ASSIGNMENT BRIEF

HTU Course No: 00203280	**HTU Course Name:** Security
BTEC Unit Code: D/618/7406	**BTEC UNIT Name:** Security

Student Name/ID Number/Section	
HTU Course Number and Title	00203280 Security
BTEC Unit Code and Title	D/618/7406 Security
Academic Year	2023-2024 Summer
Assignment Author	Isra' Hasan
Course Tutor	Isra' Hasan - Sami Almashaqbeh - Fawaz Khasawneh
Assignment Title	Sofix Company
Assignment Ref No	1
Issue Date	04/08/2024
Formative Assessment dates	From 05/08/2024 to 22/08/2024
Submission Date	04/09/2024
IV Name & Date	Hazem Arabiyat 03/08/2024

Submission Format

Report guidelines:

In your report, you should make use of headings, paragraphs, and subsections as appropriate. The expected word limit is about 5000 words (recommended 20-25 pages including appendix), although you will not be penalised for exceeding the total word limit. Do your best to be within the word limit. Your report should be:

1. In a form of a soft copy submitted via the URL below.
2. Written in a formal business style using single spacing and font size 12.
3. Must be supported with research and referenced using the Harvard or APA referencing system.
4. An individual written detailed report (word format) that provides thorough, evaluated, or critically reviewed technical information on all the points illustrated in the Assignment Brief and Guidance section.
5. Signed declaration form

Note: Soft copies submissions should be done through the university's eLearning system within the deadline specified above from below link: https://elearning.htu.edu.jo

Unit Learning Outcomes

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

LO3 Review mechanisms to control organisational IT security.

LO4 Manage organisational security.

Assignment Brief and Guidance

This assignment includes two Parts :
Part One: written exam the exam will take place on campus on the date 8/24/2024.

P1,P2,P3,P4,M1,M2,D1 are the criteria that will be covered in the exam.

Part Two: the report.

Sofix Company Scenario:

Sofix Company is a leading entity in the technical support of networks and security devices industry, renowned for its innovative solutions and exceptional support services. Since its inception, Sofix Company has quickly become a trusted partner for businesses seeking to enhance their network security and performance. Central to its success is the utilization of advanced IT infrastructure to ensure efficient operations, secure data management, and compliance with digital communication standards. Here is an overview of the crucial IT servers and systems used by Sofix Company.

Application Servers: Host various applications essential for managing network inquiries, customer feedback, and support ticketing systems. These servers ensure that customer interactions are handled promptly and efficiently.

Database Servers: Store a vast amount of data, including user profiles, network analytics, and interaction histories. These are vital for providing personalized support and insights.

Web Servers: Serve the company's website and client dashboards, ensuring a seamless and responsive user experience for accessing reports, support tools, and analytics.

Communication Servers: Manage all forms of communication, including emails and notifications, facilitating effective interaction between the team and clients.

File Servers: Allow for the organized storage and sharing of documents, templates, and support materials.

Backup and Recovery Servers: Essential for data integrity, these servers handle regular backups and swift recovery in the event of data loss.

Firewalls and Security Servers: Protect the network from unauthorized access and various cyber threats.

Monitoring and Management Servers: Monitor the health and performance of IT infrastructure, enabling proactive management and maintenance.

Compliance and Audit Servers: Help maintain compliance with relevant network security regulations and standards, storing logs and records for audits.

Customer Interaction Points:

Online Dashboard: The primary interface for clients to monitor their network metrics, access support, and manage their accounts.

Mobile Apps: Provide clients with the convenience of managing their network support needs on the go.

APIs for Integration: Allow business clients to seamlessly integrate Sofix Company's services into their platforms.

Payment Systems: Offer a variety of payment methods for services, including online and contactless options.

Your Role:

You have been appointed as the Information Security Risk Officer at Sofix Company, a leader in network and security device support services. Your primary responsibility is to assess the security landscape of the company's existing infrastructure and processes to enhance the overall security and reliability of operations. A key aspect of your role involves ensuring the confidentiality, integrity, and availability (CIA) of all data and services provided by the company. Through a detailed security assessment encompassing applications, systems, policies, procedures, and devices, the following observations have been made:

Observations:

1. Employees at Sofix Company often use their devices for both work and personal activities, which heightens the risk of malware infections. Many devices lack up-to-date anti-malware solutions, and crucial updates for operating systems and applications remain pending. Additionally, the company does not have a Host-Based Intrusion Detection System (HIDS) in place to monitor and report malicious activities. Several workstations have unauthorized software, including cracked versions. While measures have been

taken to disable external storage devices, resistance from staff is obstructing security assessments due to the absence of formal authorization.

