Information Security - UE20CS346

SRN : PES1UG20CS825	NAME : PREM SAGAR J S	SEC : ‘H’

Case Study Assignment - 1

Q No	Answers
1	There seem to be multiple reasons why Target was susceptible to the security breach. ➢ Initially, Attackers got access to Target's systems via a third-party vendor with network access to Target. This emphasizes the necessity of vendor management and the need for firms to evaluate their third-party providers' security processes. ➢ Second, Target's network segmentation was ineffective, allowing attackers to move laterally and get access to critical information. ➢ Finally, Target did not discover the assault in time, allowing the attackers to take data for several weeks. Ultimately, it seems that the breach at Target was not simply a matter of bad luck, but rather a result of vulnerabilities in their security practices and the failure to detect and respond to the attack in a timely manner.
2	Target could have taken several steps to avoid being breached, including: ➢ Regular vulnerability assessments and penetration testing are carried out to uncover and resolve security flaws in their systems. ➢ Stronger access restrictions and monitoring systems are being implemented to prevent unwanted access to sensitive data.

- Ensuring that all software and systems are updated with the latest security patches and upgrades.

- Increasing staff awareness and training to detect and avoid phishing and social engineering attacks.

- Developing a more centralized and coordinated approach to cyber security across the organization, with clearly defined roles and responsibilities for all stakeholders.

Yet, Target may have been unable to take such activities due to a variety of technological and organizational restrictions.

These are some examples:

- Financial constraints: Strong security procedures may be costly to implement, and Target may have been reluctant or unable to dedicate adequate money to cybersecurity.

- Target's IT architecture may have featured antiquated systems that were difficult to modify or protect, making them exposed to attack.

- Target may have lacked the internal competence to successfully detect and mitigate cyber security threats, or they may have relied too heavily on third-party contractors to handle their security.

- Decentralized structure: Target's business groups may have had diverse cyber security goals and methodologies, making it difficult to develop a centralized and coordinated plan.

Ultimately, the Target cyber breach emphasizes the need of investing in strong cyber security measures and taking a proactive approach to identifying and mitigating cyber security threats.

3	Target’s reaction to the occurrence has both advantageous and disadvantageous aspects. Below is analysis of Target’s successful and unsuccessful actions: What Target Did Well: ➢ Target’s CEO issued an immediate apology for the incident, reassuring consumers and stakeholders that the firm was treating the problem seriously. ➢ The corporation enlisted the help of a third-party forensics firm to examine the breach and uncover the flaws in their systems that allowed the assault to take place. ➢ Affected clients were provided free credit monitoring services by Target. ➢ Target made significant investments in security changes, including as deploying chip-and-PIN technology for credit card transactions, enhancing network segmentation, and expanding their security staff. What Target Did Poorly: ➢ Target took too long to identify the breach, giving the hackers plenty of opportunity to grab data and undermine the company’s systems. ➢ Target’s early response was inadequate, with staff downplaying the gravity of the breach and failing to properly communicate with consumers and the general public. ➢ Target’s response to the breach was disjointed and uneven, with contradictory information coming from

	various areas inside the firm. ➢ As proven by later data breaches at Target and other shops, the company’s attempts to remedy the breach did not go far enough to prevent similar instances in the future. Ultimately, while Target took several critical actions to resolve the hack and avoid future assaults, the firm fell short in other areas.
4	Target’s board of directors holds the ultimate responsibility for the cyber attack and its aftermath. They are accountable for supervising the organization’s risk management and guaranteeing the implementation of adequate cyber security protocols to protect confidential information. The case study, on the other hand, argues that the board did not offer adequate supervision or prioritize cyber security, which led to the intrusion. ➢ After the breach, if I were a member of the Target board, I would advocate for various measures to prevent similar issues from happening again.These changes could comprise: ■ Target’s cyber security policies and processes are being reviewed and improved to ensure that they are robust and effective. ■ Assuring that the organization has the resources and knowledge needed to address cybersecurity threats, including the appointment of specialist cybersecurity employees. ■ Creating a regular reporting and monitoring system for cybersecurity threats to the board.

