UVA Case Study

Navya Peram
PES1UG21CS924

Question #	Answer
1	One of the main components of UVA's IT is the ITS organization. It maintains multiple servers, almost a hundred that are used to run a huge amount of applications and services. They are used to manage core university services. With their servers covering various domains, ranging from HR, student information, financial information, and other data. Apart from this, multiple computers are used daily by the student body, in various labs, by employees, and by the multitude of professors from multiple departments. These computers have to be updated and patched constantly. All these functions are performed by the ITS. It ensures that the entire university has reliable and secure internet access. Overall, they managed and created multiple applications that are being used by UVA to protect them from cyber-attacks.
2	Universities are considered as a major target for cyber-attacks due to a multitude of reasons. Universities such as UVA with a focus on research, usually contain large amounts of research information ranging over various disciplines. The large collection of PII of the students, faculty, scholars or alumni could be used by the attackers to gain an edge over other competitors in the industry. This information could also be used as ransom by the attackers, to gain huge amounts of money. Private information of the student and teaching body could be stolen and sold to various nefarious and closeted black market enterprises. Financial information, such as tuition and bank accounts from students, research grants, endowments, and tax information of the employees and the alumni can be stolen. Lastly, the large bandwidth of the university network could be used to perform multiple large-scale attacks. Attacks such as DDoS attacks for cryptocurrency mining and several others could be performed which would affect the university to a very large extent.
3	The most common methods of carrying out the previously mentioned attacks are phishing attacks(T1566), MitM attacks(T1557), network sniffing(T1040), and supply chain attacks(T1195). In case of phishing attacks, deceptive emails or messages are sent to the university staff or students. These emails trick them into revealing login credentials or clicking on malicious links. This would give the cybercriminal unauthorized access to the system. Phishing attacks can be avoided by email filtering(M1021) and by training users to recognize any phishing attempts(M1017) while checking emails. A ransomware attack consists of the deployment of malicious software into the system through any infected files, emails, or compromised websites. This can be prevented by monitoring the system for unusual files or activities and by using reputed antivirus software. In the case of an MITM attack, the attacker intercepts a connection between the user and a system on the network. He can then gain access to any sensitive information being transmitted through the network. Implementation of strong encryption(M1041), filtering network traffic(M1037), and regularly checking for unauthorized devices on the network

Navya Peram
PES1UG21CS924

	can be used to prevent these attacks. The attackers could also intercept sensitive data transmitted along the network. This is called network sniffing(T1040), which can be mitigated by encrypting sensitive data(M1041) and multi-factor authentication(M1032). During supply chain attacks, third-party vendors or service providers connected to the university's network are targeted to gain access to the system. Some of the mitigations for this attack are updating software frequently(M1051) and vulnerability scanning(M1016).
4	The internal stakeholders in the case of the Phoenix project consisted of multiple levels, starting with the senior level consisting of the BOV, deans and vice presidents, followed by the faculty, students, and staff. They are accompanied by the retirees and the alumni. The external stakeholders include the governor's office, the attorney general, the public, and the press, which consists of the local newspaper and the TV stations. The various communication plans that could be used are: • Frequent meetings, executive briefings, and a special online portal that can emphasize budget reports focusing on any changes or increases in costs can be used as the main means of communication for the BOV, deans and vice presidents. It can also include any important achievements along with updates on the current status of the project. In the case of faculty, they could receive information through departmental meetings, email newsletters and collaborative platforms. Students, on the other hand, can receive information through social media, university-wide mailings, and student forums. The staff members could receive information through staff meetings and announcements. A specialized website can be created to spread information to the alumni and retirees. This could also be done through the weekly or monthly newsletters. • External stakeholders such as the Governor's office, the Attorney General, the public and the press could receive information through formal reports and periodic briefings. Direct meetings could be initiated to pass on any sensitive information. Information regarding the current project status and budget allocations could be conveyed to the external stakeholders. The Attorney General can be briefed through legal briefings, official documentation and scheduled meetings. This can be done so as to make sure that every aspect of the recovery process is legal. • The draft for the communication plan begins by identifying the stakeholders and by understanding their main preferences. The university must make sure that the method of communication should be tailored appropriately to each stakeholder depending on their position and necessity. This can be done to prevent any unauthorized information from reaching people below their classification levels. They must establish a regular schedule for constant and continuous updates. This schedule should be flexible, to be able to change in the case of any milestones or setbacks. Feedback mechanisms should be implemented