2. The corporate network is divided into two segments: one for internal access and another for external access. However, there is insufficient segregation between critical servers, which increases the risk of sensitive data breaches. Access to sensitive departments, such as HR and Finance, is poorly controlled, leaving them vulnerable to internal and guest network traffic. Additionally, the firewall solutions have expired licenses, which further compromises network security.
3. Users of Sofix Company's platforms can store personal and sensitive data, including payment information, which is transmitted over an insecure connection, relying on outdated cryptographic methods like MD5 for integrity checks, raising serious concerns over data security during transmission. While regular backups are performed, including customer data, one critical backup is stored on a public cloud service without encryption at rest. Although transmission is secured with SSL/TLS, the data remains vulnerable at rest, utilizing the weaker SHA1 for integrity checks.
4. The discovery of the use of an outdated OpenSSH version susceptible to a severe vulnerability underscores the risks associated with remote administration services. This highlights the need for immediate patching and the implementation of more stringent access controls.
5. A reported incident involving a phishing attempt that nearly led to ransomware infection points to a critical need for improved email security measures and employee awareness training to identify and mitigate such threats.
6. Physical security controls at the data center are found to be lacking, with unsecured access points, inadequate environmental controls, and the absence of essential disaster recovery infrastructure such as UPS systems or fire suppression mechanisms.
7. Unregulated VPN access granted to third parties without proper oversight and the expiry of digital certificates for VPN connections expose the company to increased risk of data breaches.
8. Observations of poor password management practices among employees, including the physical writing down of passwords, underline a significant lapse in security awareness and control.
9. A general absence of comprehensive security, data handling, and incident response policies, combined with inadequate training to counteract social engineering attacks, raises significant concerns over Sofix Company's ability to adhere to industry standards and regulations like GDPR.
10. Employees have fallen prey to elaborate phishing campaigns. Attackers, posing as trusted entities, have successfully extracted sensitive information by exploiting human trust. These schemes range from direct email phishing to more insidious approaches using fake social media profiles, aiming to infiltrate the company's secure environment.
11. The company has been subjected to Distributed Denial of Service (DDoS) attacks, aimed at crippling its online platforms. These external threats not only disrupt services but could also mask more sensitive data breach attempts or malware insertions, aiming to exploit any moment of weakness.
12. The danger also lurks from within, with instances of employees misusing their access for unauthorized data access or manipulation, threatening the company's data integrity and exposing it to severe regulatory and reputational damage.
13. The company's use of glass doors for its main entrances, without adequate reinforcement, presents a clear physical security risk. This vulnerability could potentially allow unauthorized physical access, leading to direct access to sensitive areas such as server rooms, posing a critical threat to the company's operational security.
14. The lack of effective surveillance and modern access control systems at Sofix Company's premises has further exacerbated its security woes. Critical areas, particularly the data center, lack comprehensive monitoring, relying instead on outdated physical key systems susceptible to duplication, inviting unauthorized access.
15. External parties have been provided VPN access without proper security measures or oversight. The use of expired digital certificates for these connections reflects a critical lapse in maintaining up-to-date encryption standards, posing a direct threat to network security.
16. The company's Wi-Fi networks, used by employees and guests, lack sufficient security measures, providing a potential entry point for cyber attacks aimed at intercepting sensitive information.
17. Sofix is reviewing its risk assessment procedures due to increased client data and evolving cybersecurity threats. The company conducts annual risk assessments to identify threats using internal audits and industry reports. Risks are evaluated through qualitative risk management methods, as outlined in the

Silver Star Mines Risk Register, and controls such as firewalls, encryption, and multi-factor authentication are in place. However, the last update to these procedures was six months ago, and recent technological advancements and new threats may not be fully addressed. The company needs to assess whether its risk management practices and existing controls effectively address current and emerging risks and if the frequency of updates is adequate.

Your Task:

As the newly appointed Information Security Analyst at Sofix Company, your task is to conduct a thorough security assessment focusing on the identified risks. Your findings will form the basis of a detailed report and presentation aimed at the CEO, highlighting vulnerabilities, potential impacts, and recommending strategic measures to enhance security and reliability. Your ultimate goal is to ensure the confidentiality, integrity, and availability (CIA) of data and services across Sofix Company's operations.

PART 2:

A. Propose a method to assess the company system's possible risks, their likelihood (rare, unlikely, possible, likely, and almost certain), and exploitation consequences (insignificant, minor, moderate, major, catastrophic, and doomsday). And finally determine the Risk level (Extreme, High, Medium, and Low) and suggest controls (countermeasures) to protect and improve the security of most critical assets. As in Silver Star Mines Risk Register

Asset	Threat/ vulnerability	Existing Controls	Impact	Likelihood	Level of Risk	Suggested control

B. Explain data protection regulation that Sofix Company has to implement. Also, explain what procedure Sofix Company has implemented to achieve the listed regulation.

C. How does the organization identify, evaluate, and manage risks, and how frequently are these risk assessment procedures reviewed and updated to ensure they address current and emerging threats?

D. Summarize the ISO 31000 risk management methodology and its application in Sofix Company

E. What do we mean by IT security audit? What is its impact on Sofix Company?

F. Recommend how IT security can be aligned with organizational policy, detailing the security impact of any misalignment.

G. Discuss the roles of stakeholders in Sofix Company to implement IT security audit recommendations.

H. Design Three security policies for Sofix Company one of the policies is a disaster recovery plan.

Your design should include the following:

1. What is the policy and its scope.
2. Its importance.
3. Evaluate the tools used in the policy.

Learning Outcomes and Assessment Criteria			
Learning Outcome	**Pass**	**Merit**	**Distinction**
LO1 Assess risks to IT security.	**P1** Discuss types of security risks to organisations. table **P2** Assess organisational security procedures.	**M1** Analyse the benefits of implementing network monitoring systems with supporting reasons.	**D1** Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
LO2 Describe IT security solutions.	**P3** Discuss the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs. **P4** Discuss, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve network security.	**M2** Propose a method to assess and treat IT security risks.	
LO3 Review mechanisms to control organisational IT security.	**P5** Review risk assessment procedures in an organisation. **P6** Explain data protection processes and regulations as applicable to an organisation.	**M3** Summarise an appropriate risk management approach or ISO standard and its application in IT security. **M4** Analyse possible impacts to organisational security resulting from an IT security audit.	**D2** Recommend how IT security can be aligned with an organizational policy, detailing the security impact of any misalignment.
LO4 Manage organisational security.	**P7** Design a suitable security policy for an organisation, including the main components of an organisational disaster recovery plan. **P8** Discuss the roles of stakeholders in the organisation in implementing security audits.	**M5** Justify the security plan developed giving reasons for the elements selected.	**D3** Evaluate the suitability of the tools used in the organisational policy to meet business needs.