Network Risk Management Implementation Plan

- **Create a list of Cybersecurity Implementation controls discussed in class for**

- Enclave Protection
  - Defense in Depth: Defense in depth is a layered approach where the security controls are implemented at multiple levels. The assets which we want to protect the most are placed in the innermost levels.
  - Firewalls: Firewalls are security devices which are used for monitoring and filtering of network traffic. This can be done through setting up rules or policies on the firewalls.
  - Routers: Routers are network security devices which forwards the packets from source to destination. Apart from directing internet traffic, a router also offers several other features like Network Address Translation (NAT), VPN, WPS etc.
  - IDS/IPS: Intrusion Detection System is a framework which monitors the network traffic to recognize malicious activities, while Intrusion Prevention System is a framework that not only identifies malicious traffic but also take steps to counteract them.
  - Encryption: Encryption is crucial as it helps safeguards against unauthorized access. Even if the attacker has access to the information, he cannot read it as he requires the keys to decrypt it.
  - Enclave DMZ: Enclave DMZ try to limit the interior access to a particular segment of the network.
  - Network Test Access Ports: Network Test Access ports are Network Security devices that duplicates the packets and sends them to the monitor ports for analysis.
  - Wireless IDS: These are employed to alert the sys-admins whenever wireless attack tools are used, or rouge access points are detected.
  - Backdoor connections: It is a strategy where the normal authentication is circumvented to get to a system or its information.
  - IPSec VPN Tunnel: An encrypted tunnel is established for secure communication. Here, the whole packet is encrypted.

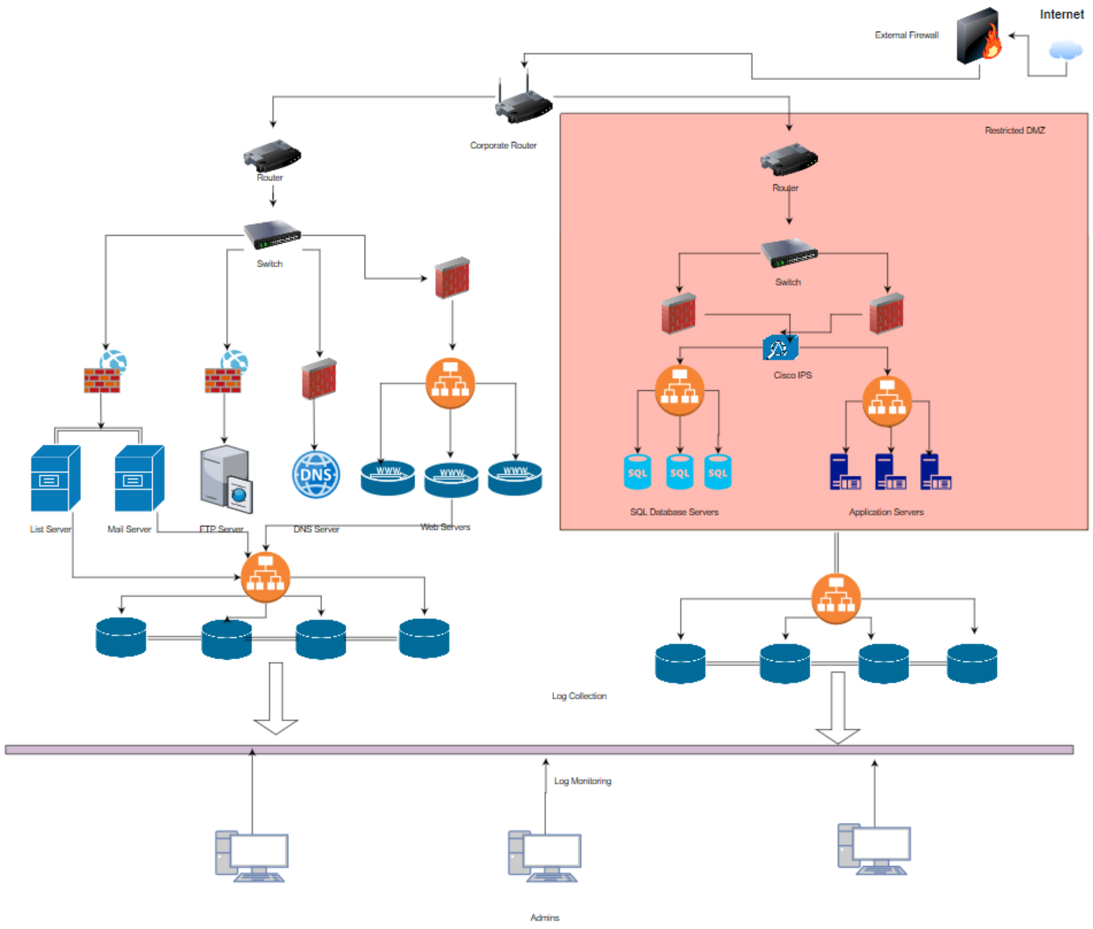
- Firewalls
  - Packet filters: It is a type of firewall method in which the network packets are allowed or blocked depending on addresses, ports or firewall policies.
  - Bastion Host: It is a hardening mechanism used to withstand all kinds of attacks.
  - Stateful Inspection: It has a table consisting of all the legitimate connections and ports and only allows them. Only examines the headers and not the data.
  - Deep Packet Inspection: Unlike stateful inspection which only examines the headers, deep packet inspection also examines the contents of the packets for virus, trojans and other malware.

