SRN : PES1UG23CS433
Name : Pranav Hemanth

Question #	Your Answer
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?	In the first 75 minutes of the attack iPremier had a mixed response. They responded well to some issues while making huge mistakes on some others. This crisis exposed the unpreparedness of the company in case of a cybersecurity incident, poor communication internal to the company and with external stakeholders, and a lack of clear hierarchy while managing a crisis. In terms of technical they were lacking as they didnt have any SOPs, IRPs or playbooks to aid in a crisis such as this. They did not have robust logging or new gen firewalls and IDS systems. They also had poor communication between the higher position executives during the crisis. All this led to a chaotic response during the crisis. Bob Turtly, being the CIO should have been more rational and forthcoming in his response to the crisis. When faced with different options and opinions from the legal counsel, the CTO, Operations Head and CEO, Bob should have taken stronger steps to ensure the crisis didnt last as long. As Bob turtley i would have: - Created a ‘war room’ to ensure complete and transparent communication between all important heads to ensure fast decisions and prompt action - Recommended for creation of a temporary hierarchy of command to prevent slowdowns in action - Focused on clearly communicating to all stakeholders (including customers) to prevent any possible compromise to infrastructure and data
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 deficient in responding to this attack? What additional procedures might have been in place to better handle the	iPremiers operating procedures were deficient and almost non existent. They did not have a crisis playbook, any incident response plans or SOPs for management of a crisis. The CEOs warning of an absence of procedure was clearly seen during the crisis. The major loopholes in

attack?	the companies cyber resilience policies included: - No updated business continuity plan or incident response plan - Poor logging and monitoring of alerts - Overdependence on third party infrastructure partners - Qdata - No DDoS mitigation plans - No security training of employees - No clear idea of assets and inventory If these procedures were present during the crisis, it could have been tackled with close to no losses in operation or assets. The main policies and plans that iPremier could have benefitted from is a tested IRP, SOP and cyber crisis trained and aware employees. Additionally we can look at NIST's CSF for the gaps to address that perfectly fit this case study. As a company iPremier had to focus on: 'Identify', 'Protect', 'Detect', 'Respond' and 'Recover' strategies recommended by the NIST framework.
Now that the attack has ended, what can the iPremier Company do to prepare for another such attack?	As we can see in the part B of the case study, the company did a good job at communicating the event to stakeholders and pledging to strengthen security to prevent such a crisis again. A robust plan to prepare for another attack could include: - Appointing a CISO to take charge during such a crisis and more importantly create policies and plans for quick response to such attacks - Implementing robust logging of activity on machines to identify and prevent future attacks - Improve visibility of assets and avoid Shadow IT - Reduce over reliance on external infrastructure vendors such as Qdata for response during an attack and taking responsibility for the data and services of the company. - Creating and doing drills with a comprehensive IRP. Training of staff and sensitizing on such issues is also very important - Audit procedures often to ensure

	playbooks and training doesnt get obsolete and you are always as prepared as can be for an attack A hardened procedure in the company can help save a lot of loss and hardship if (when) future attacks were to manifest.
In the aftermath of the attack, what would you be worried about? What actions would you recommend? Consider the prevalence and sophistication of DDoS attacks and proliferation of DDoS attack kits in the Dark web.	As we saw in Part C of the case study, the major worry in the aftermath of the attack would be to flush out any persistent APTs in the systems. As Joanne ripley predicted there was such a virus which caused iPremiers machines to aid in the attack of its competitor, complicating the crisis further. We saw that the DDoS attack on iPremier was indeed a misdirection and the overall damage planned was much greater. Some major concerns to address would be: - Detection and Removal of all possible APTs from company systems - Trace for any possible data exfiltration or integrity compromise on the systems - Management of legal and reputational damage to the company - Co operate with the FBI proactively to get as much information about the attack on the competitor to address deficiencies in their system and manage legal repercussions for aiding in attack Here as we saw the measures taken by the company in Part B of the case study were not sufficient. Hence recommendations to implement in the company would be: - Follow Ripley's suggestion to rebuild the systems, not by shutting down all service but moving all operations as quickly as possible to new infrastructure. - Harden security measure by investing in stronger defense software such as better firewalls, IDS systems and locally owned infrastructure for operations. - Create a SIEM for robust monitoring of the companies digital operations and safety - Be radically transparent contrary to the suggestion of the CFO since the company's main clients were wealthy customers who valued trust. Hiding information of possible compromised

	could have hurt and completely killed the business of the company - Co operate with markettop and be proactive to help safeguard the entire industry from such attacks and as a return garner good reputation amongst people

Note: Your response should be type written in your own words.
There is NO one right answer.
Your responses should be succinct, crisp, cogent and well presented.
All references should be cited appropriately including from AI tools like ChatGPT.

References :

Answer 1 & 2 (Performance and Deficiencies):

- "The iPremier Company (A): Distributed Denial of Service Attack" by Robert D. Austin
- "4 Phases of Cybersecurity Crisis Communications" by PES University
- "Computer Network Security Case Study Slides" by Prasad Honnavalli, Prof. Preet Kanwal, Dr. Gokul Kannan Sadasivam, PES University
- "The 18 CIS Critical Security Controls" by Center for Internet Security
- "The NIST Cybersecurity Framework (CSF) 2.0" by National Institute of Standards and Technology, U.S. Department of Commerce

Answer 3 (Preparation):

- "The iPremier Company (B): Distributed Denial of Service Attack" by Robert D. Austin
- "Computer Network Security Case Study Slides" by Prasad Honnavalli, Prof. Preet Kanwal, Dr. Gokul Kannan Sadasivam, PES University
- "The 18 CIS Critical Security Controls" by Center for Internet Security

Answer 4 (Aftermath and Recommendations):

- "The iPremier Company (A): Distributed Denial of Service Attack" by Robert D. Austin
- "The iPremier Company (B): Distributed Denial of Service Attack" by Robert D. Austin
- "The iPremier Company (C): Distributed Denial of Service Attack" by Robert D. Austin
- "4 Phases of Cybersecurity Crisis Communications" by PES University
- "The Myth of Secure Computing" by Robert D. Austin and Christopher A.R. Darby
- "Computer Network Security Case Study Slides" by Prasad Honnavalli, Prof. Preet Kanwal, Dr. Gokul Kannan Sadasivam, PES University

- General knowledge of DDoS kits (supported by source material's mention of botnets and sophisticated attacks).
- ChatGPT and Gemini, used as a tool to enhance understanding of reference materials