Name: Vishwas M
SRN: PES2UG20CS390
Case Study: The Phoenix Project

Question #	Answer
1	ITS (Information Technology Services) main role was to plan and coordinate central Information Technology (IT) structure, information security, application and support. The agenda of this ITS was to look after the servers in UVA. There were servers more than 100 based on various workgroups. Apart from these servers the university had thousands of servers in the campus used by the students. In all these computers and servers IST had to keep an eye on the patches. ITS had to update the patches frequently and had to rectify the mistakes or any bugs or issues if exists in any of the computers or the servers in UVA. However, in this case ITS had very little knowledge about these patches or updates in all the computers or servers in UVA. ITS had to check if there is an intrusion in the system or databases. If there is an intrusion then at what level is the intrusion taken place. ITS checked if there are any data breach or data loss in the servers or in any of the computer.

2	As we can observe from the recent past years when it comes to cybersecurity hacks, Universities are becoming the favourite snack for the hackers to feed on. Universities are becoming the famous snack for hackers because of their openness and decentralized nature. Universities have a lot of research papers and intellectual property which are more valuable than other information. Universities also contain a large store of PII and financial information. Apart from all these information, universities also contain the personal information of students and employees. Universities are the third most attracted place for the hackers to hack after health care and retail where the attackers are targeting the financial assets of the employees.
3	The common attack methods used are: a) Spear phishing b) Unpatched systems c) Zero-day attacks In Spear Phishing attack, the attacker sends malicious emails or files to the victim computer and when the victim downloads or opens those malicious files, then the attack will be successful. When the victim downloads those files, the virus will spread across the systems and eventually spread across the university. In spear phishing, the attacker will

	send malicious emails only to some particular employees instead of sending it to everyone. The advantage of doing this is to not let the spam detector to find those files and filter them out. Unpatched systems are systems which are not patched properly. The systems are not updated to the latest versions. If the patches are not cleared then it will pave the way for the hackers to hack as the systems will be vulnerable. Zero-day attacks are attacks which says the number of days the victim got to know about the attack.
4	The five objectives are: 1) We have to detect whether there is any intrusion. If there is any intrusion, then we have to find the level of intrusion. We have to find if there were any data breach or data loss. We have to perform all the tests to get to know about all these information in depth. 2) We have to come up with a remediation plan as soon as possible. The main agenda of this remediation plan is to come up with an idea to secure the university with a new security system. Going dark would be one

	of the first step taken by the university in this remediation plan. 3) After planning the remediation plan, in this step we are going to execute that plan. Tracking the foreign activities happening in the systems. Then we have to identify all the servers or the workstations that are affected by data breach or data loss or intrusion. Then we have to set new passwords and login credentials. By doing this all the employees and the students can have new credentials with which they can login securely without thinking about any leakage in privacy. In this phase we have to prepare the end users during and after the Go dark phase. 4) We have to strengthen the security of the University from the further illegal or malicious activities. The systems should be prepared in such a way that it can block the further attacks. 5) After strengthening and fixing all the issues, all the systems are tested again before the end of go dark phase. Confirmation is done at the end to make sure everything is on board.
5	The communication team has to communicate with both internal and external stakeholders. They have to give updates to both internal and

	external stakeholders. When it comes to internal stakeholders, the communication team has to do a good job in helping to create and develop a good plan and to address it to all the stakeholders. The external stakeholders are press, newspaper editors, governor's office, public and television stations. Stakeholders got affected by the university going dark. All the steps initiated by the university to come over with the attack has to be clearly communicated to internal and external stakeholders by the communication team. This crystal-clear communication helps the stakeholders from falling into dilemma and worry about what is happening. Each and every progress and failure should be communicated and informed to each and every stakeholder so that the plan would get executed without any obstacles.
6	If there is a cyber-attack to any company or universities, then they have to take a lot of risks to get over it. As we all know "with great responsibility comes great risks", we have to take all the necessary risk to mitigate the attacks. One of the main risks is to secure all the data from the attackers. All the risks should be taken to prevent the attacker from reaching the servers and stealing all the data. The internal stakeholders should take utmost care while working in go dark period. The internal

	and external workers have to take high risks to maintain and stabilize the network to normal state.
7	If everything goes according to the plan in the go dark phase, we can say that the Phoenix project was successful. The success of the project depends on how the developed plan is executed. If the security team after developing the new security and implementing it, still there is a possibility of data breach then we can say that this project is a total failure. The main idea of this project is to make sure that there is no data breach or loss of information should take place. And the security should get updated to prevent all the future attacks. If this project didn’t meet all these expectations, then we can say the project is a failure. The idea of go dark phase is to set up the security system up to date and strengthen the servers and computers to prevent the attack.