PES UNIVERSITY
COMPUTER NETWORK SECURITY
ASSIGNMENT 5 - PHOENIX PROJECT

Aayush Kapoor PES2201800211

1. **Describe the role of Information Technology Services (ITS) in fulfilling UVA's mission.**

-> Information Technology Services (ITS) organisation is a place where all the IT operations of UVA are handled. It describes its mission as "Being a trustedpartner and strategic resource to the University community, aligning technology to advance the University's mission". The ITS team is involved in managing all the core university services. They maintain hundreds of servers containing all the personal information of the students, parents, staff and faculty. Maintaining the security of all this personal information is very important for the university and this is accomplished by the ITS. It is also the top priority of ITS to secure the financial information, including payment information from the students, the tax information for employees and the intellectual property, which can be misused by the cybercriminals if they gain access to the systems. As the university was also involved in research and development, all the information about these researches are valuable assets which can be patented, so the security of this information was of utmost importance and this was again the responsibility of ITS to secure all the systems used in the research and developmental activities. So, "data " is a very important component in accomplishing UVA's mission and securing this data is the main responsibility of ITS. They need to develop proper security systems in-order to safeguard the assets of the university so that there are no vulnerabilities or security holes in the system that can be exploited by the attackers to get into the network and misuse the information which can cause a high degree of damage to the university.

2. **What attracts cyber attackers to universities?**

-> The degree of threat and attacks is high in universities and higher education establishments mainly because of their target-rich environment. These Education institutes are home for a large amount of information in their databases. They manage all the student, parent, alumni, staff and faculty information. Universities could be a prime target because they often have significant financial information, including payment information from students and tax information for employees. Many universities are centers for cutting-edge research and development work that creates potentially valuable patents as well as trade-secret related data which are attractive targets for cybercriminals. Openness of these educational institutions may also be a component that attracts the cybercriminals to pose an attack. They are the platform that encourages and promotes the free exchange of ideas and information for the constantly changing population of students,researchers, academics and staff. The wide variety of digital devices used by these people would require access to the network.

3. **What are the most common attack methods and approaches for mitigating those attacks?**

-> 1. _Spear Phishing_ - Evolved from phishing, involved millions of emails asking the victims to click on a malicious link or download an infected file. Attack on human vulnerability, very difficult for spam filters and automated phishing-detection system to spot spear phishing as only few selected victims in an organisation were sent these tailored e-mail messages.

2. _Unpatched Systems_ - Patches were software updates installed on computers that fixed a known system vulnerability. Since UVA's ITS managed several hundreds of computers, it became very difficult to manage all the updates to the computer systems. ITS had very little control over how and when these devices were updated with the latest security patches.

3. _Zero-Day Exploits_ - Not publicly known and did not have a patch or workaround available to fix the security hole. Severe and very difficult to detect and mitigate.

4. **Describe each of the five objectives of the Phoenix Project. What level of effort would be required to accomplish these objectives?**

-> 1. Determine the extent of the intrusion. Although Mandiant had performed a preliminary investigation of the intrusion over the past several weeks, a more in-depth assessment was necessary to ensure that everyone had full information.

2. Develop a remediation plan. A detailed plan for addressing system deficiencies needed to be developed over the next few days, and given that the final remediation activity would involve bringing all UVA systems down to allow a new security system to be enacted, one of the very first decisions would be to schedule a go-dark phase.

3. Execute the remediation plan. Execution involved performing all necessary activities leading up to the go-dark phase, including:

- tracking foreign attacker activities and responding as necessary,
- Developing methods of procedure (MOP) to rebuild and protect critical applications and data on the compromised systems,
- Identifying all workstations impacted by the intrusion,
- Evaluating UVA’s password-management system,
- Preparing to support end users during and after the go-dark phase, and
- Communicating with all internal and external constituencies.

4. Harden UVA’s defenses.Alongside all the above, it was obvious that UVA’s systems needed to be further strengthened to block further malicious activity.

5. Restore services. All systems would have to be restored and tested toward the end of the go-dark phase.

To accomplish these objectives, a large number of diverse personnel would be necessary. The challenges involved with identifying the necessary skill sets, "borrowing" the personnel from their assessments, and then organising them into a high-functioning team were almost too much to comprehend.

