Business Information Security
Assignment 1 worth 40% of overall course marks
Dr Alex Pudmenzky – 2024 S2

Assignment overview

This assignment must be completed individually by each student. This assignment requires a student to answer 4 questions (each with sub-parts) that focus on the course material covered across the first four weeks of the course. Assignment 1 is worth 40% of the overall course marks and will be marked as per the rubric in Table 1. A student's answer to each of the 4 questions (that is, each question and all its sub-parts) must not exceed 300 words (+10% tolerance per UQ policy). This word limit per question requires a student to soundly analyse/research each question and then structure a response in a concise, business informative fashion. There is no need to reference an answer unless referencing is specifically requested in the question. A student must construct each answer in her/his own words and in 'plain English' business language. Please note that each question in this assignment may well span work covered across all weeks (and not simply relate to one specific week).

This assignment assumes that a student is capable to assimilate information from not only this course, but also many other courses and reputable sources on the Internet as would be required in a business setting. Students are advised that the use of AI technologies to develop responses is strictly prohibited and may constitute student misconduct under the student code of conduct. Each assessment question evaluates students' abilities, skills and knowledge without the aid of AI.

Submission and formatting instructions

- Create and upload a single PDF document containing all answers to Turnitin on Blackboard.
- Use the file naming convention described in the submission link when it becomes available closer to the submission deadline (you may receive a deduction for incorrectly named files).
- Please ensure your student details (name & student number) are contained on each page of the submission in a suitably designed footer.
- Clearly label which question and if relevant sub-question you answer (e.g., Question 2a). You don't have to repeat the question.
- Answer in full sentences but you may want to use bullet points, numbering, or headers to help structuring your answer.
- Read each question carefully for additional formatting requirements specific to the question.

Table 1 - Marking rubric for Assignment 1.

Criteria	High distinction (10)	Distinction (8)	Credit (6)	Pass (5)	Marginal fail (4)	Fail (2)	Low fail (0)
Question 1 (10 marks)	All cyphers correctly decoded/created and cypher correctly identified.	Cypher decoded correctly AND correct cypher created.	Cypher type correctly identified and cypher correctly decoded OR created.	n/a	Cypher decoded correctly OR correct cypher created.	Cypher type correctly identified.	No attempt or no cypher correctly decoded/created and cypher type not correctly identified.
Question 2 (10 marks)	All questions correctly answered.	Received 8 or 9 marks for correct answers.	Received 6 or 7 marks for correct answers.	Received 5 marks for correct answers.	Received 3 or 4 marks for correct answers.	Received 1 or 2 marks for correct answers.	No attempt or no answer correct.
Question 3 (10 marks)	•Identifies and describes all three notices (TAR, TAN, TCN) clearly and thoroughly, with precise details on purpose, conditions, and implications. •Provides comprehensive and accurate information on legal and procedural requirements, including issuing	•Identifies and describes all three notices adequately, with minor omissions or less detailed descriptions. •Provides detailed information on most legal and procedural requirements, with minor omissions or inaccuracies.	•Identifies and describes two out of the three notices adequately. •Provides adequate information on most legal and procedural requirements, though lacking in detail or with some inaccuracies. •Provides an adequate	•Identifies and describes one notice adequately. •Provides basic information on legal and procedural requirements, with significant omissions or inaccuracies. •Provides a basic analysis of the impact on stakeholders, with significant	•Identifies all notices but with significant inaccuracies or misunderstandings. •Provides some correct information on legal and procedural requirements but with major inaccuracies or misunderstandings. •Attempts to discuss impact on stakeholders but with major	•Identifies some notices but with major inaccuracies or misunderstandings. •Provides minimal correct information on legal and procedural requirements with significant inaccuracies or misunderstandings. •Provides minimal or incorrect analysis of impact on stakeholders.	•Does not identify any notices correctly. •Provides incorrect or very limited information on legal and procedural requirements. •Does not discuss impact on stakeholders.