Navya Peram
PES1UG21CS924

	to allow the stakeholders to ask questions, make any inputs, or to express concerns. A detailed and adaptable communication plan could greatly benefit the university by building trust and ensuring transparency of the process. Thereby, contributing to the overall success of the project.
5	The risks associated with the project were assessed based on two factors – impact and probability. The various identified risks include public knowledge of the security compromise, scheduling conflicts with UVA programs and events, issues in the system documentation, and the occurrence of any technical or human resource issues. • The first risk refers to any possible public knowledge regarding the compromise in the security of the university. This would have a high impact on the university. The issue can be resolved by establishing stringent and robust security measures, by performing audits on the system constantly, by developing a contingency plan that consists of appropriate communication approaches and by establishing a rapid response strategy. • The second risk refers to the occurrence of any scheduling conflicts between a large number of events and programs conducted at UVA. Various strategies can be used, such as establishing clear communication channels and by coordinating events in advance. Identifying alternative dates for important events and programs, to be used in the case of any emergencies, such as the current attack, would also be very beneficial. • The third risk is based on any potential shortcomings in the system documentation. A robust documentation would be highly beneficial in the case of regular training or as an excellent source of reference in case of any attacks. Strategies involve implementing a thorough documentation process and regular reviews. Developing a contingency plan with multiple training sessions and continuous integration of knowledge would also be extremely helpful. • Finally, the fourth risk is based on any future issues with technical or human resources. This can be avoided by regular skill assessments and constant learning. Establishing detailed plans featuring backup resource plans, with continuous evaluations and training exercises would be very beneficial. The university could organize regular checkups by industry experts along with various seminars regarding the changing tech environment. The above plans must be evaluated constantly and continuously. They must be flexible and have room for change to be able to adapt to the changing technology. Each project must have thorough documentation with constant day-to-day updates, along with detailed reviews and indications of any future risks.

UVA Case Study

Navya Peram
PES1UG21CS924

6	The Phoenix Project can be evaluated in several phases, beginning from the initial phase of attack response to the final remediation of the attack. • We begin with the evaluation of the initial response phase, which occurs immediately after the attack is identified and reported. The various criteria over which we can assess the effectiveness of the response are the methods of detection of the attack, the timeline of communication of the attack to multiple levels including the senior levels, the effectiveness of the immediate response of the detector, and the adherence to the contingent plans in place. The success of this phase is measured based on the speed and the accuracy of the response. • The second part involves the formation of response teams and the employment of various risk mitigation strategies. The teams are evaluated based on the team members' expertise , their ability to collaborate efficiently, and the speed with which the teams are formed. In the case of the various strategies implemented, it depends on the effectiveness of the strategies proposed by the teams and the ability to identify key parts to focus the efforts on to minimize the impact of the attack. • The third part involves the initiation and employment of plans to mitigate the attack. It depends on the clarity of the plans created and the timelines of the internal and external communication. It also depends on the methods used to keep the stakeholders involved, the ability to employ dynamic and flexible measures, the ability to identify any lingering issues, and the smooth transition back to regular operations. • The final part involves the working of the systems post-restoration. It depends on the detailed review process conducted during and after the attack, the plans implemented for constant and continuous learning in the future, and the effectiveness of the methods used during the restoration process.
7	The lessons learned from the project are: • Developing an incident response plan is of the highest importance in the case of an attack. Evans and German were able to develop a detailed and meticulous plan covering the most important and risk-associated areas, which in turn increased the success of the project. They were able to highlight and outline all the roles and responsibilities required of each and every team and it’s members. • The leads of the project broke down the roles and responsibilities into multiple groups. This made sure that various facets and points of the attack would be covered by people with expertise in that particular area. This is highly beneficial as along with internal teams who had knowledge of the systems, external teams were called in to help with difficult and pesky tasks. Thereby, ensuring that the project would be well covered without any discrepancies or left out solutions.

Navya Peram
PES1UG21CS924

	• Establishment of proper communication, Evans understood the importance of transparency and communication. Transparency among stakeholders is necessary for the flow and the success of the project. This can be done by establishing regular communication channels like security meetings and debriefs • Cybersecurity must be prioritized by establishing secure protocols and constant and continuous monitoring. Security scans and assessments must be performed regularly to detect the presence of any unwanted software. • Sensitive data must be prioritized, as in the case of UVA. They had established multiple levels of protection to encase sensitive data, which was extremely beneficial to the university. This prevents the attackers from accessing highly valuable information in case of any breaches. The various actions that can be taken to prevent future attacks are: • The university can implement a zero-trust security model. This model automatically assumes that no user or device is trustworthy. The user must take part in constant and continuous verification of their identity every time they access their privileges. This approach can be extremely beneficial as it reduces the potential for unauthorized access and data breaches. • Segment networks can be used to isolate sensitive data and systems from less sensitive and secure areas. This would be very helpful in the case of any data breaches by reducing its impact on the system and the database. • Multi-factor authentication could be established for all user accounts. It can strengthen the security of the accounts by requiring additional private information beyond just passwords. Various methods such as secret code or secret questions can be used to enhance the account's security. • Constant and continuous audits must be conducted on the systems to check for the presence of any unwanted software or security risks. This should be done both by the university and by an external company with a higher area of expertise. It is used to identify any security risk or potential vulnerabilities in the system. • Establishment of stringent security protocols and mechanisms to be considered during an attack or breach of the systems. Create multiple plans as backups for the various courses of action to be taken in case any single plan falls through. • The users must be educated and trained on the various threats present in cybersecurity. Periodic training camps and seminars can be implemented to educate the users about safe online practices and suspicious activities. • Universities must make cybersecurity a priority. With the increasing number of attacks every single day, cybersecurity should also be given

Navya Peram
PES1UG21CS924

		prime importance in multiple cases such as investments, education and resources. This in turn protects the people and the interests of the university.