**ALEXZANDRA SABANGAN  
SOUTH 3   
ITE 370 – IAS 2**

**Case Study 1: Threat Assessment and Risk Management**  
**Scenario:**  
A mid-sized financial institution experiences a surge in cyberattacks targeting their online banking system. The institution has outdated threat assessment procedures and no clear risk management strategy.

Taking into consideration the case of the mid-sized financial institution which experiences a crisis time that leads to more and frequent cyberattacks toward its online banking system, it is crucial to minimize the identified threats and risks with the help of a strategic risk management plan.

**1. Identifying Potential Threats and Vulnerabilities**

Potential Threats

* Phishing Attacks
* Malware Infections
* Credential Stuffing

Vulnerabilities

* Outdated Software
* Weak Authentication
* Lacking Response to incidents Approach

**2. Risk Management Plan?**

|  |  |  |
| --- | --- | --- |
| **Step** | **Action** | **Description** |
| Assessment | Security Audit | Determine the weaknesses and gaps. |
| Assessment | Evaluation for penetration | Evaluate vulnerabilities by simulating attacks. |
| Prioritization | Risk Ranking | Focus on high-priority threats. |
| Implementation | Phishing Mitigation | Implement anti-phishing tools and provide user training. |
| Implementation | Malware Protection | Install and update antivirus software. |
| Implementation | MFA | Strengthen account security. |
| Implementation | Software updates | Apply patches regularly. |
| Monitoring | Daily Monitoring | Detect and log unusual activities |
| Testing | Simulated Attacks | Test system defenses regularly. |
| Testing | Backup and testing | Verify data recovery processes |

**3. Evolving Processes to Address Emerging Threats?**

*Continuous Training and Awareness*

* Organize sessions to create awareness for products among employees and prospective buyers such as phishing threats.
* Use mock phishing simulations to improve user readiness.
* Ensure that training materials contain the current threat trends so that this activity is up to date.

*Strengthening Collaboration*

* Facilitate the communication between the top management of the university, Information Technology personnel and other employees.
* Integrate cybersecurity to enhance the ways of handling risks.

*Policy Adaptation*

* Get feedbacks from employers and customers on security issues.
* Modify policies periodically as it fulfills the requirements of the best practice and emerging risks.

*Promoting a Security Culture*

* Recognize and reward employees for identifying and reporting threats.
* Launch awareness campaigns to reinforce security best practices.