UNIVERSITY OF JOHANNESBURG
FACULTY OF SCIENCE

# MEMO

**ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING**

**MODULE:** **IT28X80/IT8X299**
INFORMATION SECURITY GOVERNANCE

**CAMPUS:** **APK**

**EXAM:** **OCTOBER 2021**

QR Access Code: aa134d3c

**DATE** 2021-10-25 **SESSION** Morning

**INTERNAL EXAMINER** Dr J du Toit

**EXTERNAL EXAMINER** Dr H Abdullah

**DURATION** 2 Hours **MARKS** 100

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. This paper consists of 7 pages
4. Start the invigilator app before taking the exam.
5. **Not using the invigilator app during the exam is seen as an assessment transgression and the test submission will not be marked**. Exams are only eligible for marking if the uploaded assessment images in Invigilator matches the uploaded submissions on eve.
6. You are not allowed to assist or gain assistance from anyone. You are only allowed to communicate with the lecturer during the assessment.
7. You are not allowed to copy text from any source and use that as your answer. All answers must be written by yourself during the assessment.

**QUESTION 1 (Multi-dimension discipline)** **[23]**

Yellow Cab-Taxis (YCT) is a taxi company operating in Utopia. The company employs many drivers and owns its own fleet of taxis. Historically people would have to phone YCT to arrange a taxi to drive them from one point to another. The management of YCT has decided to embrace the digitalisation of the system.

The digital product allows customers to register their details using a mobile app, including a valid credit card number. The customer can then use the app to book a ride, track the assigned taxi, and make the necessary payment. The whole system is run without any staff operating the phones. Payments are also handled by the system, minimising the risk of riding around with cash.

The CEO is very happy about the success of the new system. At a recent business conference, the CEO heard that the IT department might not have the capacity to take responsibility for all of the Information Security aspects. The CEO contacted you, hoping that you can clarify the message from the conference.

Write a memo to the CEO of YCT explaining why Information Security isn't just the responsibility of the IT department. Describe at least five (5) Information Security dimensions that are affected because of the new system. Clearly demonstrate how each of the Information Security dimensions is changed by the new system.

Marks are awarded according to the following aspects:

| | | |
|---|---|---|
| 1.1 | Describing each of the five dimensions | (10) |
| 1.2 | Describe how each of the dimensions is affected by the new system | (10) |
| | Style of memo. | (3) |

**MEMO**

| | |
|---|---|
| There are a number of valid dimensions that the student have mentioned. | |
| Describing each of the dimensions is worth two marks. (2 x 5) | 10 |
| Describing how the new system affects the new dimension is worth another two marks. The focus must be on something in Information Security in the dimension. (2 x 5) | 10 |
| The overall readability and structure of the answer is worth (3) marks | 3 |
| Here are a few examples of arguments students could make to describe how the dimension is affected by the new system:<br>From a **technical dimension** perspective, the new system must ensure availability, otherwise the system may not be available when customers or drivers need to use it.<br>The **organisation** dimension may require a stronger IT department or even a separate Information Security Compliance function to test the IS compliance.<br>The **policy** dimension needs to be updated to ensure a policy gets created or modified that clearly explains how credit card numbers or transactions are to be handled by the system, who has access to it and how it will be protected.<br>The **awareness** dimension is affected since all drivers need to be aware how to work with the new app safely and securely.<br>The **best practices** dimension may need to be relooked since the organisation may need guidance on how to include the Information Security of the new system and ensure it is based on best practices.<br>There are a lot more dimensions that the students may mention. It is vital that the student explains the dimension in context of Information Security and how it is affected. | |

**QUESTION 2 (Information Security Education, Training and Awareness)** **[23]**

Yellow Cab-Taxis (YCT) employed a new Information Security Officer. The IS Officer is fully aware that they need a proper Information Security Education, Training and Awareness (ISETA) programme that must include the new taxi management system.

The IS Officer has approached you about how to implement an ISETA, based on the IS controls and risks surrounding the new taxi management system.