5. **Describe the various internal and external stakeholders associated with the Phoenix Project. How would you recommend the project team communicate with each stakeholder group?**

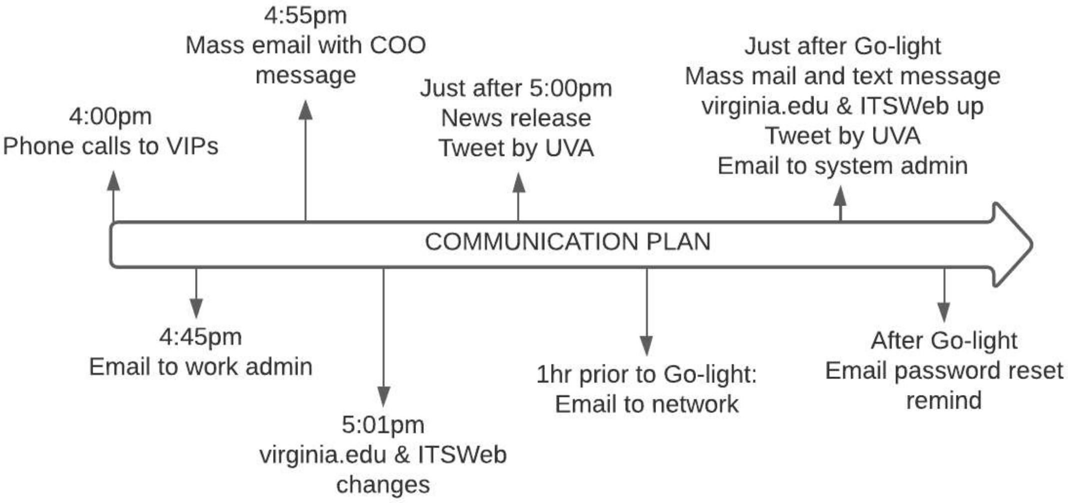
-> Internal Stakeholders :

- BOV
- Vice Presidents
- Deans
- Faculty
- Staff
- Students
- Retirees
- Alumni

External Stakeholders:

- Attorney General
- Governor's office
- General public
- University Community
- Press (local newspapers and TV stations)

The communication team of the stealth army was responsible for managing project communications.



6. **Identify the key risks inherent to this project. How would you recommend the team manage these risks?**

-> Key risks were based on:

- *Time risks* - The project has to be completed in the time allotted, otherwise they wouldn't get another chance for remediating the vulnerability.
- *Cost risks* - Biggest threat to the PII of the faculty, staff, students, retirees, alumni. If breached it would not only affect the university reputation, also the lives of these people.
- *Scope risks* - This type of risks endanger project objectives, deliverables or timeline.
- *Technology risks* - The software implemented in the Phoenix project are not outdated or have any vulnerability that could be exploited that will lead to another breach.

Each team had their own responsibility to take care off, but these risks are common in any project. What if one team were late on schedule due to some budget/resource they could not meet, this will lead to time, scope, cost risks.

This project had CISO and Enterprise Risk Manager who looked out for these shortcomings and also planned ahead if one thing goes astray. To manage these types of risks, it would be better to have a plan ready for each type of risk. During morning meetings if one of the objectives did not meet the requirement or will lead to risk, these will be addressed by CISO or Enterprise Risk Managers for alternative plans.

7. **When and how should the success of the Phoenix Project be evaluated?**

-> 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. Ask another cybersecurity firm to evaluate the system integrity, check for any vulnerability. I think that there should be evaluations quarterly to ensure the integrity of the system and to protect against any future threats.

University of Virginia surely falls into the category of a high reliability organization as throughout its process of counteracting its cyberattack, they followed a great deal of these best practices. One practice the university strongly exhibited was resilience. Virginia Evans understood that because cyberattacks operate in complex and nuanced ways, it was important the university's solution to the attack was just as rigorous. Over the span of three weeks, Evans worked with a team of professionals to assess the extent of the intrusion. Upon finding 62 servers had been compromised, they formed an initiative to resolve the attack, The Phoenix Project.