PES UNIVERSITY, BANGALORE

Department of Computer Science and Engineering

CNS (UE20CS326)

CASE STUDY II

The Phoenix Project: Remediation of a Cybersecurity Crisis at the University of Virginia

PES2UG20CS016

Submitted By:

Name: Adarsh Kumar

SRN: PES2UG20CS016

Semester -V

Section- B

Date – 02/12/2022

QUESTION Q) 1	Describe the role of Information Technology Services in fulfilling UVA’s mission.
ANSWER	As we come to know from the case study that all of the university's key services are managed by the ITS team. They manage hundreds of servers storing all of the students', parents', staff's, and faculty's personal information. The ITS is responsible for maintaining the security of all of this personal information on behalf of the university. UVA’s Information Technology Services (ITS) has a clear role to play in facilitating both the academic and personal development of UVA students. ITS’ responsibility to its students is twofold however, it must not only provide access to resources such as email, digital calendars, and the dizzying array of applications and software that dominate the modern landscape, but ensure UVA’s digital environment is safe and free from the malintent of bad actors. Inherent in having a fruitful and well-designed network is the responsibility to keep that network safe for its users. It is in this aspect of their obligations ITS is found wanting in this case. In the Project Phoenix ITS team of UVS has measure role They know complete details of defence in Depth model of IT security of UVA they also have to maintain the agility and secrecy of the internal System during the black out duration, these are also the main people to communicate between the external agencies such as Microsoft and Mandiant.
QUESTION Q) 2	What attracts cyber attackers to university?
ANSWER	Universities are incredibly attractive targets for all manner of cybercriminals as valuable assets and information abound. Thousands of end users – many ignorant and without the training required to equip themselves with the tools needed for protection against bad actors – represent a veritable buffet of potential targets. Digging deeper, large institutions store massive quantities of PII which naturally, would be desirable to a hacker. The kinds of data and information of interest to a cybercriminal or state-sponsored actor may be: • Emails • Personal information on staff and students • Technical resources such as documentation and standards • Sensitive research and intellectual property UVA has social security numbers/citizenship information about every student, faculty and staff member; Additionally, the university has banking information (account numbers, routing numbers, etc.) for all employees and vendors. UVA also stores insurance and medical information about students, faculty and staff members in addition to being home to a fully functioning hospital. Even some of the more mundane (and less secured) information would be of some interest to cyber criminals such as phone numbers, emails, home addresses, vehicle information such

PES2UG20CS016

	as license plate numbers, make, model etc. Perhaps a hacker wouldn't go out of their way to pursue such commonplace information on a single target, but the prospect of making off with thousands of records (phone numbers, addresses, etc.) from a single centralized database might be harder to pass up.
QUESTION Q) 3	What are the most common attack methods and approaches for mitigating those attacks you listed in question 2?
ANSWER	The most common form of cyber-attack is phishing and ITS must be especially wary of spear phishing – the most effective form of phishing in which the attacker leverages research on the target to construct a tailored weapon with which to attack. Other major vulnerabilities include zero-day exploits in which an attack using an existing fissure in new software is exploited as well as the ongoing challenge of continually patching software on the thousands of machines within the UVA network that fall under the purview of ITS. Another other major threat is user error. Thousands of individuals, many untrained, use the UVA server every day, any could in advertently fall victim to cybercrime. Two important tactics to mitigate these vulnerabilities include a strategic defensive IT strategy and education programs to better prepare end users for when they are target of a hack (which is very likely in the current cybersecurity landscape). UVA employed a "defence in depth" IT strategy to combat the threat of cyber criminals. This "castle defence" is a layered approach to cybersecurity that is meant to mimic military strategies. ITS set the system up in tranches with less sensitive/secured applications and information in the outer and more/most secured information located in the inner layers or "layer 0" (i.e., the centre). Virus detection software and the like blanket the entire system with access barriers in between the layers. The system is set up that higher and higher levels of permission are required to access the inner layers of the network this way, if a layer is breached and compromised, the damage will be localized to just that layer and the security of the inner layers will remain intact. Education is another very important aspect of mitigating these vulnerabilities. User error is the most likely source of a breach and an informed end user base is much less likely to fall victim to cyber criminals. One relatively new yet useful technique is to honeypot, this technique we capture the hacker into our network which look like original one and try to learn its technique and make our system defences harden to that kind of attack.
QUESTION Q) 4	Describe each of the 5 objectives of the Phoenix project.
ANSWER	The Phoenix project outlined five very ambitious goals for combatting the hack. 1. Determining the full extent of the hack is very challenging, here they (UVA) also took the help of Mandiant. 2. Developing the remediation plan. Even after identifying which layers of the network were compromised, discovering the true extent of the hack would require combing through potentially terabytes of information, scrutinizing all