2.1 It is important to consider the Conscious Competency Learning Model (CCLM) when planning an ISETA. **Name** and **briefly describe** each of the four stages of this model (8)

2.2 Clearly explain how the CCLM can be used to plan and implement a SETA programme that addresses the new taxi system. Clearly explain what will be done in each of the four CCLM phases. The explanation must be relevant to the new taxi management system (12)

Answering questions 2.1 and 2.2 in a structured and readable manner. (3)

**MEMO**

| | | |
|---|---|---|
| 2.1 | Two marks for each phase.<br>**Unconscious Incompetence**<br>You don't know what you don't know<br>**Conscious Incompetence**<br>They know what they don't know<br>**Conscious Competence**<br>There is a conscious effort to ensure they do it right<br>**Unconscious Competence**<br>Doing the right thing comes automatically. | 8 |
| 2.2 | Three marks awarded per phase for the student explaining the programme approach in each of the phases. | 12 |
| Style | | 3 |

**QUESTION 3 (Generalised attack process)** **[24]**

On Friday, you received an urgent message from the IS Officer of Yellow Cab-Taxis (YCT). It seems as if they have been a victim of a coordinated cyber-attack. Without any warning, the IS Officer received an email from an anonymous person. The email claims that all the customer information, including credit card information, has been stolen and is now in the hands of cyber attackers. The email provided proof of the attack by including 100 customer records with the credit card details of the 100 customers. The attackers claim that they have all the customer records that YCT stored.

A forensic investigation showed that the attackers got access to the taxi system six months ago already. It seems as if an employee accidentally accessed a fake email site while working from home and accidentally logged in using their login credentials. The attackers used the login credentials to access the VPN system and plant a password cracking program inside the taxi management system server. The original user account did not have the necessary permission to access the customer

database. The password cracking program eventually returned the login credentials of a database admin, which was used to access the customer information.

The IS Officer would like to know what process the attackers might have followed to exfiltrate the results.

Explain to the IS Officer the eight (8) phases a general attack goes through and explain what the attackers did in each phase to access customer information eventually.

Marks are awarded as follow:

- Naming each of the phases. (8)
- Describing the activities of the attackers in each of the phases. (16)

**MEMO**

| | | |
|---|---|---|
| | There are eight phases. Some of them are fairly close. If the student copied and pasted from the book, then marks may only be granted for naming the 8 phases. No marks for describing the activities of the attacker in this scenario. The phases application of the scenario in the phases are a bit debatable. Two main attack stages might have been highlighted:<br>1. Getting the user's password and putting the password cracking program on the server and exfiltrate the admin password from the server.<br>2. Using the admin password to gain access to the DB.<br><br>Marks have been loosely based on seeing whether the student identified and discussed at least one of these stages. | |
| Perform reconnaissance | The attacker might have a ping sweep and detected the VPN system, as well as email addresses of employees. Could have used other mechanisms as well to try and get access to the email address of the victim. | 3 |
| Create attack tools | A fake email web site was created to harvest log in credentials of employees. They also created the actual fake email as well as the password cracking software. | 3 |
| Deliver malicious capabilities | The attacker used the VPN and planted a password cracking program in the Taxi Management System. | 3 |
| Exploit and compromise | This one is not clear, but the attacker may have exploited the ability of the system to allow normal users to login to the system in order for them to run the password cracking program. OR<br><br>The attacker uses the exploited admin password and logs back in to the server. | 3 |
| Conduct an attack | The password cracking program is running, and some user account passwords are returned. OR<br><br>The attacker logs in using the exfiltrated admin account and opens the customer DB. | 3 |

| | | |
|---|---|---|
| Achieve results | The attacker logs in using the cracked login credentials of the DB admin. OR the attacker gets access to the customer DB. | 3 |
| Maintain a presence or set of capabilities | The attacker may have create their own login details at this point to ensure that they can always get back into the system | 3 |
| Coordinate a campaign | The attack was multi-staged. First getting access to the basic system and then cracking passwords and eventually using DB admin rights to get a copy of the Customer DB. | 3 |

