NATIONAL UNIVERSITY OF SINGAPORE

IS4231 –Information Security Management

(Semester 1: AY2018/19)

Time Allowed : 2 Hours

INSTRUCTIONS TO STUDENTS

1. Please write your Student Number only. **Do not write your name**.
2. This assessment paper contains of **THREE** sections and **15** printed pages.
3. Section A consists of 20 multiple-choice questions worth 10 marks. Answer **All** questions by shading your answers on the OCR form provided. Please use a 2B or darker pencil, and shade your answers completely. Please write and shade your student number clearly on the OCR form provided.
4. Section B and C must be answered within the designated spaces of the assessment paper using a **BLUE OR BLACK BALL POINT PEN ONLY**. However, you may use a 2B pencil for any drawings.
5. No electronically stored material or device is permitted. However, you may use an electronic calculator that is approved by the University.
6. This is an OPEN BOOK assessment.

STUDENT NO: _____

This portion is for examiner's use only

Section	Marks	Remarks
A (MCQ)		10 Marks
B (TOF)		10 Marks
C (Structured Question)		30 Marks
Total		50 Marks

Section B – True or False questions (10 marks).
Read each of the statements and decide whether it is true or false. For a statement that you find false, briefly explain why to earn the credit. Each correct answer is awarded 1 mark.

1. Red-teaming is considered as a reactive security protection method.

False. Red teaming is considered a proactive security protection method as it simulates an attack, to test for vulnerabilities in the system before an actual attack has occured

2. The laws are the only regulations industry players need to comply with compulsively.

No. Compliance standards such as PCI DSS have regulations for industry players to comply with compulsively else the company is not allowed to use any payment system from the cards

3. A clearly directed strategy flows from top to bottom rather than from bottom to top.

True.

4. A need-to-know access control principle is a more flexible model compared with BLP confidentiality model.

True.

5. According to the Evaluation Assurance Levels in Common Criteria scheme, a firewall product receiving EAL 7 certificate is more secured than another firewall product receiving EAL 4 certificate.

True.

6. Training should be as specialized as possible; personnel who are responsible for one duty should not be trained on other duties to avoid confusion during a disaster.

False. Although duties should be separated to reduce the chance of corruption or conflict of interest, personnels can be cross trained as a means to minimise misconduct and for backup purposes

7. In risk analysis phase, if there are two exclusive categories: security software and cryptography. PKI (Public Key Infrastructure) can be placed in both categories at the same time, so as to make a more intercorrelated and comprehensive categorization scheme.

False. This would break the Mutually exclusive principle and this might create conflict of policies with regards to applying them to PKI

8. Implementing IDPS (Intrusion Detection and Prevention System) is a method reflecting deterrence security management approach.

True

9. Currently, most of the incidents that happened to an organization are due to the attacks from external world.

False. Start from internal attacks

10. Role-based access control approach is better than task-based access control approach as it is more consistent and easier to implement.

True.

Section C-Structured Questions (30 marks)
Answer each of the questions in the space provided.

Question 1 (4 marks)

Separation of duties is a control that makes it difficult for an individual to violate InfoSec and reach the confidentiality, integrity or availability of information. For example, banks typically require that it takes two employees to issue a cashier's check.

Please propose TWO separation of duties designs that you think should be adopted in information security management practices. For each proposed design, please explain why it can help better protect the information security in an organization.

1) One such example would be for the software development and software testing to be split up, this would ensure that for any new software, collusion is reduced as the creator has no say in how secured the software is as it is tested by another team

2) Another example would be the the owners of the systems should only do Risk Assessment for their own system, and then the overall ranked risk worksheet should be done by another team. This would reduce the chances of conflict of interest where an owner of a system will unfairly rank their system as more critical or less than it is

Question 2 (4 marks)

An asset has a value of $1,000,000. In an attack, it is expected to lose 60 percent of its value. An attack is expected to be successful once every ten years. Countermeasure X will cut the amount lost per incident by two-thirds. Counter measure Y will cut the frequency of successful attack in half. Countermeasure X will cost $30,000 per year, while Countermeasure Y will cost $5,000 per year. Do an analysis of these countermeasures and then give your recommendation for which to select.

