**MIS761 Cyber Security Strategies**

***Trimester 2 2024***

**Mock EXAM**

|  |  |
| --- | --- |
| **DUE DATE AND TIME:** | The start date and time will be as per the University Exam T2 2024 Exam timetable available via [StudentConnect](https://studentconnect.deakin.edu.au/connect/webconnect?_ga=2.252141577.1606775663.1650411573-2039575531.1649376333). |
| **PERCENTAGE OF FINAL GRADE:** | 50% |
| **HURDLE DETAILS:** | Not Applicable |
| **SUGGESTED WRITING TIME:** | 2 hours |
| **WORD COUNT:** | 2000 words |

Instructions

* This end of unit assessment task is available for 24 hours, with a suggested writing time of 2 hours. You may choose when to complete the task within this time frame.
* You are allowed to access all resources during the assessment, except for contract cheating sites, artificial intelligence content generation sites, resources that undermine the purpose of the assessment, and help from peers or others (unless specified otherwise in the assessment instructions). It is important that you complete this task individually. Your submission will be reviewed to detect contract cheating, collusion, and/or plagiarism.
* The end of unit assessment task will be released in the CloudDeakin unit site under a dedicated End of Unit Assessment module at the date and time scheduled in the University Exam T2 2024 Exam timetable.
* This end of unit assessment task constitutes **50%** of your assessment in this unit.
* This end of unit assessment task comprises **4** questions. You are required to answer **ALL 4** questions**.**
* Download the assessment paper and review the questions. You are required to type all your answers into a separate single **Microsoft Word document (.docx)**. Save your answer document on your computer using the following naming convention: **[Student ID]\_*[Unit Code]\_*EOUA**. For example: **216123123\_UNITCODE\_EOUA**. Once completed, submit the answer document to the **End of Unit Assessment Submission folder** on the CloudDeakin unit site.
* Late submissions and/or submissions in a file format other than Microsoft Word (.docx) **will not** be marked.
* **Remember to save your work regularly.** If you encounter any technical issues with CloudDeakin, please contact the [IT Service Desk](https://www.deakin.edu.au/students/help/it-help/send-a-support-ticket) online or via phone (1800 463 888; +61 5227 8888 if calling from outside Australia) and record your ticket number. This evidence is necessary for any [Special Consideration](https://www.deakin.edu.au/students/study-support/assessments-and-examinations/special-consideration?SQ_VARIATION_2507602=0) application due to technical issues during the end-of-unit assessment period.

**MIS761 Cyber Security Strategies**

***Trimester 2 2024***

**Final Assessment Task – End of Unit Assessment**

**Case Study**

***TechStream*** Solutions is a leading enterprise software solutions provider, dedicated to offering state-of-the-art business automation tools to companies around the globe. With the commitment of free software updates and responsive support services, they have positioned themselves as a trusted partner in the industry. ***TechStream***'s founder and CEO, Liam, stands behind every software module they release, ensuring it meets the top-notch standards the B2B sector demands. Launching in 2015, Liam transformed his deep-seated passion for technology and innovation into a business that caters to the specific needs of modern enterprises.

***TechStream***'s primary operations revolve around an annual tech conference held in Melbourne, allowing businesses to get firsthand experience of their groundbreaking software modules. Through ***TechStream***’s interactive B2B portal, corporate clients can browse, demo, and purchase tailored software solutions that cater to their unique challenges. The purchasing process is marked by an initial online inquiry, following which clients receive a comprehensive consultation from Liam or one of the senior solutions architects. Every software license from ***TechStream*** comes with a detailed onboarding process, ensuring smooth integration and deployment. And, for those looking to customize or scale their solutions, Liam's team is always on standby, ready to assist.

Building on this solid foundation and recognizing the evolving needs of businesses, ***TechStream*** recently embarked on an ambitious strategic shift. This shift is part of ***TechStream*** 's strategy to pivot towards offering cloud-based solutions tailored for small to medium enterprises, tapping into a growing segment of businesses that prefer scalable software tools without the traditional upfront costs. With the digital transformation wave in full swing, ***TechStream*** 's innovative approach positions them as a key player in the B2B software sector.