    - Application proxy gateway: Unlike a stateful inspection firewall, this can control applications and administrations explicitly.
    - Hybrid Technology firewalls: It offers the advantages of both stateful inspection and application proxy gateways.
    - Proxy Servers: It sits in between the main firewall and application to reduce the load on firewalls, also has monitoring and logging capabilities.
    - DMZ and content filtering: Content filtering can be employed to filter content like social networking sites or sites against company policy.

- Routers
    - Static Routers: It is the most secure method and employed when there is only one path to the network.
    - Neighbor Router Authentication: Prevents fraudulent route updates.
    - Authenticate Routing protocol: It uses SHA-2 or IPSec Signatures for authentication.
    - Packet Assembler Dissembler (PAD): It gathers information from terminals and places them into X.25 packets and vice versa.
    - Finger Service: It gives out information about the users logged on the system and can be abused by the attacker via social engineering.
    - Logging Integrity: Attackers can alter the log files and timestamps, hence only NTP server or GPS must be used.
    - Router Control Policy: Policies should be set to restrict access to internal network interfaces.

- **Create a network topology diagram for your company.**

The Network Topology diagram consists of a restricted DMZ. Here, there are several SQL database servers and Application Servers. The distribution of workloads across multiple servers is achieved by load balancers. Inside the Restricted DMZ are two stateful inspection firewalls to monitor malicious traffic. There is also a Cisco IPS to identify and block malicious activities. This is connected to a router which is in-turn connected to a corporate router. The other servers like the Mail server, FTP server, DNS Servers and Web servers are connected to packet filter firewalls. The log collection from all the servers is done by the log collectors. There are several admins to monitor and analyze the collected logs for malicious activities.



➢ **Create a list of Cybersecurity Implementation controls that exist at your company**

- Enclave Protection:
    - Defense in Depth: Defense in depth is implemented where the first level is for VPNs and requires 2 factor authentications. The second level is for normal server logins which also requires 2FA. The third level is for particular servers like connecting to databases which again requires 2FA.
    - Firewalls: Multiple firewalls are implemented at my organization like Web Access Firewalls, packet filter firewalls, stateful inspection firewalls etc.
    - Routers: Multiple routers are implemented at my organization with features like Network Address Translation (NAT), VPN, WPS etc. Different set of routers provide different services like connection to network, access to databases, connection to servers etc.
    - IDS/IPS: Software as well as hardware Intrusion Detection System are implemented at my organization. Cisco IPS is implemented.
    - Encryption: Data as well as network traffic is encrypted.

  - Enclave DMZ: Non-essential services are placed here in the Enclave DMZ and employees can connect to these DMZ Servers;
  - IPSec VPN Tunnel: Secure tunnel is created for employees to connect from outside the network.

- Firewalls
  - Packet filters: Deny by default policy is used in my organization. Only legit traffic is allowed into the organization based on the firewall policies.
  - Stateful Inspection: It checks all the packets based on its headers and allows access into the network.
  - Application proxy gateway: Unlike a stateful inspection firewall, this can control applications and administrations explicitly.
  - Proxy Servers: It sits in between the main firewall and application to reduce the load on firewalls, also has monitoring and logging capabilities.
  - DMZ and content filtering: Access to Social networking sites like Facebook, YouTube are blocked by using content filtering Technology.

- Routers
  - Neighbor Router Authentication: This is implemented at our organization to prevent fraudulent route updates.
  - Authenticate Routing protocol: This is special kind of authentication protocol implemented at our organization and depends on SHA-2 and IPSec Signatures.
  - Packet Assembler Dissembler (PAD): PAD is implemented and is used to gather terminal information and places them into X.25 packets and vice versa.
  - Logging Integrity: Attackers can alter the log files and timestamps, hence only NTP server or GPS must be used.
  - Router Control Policy: Different kind of router policies are implemented at our organization for allowing access to our internal networks.

