PES UNIVERSITY
COMPUTER NETWORK SECURITY
iPremier ASSIGNMENT

Aayush Kapoor PES2201800211

1. **How well did the iPremier Company perform during the seventy-five minute attack? If you were Bob Turley, what might you have done differently during the attack?**

From my point of view, the company iPremier was not prepared for any attack that will lead to an intrusion and they were in a confused state during the seventy-five minute attack, but everyone from CEO to new ops engineer did a decent job to prevent the attackers from stealing the customers credit card number and other information.

As for being Bob Turley, I would have called Qdata to pull the plug and disconnect the website as their firewall had been breached through and not via some website bug. I would take this step so that the attackers could not steal the customers information from the website. And this information was brought to Bob Turley's attention, when Joanne Ripley asked for 24/7 support from the Qdata. Secondly, I would offer more support to Joanne Ripley as she worked through the identification and fixing of the problem at hand.

2. **The iPremier Company CEO, Jack Samuelson, had already expressed to Bob Turley his concern that the company might eventually suffer from a "deficit in operating procedures". Were the company's operating procedures deficit in responding to this attack? What additional procedures might have been in place to better handle the attack?**

Yes, the company was deficit in operating procedures. The Business Continuity Plan (BCP) was out of date and they did not train the employee with it. Lots of people on the call list did not work there because of iPremier's intense job filtering. New technology has come since the BCP was written. Turley did not check the Disaster Recovery Plan (DRP) and Incident Response Plan (IRP) thinking that as a public-listed company, iPremier had such plans.

Like above the plan was outdated, hence quarterly they should update the plan and train the employee semi-annually so that they are on their feet when such an attack happens again and not be in a confused state. They should have a third-party cybersecurity team to analyze the website and give them reports or alert them when an attack happens.

3. **Now the attack has ended, what can the iPremier company do to prepare for another such attack?**

- First and foremost is to trace the attacker and check whether the customer's information is breached so that people do not lose any trust in them as they pay a very high price for the items sold by the company.
- Secondly, they can upgrade the firewall and their security system and move to a better IT service provider as Qdata was not very secure in providing the security to iPremier.
- Now since the attack has come to an end, they should update the backup plan like DRP and IRP.

4. **In the aftermath of the attack, what would you be worried about? What actions would you recommend?**

- I would be concerned about the breach of the database, such that the customer's information is not misused for embezzlement of their wealth after the attack, hence the customers losing the trust in the company iPremier.
- Engage with law to identify the attackers, seek legal counsel and lastly document the breach like how the company breached, what caused it, what did we do post-breach and so on.
- Second as stated above try to update the DRP and IRP or in simple words backup plan for future attacks and also train employees in such cases.
- Strengthen the security and firewall of the company by installing the latest security technologies and improving the website program to avoid any website hacking via XSS or CSRF attacks.
- Approach a third-party company for analysis and assessment of the website for further enhancement of the security.
- Working a plan to show the law enforcement and the public that your intentions are good and thereby reducing fallout or affecting the stock of the company.