Network Risk Management Implementation Plan II

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

- Ports, Protocols and Services
    - Block ICMPv4 Echo request and reply Packets – Denial of service attacks can be performed by the attacker by overwhelming the router and other hosts with ping packets.
    - Disable Traceroute – The IP addresses of the routers handling a particular packet can be found out and this information can be misused by the attacker.
    - Restrict Inbound and Outbound traffic – Adding policies/rules to the Access control lists can be used to control the inbound and outbound traffic.
    - IPv6 Address Filtering – Policies/rules should be set to block site local address usage, loopback address as source, unspecified address as destination and multicast addresses.
    - Unicast Reverse Path Forwarding – IP Address spoofing can be safeguarded. All the major router vendors have implemented this mechanism.
    - SYN Flood Attacks – Restriction on time window or packet rate should be implemented on routers and firewalls to defend against SYN flood attacks.

- Device Management
    - Vulnerability Management System (VMS) – It is a system for managing different kind of security vulnerabilities.
    - Current version of software and firmware: Regular patching and running the recent version of software and firmware would prevent most security incidents at any company.
    - Out of Band Management – A management technique for managing systems and devices through a connection which is separate from the actual network.
    - WAN Implementation – It is a wireless computer network which can be implemented by extending the management network.
    - In band Implementation – It is inherently vulnerable to all kinds of attacks. Security controls like advanced encryption, automatic lockouts, remote authentication etc. should be implemented to make it secure.
    - SSH Implementation – It is a secure means of encryption and remote authentication

- Device Monitoring
    - SNMP – Simple Network Management protocol is used for monitoring and managing the network devices. Only SNMPv3 is secure when compared to its previous versions.
    - Network Management Station – It provides user interface to various network management applications.

  - SNMP Management – Due to its inherent vulnerabilities, SNMP needs to be protected with proper risk management policies.

- Network Authentication, Authorization and Accounting (AAA)
  - Network Authentication – A process of confirming a user's/object's identity to gain access/use a network's resources.
  - Network Authorization – The process after authentication, which tells the user/object about its permissions of what all resources it can access.
  - Network Accounting – The process of collecting and send the security information to a centralized location for further analysis.
  - Implementation of Authentication Server – Protocols like Kerberos, RADIUS, TACACS+ and group-name for remote access.
  - Two Factor Authentication – Multiple factor authentication provides additional layers of security against any kinds of malicious attacks.
  - Implementation of Syslog Server – Configuration of all logging devices can be made easy for sysadmins by the implementation of syslog servers.
  - Router Password Protection – Different password protection policies which make use of SHA and MD5 algorithms.

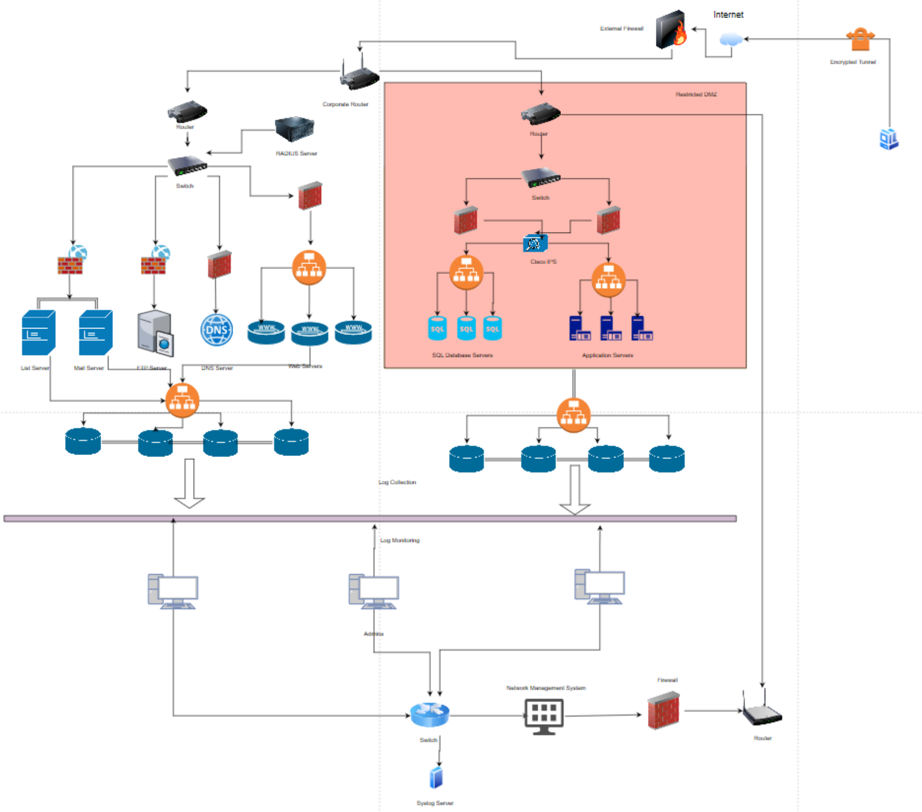
- Network Intrusion Detection Systems (NIDS)
  - Enclave NIDS – Detection, Collection and analysis of internal traffic and provides real time alerts.
  - Signature based, Anomaly based or rule-based NIDS – This is an external NIDS which notifies and alerts the CNDSP in case of any malicious attempts.

