SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BSc. BUSINESS INFORMATION TECHNOLOGY

CASE STUDY 3 – 10 Marks

152239- Yvonne Gikundi

BBT4201: INFORMATION SYSTEMS AUDITING & FORENSICS

Instructions: This is a group discussion assignment. Each learner will be required to upload a PDF document (Typed format) write-up of the group discussions on the online portal by the specified deadline.

Case Study: Risk Assessment

You are the chief Information Officer of the University of Higher Education.

From lesson in class, Applying the concept of a Heat Map, list and briefly discuss the Likelihood and Impact of Cyber Security threats that could target the University?

A Heat Map visualizes and prioritizes risks by assessing two factors:

Likelihood: How likely the threat is to materialize.

Impact: The severity of damage if the threat happens.

Using this paradigm, the following are the key cybersecurity threats relevant to a university environment:

1. Phishing attacks.

Emails are a common attack vector in universities due to their large student and staff populations. Attackers routinely target academic institutions with bogus login pages, scholarship offers, and password reset frauds.

Impact: High.

Successful phishing can result in credential theft, financial loss, email compromise, data leaks, and unauthorized access to internal systems.

2. Ransomware.

Universities are potential targets owing to their massive datasets and decentralized IT systems.

Likelihood: Medium to High.

Attackers use unpatched systems, weak passwords, and phishing techniques.

Impact: Very high.

Ransomware can disrupt learning management systems, research data, and administrative systems, causing significant financial and reputational harm.

3. Insider Threats (Staff/Students)

Insiders may actively misuse access or unintentionally compromise systems (e.g., poor password practices).

Likelihood: Medium.

Insiders' direct access to internal systems poses a high risk of data leaks, grade manipulation, and system misuse.

4. DDoS (Denial of Service) Attacks

DDoS attacks from hackers or competitors can interrupt universities' online services, including portals, LMS, and websites.

High-level DDoS assaults can disrupt university activities, including exams, registration, fee payments, and online learning.

5. Data Breaches (Personal and Academic Records)

The **likelihood** is medium.

Large databases containing student records, financial data, health information, and research data are appealing to cybercriminals.

The **impact** is quite high, with consequences such as identity theft, legal penalties, compliance violations, and stakeholder confidence erosion.

6. Malware Infections.

The **likelihood** of students and staff connecting personal devices to the network is high. This increases the likelihood of spreading malware.

Impact: Medium - High Malware can cause file corruption, system slowdown, backdoor creation, and data theft.

7. Social Engineering Attacks

High **likelihood** of attackers impersonating IT support, lecturers, or administrators and tricking users into revealing passwords or granting unauthorized access.

Impact: Medium-High

This can result in illegal access, data theft, or account compromise.

8. Weak Authentication and Password Attacks

The **likelihood** is high.

Many people reuse passwords or create weak combinations. Attackers can use brute-force or credential-stuffing attacks.

Impact: Medium-High

An attacker who gains access to professor or administrator accounts can change grades, read sensitive emails, and interfere with systems.

9. Network Intrusions/Exploiting Unpatched Systems

Medium **likelihood** of unpatched vulnerabilities due to research labs, aging systems, and decentralized IT management.

Impact: High Intruders can obtain extensive access to systems, databases, research data, and deploy malware.

10. Cloud Security Risks

The likelihood is medium.

Universities rely on cloud-based services such as Gmail, LMS systems, and ERP solutions. Misconfigurations can result in exposure.

High impact: Leaked cloud datasets or misconfigured access controls can expose thousands of records.