- **Compare the Implementation controls discussed in class with your company's existing Cybersecurity Implementation controls**

Implementation Controls	**Status**
Enclave Protection	
Defense in Depth	Implemented
Firewalls	Implemented
Routers	Implemented
IDS/IPS	Implemented
Encryption	Implemented
Enclave DMZ	Implemented
Network Test Access Ports	NOT Implemented
Wireless IDS	NOT Implemented

Backdoor Connections	NOT Implemented
IPSec VPN Tunnel	Implemented
Firewalls	
Packet Filters	Implemented
Bastion Host	Implemented
Stateful Inspection	Implemented
Deep Packet Inspection	NOT Implemented
Application Proxy Gateway	Implemented
Hybrid Technology Firewalls	NOT Implemented
Proxy Servers	Implemented
DMZ and Content Filtering	Implemented
Routers	
Static Routers	Implemented
Neighbor Router Authentication	Implemented
Authenticate Routing Protocol	Implemented
Packet Assembler Dissembler	Implemented
Finger Service	NOT Implemented
Logging Integrity	Implemented
Router Control Policy	Implemented

- **Create a list of critical assets in $ that exist in your company**

Data is the most important asset at our company.
Some of the critical assets are:

Patients health records: Maintaining Patients health records is crucial to our organization. It will cost millions if there is any breach involving patient's health records.

Client Information: Doctors and patient's information are one of the crucial assets. Damage control will cost millions if there are any data leaks.

Employee Information: It consists of HR records. Damage control and credit monitoring services would cost the company thousands of dollars of there is a breach.

Organization Reputation: Positive Reputation for a corporation is essential for building trust and is one of the critical assets. It is intangible.

Network Devices: There are numerous network devices which could be categorized as critical assets. As Data is the most important asset, servers like SQL database are the most critical assets at our organization. Other important assets include Servers, firewalls, routers, Cisco IPS etc. These network devices cost hundreds of thousands of dollars.

- **Create a list of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing**

  - My organization uses Port Mirroring (SPAN) instead Network Test Access Ports for packet capture. Quality data is not available for monitoring.
  - In my organization, Wireless IDS (WIDS) is not implemented. WIDS helps in detection of wireless DOS attacks.
  - Deep packet inspection and hybrid technology firewalls are missing in my organization which play a key role in detection of trojans email viruses etc.
  - Finger Services is not disabled in my organization which provides presence information which can be really useful for hackers.

- **Create a list of potential threats to your company that could exploit vulnerabilities of critical assets.**

  - Span ports are used instead of network TAPs (Test Access Points), which results in data quality issues like dropping of packets, alteration of packets etc. This information may be crucial for an organization as they depend on this to detect all types of attacks or intrusions.
  - WLAN attacks cannot be detected due to the absence of WIDS as they are different from their wired counterparts. Also, knowing details of DOS attacks, like where the attack is originating from and when they would occur; would be difficult without WIDS.
  - Due to the absence of Deep packet inspection and hybrid technology firewalls only header part evaluation would be possible. Inspection of data part is also crucial as we can weed out any non-compliant protocols, intrusions and spam, which isn't possible here.
  - As Finger Service is not disabled, the user login information can be collected and be used for social engineering scams.

- **Create a list of potential risks for critical assets where Cybersecurity Implementation Controls are missing**

- Unauthorized access: Due to the absence of network TAPs, data cannot be properly monitored and collected. This can lead to unauthorized access not being detected.
- Disclosure of sensitive information: As Deep packet inspection and hybrid firewalls are not implemented, content leaving the organization cannot be detected. Data being one of the most crucial assets, disclosure of confidential information is one of the serious risks to our organization.
- Denial of Service: DOS attacks are also a possibility due to the few missing controls.

- **Provide a list of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy.**

  - Network TAPs needs to be implemented to monitor and detect malicious activities by analyzing quality packet captures.
  - Wireless IDS need to be implemented to detect WLAN attacks and DOS attacks
  - Implementation of deep packet inspection and hybrid firewall technologies is crucial as they can be able to detect malicious payload and prevent some critical cyber-attacks on the organization.

- **Provide a list of recommended Hardening methods and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy**

  - Network TAPs and Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
  - A Wireless Intrusion Detection System and Network based Intrusion Detection System can be implemented for closely monitoring, analyzing the packets, logging and notifying authorities.
  - Full scans must be run for malware from time to time basis.
  - Backdoors could be implemented by the organization for admins to regain control of the systems after the attacker has compromised and changed the credentials of the critical applications and services.

- **Create a detailed policy for the Router Security Policy using a SANS template as provided in class**

Router Security Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of company.

2.0 Scope

All routers and switches connected to company production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentications.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device."

8. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms **Definitions**

Production Network The "production network" is the network used in the daily business of company. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to company employees or impact their ability to do work.

Lab Network A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to company nor affect the production network.

6.0 Revision History

2007-04-18

- Added 3.0.8 “Telnet”

Version	Revision Date	Author
1.0	**10/27/2019**	**Abhishek Ningala**