ASSESSMENT 1 BRIEF

Subject Code and Title	MIS301 Cybersecurity
Assessment	Research Report
Individual/Group	Individual
Length	1500 words (+/- 10%)
Learning Outcomes	The Subject Learning Outcomes demonstrated by successful completion of the task below include: *a)* Investigate and analyse the tenets of cybersecurity *b)* Identify and communicate a range of threats and vulnerabilities to informational assets.
Submission	Due by 11:55pm AEST *Sunday of Module 2.2*
Weighting	25%
Total Marks	100 marks

Context:

CNN reported in May 2016: 'LinkedIn was hacked four years ago, and what initially seemed to be a theft of 6.5 million passwords has actually turned out to be a breach of 117 million passwords' (Pagliery, 2016).

The New York Times reported in March 2018: 'Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to information on 50 million Facebook users as a way to identify the personalities of American voters and influence their behaviour' (Granville, 2018).

Reuters reported in October 2017: 'Yahoo on Tuesday said that all 3 billion of its accounts were hacked in a 2013 data theft, tripling its earlier estimate of the size of the largest breach in history, in a disclosure that attorneys said sharply increased the legal exposure of its new owner, Verizon Communications Inc' (Stempel & Finkle, 2017).

More recently, BBC reported in June 2020: 'Australia's government and institutions are being targeted by ongoing sophisticated state-based cyber hacks' (BBC, 2020).

Headlines regarding cyber-attacks have appeared more and more often in the news in recent years. With the prevalence of and the reliance on internet in the modern world, cybersecurity becomes more relevant to government, organisations and individuals alike.

In the first three weeks, we have explored some fundamental concepts about cybersecurity, vulnerabilities and common cybersecurity attacks. This first assessment develops your understanding of the various tenets of cybersecurity by asking you to apply what you have learnt in the first three weeks to previous cyber-attack incidents. You will undertake extensive research into the cybersecurity literature and/or media coverage, analyse past cyber-attacks of various types and report your findings.

Instructions:

In Module 1, you learnt the five types of hacker threats that are common on the internet: commodity threats, hacktivists, organised crime, espionage and cyberwar. In Assessment 1, you are required to choose any three of the five types of hacker threats and undertake some research into the cybersecurity literature and/or media coverage to find one incident for each of the chosen three types of hacker threats. For each incident, you will:

1. **describe** the attack and the immediate result of the attack (i.e. what was the asset that was compromised?)
2. **describe** the motivation behind the attack
3. **identify** and **describe** the vulnerability (or vulnerabilities) in the organisation that made the attack possible
4. **describe** the short-term and long-term impact (financial, reputational or otherwise) of the attack on the organisation
5. **describe** the responses from the affected organisation and society as a whole.

Reflect on all the incidents, and critically **discuss** the factors that make the prevention of cyber-attack challenging.

The incidents should meet the following criteria:

- The attack must be a cyber-attack.
- The attack was within the last ten years.

Your report should include the following:

Title page: It should include subject code and name, assessment number, report title, assessment due date, word count (actual), student name, student ID, Torrens email address, campus learning facilitator, and subject coordinator.

Table of Contents (ToC): It should list the report topics using decimal notation. It needs to include the main headings and subheadings with corresponding page numbers, using a format that makes the hierarchy of topics clear. Because you are including a ToC, the report pages should be numbered in the footer as follows: the title page has no page number, and the main text should have Arabic numerals commencing at 1. Create the ToC using Microsoft Word's ToC auto-generator rather than manually typing out the ToC. Instructions can be found here https://support.office.com/en-gb/article/Create- a-table-of-contents-or-update-a-table-of-contents-eb275189-b93e-4559-8dd9-c279457bfd72#__create_a_table.

Introduction *(90-110 words)*: It needs to provide a concise overview of the problem you have been asked to research, the main aims/purpose of the report, the objectives to be achieved by writing the report and how you investigated the problem. Provide an outline of the sections of the report.

Body of the report (use appropriate headings in the body of the report) ***(1170-1430 words)***: Ensure that you address the tasks listed above. Do NOT use generic words such as 'Body, Body of the Report, Tasks' as section headings. Create meaningful headings and subheadings that reflect the topic and content of your report.

The body of your report should have the following structure:

2.0 Hacker threat 1

2.1 Description of the incident (approximately 80 words)

2.2 Motivation (approximately 50 words)

2.3 Vulnerabilities (approximately 80 words)

2.4 Short-term and long-term impact (approximately 70 words)

2.5 Responses (approximately 70 words)

3.0 Hacker threat 2

3.1 Description of the incident (approximately 80 words)

3.2 Motivation (approximately 50 words)

3.3 Vulnerabilities (approximately 80 words)

3.4 Short-term and long-term impact (approximately 70 words)

3.5 Responses (approximately 70 words)

4.0 Hacker threat 3

4.1 Description of the incident (approximately 80 words)

4.2 Motivation (approximately 50 words)

4.3 Vulnerabilities (approximately 80 words)

4.4 Short-term and long-term impact (approximately 70 words)

4.5 Responses (approximately 70 words)

5.0 Factors that make the prevention of cyber-attack challenging (approximately 250 words)

Conclusion ***(90-110 words)***: Restate the purpose of the report and key issues investigated, and the related findings based on your research and analysis.

