**Cyber Security Assessment 2**

*Risk Assessment Scenario Description for Learning Management System (LMS)*

*\*\*\*\*apply the confidentiality, integrity and availability to this assignment*

*Confidentiality- encryption- if this is broken then can get sued etc*

*Increase in one can bring down another one- so important to weigh up what the asset is to determine which one gets most etc*

Step1- identify what the digital assets you are going to protect

* Student data
* Student ID data- name, address, personal information
* Course information
* Staff personal information
* Student fees
* School information
* Contractual documents
* Financial assets
* Web server information
* If LMS is down then students cannot be taught (loss of business and money)

*Using the CIA triad, will need to identify of these which will require which resources eg the student personal information will require more confidentiality than the course information*

**Things like more availability means public looking which means confidentiality goes down and integrity has more risk because public infmration.**

**If more confidentiality then less availability because information is hidden- integrity is balanced**

* Some government regulations have to abide by othersise business cannot run (privatised informration of students) – university policy document (maybe in assignment?)- things like 2FA, MFA- dunno if actually part of the assignment, then just make suggestion why it should be implemented if no policy

**Terminology**

* **Asset- digital information**
* **Vulnerability (weakness a threat can exploit)- bugs in code, no 2FA/MFA, sanitization error, Web server installed on server machines so hosting the website on that web server available for people- apache, nginx, tomki (if webserver outdated its vulnerability)- something you exploit**
* **Threat(actor looking for weakness )- hacker, system downtime, malware, virus. Phishing (use symbols in diagram)- potential cause of unwanted incident**
* **Threat scenario- series of events that is initiated by a threat adnd may lead to unwanted incident**
* **Unwanted incident- event that harms or reduces the value of an asset**
* **Risk- likelihood of unwanted incident and its conseuquence for a specific asset**
* **Consequence- loss of CIA triad, reputation of business ruined, loss revenue**
* **Likelihood- frequency of probability of something to occur**
* **Party- organisation, company, person, group or other body on whose behalf a risk analysis is conducted**
* **Treatment- appropriate measure to reduce risk level- mitigates the risk- treatment to the vulnerability**

create security mechanisms to mitigate these vulnerabilities

if mitigating anything look for the treatment symbol

the risk assessment- need to use the ISO 310000 risk management process- look at CORAS->Coras process in notes- has the process in a diagram

don’t think these indented below are important, just telling us

every stage is consulting with management to discuss what you have identified

approval of management to accept the risk or not

SURVEY AND EVALUATE are for management

always a cost with mitigating a risk

**HOW TO USE CORAS**

When making diagram

Define scope- must do this first to identify the assets before making diagram

List down all the assets

Identiofy the threats- non human can be bots, natural distasiters (disaster recovery plan)- describe the threat

Identify the threat scenario (how can this threat compromise the asset)- things like unwanted incident

*NEED TO MAKE 5 diagrams*

- \*\*Asset Diagrams\*\*- devsribe the focus of the analysis

- \*\*Threat Diagrams\*\*- describe scenarios that may cause harm to the assets

- \*\*Risk Diagrams\*\*- summarise the risks presented in the threat diagrams

- \*\*Treatment Diagrams\*\*- add proposed treatments to the threat diagrams

- \*\*Treatment Overview Diagrams\*\*- add the proposed treatments to the risk diagrams

Have to make a threat scenario diagram for each threat to a specific asset, an asset could have multiple threats and therefore many threat scenarios. Could be More than one vulnerability and more than one vulnerability diagram could also mean more than one treatment diagram- all of these are diagrams

1:06