COM664 Coursework 2: Investigative Report on Cyber Security in Enterprise Networks

This is an individual piece of coursework, which is worth 50% of the total marks for this module.

Aim: To help you develop an appreciation and understanding of security issues associated with Enterprise Networks by producing a structured technical evidence-based report to an industry standard which represents the 'state of the art' of Enterprise Networks security.

This should demonstrate knowledge and understanding of the practices underlying the use of networks for academic, industrial or business applications.

You are responsible for cybersecurity in a large Computing Department for <*MyCompany.com*>. This is similar in scale to the Computing Services supplied to you in Block 16 (web, email, portal, software development IDEs, packages etc.).

1. Research and analyze network trends in cybersecurity, making effective use of information retrieval skills and of learning resources. The following reports are available, but you should supplement these with additional authoritative sources.
    a. Cisco's Cybersecurity Series Reports.
    b. OWASP, The Ten Most Critical Web Application Security Risks, 2017 and 2021.
2. Provide a specification of the technical services supplied to *MyCompany.com*. This should be designed by you. Services can be supplied from local servers and/or from the Cloud (you can specify provider). The services should be selected to allow security aspects to be assessed (2-4 services should be sufficient).
3. Defender Landscape: Identify risks and make practical recommendations on maintaining cybersecurity for services delivered by *MyCompany.com*.

Deliverables: In addition to Cisco's Reports and OWASP Top 10 Security Risks, materials that have informed your research should be referenced throughout the report and listed in an appropriate References section. Sources should include textbooks, academic web sites, manufacturers' web sites, RFCs, white papers and academic literature (conferences and journals). The report should be approximately 2000 words (this word count does **not** include references, bibliography, Appendices). The word count should be provided at the top of the report. The report should be formatted to IEEE specification (a template will be provided on Blackboard).

NOTE: You should **not** reuse any original figures from the Cisco and OWASP reports (i.e., do not cut & paste figures). You can use data from the reports as evidence, but you need to express this in your own words. This is an individual assignment and all work submitted must be your own. Plagiarism will not be tolerated and will be dealt with according to university policy: http://www.ulster.ac.uk/academicservices/student/plagiarism.pdf

Marking Scheme: Marks will be awarded based on the following distribution of the overall possible percentage for aspects of the report:

- Research and analyse trends in cybersecurity for Enterprise Networks **40 marks**
- Specification of IT services for *MyCompany.com* **20 marks**
- Risks and Defender landscape for *MyCompany.com* **30 marks**
- Presentation, grammar, spelling and adherence to submission guidelines **10 marks**

NOTE: Late submission, with the exemption of those supported by prior submission of an EC1 form, will be awarded a mark of 0%.

Coursework Release Date: Week 1

Coursework Submission Deadline: Week 9 (date subject to confirmation)

Coursework Submission Information: A copy of the report (in IEEE format) must be uploaded to the Turnitin assignment folder **Coursework 2** in the COM664 module area of Blackboard by the submission deadline.

NOTE: The filename for the report (PDF file) should be given as: **B00CODE_CW2**, e.g. "B00123456_CW2.pdf"

Feedback will be provided by **20 working days**

References

Cisco Cybersecurity Report Series: Defending against critical threats, threats-year-report.pdf (cisco.com)

https://www.cisco.com/c/dam/global/en_uk/solutions/security/UK-CISO-Benchmark-Report-2020.pdf

OWASP Top 10 2017, The Ten Most Critical Web Application Security Risks, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Top 10:2021

Transactions-template-and-instructions-on-how-to-create-your-article.doc (supplied on Blackboard)

COM 644 A2 Marking Rubric

	0-39%	40-49%	50-59%	60-69%	70-100%
Appraisal of cyber security network trends for Enterprise Networks (40 marks)	Inadequate description of Security implications for Enterprise Networks. Lack of critical appraisal of CISCO / OWASP reports Missing or Inadequate ideas, integration of evidence for threats/trends.	Adequate description of Security implications for Enterprise Networks. Some critical appraisals of CISCO / OWASP reports. Adequate ideas, integration of evidence for threats/trends.	Appropriate description of Security implications for Enterprise Networks. Critical appraisal of CISCO / OWASP reports. Appropriate analysis, integration of evidence on threats/trends.	Very good description of Security implications for Enterprise Networks. Very Good critical appraisal of CISCO / OWASP reports. Very good analysis, integration of evidence on threats/trends.	Excellent description of Security implications for Enterprise Networks. Excellent critical appraisal of CISCO / OWASP reports. Excellent analysis, integration of evidence on threats/trends.
Specification of IT services (20 marks)	Inadequate knowledge and depth of understanding of IT services provision. Poor or no definition/explanation, no evidence of understanding of example. Contains inaccuracies. Poor/no support through references.	Adequate knowledge and depth of understanding of IT services provision. Adequate definition/explanation, adequate evidence of understanding of example. Adequate level of accuracy - some inaccuracies may be present. Adequate support through references.	Appropriate knowledge and depth of understanding of IT services provision. Appropriate definition/explanation, good evidence of understanding of examples. Appropriate level of accuracy. Appropriate support through references - good critical evaluation.	Very good knowledge and depth of understanding of IT services provision. Very good definition/ explanation, very good evidence of understanding of IT services provision. Very good level of accuracy. Very good support through references.	Excellent knowledge and depth of understanding of IT services provision. Excellent definition/explanation. Excellent evidence of understanding of IT services provision. Excellent level of accuracy. Excellent support through references.
Defender landscape (30 marks)	Inadequate knowledge, integration of evidence and depth of discussion. Inadequate recommendations.	Adequate knowledge, integration of evidence and depth of discussion. Adequate recommendations.	Appropriate knowledge, integration of evidence and depth of discussion. Appropriate recommendations.	Very good knowledge, integration of evidence and depth of discussion. Very good recommendations, which integrate with state of the art.	Excellent knowledge, integration of evidence and depth of discussion. Excellent recommendations, which integrate with state of the art and trends.
Presentation, grammar, spelling and adherence to submission guidelines (10 marks)	Inadequate document presentation, illogically structured, or not using correct grammar and spelling. Inadequate labels on figures / tables. Inadequate/absent referencing.	Adequate document presentation, generally logically structured, using correct grammar and spelling. Adequate labels on figures / tables. Adequate/limited referencing.	Appropriate document presentation, logically structured, using correct grammar and spelling. Good use of labels on figures / tables. Good use of referencing with appropriate referencing style.	Very good document presentation, logically structured, using correct grammar and spelling. Very good use of labels on figures / tables. Very good use of referencing with very good referencing style.	Excellent document presentation, logically structured, using correct grammar and spelling. Excellent use of labels on figures / tables. Excellent use of referencing with excellent referencing style.