Wireless Risk Management Implementation Plan

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

- Wireless LAN Risk Management
    - IEEE 802.11 WLAN System Standard – It consists of some of the approved and operational WLAN IEEE standards like 802.11a, 802.11b, 802.11g etc.
    - Extensible Authentication protocol (EAP) – EAP is a standard framework for user authentication in WLAN systems.
    - EAP Transport Layer security (EAP-TLS) – The user authentication utilizes EAP protocols with TLS which provides strong security as it requires PKI certificates.
    - EAP Tunneling Transport Layer Security (EAP-TTLS) – EAP-TTLS uses only server-side certificates and uses TLS records to tunnel client authentication.
    - Protected EAP (PEAP) – When EAP protocol is used inside a tunnel, it is known as protected EAP (PEAP).
    - Lightweight EAP (LEAP) – This implementation encrypts data using WEP Keys and is used in older Cisco WLAN Access points.
    - EAP-MD5 – This authentication protocol uses Message Digest 5 algorithm and is not recommended due to its vulnerabilities since 2004.
    - Wireless Station/Client – Any device is said to be a wireless station/client if it wirelessly communicates with other network devices.
    - Wireless Network Interface Cards – Wireless NIC's are similar to their wired counterparts.
    - Access Point – They are network devices which act like a gateway between a wireless and wired network.
    - Authorized Architecture – The wireless access points and bridges should be placed in a DMZ or VLAN with a firewall.
    - Wired Equivalent Privacy (WEP) – As the name implies, it provides equivalent security of any wired medium, but was broken and replaced by WPA and WPA2.
    - Wi-Fi Protected Access (WPA) – It was a security standard replacing WEP for wireless networks but was considered insecure later due to its vulnerabilities.
    - WPA2 – It is the current security standard replacing WPA.
    - IP Security (IPSec) – IPSec is the recommended security protocol for network and transport layers.
    - WLAN Security – Secure protocols like SSL and WTLS, biometric security data encryption and user authentication can ensure WLAN security.
    - Service Set Identifier (SSID) – SSID is basically name for a Wi-Fi network.
    - MAC Address – It is unique number assigned to network interface controller.
    - RSN – It comprises of EAP protocol with AES algorithm and is used to secure wireless connections.
    - Secure Wireless networking (DoD Requirements) – There are several requirements for DoD like WPA2, AES, EAP-TLS etc.

    - Windows 2000 and XP systems – There are numerous vulnerabilities in Windows 2000 and XP systems and are not recommended for enterprises.
    - Security Boundary Implementations (DoD) – There are several security boundary implementations for DoD like WLAN devices in DMZ or VLAN with firewall and data in transit encryption policies.

- Wireless PAN Risk Management
    - Frequency-Hopping Spread Spectrum – It is a modulation used by Bluetooth which provides a 1600 hops/sec hopping rate with low power and short range.
    - Device Versions – There are several versions as follows – 1.1, 1.2, 2.0, 2.1, 3.0, 4.0, 4.1, and 4.2
    - Power Management – Low energy Bluetooth was introduced in 4.0 and updated in 4.1 and 4.2
    - Security Modes and Levels – There are 4 security modes and 4 levels with mode 1 and level 0 being least secure and mode 4 and level 4 being secure.
    - PIN/Legacy Pairing – It is a pairing mechanism in which two parties must enter a same pin code for successful paring.
    - Secure Simple Pairing – A relatively secure pairing mechanism to PIN paring which was introduced in Bluetooth 2.1
    - Security standards – There are 4 security standards which are as follows – 802.15.1, 802.15.2, 802.15.3, 802.15.3a and 802.15.4.
    - Mice and Keyboards – Wireless Mice and Keyboards cannot be protected by wireless risk management policies.

