**Answer: -**

To accomplish this project, we have chosen the scenarios to set up the new branch of UNDOC in Bangladesh. As the CSO of this project we will first understand the cybersecurity and requirements related to the setting up of the new offices and we will convey all these related things to UN Secretary-General.

As we know that cyber security is the practice which ensures the integrity, confidentiality and availability of the information. It has ability to defend against and recover from the different kind of failures like power outages and attacks by the adversaries. We also familiar with this thing that human is always the weak entity in any kind of cyber security program. How human is responsible due to these factors like writing code securely, training operation staff end users to spot phishing emails and social engineering attacks that’s why we said that cyber security begins with awareness.

 As a CSO we will take care of these cyber security types. These are as follows: -

* Critical infrastructure: - it includes the cyber-physical systems on which the society relies on, it includes the electricity grid, water purification, traffic lights and hospitals.
* Network security: - It guards against the unauthorized intrusion as well as malicious insiders. It ensures the network security which often requires trade-offs.
* Cloud security: - when our UNODC move to the cloud it imposes new security challenges.
* Application security: - The application security mainly related to the web application security, which becomes the main technical point of attack.

Trends and challenges: -

The cybersecurity lifecycle are as follows: -

protect

identify

detect

lifecycle

respond

recover

review

To protect our new UNODC organization we will need to be aware from these key trends these trends are as follows:

* Data co-relation: - Prior to adding the more devices to the network we will perform the correlation technique across the devices which are existing. To understand the all kind of traffic we need to perform the data co-relation across all the critical devices. So, that organization can understand that what is going on and we can take the appropriate action against.
* Endpoint security: - As CSO we need to protect the all kind of challenges of the operation. When more devices become portable then importance of the endpoint becomes more critical. In this case we go beyond the traditional endpoint and we will focus on the controlling, protecting and monitoring the data on the end points.
* Forensics: - Sometimes the attacks are so dangerous that once it happens we can’t recover from it. So, we will put focus on the proactively identifying the problems and rectify them before its major attack on the organization. That’s why it is known as Pro-active approach rather than reactive approach.

Approach and flow of the UNODC cybersecurity network strategy process:



Steps in UNODC Security: -

* Understand your all IT infrastructure network, network traffic and communication system.
* Make the security policy, procedures and the implementation plan
* We will take approval from the UN-general secretary
* We will implement all policies and plan
* We will make the standard documentation of the entire infrastructure
* From certain time interval we will audit the entire network security
* We will create the security awareness among the users through the training and courses in the UNODC offices.

Our security model to implement in the UNODC offices will follow the “Defence in Depth” and will follow this rule to while designing and implementing the UNODC security model. We will use the layered model approach to implement the UNODC security model. It will contain the tools which perform the data collection, analysis, reporting and generation of alarms.

 The security models contain the four key layers. These are as follows:

* Layer-1: Defence perimeter
* Layer-2: Server Protection and Operating System
* Layer-3: The protection of host
* Layer-4: Information Protection

Steps to creating a secure UNODC network. These are as follows: -

* Use of Antivirus is must. It detects and removes the malware, adware and spyware and it also filter out the potentially dangerous emails and downloads.
* By protecting the network by restricting access of the selective websites. We will configure the setting to block the authentic data and some authentic emails, it means that access should limited.
* We will use a cyber security framework which develops the policy that tells that which individual will access which type of information.
* We will try to encrypt the all data.
* Don’t give password to anyone.

As we know that machine learning provides the powerful use case for the cybersecurity applications and network applications. While, machine learning algorithms divided into two categories supervised and unsupervised. We know that supervised algorithms require labelled training dataset when we once trained the data set, we can able to correctly classify or predict the data given new input. For our implementation of the project we will use the spin-backup which is robust and we know that now these organizations have lot of data inside the cloud environments. So, spin backup will help us to identify the following problems and it will protect the valuable business-critical data. So, Spin-backup uses machine learning for detecting the cybersecurity events in UNODC as follows:

* It will protect from the malicious third-party app
* Protect us from the sensitive data leak
* Ransomware detection
* It will protect from the insider threat detection
* Also protect from the brute force login attempts

These will be the approach and algorithm implementation of the UNODC office in the Bangla- desh.