**COIT12212 Cyber Security Management (HT2, 2020)**

|  |  |  |
| --- | --- | --- |
| Due date: | Week 12 Friday (11 Feb 2022) 11:45 pm AEST | **ASSESSMENT** |
| Weighting: | Written Report 40% | 1 |
| Length: | 4000 words report by the due date  (Quality over quantity!) |

## Objectives

This assessment task can be undertaken in a group of up to 4 members. In this assessment task, you will analyse the case study below and complete the two assessment tasks outlined below. In Assessment 1, you must submit a report by the due date. In Assessment 3, you must do a presentation in-class or via Zoom.

## Case Study

Koala Health (KH) is an Australian medical centre. During COVID-19 pandemic, the company decided to adopt telehealth technology. Telehealth is the delivery of health care remotely using tools ranging from web-based videoconferencing to wearable technologies, complementing face-to-face consultation and offering significant benefits for patients, their carer, to the healthcare workers and the health system. This would also allow doctors to work from home and conduct medical consultation via video conferencing with their patients also from their homes. KH wishes to also streamline their pathology and pharmacy services and wishes to bring some sort of automation to this system as well. To help you understand how the system works, consider the following scenario:

*Bob is a patient. He wishes to be examined by a Koala Health GP. To do that, Bob visited KH websites, downloaded KH mobile application and booked an appointment with one of the doctors via the company app. Bob had to first register for an account. Where he had to register his personal information (name, address, phone number etc.), his Medicare card details and payment details (e.g., credit card details). To book an appointment, Bob was presented with a list of GPs (doctors) available on that day with their available timeslots. Bob then booked an appointment with Doctor Alice.*

*At the time of the appointment, Dr Alice medically examined Bob via video conference- a function supported by KH mobile application. During the examination Dr Alice requested some blood tests to be done on Bob. The request was digitally processed using Alice’s medical system and the request was digitally sent to Koala Health Pathology department. Bob was then issued with a transaction number on his mobile application. The following day, Bob presented to KH Pathology, showed the transaction number form his phone to the staff at the lab. The nurse then took some blood samples from Bob. Bob was then told that Dr Alice will be in touch with him to give him the results. Bob then happily went home. The next day, Bob received a video conference call from Dr Alice to discuss his blood test results. Alice explained to Bob that he must take a prescribed medication for 5 days. To do that, Dr Alice issued a digital prescription to Bob which was sent to Koala Health Pharmacy department. The pharmacy then received Alice’s request, accessed Bob’s records on the system (medicare details, credit card payment, delivery address etc.) and processed the order remotely for Bob. The next day. Bob received his medication in the mail box.*

*In addition to the telehealth examinations, all other three transactions (Processing the Blood test results, Alice issuance of the prescription, and medication processing and delivery) were all done remotely.*

The above scenario assumes to use several interconnected systems or subsystems. These are:

* The mobile app used by Bob for appointment and video conference
* The system used by Alice to manage appointment and conduct telehealth consultations
* The system used by Alice to order Bob blood test
* The system(s) used by the pathology department to access and process the blood test results
* The system used by Alice to order medications for Bob
* The system(s) used by the pharmacy to process Bob’s medication.

**Assessment 1- Written assessment (40%):**

This complex interconnected system has several Cybersecurity requirements, which need to be achieved first. Your task in this assessment is to:

**Conduct a comprehensive cybersecurity risk management for Koala health. You are free to either use the Risk management framework discussed in the book or the NIST Cybersecurity framework.**

The report should include the following sections:

* 1. Executive Summary
  2. Table of Contents
  3. Introduction
  4. Risk management (RM)
  5. Conclusion
  6. References

**The Risk Management framework should include the followings subsections:**

## Asset Identification and Assessment- (Physical Assets and Non-Physical Assets)

## Risks- (Individual Asset Risk Analysis)

## Threats, Challenges and Vulnerabilities

# Disaster Recovery and Business Continuity plan (Incident Response Team, Incident Response Procedures, Restoration Procedures, Business continuety plan)

# Security Strategies and Recommended Controls (Mitigation/treatment of Risks) and Residual Risks

**Further guidelines:**

* Asset Identification and Assessment- (Physical Assets and Non-Physical Assets). So, we have about 3-4 categories (hardware, software, data, people). You need at least 2-4 main assets from each category. So, say in total about 10-15 assets. In your work always consider quality over quantity. For example, it is very easy to say that a database is an asset under data or software category. But to indicate the prescription as an asset under data shows the depth of your work and that you have tried, and you did not just use some template you found online
* Risks- (Individual Asset Risk Analysis).  Consult slide 31 of chapter 6. So, you need to have one table for the 10-15 assets
* Threats, Challenges and Vulnerabilities- consult slide 39. One table for each category of assets. So about 4-5 tables are a good number and then do a TVA slide 41. Then slide 58 or similar likelihood analysis.
* Disaster Recovery and Business Continuity plans. 1-2 pages for each subsection (Incident Response Team, Incident Response Procedures, Restoration Procedures, Business continuity plan). These plans can be combined in one or more plans. As discussed in the workshop DR and BC plans are sometimes presented in one document. It is important that you reference the template you are using to do the plans. Remember the incident response plan we did during the workshop (before during and after an incident). You can use that. Check out other internet resources such as NIST Contingency Planning Guide. I don’t expect you to write a full comprehensive plan just a brief on one about 2 pages max per plan.
* Security Strategies (2 pages) and Recommended Controls (2 pages) (Mitigation/treatment of Risks) and Residual Risks (max 1 page)- chapter 10- your chosen security and treatment approach (is it mitigation? Deterrence?).

|  |  |
| --- | --- |
|  |  |
| **Report Criteria** |  |
| **Heading** | **Criteria** |
| Executive Summary and TOC | Summarised all key information of the report.  Auto generated TOC is used and it is free of errors. |
| Report presentation | References used when needed with proper intext citations. The report is well written, formatted, and structured. |
| Introduction and Conclusion | The introduction sets the scene for the report and describes the purpose clearly. Outlined the sections of the report. The conclusion includes a statement of the topic and summarises the key points |
| **Cybersecurity risk management** |  |
| Identity/Asset identification and assessment | Physical Assets and Non-Physical Assets are clearly defined. Risk assessment conducted |
| protect/Risk analysis | Establishing Data Security protection to protect the confidentiality, integrity, and availability/ Individual Asset Risk Analysis |
| Detect/threats and challenges | Implementing Security Continuous Monitoring capabilities |
| Respond/DRP and BCP | Ensuring Response Planning processes are executed during and after an incident/ Incident Response Team, Incident Response Procedures, Restoration Procedures, Business continuity plan |
| Recover/recommended controls | Ensuring the organization implements Recovery Planning processes and procedures/ Security Strategies and Recommended Controls (Mitigation/treatment of Risks) and Residual Risks |