SLE = 1 000 000 × 0.6 = 600 000

ALE = 600 000 × 1/10 = 60 000

ALE_{post_X} = 1000 000 × 0.2 × 1/10 0.1 = 20000

ALE_{post_Y} = 1 000 000 × 0.6 × 0.05 = 20000

CBA_X = 60k − 20k − 30k = 10k

CBA_Y = 60k − 20k − 5k = 35k.

∴ Y is more cost efficient + same ALE post

Question 3 (6 marks)

Considering the following two information security performance measurements:

Measure 1: The percent coverage of devices by antivirus software
Measurement formula: No. of device with antivirus software/ total no. of device

Measure 2: Average frequency of audit record review and analysis for inappropriate activities
Measurement formula: average frequency during reporting period

a) For each measure, which performance measurement category does it belong? **(2 marks)**

1) Implementation performance measurement Type 1
2) Effectiveness/Efficiency performance measurement Type 2

b) Do you think these two measures are effective enough for measuring organization's information security performance? What suggestions can you make for each measure so as to improve its effectiveness or usefulness? **(4 marks)**

1) This might be effective if the organisation is sure that the antivirus is always working. A improvement would be to measure the number of devices scanned / total devices. This would show that the antivirus is working and active to scan the devices which it is installed on.

2) This might be lacking in tracking if any action has been done after reporting. Thus a better measurement might be time take for appropriate action after reporting.

Question 4 (6 marks)

Case Background

On January 13, 2018, a false ballistic missile alert was issued via the Emergency Alert System and Commercial Mobile Alert System over television, radio, and cellphones in the U.S. state of Hawaii. The alert stated that there was an incoming ballistic missile threat to Hawaii, advised residents to seek shelter, and concluded "This is not a drill". The message was sent at 8:07 a.m. local time. It set off widespread panic in a state that was already on edge because of escalating tensions between the United States and North Korea. Within moments of the first announcement, people flocked to shelters, crowding highways in scenes of terror and helplessness.

The alert was revoked 38 minutes after it was issued. State officials and residents of a normally tranquil part of the Pacific, as well as tourists swept up in the panic, immediately expressed outrage. Officials said the alert was the result of human error and not the work of hackers or a foreign government. The mistake occurred during a shift-change drill that takes place three times a day at the emergency command post, according to Richard Rapoza, a spokesman for the agency. "Someone clicked the wrong thing on the computer," he said.

State officials said that the agency and the governor began posting notices on Facebook and Twitter announcing the mistake, but that a flaw in the alert system delayed sending out a cellphone correction. As a result, they said a "cancellation template" would be created to make it easier to fix mistaken alerts.

a) Looking at this case, what information security management controls or practices you can suggest for the agency to adopt, so as to prevent such human error from happening again in the future? **(3 marks)**

I think that the most important practice the agency can adopt would be to have 2 man control, before sending out any serious notices. This would prevent such human error where 1 person accidentally makes a mistake in pressing the wrong thing. Having 2 person would mean that both person would have to make the exact same mistake which is much more rare and difficult.

b) In addition to the "cancellation template" creation, propose THREE actions that should be included in the response plan so as to better deal with such incident. Provide your justification for each action proposed. **(3 marks)**

1) I think they would need to have an official broadcast maybe on radio or TV to better inform residents that this was a false alarm
2)

Question 5 (10 marks)

Facebook "View as" Data Breach

Case Background

Facebook discovered a security issue that allowed hackers to access information that could have let them take over around 50 million accounts, the company announced Friday, 28 Sept 2018. The company said in a blog post that its engineering team found on Tuesday that attackers identified a weakness in Facebook's code regarding its "View As" feature. Facebook became aware of a potential attack after it noticed a spike in user activity on Sept. 16.