**QUESTION 4 (Cyber security frameworks)** **[30]**

A few months after your last engagement with YCT you receive the following email from the IS Officer

***To:*** *isconsultant@security.co.ut*

***From:*** *iso@yct.co.ut*

***Subject:*** *Cyber security frameworks*

*Dear consultant,*

*We have made great strides in enabling Information Security in YCT. One of my problems is that I do not always know whether we are doing the right things. We have limited Information Security Risk Management processes, but I would like to be more proactive.*

*I can remember you telling me about a "deep" approach and a "wide" approach, but I cannot remember what you told me about them.*

*Can you please remind me again of the difference between a "deep" approach and a "wide" approach? What are the advantages and disadvantages of these two approaches? Can you remind me again of a framework that makes use of a "wide" approach and which one makes use of a "deep" approach?*

*Is there a way both approaches can be combined to ensure we can get the best of both worlds? How would we implement such an approach that considers both "wide" and "deep"?*

*Information Security Officer*

**Write** a reply to the IS Officer, where you address all the questions in the email. Remember that you are replying to the IS Officer. Ensure that the IS Officer can understand your response, but also so that they know you are answering each of their questions.

Marks are awarded as follow:

| | | |
|---|---|---|
| 4.1 | Critically evaluating a "deep" approach and a "wide" approach against each other. (Listing and evaluating the various advantages and disadvantages of both and weighing them up against each other) | (10) |
| 4.2 | For both a "deep" and "wide" approach, briefly describing a real-world framework and why that framework is seen as either "deep" or "wide." | (6) |
| 4.3 | Discuss how both approaches can be used to implement an Information Security programme. | (10) |
| | Style of email: | (4) |

**MEMO**

| | | |
|---|---|---|
| Evaluating deep vs wide | Depending on the argument up to two marks may be awarded for an advantage and disadvantage.<br>Wide:<br>• Very useful to cover "most" of the basis.<br>• The Risk Management process can identify areas that require higher priority.<br>• Based on industry accepted best-practices. | (10) |

| | | |
|---|---|---|
| | • May spend too much time and money on areas that may not have as much risk.<br>• Depending on the level of implementation may not fully cover the highest risk systems.<br><br>Deep<br><br>• Improve the detection and response of a specific system significantly.<br>• Uses a lot of effort on one system.<br>• May cause the IS department to "over"-focus and forget about other systems.<br>• Requires significant investment in IS employees to fully address the detect and response. | |
| Example of both deep and wide framework | Wide:<br><br>• CIS Top 20 or ISO 27002 or NIST Framework for Infrastructure Protection<br>• Top 20 has 20 categories of focus. NIST covers 5 high level categories, which is then broken down into multiple categories. Each of these systems try and cover the spectrum of important IS controls.<br><br>Deep:<br><br>• Mitre Att&ck<br>• Focusses on detection, prevention and response for a specific attack technique.<br>• Requires the use of some threat modelling, because that is the starting point. | (6) |
| Implement | • Start with a risk management process.<br>• All systems with a certain level of risk must be included in a wide approach.<br>• Decide on the level of implementation for the wide approach. Use a framework that gives you an option in prioritising controls against the known risks.<br>• Evaluate the risk after the wide approach has been implemented and confirm the level of risk is now at an acceptable level.<br>• All systems over a certain level of risk must be included in the deep approach.<br>• Prioritise systems according to risk. Highest risk systems first.<br>• Identify threat techniques most relevant to the system.<br>• For each threat technique ensure that the team understands how the technique works.<br>• Implement mitigation steps described by Mitre.<br>• Implement detection strategies.<br>• Train the team in the mitigation, detection and response techniques.<br>• Test the team by conducting and red team exercise. | (10) |
| Style | It must look like an email. Easy to read. | (4) |

**TOTAL PAPER** **[100]**