Being at the forefront of such transitions comes with its challenges. In an industry where even minor software vulnerabilities can break trust, ***TechStream*** prides itself on its track record of reliability and the safety of its digital tools. Their software undergoes rigorous testing and evaluations, a testament to their commitment towards delivering unparalleled service quality.

In a global marketplace, adhering to best practices isn't just about meeting standards; it's about weaving them into the company's fabric. ***TechStream*** keeps a close eye on international cybersecurity guidelines, as well as regional data handling protocols. With clients hailing from various jurisdictions, ensuring each software module respects both global and local nuances become paramount.

Understanding that businesses have varying operational demands, ***TechStream*** offers modular solutions. For instance, those in data-sensitive industries can expect robust protocols, while businesses focused on collaboration might find features that facilitate teamwork without compromising on data security.

As ***TechStream***'s focus broadened with its cloud-based solutions, the pace of growth introduced complexities, especially in its digital transition. The evolution of ***TechStream***, tailored to serve small to medium enterprises, experienced remarkable growth. But with this swift expansion, challenges were inevitable. Notably, the entirety of this digital evolution was shouldered by the IT department, which found itself at the very heart of ensuring software reliability and addressing safety concerns. This pivotal role magnified the pressures and responsibilities faced by the team, as they became the solitary custodians of the company's digital integrity.

Amidst this evolutionary phase, James, the company's CIO, found himself becoming the primary touchpoint for all decisions related to information systems. A technical savant, James was more than capable of addressing the intricacies of the software. Yet, navigating the confluence of business strategy and IS posed its dilemmas, often leaving him overwhelmed with the system-wide responsibility.

As ***TechStream*** ventured forth, it embraced several changes: innovative features, updated software modules, and expanded client services. However, the sheer pace of these changes sometimes overshadowed the necessity to reflect on their broader implications.

At the board level, meetings predominantly revolved around financial performance and market outreach. Rarely did the discussions delve deep into the core of the company's digital infrastructure. This approach occasionally left the technical team with a feeling that their efforts, both in terms of potential and inherent risks, weren't fully recognized.

Aware of these intricacies, ***TechStream*** has initiated a cybersecurity strategy:

**Threat Monitoring**: A specialized team keeps a pulse on the cyber landscape, identifying potential threats and vulnerabilities.

**Employee Training**: Periodic sessions to arm the staff with knowledge about cyber threats and best practices.

**Zero Trust Architecture**: Implementing stringent access controls and authentication processes.

Building on this, they're formulating a cybersecurity framework:

**Data Integrity**: Evaluating cryptographic measures and secure storage to ensure data sanctity.

**Routine Audits**: Ensuring their cybersecurity measures remain contemporary through regular security checks.

**Incident Response Plan**: Outlining rapid response protocols for potential breaches.

As ***TechStream*** continues its journey, the nuances of striking the right balance between innovation and security become ever more critical.

You are a cybersecurity consultant hired by ***TechStream*** in light of their rapid digital transition and the complexities that have arisen. After immersing yourself in the company's operations and working closely with James, the CIO, you've identified areas where the firm could strengthen its cybersecurity measures and operational integrity. Recognizing the pivotal role you play in aligning ***TechStream***'s goals with security best practices, James has tasked you with providing advice and suggestions in response to the following questions.**Question 1.**

As you delve into the intricacies of ***TechStream*** Solutions' operations and its information security governance, a closer look at Paragraphs 3-10 will provide valuable insights. These sections highlight both the strategic goals and the challenges the company faces, laying a foundation for you to understand its current governance scenario.

a) Identify the ***four*** key indicators of ***TechStream***'s ineffective information security governance.

**[13 Marks]**

**Answer below here**

b) Evaluate ***three*** potential negative impacts that might arise ***TechStream***'s highlighted business objectives with inadequate information security governance. *You should determine business objective and then evaluate the negative impact.*

**[12 Marks]**

**Answer below here**

**Question 2.**

***TechStream***, with its expansive digital footprint, faces potential security risks such as phishing and ransomware.

a) Briefly describe what phishing is and explain why it is difficult to manage this risk at ***TechStream***. Identify and discuss **two** different measures that can align with ***TechStream*** 's cybersecurity measures.