"View As" lets users see what their profile looks like to other users on the platform. This vulnerability, which consisted of three separate bugs, also allowed the hackers to get access tokens — digital keys which let people stay logged into the service without having to re-enter their password — which could be used to control other people's accounts.

To be more specific, regarding this vulnerability: when using the View As feature to view your profile as a friend, the code did not remove the composer that lets people wish you happy birthday; the video uploader would generate an access token when it shouldn't have; and when the access token was generated, it was not for you but the person being looked up. That access token was then available in the HTML of the page, which the attackers were able to extract and

exploit to log in as another user. The attackers were then able to pivot from that access token to other accounts, performing the same actions and obtaining further access tokens.

Almost 50 million accounts had their access tokens taken, and Facebook has reset those tokens. The company also reset tokens for an additional 40 million accounts who used the "View As" feature in the last year as a precautionary measure, for a total of 90 million accounts. Facebook had 2.23 billion monthly active users as of June 30.

The reset will require these users to re-enter their password when they return to Facebook or access an app that uses Facebook Login. They will also receive a notification at the top of their News Feed explaining what happened. In addition, the company suspended the "View As" feature while it reviews its security. Facebook said it fixed the issue on Thursday night and has notified law enforcement including the FBI and the Irish Data Protection Commission in order to any address General Data Protection Regulation (GDPR) issues.

Approximately 3 million Europeans were affected by this incident. This security breach is expected to be the first major test of Europe's new General Data Protection Regulation, and the number of European users affected could help determine the severity of any penalties against the company. Under GDPR, companies handling the personal data of Europeans must adhere to strict requirements for holding and securing that information, and must report breaches to authorities within 72 hours. Under the regulation, companies can face fines of up to 4 percent of their annual global revenue. For Facebook, which made more than $40.65 billion in revenue in 2017, that fine could be as much as $1.63 billion.

Facebook said it has just begun its investigation and has not determined if any information was misused, but the initial investigation has not uncovered any information abuse. The hackers did query Facebook's API system, which lets applications communicate with the platform, to get more user information. The company is not sure if the hackers used that data, nor does it know who orchestrated the hack or where the person or people are based.

The company said there is no need to change passwords. If additional accounts are affected, Facebook said it will immediately reset those users' access tokens. Facebook is doubling the number of employees who are working to improve security from 10,000 to 20,000, the company reiterated.

"Security is an arms race, and we're continuing to improve our defenses," Zuckerberg said. "This just underscores there are constant attacks from people who are trying to underscore accounts in our community."

a) Considering this data breach, it represents what kind of threat(s) here? **(1 mark)**

Espionage

b) In addition to the mentioned security controls already taken by Facebook to resolve this incident, what else you can suggest for Facebook to take? Please suggest THREE additional information security controls that you suggest Facebook to take and provide justification for each control you propose. **(3 marks)**

c) Based on the three security controls you suggest, propose ONE performance measure for each control you think is critical for Facebook to adopt to improve its information security performance monitoring. Provide justification for each measure you propose. (**3 marks**)

d) Assume users' data in Facebook values $10 billion, and the attack in this case happens once every 5 years. If such attack happens, the hacked percentage of user data is of 5%. From a cost-benefit analysis perspective, what is the highest amount you would recommend Facebook to invest annually on a counter-measure for protecting users' data from such threat? From your perspective, should Facebook follow the cost-benefit analysis result and use it to determine the investment on the counter-measure of such threat? **(3 mark)**

SLE = 10bil x 5% = 500 mil

ALE = 500mil x 1/5 = 100 mil

CBA = 100 − ALE_{post} − ACS.

Thus i would recommend them to invest up to 50 million if the measure is able to reduce the chances of successful attack by half. I believe FaceBook should follow the cost-benecefit result since they are a public company and it is easier to value their reputation through market shares. Moreover it would be easier to find the price of certain data and use that for evaluation

END OF PAPER