PES2UG20CS016

	university apps, software, and websites for malicious code that may have been embedded. 3. Next Evan's and her teams had to execute the remediation plan. Luckily ITS had good help from Mandiant and others. There is literally an infinite number of things that could go wrong during this phase. Murphy's law comes to mind in this phase: anything that can go wrong will. 4. Harden UVA' Defences in this there should be some strict policies must be applied this include applying system patches and separating or segmenting the employees (staff), student and research data. 5. All the system must be restored and tested by the end of the Dark phase. UVA had never been hacked like this before and therefore had no experience in restoring systems. The blackout period required to restore the network may be painful, made even more so by its proximity to the start of a new semester.
QUESTION Q) 5	Describe the various internal and external stakeholders associated with the Phoenix project. How would you recommend the project team communicated with each stakeholder group?
ANSWER	Internal stakeholders are those individuals or groups within a business such as employees, owners, shareholders and management who have an interest in the company. (Vice President, Dean, faculty, staff, students, Retirees, alumni, University community) External stakeholders are groups, individuals or organizations outside of a company such as its customers, etc (BOV, Governor's office, general public and the press) Communicating with all internal and external constituencies Depending on which PII was compromised, UVA could be exposed to litigation related to negligence and the mishandling of information if it's discovered that the university did not do enough to protect their data. Communicating with both the public from a PR perspective, but also those personally impacted by the breach is essential. Next, hardening UVA's defences going forward is the most challenging component. I personally would recommend that each team first talk every detail to the Project Manager (Dana German) first and she should discuss with the Project Sponsor (Virginia Evans) and then only disclose any thing to the public or external stakeholder, but for internal project director approval would be sufficient other wise it will be I big process just for approvals.
QUESTION Q) 6	Identify the key risks inherent to this project. How would you recommend the team manage these risks?
ANSWER	The first risk I identified is the risk of litigation for the potential mishandling of information, this risk is related to the importance of getting ahead of the narrative and ensuring that external communication/PR is as transparent, positive and proactive as possible. This risk can be managed by taking care and being strategic when making statements/releasing information about the hack. Another risk I identified is the risk of reputational damage caused by the university's security breach to individuals affected by the hack through the release of PII).

PES2UG20CS016

	This risk can be mitigated by discovering what information was taken and then identifying and alerting all impacted parties about the breach as soon as possible so they can prepare themselves in the event PII is released. A third potential threat that is risk that the remediation plan or system restoration goes awry and there in additional/unnecessary damage done during that process. This risk can be addressed by consulting campus calendars and selecting a time for the blackout period/system restoration that disturbs as little other campus activity as possible.
QUESTION Q) 7	When and how should the success of Phoenix project be evaluated?
ANSWER	The Phoenix Project should be evaluated following its completion at various intervals to determine its success. After the go-dark phase would be an ideal time for the first evaluation where we would test the adjustments made to the systems and test the strength of its security. There are many aspects involved in evaluating the success of the project. Firstly, we need to check if all the objectives of the project were met and the project implementation went as per the plan. And the second thing is to check how efficient the newly implemented security plan is working. If the plan is only got rid of attackers temporarily, and there is no future guarantee to protection against such kind of attack then we can't say that the Project Phenix is successful. Some of the parameters of this project are: • Time: taken to come complete this project. i.e. weather their team were able to complete the project in the given time. • Cost: did all the remediation planed thing come into their budget like the system repair and etc. • How much is the new improved security is really secure to present and new types of future attack

PES2UG20CS016

THE END