	■ Conducting frequent cybersecurity training and awareness campaigns for staff. ■ Assessing and upgrading the company's crisis management strategies to guarantee a complete response to cybersecurity events. To sum up, the Target company's board of directors is accountable for the security breach and its consequences. If I were a member of the board, I would advocate for improvements to Target's cybersecurity measures, such as policies, processes, resources, reporting, monitoring, staff education, and crisis management plans.
5	The cyber attack on Target holds valuable lessons on how to prevent and handle similar breaches: ➢ Cybersecurity is the responsibility of every member of the organization, regardless of their position, and they should all recognize its significance and their duty to safeguard the company's information assets. ➢ Invest in security technology and infrastructure: Companies must budget enough to implement and maintain effective security measures such as firewalls, intrusion detection systems, and encryption protocols. ➢ Develop effective incident response plans: Companies must have a plan in place to respond to any cyber breach as soon as possible. The strategy should include procedures for identifying and containing the breach, notifying appropriate parties, and mitigating the effect of the breach. ➢ Frequent monitoring and testing of security measures can help discover system flaws and vulnerabilities, allowing firms to rectify them before an actual breach happens.

	➢ Collaborate with outside partners: Companies should collaborate with outside partners such as law enforcement, cybersecurity specialists, and other organizations to exchange information and best practices for avoiding and reacting to cyber attacks. ➢ Transparency and prompt communication with impacted parties: It is critical to convey the breadth and effect of the breach to affected parties in a clear and transparent manner, and to give timely updates as the situation changes. Organizations may lessen the likelihood of cyber breaches and the effect of any events that do occur by following these lessons and establishing comprehensive security measures and response strategies.
6	Directors play an important role in supervising cyber security at their firms. They must ensure that their organization has a strong cybersecurity policy in place to defend against any cyber threats. Some specific actions that directors can take to supervise this domain include: ➢ Establishing a clear cybersecurity plan: Directors should collaborate with management to create the organization’s cybersecurity strategy, which should include policies and procedures to handle cybersecurity threats. ➢ Provide enough resources: Directors must ensure that the business has the required resources, such as a budget, employees, and technology, to properly implement its cybersecurity policy. ➢ Reviewing cybersecurity measures on a frequent basis: Directors should examine the organization’s cyber security measures on a regular basis to ensure they remain effective and up to date. They should also keep

	an eye on cybersecurity threats and trends and change their approach accordingly. ➢ Cybersecurity awareness should be promoted throughout the business, ensuring that all workers understand the importance of cybersecurity and their responsibility in defending the firm. ➢ Regular cybersecurity training: Directors should make sure that all workers receive frequent cybersecurity training to assist them detect possible dangers and respond to a cyber assault. ➢ Interacting with external stakeholders: To stay up to speed on best practices and new risks, directors should communicate with external stakeholders like as regulators, law enforcement, and cybersecurity specialists. Overall, directors should take a proactive approach to cybersecurity and work closely with management to ensure that their organization is well-protected against potential cyber threats.
7	There are several approaches that companies can adopt to improve their protection against cyber attacks and strengthen their response after a security breach occurs. ➢ System updates and patches should be performed on a regular basis to fix vulnerabilities that hackers may exploit. ➢ Adopt multi-factor authentication: Businesses may strengthen their security by requiring users to give various forms of identity before accessing a system. ➢ Educate staff on cybersecurity: Businesses should engage in employee training to educate their personnel about

	cybersecurity dangers and best practices for preventing data breaches. ➢ Businesses can employ monitoring technologies to spot odd behaviour on their networks and systems, which could suggest a possible breach. ➢ Establish an incident response strategy: To prepare for a breach, it is important for businesses to create a plan for incident response that outlines the steps to be taken. This plan should be regularly reviewed and updated. ➢ Collaboration with external cybersecurity experts: Businesses can benefit from collaboration with external cybersecurity experts who can give best practices advise and assistance in responding to breaches. ➢ Increase communication and transparency: In the case of a breach, companies should emphasize clear and timely communication with customers, stakeholders, and the public in order to preserve confidence and prevent reputational harm.