- Switches, VLANs
  - Intermediate Distribution Frames (IDF) – It is a distribution frame for connecting the communication cable between clients and Main distribution Frame (MDF).
  - VLANs – It is a convenient way for logical separation for all the network assets and devices.
  - Separation of users – Separation of users based on their department, location can result in better performance management, and a reduction of config management overhead.
  - VLAN Trunking – Increases efficiency by sharing lines or frequencies but is vulnerable to different kind of attacks.
  - VLAN Port Security – Apply policies to allow/block access to vulnerable ports thereby dropping malicious packets.
  - Usage of Sticky Addresses in VLAN – Sticky addresses really show the mac addresses and are not lost through switch reboots.
  - VLAN Management Policy Server – They allow dynamic assignment of VLANs, but they do come with inherent vulnerabilities.

- VPN
  - Gateway-to-Gateway – This is the most widely used VPN in enterprise setting and involves tunneling using GRE or IPsec.
  - Host-to-Gateway – It can be configured via tunnel-all or split tunnel modes for encrypting traffic between the host and network gateway.
  - Host-to-Host – Encrypted tunnel can be established between two computer hosts. A good example is the connection of web client to web server using https.

➢ **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. A RADIUS server is implemented to authenticate remote users securely. A syslog server is also implemented for easy configuration of all logging devices. The clients can connect through IPsec encrypted tunnel and share data securely.



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

- Ports, Protocols and Services
  - Block ICMPv4 Echo request and reply Packets – ICMPv4 pings are blocked in my company.
  - Disable Traceroute – This utility is also blocked in my organization so that attacker cannot gain any information on the internal assets.
  - Restrict Inbound and Outbound traffic – Policies on both routers and firewalls are set to restrict malicious traffic. A deny by default policy is implemented.
  - Unicast Reverse Path Forwarding – My company uses Cisco routers, and this mechanism is implemented on the routers.
  - SYN Flood Attacks – There are several mechanisms implemented in my organization against these attacks. These attacks can also be detected and blocked by the IPS implemented at the organization. The timeout policies are set on routers to drop the packets within 30 seconds before completing a 3-way handshake.

- Device Management
  - Vulnerability Management System (VMS) – Vulnerability management system is implemented at my organization by closely following the vulnerability life cycle and for managing different kinds of vulnerabilities.
  - Current version of software and firmware: My company always runs on the latest version of software and firmware. Also, there are regular checks particularly for this issue and are updated and patched if any outdated software or vulnerabilities found.
  - WAN Implementation – WAN is implemented at our organizations to connect the different LANs. It is also used to connect to different branches and data centers throughout the country.
  - In band Implementation – For managing all the devices on the network In-band network management is in place. Here, SSH protocol is used.
  - SSH Implementation – It is used in In-band management for accessing and managing all the devices.

- Device Monitoring
  - SNMP – SNMP is deployed in my organization for monitoring services. Both version 2 and version 3 of SNMP are used.
  - Network Management Station – The network management applications can be controlled using the network management station.

- Network Authentication, Authorization and Accounting (AAA)
    - Network Authentication – Kerberos V5 and SSL are used as means of network authentication.
    - Network Authorization – After successful authentication, the admin can authorize users using the ACS server.
    - Network Accounting – There are many ways to collect and send information about security events and network traffic to a centralized server like IDS, network TAPS etc.
    - Implementation of Authentication Server – In my organization RADIUS server is deployed for remote authentications.
    - Two Factor Authentication – Two Factor authentication is implemented at almost every level in my company.
    - Implementation of Syslog Server – Syslog server is implemented to configure all the logging devices which can be seen in the network diagram.
    - Router password Protection – Our company uses Cisco routers which employ type 5 encryption mechanism.

- Network Intrusion Detection Systems (NIDS)
    - Enclave NIDS – Enclave NIDS is implemented at the organization to collect, analyze, and report about the internal traffic.

- Switches, VLANs
    - VLANs – Many different kinds of VLANs like data VLAN, local VLAN, management VLAN etc. are used at my organization.
    - Separation of users – In my company, Separation of users is based on their department and function which results in better performance management.
    - VLAN Trunking – In my company VLAN trunking is achieved by sharing lines and frequencies among different users.
    - VLAN Port Security – Risk Management Policies are applied to block unused ports.
    - VLAN Management Policy Server – This server is deployed to dynamically assign VLANs.

- VPN
    - Gateway-to-Gateway – IPsec VPN services provided by the cybersecurity company Imperva are used by our company.
    - Host -to-Gateway – It is a company policy to use Host-to-Gateway VPN services for all the telecommuters.