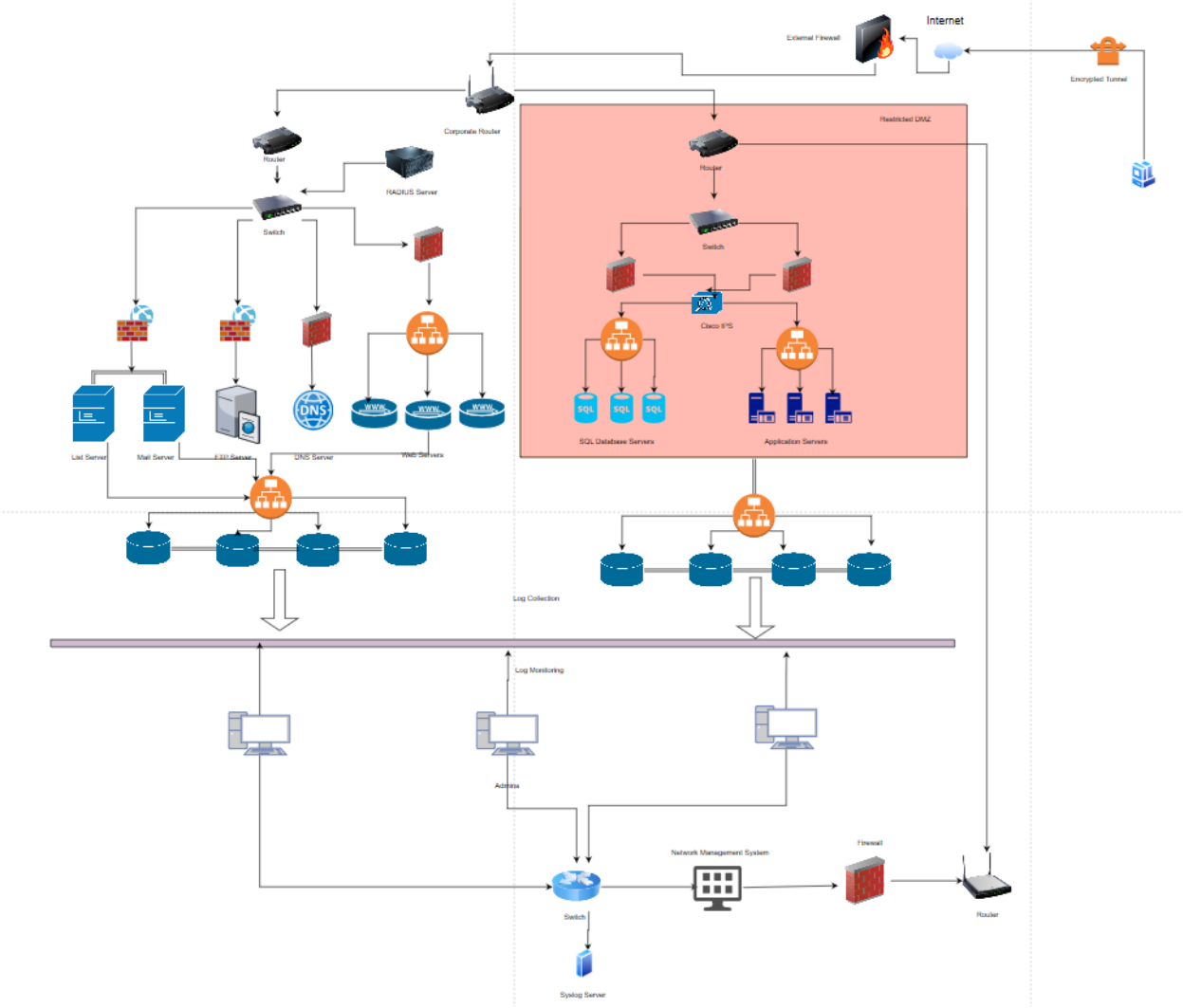
- Wireless WAN Risk Management
    - Wireless WAN security Protocols – The legacy wireless WAN protocols are as follows – Cellular digital packet data and Mobitex.
    - 802.16 Broadband Wireless Access (BWA) Standard – This standard defines interoperability requirements for wireless MANs.
    - Mobile WiMAX – It provided the users the capability to stay connected as they move between base stations.

- Wireless RFID Risk Management
    - Types of RFID Systems – There are two main types of RFID – active and passive.
    - RFID Attack Methods – There are three main attack methods – scanning tag using a reader, capturing tag while being read by authorized reader, exploitation of the network itself.

