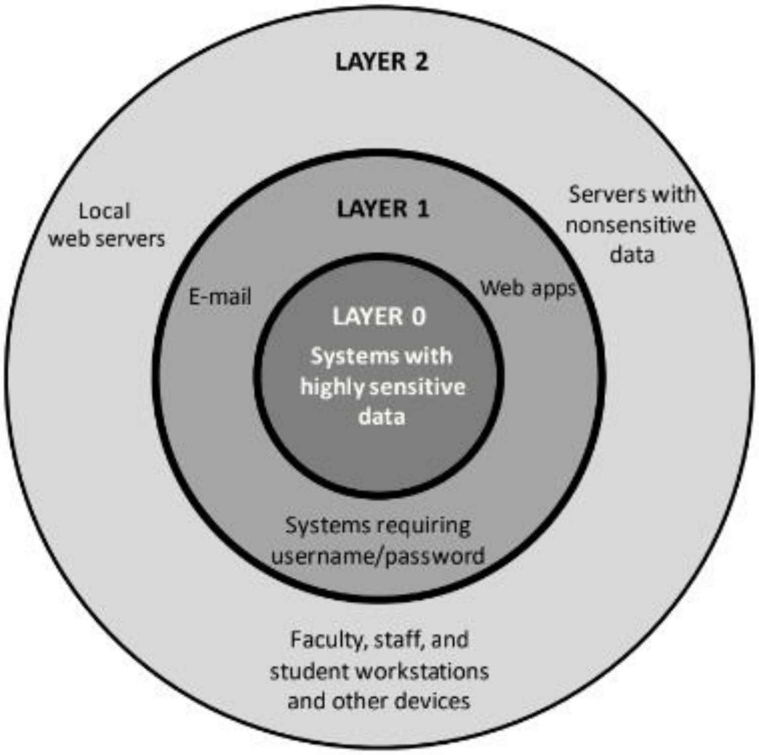
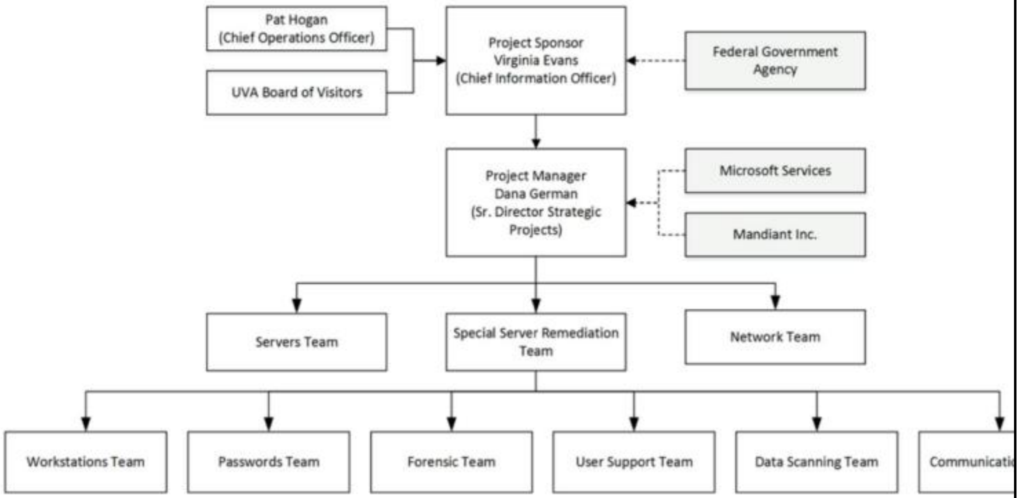
Name : Aryansh Bhargavan
SRN : PES1UG20CS084