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

Implementation Controls	Status
Ports, Protocols and Services	
Block ICMPv4 Echo request and reply Packets	Implemented
Disable Traceroute	Implemented
Restrict Inbound and Outbound traffic	Implemented
IPv6 Address Filtering	NOT Implemented
Unicast Reverse Path Forwarding	Implemented
SYN Flood Attacks	Implemented
Device Management	
Vulnerability Management System	Implemented
Current Version of Software and firmware	Implemented
Out of band Management	NOT Implemented
WAN Implementation	Implemented
In band Implementation	Implemented
SSH Implementation	Implemented
Device Monitoring	
SNMP	Implemented
Network Management Station	Implemented
SNMP Management	NOT Implemented
Network Authentication, Authorization and Auditing (AAA)	
Network Authentication	Implemented
Network Authorization	Implemented
Network Auditing	Implemented
Implementation of Authentication Server	Implemented
Two Factor Authentication	Implemented
Implementation of Syslog Server	Implemented
Router Password Protection	Implemented
Network Intrusion Detection Systems (NIDS)	
Enclave NIDS	Implemented
Signature based, Anomaly based or rule-based NIDS	NOT Implemented
Switches, VLANS	
Intermediate Distribution Frames	NOT Implemented
VLANs	Implemented
Separation of Users	Implemented
VLAN Trunking	Implemented
VLAN Port Security	Implemented
Usage of sticky addresses in VLAN	NOT Implemented

VLAN Management Policy Server	Implemented
VPN	
Gateway-to-Gateway	Implemented
Host-to-Gateway	Implemented
Host-to-Host	In Progress

- **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 millions 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.

S. No	Asset	Value (Approx.)
1	Patient Health Records	$200 Million
2	Client Information	$100 Million
3	Employee Information	$10 Million
4	Organization Reputation	Intangible
5	Network Devices	$5 Million

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

  - Out of Band Management is not implemented in my organization. This is a powerful tool for the management of critical devices which serve as a backbone for the company – for e.g., OOBM allows to remotely manage the devices even if the network is down or OS has crashed.

- In Band Management is used in my company which has many inherent vulnerabilities. Although SSH with 1024-bit RSA keys are used, the key size is small compared to today's standards.
- Both SNMP versions 2 and 3 are implemented at my company. Although SNMPv3 is secure, SNMPv2 still uses deprecated standards like MD5 and DES.
- Signature-based, Anomaly-based, or rule-based NIDS is not implemented and as a result the threat detection and analysis could not be performed effectively at the enclave gateways.
- Due to the absence of Host-to-Host VPN a secured data transfer cannot be guaranteed.

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

- As Out of Band Management is not implemented, power outages and unplanned downtime can be possible threats which could result in a possible Denial of service.
- Eavesdropping and other attacks would be possible due to the low-bit RSA key size used for in band management.
- DOS attacks, scanning attacks and other malware could hit the network in the absence of an external NIDS which usually serve as first line of defense.
- In the absence of host-to-host VPN attacks on database or servers could be possible as there is no reliable way of communication.

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

- Denial of Service: DOS attacks are also a possibility due to the absence of OOBM and external NIDS. This can have a high impact as providing services to the organization is paramount.
- Unauthorized access: Due to the absence of external NIDS, external network traffic cannot be monitored properly and malicious activities like unauthorized access may not be detected.
- Disclosure of sensitive information: Attacks like eavesdropping can play a role in disclosure of information
- Data confidentiality, Integrity and Authenticity can be compromised due to the absence of Host-to-Host VPN.

- **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.**

  - Out of Band management should be implemented alongside in band management as it is one of the best practices to manage network devices effectively.
  - Signature-based, Anomaly-based, or rule-based NIDS needs to be implemented to efficiently detect DOS attacks and other malware.
  - Host-to-Host VPN should be implemented for a secure IPsec connection using RSA between the hosts for secure data transfers and communications.

- **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**

  - It good to hire DDOS mitigation services which can handle high amounts of traffic and have data scrubbing centers in case of DOS attacks.
  - RSA key sizes should be increased to 4096 bits to safeguard against any possible attacks
  - SNMP Management system can be implemented to better analyze and monitor performance.
  - SNMPv2 should be stopped and SNMPv3 should be adopted completely as it uses much secure AES encryption standard.

➢ **Create a detailed policy for the VPN Security control using a SANS template as provided in class**

Virtual Private Network (VPN) 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

The purpose of this policy is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the company corporate network.

2.0 Scope

This policy applies to all company employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the company network. This policy applies to implementations of VPN that are directed through an IPsec Concentrator.

3.0 Policy

Approved company employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to company internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by company network operational groups.
6. All computers connected to company internal networks via VPN, or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

7. VPN users will be automatically disconnected from company's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not company-owned equipment must configure the equipment to comply with company's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of company's network, and as such are subject to the same rules and regulations that apply to company-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

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

Term	**Definition**
IPsec Concentrator	A device in which VPN connections are terminated.

6.0 Revision History

Version	Revision Date	Author
V1.0	11/3/2019	Abhishek Ningala