- Wireless PED Risk Management
    - Cellular Technologies – There are 5 cellular technologies ranging from 1G to 5G.
    - Short Messaging Service (SMS) – It is a standard protocol for GSM systems to transmit short messages and has no security features.
    - Multimedia Messaging Service (MMS) – It is similar to SMS, but also can transmit photos, graphics, media etc.
    - Wireless Two-Way Email – Wireless email is a secure form of email approved by the DoD.
    - PDA Security – PDAs have specialized OS like palm OS, Symbian, Windows, Java and Linux and have APIs to enhance security of applications.
    - Secure Mobile Environment PED (SME PED) – This is developed by NSA and provides DoD level security for communications.

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

  The Network Topology diagram stays the same as it follows defense-in-depth approach. 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**

- Wireless LAN Risk Management
  - IEEE 802.11 WLAN System Standard –Some of the standards used in my company are as follows – IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h.
  - EAP Transport Layer security (EAP-TLS) – The user authentication utilizes EAP protocols with TLS which provides strong security as it requires PKI certificates.
  - Wireless Station/Client – There are many wireless stations/clients being used at my organization.
  - Wireless Network Interface Cards – All the wireless stations are equipped with wireless NICs.
  - Access Point – Cisco Miraki Access points which continuously scan and protect against security threats are used at my company.
  - WPA2 – It is the current security standard replacing WPA.

- IP Security (IPSec) – Secure VPN tunneling using IPSec is implemented for all data exchanged in the company.
- WLAN Security – Security controls like user authentication, data encryption, TLS etc. are implemented at my company for WLAN security.
- Service Set Identifier (SSID) – All the networks have an SSID attached to them.
- MAC Address – All the devices have their own unique MAC address corresponding to the NICs.
- Secure Wireless networking (DoD Requirements) – These requirements are only followed when dealing with government projects.
- Security Boundary Implementation – These requirements are only followed when dealing with government projects

- Wireless PAN Risk Management
  - Frequency-Hopping Spread Spectrum – It is a modulation used by Bluetooth which provides a 1600 hops/sec hopping rate with low power and short range.
  - Device Versions – Only versions 4.0 and above are used in my company.
  - Power Management – Low energy Bluetooth may be used as they all included with versions 4.0 and above.
  - Standard Specification – This Bluetooth standard is usually followed in my company.
  - Security Modes and Levels – Security mode 3 and level 3 and above is followed at my organization.
  - Secure Simple Pairing – Secure Simple pairing is used for paring in my company.
  - Security standards – Al the 4 security standards are followed by my organization – 802.15.1, 802.15.2, 802.15.3, 802.15.3a and 802.15.4.
  - Mice and Keyboards – There are a few wireless mice and keyboards being used at my organization.

- Wireless PED Risk Management
  - Cellular Technologies – Some of popular cellular technologies used by employees are 3G and 4G
  - Short Messaging Service (SMS) – SMS may be used by employees but only on the guest networks.
  - Multimedia Messaging Service (MMS) – MMS is rarely used at my company.
  - PDA Security – Depending on the employee different kinds of OS may be used.

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

Implementation Controls	Status
Wireless LAN Risk Management	
IEEE 802.11 WLAN System Standard	Implemented
Extensible Authentication protocol (EAP)	NOT Implemented
EAP Transport Layer security (EAP-TLS)	Implemented
EAP Tunneling Transport Layer Security (EAP-TTLS)	NOT Implemented
Protected EAP (PEAP)	NOT Implemented
Lightweight EAP (LEAP)	NOT Implemented
EAP-MD5	NOT Implemented
Wireless Station/Client	Implemented
Wireless Network Interface Cards	Implemented
Access Point	Implemented
Authorized Architecture	NOT Implemented
Wired Equivalent Privacy (WEP)	NOT Implemented
Wi-Fi Protected Access (WPA)	NOT Implemented
WPA2	Implemented
IP Security (IPSec)	Implemented
WLAN Security	Implemented
Service Set Identifier (SSID)	Implemented
MAC Address	Implemented
RSN	NOT Implemented
Secure Wireless networking (DoD Requirements)	Implemented
Windows 2000 and XP systems	NOT Implemented
Security Boundary Implementations (DoD)	Implemented
Wireless PAN Risk Management	
Frequency-Hopping Spread Spectrum	Implemented
Device Versions	Implemented
Power Management	Implemented
Security Modes and Levels	Implemented
PIN/Legacy Pairing	NOT Implemented
Secure Simple Pairing	Implemented
Security standards	Implemented
Mice and Keyboards	Implemented
Wireless WAN Risk Management	
Wireless WAN security Protocols	NOT Implemented
802.16 Broadband Wireless Access (BWA) Standard	NOT Implemented
Mobile WiMAX	NOT Implemented
Wireless RFID Risk Management	

