* The requirement for security is important and vital for organization survival. It cut beyond all zones of life from delivering protection and offering protection for lands for which are non-living objects.
* It expands to a pc as the number of workstations keeps increasing, they used to store important data about every organization including the staff members. It also requires protection we bring to our pcs
* It is especially important to have a unique password that has eight letters long including numbers and symbols, as well as the username. Thus, it is used to avoid unauthorized entrée to any pc network and assets\
* It can available for private and public users with limited access This question evaluates the two major network security strategies which can be layered within an organization

1. **Layered Security**

* It is the preparation of merging numerous mitigating security mechanisms to safeguard all the resources and information
* Hence, it can be done at any phase of the completed data approach
* It improves the security of the network from as little as a small home network to a big organization network (Azra et al, 2014).
* The major purpose behind a layered network is that it used a defense network. Hence, it will be ending failing to add various layers that will cover the entire fault of a security layer
* The use of a firewall, encryption to protect data are commonly used as a layered security strategy to prevent intruders’ access
* It includes the use of a firewall, malware scanner, intrusion detection, encryption to protect information resources securely that intruders cannot have access to.
* It helps to stop network seize from numerous incidents
* To implement a safely used layered security strategy defense in an organization, will be looking at a firewall and how it is layered into an organization
* **Firewall**
* **To implement a layered security strategy within the organization, one needs to consider a lot of security measures or layers especially when dealing with a cyber attack**
* Firstly, system-level security. It simply ensures that all staff members have been properly been constituted in the best way possible to prevent attacks against the system. It happens to incorporate all the organizational roles by assigning user usage for gaining access to information
* Secondly, network-level security. This protects the entire organization network from intruders, it includes a firewall to verify protocols and as well as controlling the traffic of the network
* Thirdly, application-level security. An important role of a layered security strategy, it knocks down entry to vital procedure tasks by making operators log in with a username and password allocated by a certified expert.
* Fourthly, device-level security. By installing a full endpoint defense results, it can be time exhausting, as all pcs, cellphones and as well as a router have unique default settings. It is very vital to close all entry points that a hacker might exploit

1. **Defense in Depth Strategy (DiD)**

* An attempt to cybersecurity defending procedures that are layered in a way to shield important records of information.
* This multi-covered method with intended redundancies boosts of the security system it will tackle unique attack routes
* To use a more complete safety strategy than that of the layered security
* A thorough and well-executed DiD stops a network system from various outbreaks and as well as establishing a real-time alarm for arriving interference for the network administrator
* It attends an effective method of avoiding resolving automated outbreaks that arise from the same shared network
* In such an attack, the attacker will try to attack the network system from different angles using different methods that can be difficult to prevent, DiD with multiple layered security can protect the system
* It uses a VPN, intrusion detection system (IDS) are a fragment of the DiD strategy applied to avoid unlawful gain access to an organization network
* By combing both the IDS and VPN, will create a barrier for all types of attackers to easily infiltrate through the network system
* DiD is authenticated by experts to defend an organization network against invasion and attackers
* It is flexible for having to protect a pc against new raising threats, one layer of DiD has a mixed implementation of security controls which can uncover attacks way before they could enter the network security
* To implement an effectively used defense-in depth strategy in an organization, will be looking at an intrusion detection system and how it is layered into an organization
* **Intrusion Detection System**
* **To implement a defense-in depth within the organization, one needs to consider a lot of security measures or layers especially when dealing with a cyber attack**
* Firstly, network security. Things like the remote access, proxy content filters and as well as the wireless security
* Secondly, application security. This deals with movement examining every application and app the organization is currently using, the testing of the firewall application and database
* Thirdly, endpoint security. It normally ensures that all the devices accessing the network of the organization either by a remote or even wirelessly, the contented security is fully functional
* Fourthly, the administrative security. This approach ensures that all the procedures have increased in information protection and all the policies are being regulated quarterly