Information Assurance and Security
2nd sem. S.Y. 2022 – 2023
Activity 1

Name: **Trixie L. Soriano** Score: _____ Date : **02/18/23**

Section: **CEIT - 37- 601P** Schedule: **6:00 PM - 9:00 PM** Instructor: **Prof. Rowena Reyes**

Task 3

Direction: Analyze the given questions below and provide the correct answer on a separate sheet of paper.

1. What is the most important from the 3 pillars of information assurance? How it matters in your organization? Give a scenario that will support your answer. (5pts)

   Answer:

   The three pillars of information assurance are the following:

   1. Confidentiality - Confidentiality is one of the pillars of information assurance because an organization is collecting information from customers so they should protect it and also in accordance with the Data Privacy act of 2012. And also confidentiality helps an organization defend themselves from their ideas being stolen. For example, I develop a website for a certain organization, it requires the user to sign up for an account so what I'm gonna do is make their accounts confidential and secured with data encryption.

   2. Integrity - It is one of the pillars of information assurance and it matters in an organization because it safeguards the system from future threats such as viruses. For example, the way of other IT professionals tests the integrity of a system before launching it online. They tend to install a certain virus in a system then they will observe how this virus affects the system or program. If the program or system is strong enough the expected outcome of the test may be good. On the other hand, if something happens such as a loss of data then the system is not strong enough so it might result in re-programming.

   3. Availability - Lastly, availability is one of the pillars of information assurance that an organization might also look after because the users tend to have easy access to their data. If not, it might cause another hassle for the users because they need to wait for a long period of time. For example, if I use a specific mobile application for online transactions then for some reason I need to have the transaction identification number because of some verification process. If that

mobile application is not working for that time it might cause me another problem. I need to wait for a long time to retrieve the transaction identification number.

2. “In early 2018, international shipping giant FedEx discovered that hackers had managed to steal scanned images of approximately 119,000 of its customers’ personal documents, including passports and driver's licenses. Surprisingly, these images were being stored on an unsecured third-party server that has since been closed. According to a statement by FedEx officials, an internal investigation concluded that none of the information had been misappropriated. This was a stroke of luck for FedEx, but this is a compelling example of how a simple mistake can put a large amount of private data at risk.”

   In the statement above, where do you think it falls under the 3 pillars of information assurance? Why? (5pts)

   Answer:

   The statement above made me think that FedEx lacks system integrity and confidentiality. Firstly, I thought FedEx lacks system integrity because of the hacking incident. The hackers managed to steal scanned images of the customers' personal documents. Secondly, I thought of them as lacking confidentiality because the images are being stored in an unsecured third-party server.

3. There was an electronic greeting card (e-card) sent to your work email address by a friend. If you want to see the card, you need to click on the attachment. As a tradition, we connect with our friends online when we celebrate any occasion. Can work email be used for personal communications? What should you do? Provide an explanation of how we secure our computer system and ourselves against risks.

   Answer:

   Firstly, the work email must be only used for work-related purposes communication. It is provided in order to separate work from personal agendas. If this happens that someone sent a link, the link may be suspicious. And as some who always use an email address, we should be aware of phishing emails. If I am in that situation, I might double-check the sender's email and the content. If the email address ends with “@gmail.com” then it might be a phishing email. Then as for the link attached, it is easy to spot a suspicious link from a legitimate one. If the destination address doesn’t match the context of the email then it is a phishing email.

4. Such a scenario could occur at your workplace if you are undergoing on-the-job training or studying information technology. When your supervisor is very busy and asks you to log into the HR Server using her user ID and password to retrieve some reports. Your company has a policy. What should you do?
   a. This is your boss's decision, so it's fine.

b. Don't pay attention to her request and hope she forgets about it.
c. Remind your supervisor that this request is in violation of university policy.

In the choice above, choose the correct answer and explain your viewpoint based on company policy.

Answer:

In my own opinion, aside from the violation of the university policy, the task is also a risk to the confidentiality of the other files included. So the best thing to do is remind my supervisor that the request is in violation of the university policy and also a risk to the company.