COMPUTER NETWORK SECURITY

CASE-STUDY-1

iPREMIER CASE STUDY

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

DATE:16/10/2022

ASSIGNMENT QUESTIONS:

1)The iPremier company could have responded in a more challenging way. If I was in Bob Turley's position, I would have dealt with these situations slightly different manner. Of course, I would have panicked the first few minutes after listening to the news about the attack. Then I would have called the respective people working in the IT department to check the packets coming from unauthorized network or IP address. I would have asked those people to track the mails which contains the text "HA". Bob Turley got tensed and didn't have a proper plan to execute as soon as he heard the news about the malfunctioning of the website. He didn't have proper strategy to deal with such kind of situations as he was new to that company. He didn't call the right people at that time. If I was in Bob Turley's place, I would have directly called the security systems head and would have asked him the details about the attack and would have asked if he had any idea how they all could overcome such kind of situations. Instead of asking the CEO and a lawyer’s suggestion I would have asked a cybersecurity analyst about how to deal with such kind of situations. I would have thought of how to find what the actual problem is rather than thinking why it happened and thinking about what the higher authorities would think about me. After knowing that the attack was a DDos attack I would try to find all the sources which are sending the packets more frequently. My state of mind would be clear and the intentions of getting past this attack would be crystal clear unlike Bob Turley.

2)As CEO told Bob Turley that the company would eventually suffer from a deficit in operating procedures had a huge impact this attack. Because of the financial crisis undergoing by the company, they didn’t fix the security parameters which led to a breach in the security in the form of DDos attack. Because of this deficit the firewalls were not made stronger and the protection given by that firewall could be broken easily. The maintenance of the security is not up to the mark. Attackers could easily get in the servers or systems without getting noticed at all. If the company had spent some amount on the security systems of the company, then this attack would not have happened at all. If the firewall was made stronger than ever then it would have been very difficult for the attacker to pass through that particular firewall and eventually this attack would not have been taken place. The company should have an efficient system to detect all the signs prior to an attack. Maintenance system should be more active and the people who are working in that particular department should always keep an eye on the data or security breaches

3)We all know about the quote “prevention is better than cure”, all the companies should follow this when it comes to cybersecurity threats and attacks. iPremier company should detect the attacks before it actually takes place. The company should make the firewall stronger than before and keep 24 hr surveillance on the network. By having strong security systems, the cyber-attacks on that particular company would comparatively less. The security and IT teams should check if there are any vulnerabilities or weakness in their systems and should update or patch up all the issues. The company should buy additional resources in order to buy some time in case of any attacks takes place. The company should constantly keep a check on the half-opened connections and make sure they all close after a certain time limit. The half-opened connections lead to DDos attack, so we need to set up a valid TTL for all the half-opened connections. These are the changes that iPremier company can make to face this attack in future.

4) In the aftermath of the attack, I would be worried about the data loss or any data would be stolen from the servers. I would also think about whether the data in the server is manipulated or not. All these questions would be running in my mind. So, what I would do is shut down the system or at least disconnect the internet from public internet for some time. Then update all the security systems in order to prevent these types of attacks in future. Then the firewall should be strengthened even more. Then we have to track down if there were any intrusions taken place. I also check if the data in the servers are modified or not. If the data is modified then we have to change all those data to the original data. After performing all these above-mentioned tasks, I would restart the servers again. By doing this we can prevent the attack happening again. I would also try to

track down the attacker if possible and try to avoid the connection requests sent by that system. These are the actions I would like to recommend to prevent the attacks in future.