Question #	Answer
1	ITS is responsible for proper utilization of technology. ITS provided UVA with several reps and $50 million. It manages a large number of servers that belong to several organizations. ITS has been handed the duty to ensure that all the servers perform up to standards and are constantly updated so as to maintain latest standards. The head of ITS, Virginia Evans has been involved with IT for over 25 years so that has also contributed to fulfilling UVA's mission.
2	1) Huge amounts of PII Data: From the eyes of a hacker, a university is an easy target and a source of massive amounts of data. For example bank account details, aadhar card details, PAN card SSN details etc. They are also a source of Contact details, and it has been well documented that massive amounts of contact details can be sold for various nefarious purposes 2) Intellectual property such as pending patents, new technology, research funding, etc which can give an understanding of current research trends and can be used as a form of insider trading.
3	Most common attack methods are: 1) Spear Phishing: Unlike regular phishing, this involves selected targets to whom personalized phishing methods are implemented. 2) Unpatched Systems: This takes advantage of systems that run old versions of software on which vulnerabilities have been discovered. 3) Zero Day exploits: This takes advantage of newly discovered/undiscovered vulnerabilities in software to which a fix has not yet been made. UVA has implemented layer-wise security as a means of mitigation: 1) Layer-0: Also called kernel, this contains most sensitive information, and access is severely limited. 2) Layer-1: This includes services that are accessed using credentials. Used by teachers and students alike with valid credentials. 3) Layer-2: Contains no sensitive information. It can be accessed by external organizations. These servers cannot access the rest of the University network

	 LAYER 2 Local web servers Servers with nonsensitive data LAYER 1 E-mail Web apps LAYER 0 Systems with highly sensitive data Systems requiring username/password Faculty, staff, and student workstations and other devices
4	1) Determining the degree of infiltration: This is so that every member of the remediation team is aware of the problem at hand and the degree of said problem and a proper remediation plan can be made. 2) Develop a Remediation Plan: It involves an analysis of the current situation and a schedule of when to perform a go dark stage. 3) Execution of said plan: 4) Hardening security of UVA: This is for prevention of future attacks. 5) Restore Administration: and restore so that regular work can go on like before, as best as possible. Performing these steps requires several types workers with varying level of skill. All objectives are crucial and require a decent amount of effort to perform.
5	There were a total of 176 people working on the project. They can be classified as internal and external stakeholders. Internal stakeholders include: 1) Server Team 2) Network Team 3) Passwords Team 4) User Support Team 5) Forensics Team 6) Specialty Server Remediation Team 7) Workstations Team 8) Data Scanning Team 9) Communications Team - The Server Team is responsible for finding out which server has been broken into. Their main task is to come up with a plan to either isolate an unsafe server from the remaining server while formulating a strategy to make the infected servers safe or decide whether or not they should discard the unsafe server, to prevent spread of damage. - Network Team is supposed to monitor the network and alert any suspicious activity on the network. - Passwords Team essentially is responsible for maintenance and security of stored user credentials that includes username, passwords and more.

	- User Supports Team should provide timely support to a user regarding any issued with a user account. Their activities include and are not limited to password related issues, addition of new accounts, etc. - Forensics Team is responsible for tracing an attacker by observing and analyzing footprints left behind by the attacker (if any). - Workstations Team is responsible for identifying workstations that are vulnerable or have been infected by an intrusion. - Data Scanning Team is responsible for scanning all the data that has been compromised and finding out information that may have been exposed and is sensitive. - Communications Team maintains communication between internal and organizations. External Stakeholders include: 1) Federal Government Agency 2) Microsoft Services 3) Mandiant Inc.  Pat Hogan (Chief Operations Officer) UVA Board of Visitors Project Sponsor Virginia Evans (Chief Information Officer) Federal Government Agency Project Manager Dana German (Sr. Director Strategic Projects) Microsoft Services Mandiant Inc. Servers Team Special Server Remediation Team Network Team Workstations Team Passwords Team Forensic Team User Support Team Data Scanning Team Communicati
6	1) Due to the scale of the project, confidentiality becomes a tough task to maintain. All communication must be monitored, certain forms of communication must be used and certain forms must be restricted. 2) Scheduling conflicts with UVA programs and events 3) System documentation shortcomings Resources like Evans and Dan (who are experienced in handling teams) must be applied and utilized to the best of their abilities, since that may lead to project success. Harden each layer of network to prevent any further damage. Remove compromised accounts to prevent attackers from accessing any more sensitive data or expanding the list of vulnerable accounts.
7	Project must be evaluated after the go-dark phase since it is the last phase of the project. Based on how the objectives of the project were reached, one can come to a conclusion regarding the success of the project. - How many infected servers - How quick was a remediation plan made and executed - How long was the go dark phase, how much data was recovered and restored