Criteria	High distinction (10)	Distinction (8)	Credit (6)	Pass (5)	Marginal fail (4)	Fail (2)	Low fail (0)
	notices, oversight and consultation requirements, and legal authorizations. •Provides a thorough analysis of the impact on SecureChat, users, and broader societal implications, addressing all aspects with depth and insight. •Is within word limit.	•Provides a detailed analysis of the impact on stakeholders, covering most aspects with minor omissions or less detailed analysis.	analysis of the impact on stakeholders, though lacking in depth or missing some aspects.	omissions or superficial analysis.	inaccuracies or misunderstandings.		
Question 4 (10 marks)	Both relative risks correct and both asset values correct. Correct asset in red.	Both relative risks correct and both asset values correct. Incorrect or no highlighting of risk.	One relative risk correct and two asset values correct.	One relative risk correct and one asset value correct.	No relative risk correct and two asset values correct.	No relative risk correct and one asset value correct.	No attempt or no relative risk or asset value correct.

Question 1

Encipher/decipher with the WW2 Enigma machine.

The Enigma was used by the German military, among others, around the WW2 era as a portable cipher machine to protect sensitive military, diplomatic and commercial communications. The Enigma machine was considered so secure that it was used to encipher the most top-secret messages.

You can look at this video of someone using an Enigma to encode a message and then decode the same message again back to clear text:
https://upload.wikimedia.org/wikipedia/commons/f/f7/Encrypting_and_decrypting_using_an_enigma_machine.webm

a) The following message

LPRHOCFPJXFEKKLFDNBISSBIFEYHHMVZGPSPVTXOQTWYYQCYGVHIBPUDTTH

was sent from an Enigma 1 machine with 3 rotors and the following settings:

Walzenlage (rotors): 1-5-8
Grundstellung links (left hand rotor): A
Grundstellung mitte (middle rotor): L
Grundstellung rechts (right hand rotor): X
Umkehrwalze (reflector): B
Ringstellung links (left hand rotor ring): P
Ringstellung mitte (middle rotor ring): U
Ringstellung rechts (right hand rotor ring): D
Steckerbrett (plugboard): ME NZ KY

What does the message say?

(4%)

b) What type of cypher is utilised by the Enigma?

(2%)

c) Change the following settings on your Enigma machine leaving the remaining settings the same:

Walzenlage (rotors): 1-2-3
Umkehrwalze (reflector): C

and insert the answer you received in question 1a), what secret message cypher will your Enigma produce now?

(4%)

Question 2

The video "Phishing Attacks" (https://youtu.be/u9dBGWVwMMA also on Blackboard under "Assessment") demonstrates how easy it is even for non-IT trained people to create a convincing phishing attack. NB: A computer with a Unix-like operating system can be purchased for AU$67 (Raspberry Pi 4 Model B 1GB).

a) Describe what a phishing attack is and when it was first used for what purpose.
b) What is spear phishing?
c) What is clone phishing?
d) What is whaling?
e) What is vishing?
f) What is Pharming?

(3%)

g) The URL https://www.apple.com/ does not lead you to the place you would expect it to go. Click on it using different browsers including Firefox, look at the URL that is displayed each time. What is this kind of attack called and how does it work?

(1%)

h) How can you prevent organisational staff to fall for phishing scams? Name four different methods.

(4%)

i) How many "1's" can I send on a 10Mbps digital communication link in one second under ideal conditions (no latency, jitter or packet loss)?

(1%)

j) Is it better to use SHA256 rather than MD5 to hash your valuable data before backing it up just in case, so that people can't read it if they get hold of your backup somehow?

(1%)

Question 3

The article by *Arthur Kopsias APM* discusses the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)*, which became law on 8 December 2018. This law aims to address the challenge of *going dark*, where law enforcement agencies face difficulties accessing encrypted data used by terrorists and criminals.

Purpose: The Act enables law enforcement and security agencies to access encrypted communications by creating a new industry framework.

Framework: It introduces three types of notices for requesting assistance from communication providers.

Scope: Applies to both Australian and offshore communication providers, including major tech companies and equipment manufacturers.