Types of RFID Systems	NOT Implemented
RFID Attack Methods	NOT Implemented
Wireless PED Risk Management	
Cellular Technologies	Implemented
Short Messaging Service (SMS)	Implemented
Multimedia Messaging Service (MMS)	Implemented
Wireless Two-Way Email	NOT Implemented
PDA Security	Implemented
Secure Mobile Environment PED (SME PED)	NOT 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 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 and software: There are numerous network devices and software 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 and applications 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**

    - Protected EAP is not implemented at my company. This method of tunneling the network communication can provide additional security.
    - My organization does not implement authorized architecture. This missing wireless risk management policy can lead to poor security of access points and bridges. Rogue access points and Evil twin access points can be easily be created.
    - Robust security network (RSN) is not implemented at my company. This can lead to poor authentication, encryption and key management services.
    - Secure Wireless networking and security boundary controls are Implemented only when dealing with government projects. This can be a vulnerability during non-government projects.

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

    - Denial of service, broken authentication attacks and MAC address spoofing are are possible due to the absence of RSN.
    - As authorized architecture is not implemented this can lead to DOS and sniffing attacks with a simple application like ethereal.
    - As Secure Wireless networking and security boundary controls are not Implemented, several network related threats are possible from phishing attacks to Advanced Persistent Threats.
    - SSIDs are not hidden at my company. This can make attackers work easy for launching a successful attack.

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

    - Denial of Service: DOS attacks are a possibility due to absence of RSN and authorized architecture. This can have a high impact as providing services to the organization is paramount.
    - Unauthorized access: Due to the absence of RSN and authorized architecture, MAC address spoofing and sniffing attacks are possible which can lead to unauthorized access.
    - Disclosure of sensitive information: As Secure Wireless networking and security boundary controls are not implemented for non-government projects, disclosure of sensitive data can be a possibility.
    - Data confidentiality can be compromised as secure tunneling method like PEAP in not used for network communication.

- **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.**

    - Additional protocols like PEAP should be used to ensure data confidentiality and integrity.
    - Authorized architecture should be implemented to secure the wireless access points and bridges.
    - Secure Wireless networking and security boundary controls must be implemented for all projects, not just govt. projects.
    - RSN can be implemented to prevent MAC address spoofing and other sniffing attacks.

- **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**

    - Wireless two-way email can be implemented for securing wireless emails for additional security.
    - SSIDs can be made hidden which makes the attackers work harder to carry out a successful attack.
    - Secure Mobile Environment PED can be used for secure voice and data communication.
    - Bluetooth mice and keyboard should be replaced with wired counterparts.

- **Create a detailed policy for the Application Service Provider Standards control using a SANS template as provided in class**

Consensus Policy Resource Community

Wireless Communication Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Last Update Status: *Updated June 2014*

1. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by company. company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. company grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to company network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a company network.

3. Scope

All employees, contractors, consultants, temporary and other workers at company, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of company must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a company network or reside on a company site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a company site and connect to a company network, or provide access to information classified as company Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use company approved authentication protocols and infrastructure.
- Use company approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to company Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the company network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

4.3.1 Wireless infrastructure devices that provide direct access to the company corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

4.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the company corporate network. Access to the company corporate network through this device must use standard remote access authentication.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- MAC Address

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Version	Revision Date	Author
V1.0	11/24/2019	Abhishek Ningala