emergent trends and challenges and allow you to propose possible solutions and roadmaps. It will also help to develop your critical reasoning skills for identifying appropriate mitigation strategies to avoid future security incidents. If you have questions about this assignment, please post them on the discussion board on Blackboard.

Section 2:   Task Specification

Part 1A (Assessment component B) (Report): individual report

Component B - worth 75% towards the final grade):

For this assignment, you are expected to identify and explore emerging trends in cyber security within a selected theme that you are interested in or have been covered during the regular workshops and lectures (**this should not be the same topic or area with your dissertation topic**). You need to conduct a literature review within this domain, critique the selected and identified materials, identify key contributions, and draw conclusions about the implications for Cyber Security of your chosen topic. Your report must include suggestions as to how future development and challenges in network security can be addressed.

Your report should be written for a professional audience and should make an influencing case as to why your proposal issue/solution/road-map is both important. The report is expected to be no more than 3000 words using IEEE format and template provided, please refer to the UWE word count policy: http://www1.uwe.ac.uk/aboutus/policies.aspx

Component A -worth 25% towards the final grade

Your presentation should consider the critical review from Component B, to discuss the limitations faced, comparison and discussion of different authors' views, presenting your proposed issue/trend/solution/road-map and how the work could be developed further. The presentation must include visual materials such as PowerPoint slides. The presentation must be no longer than 15 minutes and contributes towards 25% of the module's assessment.

The presentation should address the following questions:

- What are the chosen topics and their implications for cyber security?
- A brief overview of your findings in the literature review.
- Provide a comparison of similar selected papers and related cyber security issues, describing contributions, strengths, limitations, and weaknesses.
- Your conclusions

Section 3:   Deliverables

Component B: A written report is to be submitted via Blackboard the set date for submission **02/04/2020** in either DOC or PDF format:

Component A: You need to present your findings and proposed solutions to the staff during the assessment period, and the supporting PowerPoint slides are to be submitted in either PPT or PDF format before the demonstration date <<to be published centrally with assessment timetable>>**.**

Section 4:   Marking Criteria

Marking criteria for Component B:

85% and above:

Publishable material; well-presented evaluation of proposed improvements with:

Outstanding description of the selected theme and how they affect cyber security, providing examples from case studies; use of additional sources,

Outstanding analysis of the threat landscape and current cyber security approaches, providing examples from case studies; use of additional sources

Outstanding work on suggestions to improve cyber security and merging trends; based on a detailed analysis of current approaches as identified in relevant papers and case studies

Uses appropriate terminology accurately; professionally presented in both layout on the page and logical structure; impressively presented in an appropriate style; grammatically of an extremely high standard.

Outstanding use of references, citations, up-to-date list of references and cross-comparison of various viewpoints identified during the literature review and an outstanding proposed solution that addressing emerging trends in cyber security.

70% and above:

You need to show very clear evidence of independent research and own critical evaluation while discussing, providing comprehensive critique and comparisons of different views from selected papers and the approaches attempted in addressing your chosen cyber security dilemma, but this should be detailed enough with sufficient citations to relevant references. A conclusion will have as well to follow from this critical evaluation in relation to cited or

suggested future research directions that are naturally the product of such evaluation or conclusion.

60% and above:

You need to provide a critique that fully addresses the above specific report issues, detailed enough with sufficient citations to relevant references. Also, you need to show evidence of critical analysis of the different views and findings of papers discussed in your literature review.

50% and above: pass

You need to provide a critique that fully addresses the identified challenges and emerging trends and issues within your chosen theme, detailed enough with sufficient citations to relevant references.

Less than 50%: a straight-forward recall of approaches with no critical analysis, citations to references, and/or evaluation.

Cyber Security Futures Assessment Component A and B

Marking criteria for Component A

	0-29	30-39	40-49	50-59	60-69	70-84	85-100	Mark & Feedback
Demonstration of knowledge and understanding of the real-world cyber security incident and emerging trends (30%)	Little or no discussion on a chosen topic and its implications	Limited discussion on a chosen topic and its implications	Some discussion on the chosen topic and its implications	Discussion on a chosen topic and its implications with some detail regarding threats, vulnerabilities, risks, and impact	Discussion on a chosen topic and its implications with good detail regarding threats, vulnerabilities, risks, and impact,	Excellent discussion on a chosen topic and its implications with excellent detail regarding threats, vulnerabilities, risks, and impact,	*Outstanding **depth of content**; addressed all questions; comprehensive coverage/scope, with a detailed comparison of similar selected papers and related cyber security issues, describing contributions, strengths,*	

							limitations, and weaknesses.	
Demonstration of knowledge and understanding trends in cyber security (30%)	Little or no discussion on the chosen topic and its implications	Limited discussion on the chosen topic and its implications	Some discussion on the chosen topic and its implications	Some discussion on the chosen topic and its implications, making clear the stages of preventing Cyber security issues without proposed solutions/roadmap	Discussion on a chosen topic and its implications, making clear the stages of preventing Cyber security issues, and application of this to the chosen theme with proposed solution/roadmap	Discussion on a chosen topic and its implications, making clear the stages of preventing Cyber security issues, and good application of this to the chosen organisation and **excellent** discussion on proposed	*Outstanding critique; appropriate use of references and citations; excellent balance between visual and textual information; appropriate language; excellent use of diagrams/ tables/ screenshots,* **excellent** discussion on	

							solutions and roadmap	proposed solutions and roadmap and how has this (your solution) addressed emerging trends and threats in cyber security within your selected domain	
Extension of the material presented in the report (30%)	The presentation contains no extension to the report	The presentation contains a limited extension to the report	The presentation contains some extension to the report	The presentation is appropriately pitched at the audience with some evidence of extending the report	The presentation is appropriately pitched at the audience with evidence of extending the report	The presentation is appropriately pitched at the audience with good choices of how to	The presentation is appropriately pitched at the audience with excellent choices of how	

						extend the original report	to extend the original report	
Presentation skills and subject clarity (10%)	The presentation is poorly delivered and lacks in clarity	The presentation is weak but lacks in clarity	The presentation is fair and some clarity	The presentation is fair but the clarity of content is clear	The presentation is good and clarity of content is clear	The presentation is excellent and clarity of content is good	*Outstanding presentation skills; appropriate presentation style; maintains eye contact with audience; use of appropriate language; no notes used; looks and sounds confident in a well-balanced manner;*	

							excellent use of visual and textual information on the slides; excellent use of the slides. Well-paced and clearly audible without overreacting.	

Section 5:   Feedback mechanisms

I will be holding sessions within the teaching and lab sessions for feedback within the semester to clarify things before submission. Some lectures (as indicated in the schedule) are directly for feedback. You can use regular lab sessions to ask for feedback and advice from tutors. You can post your question in the discussion forum and tutors will respond as appropriate. If required you can book an appointment with the module leader or tutors for more advice and feedback on the project.

Feedback after marking will be provided online – as an attachment to your marks.