M T W T F S ASSIGNMENT 1 DATE: __/__/____

MUNEEB IQBAL
SP22-BCS-030
BCS-6C

Question 1

1) **Do you think this event was caused by an insider or outsider?**

I believe an outsider was responsible for this incident. It appears that the problem is widespread and not exclusive to any one person or department because several people, including Bob and Erin, are having identical issues with their PCs. The possibility that the issue is connected to a malicious email or attachment is suggested by the fact that Amy's computer stalls when she clicks on a dubious email attachment.

2) **Other than installing virus and worm control software, what can SIS do to prepare for the next direction?**

→ To guarantee that vital data can be promptly restored in the event of an attack, put in place a strong backup and disaster backup plan.

→ To find and fix any possible vulnerabilities in their systems, do routine security audits and vulnerability assessments.

(M)(T)(W)(T)(F)(S) DATE __/__/__

→ Employees should receive frequent security awareness training to help them recognize potential security threats and learn safe computer practices.

→ Implement an email filtering system to block suspicious emails.

3) Do you think this attack was the result of a virus or a worm?

The attack causing similar issues and spreading quickly, may be caused by a self-replicating malware like a worm. Amy's computer freezes after clicking on suspicious email attachments, indicating worms spread quickly and automatically without human intervention, confirming the case study's rapid spread.

Question 2

1) How do Fred, Glady, and Charlie perceive the scope and scale of the new information security effort?

Fred initially hesitates to invest in a comprehensive information security program due to cost concerns. However, as the conversation progresses, he begins to understand the importance of a thorough approach. Glady who has researched information security, is more aware of

M T W T F S DATE: __/__/____

the problem's severity and advocates for a comprehensive programs including a thorough review of policies and practices.

2) How will Fred measure success when he evaluates Glady's performance for this project?

Fred will asses the project's success by assessing its progress, including the creation of a robust information security Program, policy implementation, and security incident reduction. He may also assess the program's cost-benefit analysis and return on investments. Gra Glady's performance will be assessed for her leadership, Team management, and Effective communication.

3) Which of the threats discussed in this chapter should receive Charlie's attention easily in his planning process?

Charlie should prioritize insider threats, network threats, data breaches, and physical security threats in his planning process, as the worms affected the company's computer network resulting in lost production and expenses. The company's server and critical infrastructure are located in a

M T W T F S DATE: / /

controlled environment, highlighting these threats.

Question 3

UNAUTHORIZED ACCESS

The hacker gains access to network without permission. This is a serious security breach that can lead to further problems.

DATA THEFT

The hacker steals sensitive data, such as credit card numbers which can lead to identity theft and financial loss.

VANDALISM

The hacker damages the website, causing reputational damage which can harm the organization's outline presence and reputation.

MALICIOUS CODE

The hacker uses malware or viruses to harm the network. This can cause serious damage and compromise sensitive data.