**[10 Marks]**

**Answer below here**

b) Briefly describe what ransomware is and explain why it is challenging for ***TechStream*** to manage this risk. Identify and briefly discuss **two** different measures that ***TechStream*** could implement to help manage the ransomware risk.

**[10 Marks]**

**Answer below here**

c) In the backdrop of ***TechStream***'s extensive digital operations and client interactions, examine the relevance of Virtual Private Networks (VPNs) as a protective shield for sensitive data. Provide a ‘plain language’ explanation of VPNs and their potential role in safeguarding ***TechStream***'s digital assets.

**[10 Marks]**

**Answer below here**

**Question 3.**

a) As **TechStream** transitions toward offering cloud-based solutions and expanding its digital operations, it is critical to prioritize the company’s information assets based on various risk factors. Below is a table outlining **Criterion Weights** for three key criteria and the importance of each asset in relation to those criteria. Calculate the **Weighted Score** for each asset, rank them in order of priority, and provide a justification for your ranking.

**Answer below here**

| **Asset** | **Criteria 1 Critical to Success** | **Criteria 2**  **Cost to Replace/Protect** | **Criteria 3 Public Image** | **Weighted Score** |
| --- | --- | --- | --- | --- |
| **Criterion Weight (1-100)** | 40 | 30 | 30 | 100 |
| Client Database | 0.9 | 0.8 | 1.0 |  |
| Proprietary Software Modules | 0.8 | 0.9 | 0.7 |  |
| Cloud Infrastructure | 1.0 | 0.9 | 0.9 |  |
| Employee Personal Data | 0.6 | 0.7 | 0.8 |  |
| Financial Systems | 0.7 | 0.8 | 0.9 |  |

**[15 Marks]**

b) As part of your cybersecurity assessment for **TechStream**, you are required to evaluate the potential risks associated with various assets. The following table outlines the vulnerabilities identified for three key assets, along with their likelihood and impact scores.

Calculate the **Risk Rating** for each vulnerability by multiplying the **Likelihood** by the **Impact**. Rank the vulnerabilities based on the **Risk Rating**.

**Answer below here**

| **Asset** | **Vulnerability** | **Likelihood (1-10)** | **Impact (1-10)** | **Risk Rating (Likelihood × Impact)** |
| --- | --- | --- | --- | --- |
| Client Database | Phishing Attacks | 8 | 9 |  |
| Unauthorized Access | 5 | 7 |  |
| Proprietary Software Modules | Unpatched Software | 6 | 8 |  |
| Software Exploits | 7 | 7 |  |
| Cloud Infrastructure | DDoS Attacks | 6 | 9 |  |
| Poor Access Control | 4 | 8 |  |

**[10 Marks]**

**Question 4.**

**TechStream** is planning its disaster recovery strategies and has set goals for how quickly services should be restored, how much data loss can be tolerated, and the required availability of its services.

Below are the recovery targets for two key systems:

System 1: Customer Database

* RTO (Recovery Time Objective): 2 hours
* RPO (Recovery Point Objective): 30 minutes
* RSL (Recovery Service Level): 99.9%

System 2: Online Order Management

* RTO (Recovery Time Objective): 4 hours
* RPO (Recovery Point Objective): 1 hour
* RSL (Recovery Service Level): 99.5%

Questions:

a) What does the RTO mean for each system? If the Customer Database is down for more than 2 hours, what impact could this have?

**Answer below here**

**[6 Marks]**

b) What is the significance of the RPO for both systems? If the Online Order Management system has an RPO of 1 hour, how much data loss is acceptable?

**Answer below here**

**[7 Marks]**

c) Explain the RSL for each system. Which system has the higher availability requirement, and why might this be important for **TechStream's** operations?

**Answer below here**

**[7 Marks]**

**- END OF EXAMINATION -**