Powers and Oversight: Agencies must have existing legal authority, such as a warrant, to use these powers.

Background:
Alex, an Australian resident, is suspected of being involved in an organized cybercrime group that uses encrypted messaging apps to coordinate illegal activities, including hacking into financial institutions and conducting large-scale fraud. The Australian Federal Police (AFP) has been investigating the group for several months but has encountered difficulties accessing the encrypted communications between members.

Scenario:
To advance their investigation, the AFP decides to use the powers granted by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act). They plan to approach SecureChat, a popular encrypted messaging app used by the suspects, to gain access to their communications.

Task:
You are part of the legal team advising the AFP on how to proceed under the TOLA Act. Your task is to analyse the situation and provide a detailed plan, ensuring compliance with the Act while addressing potential legal and ethical issues.

Questions (make sure you stay within the 300+10% word limit):

1. **Identify the Appropriate Notices:**
    - Which specific notices should the AFP consider issuing to SecureChat? Provide reasons for your choices.
2. **Legal and Procedural Requirements:**
    - Outline the legal and procedural steps the AFP must follow to issue these notices. Include any necessary approvals, oversight mechanisms, and consultation requirements.
    - Discuss how the AFP can ensure that their requests do not require SecureChat to create systemic weaknesses or vulnerabilities in their encryption.

3. **Impact on Stakeholders:**
    - Analyze the potential impact of these notices on SecureChat, its users, and broader societal implications. Consider privacy concerns, public trust in encryption, and the balance between security and privacy.

Guidelines for Answer:

- **Identify the Appropriate Notices:**
    - Clearly identify which notices are most appropriate for the AFP to issue.
    - Provide a rationale for each notice, explaining how it aligns with the Act's provisions and the investigation's needs.
- **Legal and Procedural Requirements:**
    - Detail the procedural steps and legal requirements for issuing the notices.
    - Explain how to comply with safeguards against creating systemic weaknesses.
- **Impact on Stakeholders:**
    - Discuss the implications for SecureChat and its users, considering both positive and negative outcomes.
    - Reflect on the broader societal impact and the balance between national security and privacy rights.

(10%)

Question 4

You are a business analyst participating in the risk assessment process for your business. You have completed many different courses at UQ and are therefore familiar not only with how to do this but you are also an expert in setting up spreadsheets. Senior management has devised a *Weighted Factor Analysis* policy for the valuations of all assets within the risk assessment process and your business uses a combination of *quantitative and qualitative risk data points* to describe impact. All relevant data is contained in a spreadsheet already that your predecessor Alex has created (this spreadsheet is available to you on Blackboard). However, you have found out the reason for Alex not working in your company anymore is because he made **too many errors in his spreadsheet formulas**.

As part of an overall risk assessment process, you are asked to assess the risk in relation to two information assets using a version of this spreadsheet **corrected by you**.

The assets under investigation are:

(1) An Oracle SQL database containing product information. You have assessed that the database has a high impact on revenues earned by your business, and a moderate business impact on the public image of your business. The most likely attack against this database is insider abuse, and this is estimated to be 10% probable. The current controls in place to counter this attack are estimated to be 70% effective. You are 80% certain of your assumptions and data.

(2) A UNIX transaction server for the business organisation is hosted in-house and those transactions have very high impact on revenue, and a high impact on the public image of your business. The server can be attacked using malware with a likelihood of a single attack estimated to be 0.2. A control has been implemented that reduces the impact of any vulnerability by 50%. You are 90% certain of your assumptions and data.

You are now required to do the following:

Calculate the asset valuations and the relative risk for each of the two assets using the formula (3) from the seminar (*Risk = likelihood * asset_value - controlled risk + uncertain risk*) using a corrected version of the spreadsheet made available to you. Highlight the risk of the asset you would recommend for further security in red.

You must insert a **screenshot** of your final spreadsheet created from the template given to you into your document in **landscape mode as a picture**. All intermediate and final values must be clearly visible (range A1:P15). **Do not show any formulas** or you may lose marks. **Do NOT submit your spreadsheet, it will be discarded!**

(10%)