Reference list.

Appendices if necessary.

You are expected to begin this assessment when you begin the trimester. Be sure to keep several drafts of your work as well as your notes and any sources you used to draw on in preparing your report.

Before submitting your assessment, you should check it against the assessment criteria and the marking rubric included in this specification to ensure that you have satisfactorily addressed all the criteria that will be used to mark your submission.

Referencing

It is essential that you use appropriate APA style for citing and referencing research. Please see more information on referencing here https://library.torrens.edu.au/academicskills/apa/tool

Submission Instructions

Please submit ONE Microsoft Word document (.doc or .docx) via the Assessment link in the main navigation menu in Blackboard. The Learning Facilitator will provide feedback via the Grade Centre in the LMS portal. Feedback can be viewed in My Grades.

Academic Integrity Declaration

I declare that except where I have referenced, the work I am submitting for this assessment task is my own work. I have read and am aware of Torrens University Australia Academic Integrity Policy and Procedure viewable online at http://www.torrens.edu.au/policies-and-forms

I am aware that I need to keep a copy of all submitted material and their drafts, and I will do so accordingly.

References

BBC. (2020). *Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack*. Retrieved from https://www.bbc.com/news/world-australia-46096768

Granville, K. (2018). Facebook and Cambridge Analytica: What you need to know as fallout widens. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Pagliery, J. (2016). Hackers selling 117 million LinkedIn passwords. *CNN Business*. Retrieved from https://money.cnn.com/2016/05/19/technology/linkedin-hack/

Stempel, J. & Finkle, J. (2017). Yahoo says all three billion accounts hacked in 2013 data theft. *Reuters*. Retrieved from https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1

Assessment Rubric

Assessment attributes	Fail (Unacceptable) 0-49%	Pass (Functional) 50-64%	Credit (Proficient) 65-74%	Distinction (Advanced) 75 -84%	High Distinction (Exceptional) 85-100%
Knowledge and understanding of the terminologies in cybersecurity, including attack, asset, vulnerability and challenges in preventing cyber-attacks. **40%**	Limited understanding of required concepts and knowledge in cybersecurity terminologies. Key components of the assignment are not addressed.	Adequate knowledge or understanding of the terminologies in cybersecurity. Some of the key components of the assessment are not addressed	Thorough knowledge or understanding of the terminologies in cybersecurity. All key components of the assessment are addressed with an adequate capacity to explain and apply relevant key concepts.	Highly developed understanding of the terminologies in cybersecurity All of the key components are addressed. Well demonstrated capacity to explain and apply relevant key concepts.	A sophisticated understanding of the terminologies in cybersecurity. All of the key components are addressed. Demonstrates mastery and application of key concepts.
Evaluation of information selected for each chosen type of hacker attack **40%**	Confuses logic and emotion. Information taken from reliable sources but without a coherent analysis or synthesis. Viewpoints of experts are taken as fact with little questioning.	Resembles a recall or summary of key ideas. Often conflates/confuses assertion of personal opinion with information substantiated by evidence from the research/course materials. Analysis and evaluation do not reflect expert judgement, intellectual independence, rigor and adaptability.	Supports personal opinion and information substantiated by evidence from the research/course materials. Demonstrates a capacity to explain and apply relevant concepts. Identifies logical flaws. Questions viewpoints of experts.	Discriminates between assertion of personal opinion and information substantiated by robust evidence from the research/course materials and extended reading. Well demonstrated capacity to explain and apply relevant concepts. Viewpoint of experts are subject to questioning.	Systematically and critically discriminates between assertion of personal opinion and information substantiated by robust evidence from the research/course materials and extended reading. Information is taken from sources with a high level of interpretation/evaluation to develop a

Assessment attributes	Fail (Unacceptable) 0-49%	Pass (Functional) 50-64%	Credit (Proficient) 65-74%	Distinction (Advanced) 75 -84%	High Distinction (Exceptional) 85-100%
				Analysis and evaluation reflect growing judgement, intellectual independence, rigour and adaptability.	comprehensive critical analysis or synthesis. Identifies gaps in knowledge. Exhibits intellectual independence, rigour, good judgement and adaptability.
Use of academic and discipline conventions *Spelling, grammar, sentence construction, appropriate use of credible resources. Correct citation of key resources using APA style of referencing.* ***20%***	Poorly written with errors in spelling and grammar. It demonstrates inconsistent use of good quality, credible and relevant resources to support and develop ideas. There are mistakes in using the APA style.	Written according to academic genre and has accurate spelling, grammar, sentence and paragraph construction. Demonstrates consistent use of credible and relevant research sources to support and develop ideas, but these are not always explicit or well developed. There are some mistakes in using APA style.	Written according to the academic genre. Demonstrates consistent use of credible and relevant research sources to support and develop ideas. There are no mistakes in using the APA style.	Well written, and adheres to the academic genre. Consistently demonstrates expert use of good quality, credible and relevant research sources to support and develop appropriate arguments and statements. Shows evidence of reading beyond the key resources. There are no mistakes in using the APA style.	Expertly written, and adheres to the academic genre. Demonstrates expert use of high-quality credible and relevant research sources to support and develop arguments and position statements. Shows extensive evidence of reading beyond the key resources. There are no mistakes in using the APA style.