Student:	Email:
Mani Sai Voore	mvoore@cbu.edu

Time on Task:	Progress:
	100%

Report Generated: Saturday, February 25, 2023 at 3:45 AM

Guided Exercises

Part 1: Research Critical Security Controls and Policy Statements

5. **Summarize** the guidelines for the *Wireless Access Control* section.

The Wireless Access Control Section provides the guidelines for security networks for a organization IT environment.
It tells us establishing the wireless security policy such as encryption, authentication and strong passwords as well setting up the protocols for monitoring and logging wireless access. It also suggest that disabling unnecessary services can be done by limiting the devices and updating the access controls.

Moreover, The wireless access control address the important of maintaining the up to date patches on end points as well as performing the few assessments to find the loop poles. It also tells us to use the intrusion detection and prevention systems for wireless security incidents.

They are three major components in wireless access control section is:

1. Continuous monitoring for access points.

2. securing the configuration wireless points.

3. Maintaining the inventory of all authorized and unauthorized wireless access points

In cut shot these comprehensive framework guidelines provides and ensure the confidentiality, integrity and availability for organization.

12. **Describe** the various components that make up a typical IT security policy.

For Typical IT security policy there is a approach to develop which ensures that data of firms is protected from unauthorized use and disruption even modification. The framework components are:
1. Definition: Which provide the how the policy and terms are used to ensure the clarity and evenly.

2. Roles and Responsibility: which provides the job for each individual in a group involved in implementing, developing and maintaining the policy.

3. Requirements: A section defines procedure and rules that need to be followed and complaining with policy to protect the data.

4. Policy Statement: which tells the scope, objective and purpose of the policy.

5. Reviewing: This can be done by monitoring and revising the policy to ensure it remains effectively.

6. References: which provide the list of resources to develop a regulations, policy and law.

Part 2: Draft Policy Requirements and Create a Wireless Standard

1. **Write** a sample requirement statement that would be a part of each of the following policies.

    - User Authentication Policy: This outlines the need for all users to be authenticated against a central database.
    - Authorized Networked Devices Policy: This outlines what device types/models are allowed.
    - Email Acceptable Use Policy: This outlines what confidential, personally identifiable data is allowed.

    Policies should be written with clear, simple, testable language. The more ambiguous the language used, the more difficult it is to enforce compliance. Remember, this is a practice exercise and there is no absolute wrong or right way to word a policy statement.

User Authentication Policy: Before Accessing any resources in a network all must be authenticate through central database using unique credentials algorithm that adheres to company password policy.
Authorized Network Device Policy: Only the devices are allowed which are approved by the company to connect its network. A list of permitted devices are monitored and updated on regular basis.

Email Acceptable use policy: The data flow packets allowed between the parties only for those who are encrypted with company security policy.

8. **Paste** the updated Wireless Communication Standard here.

Wireless Communication Policy

Last Update Status: *Updated October 2022*

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 Little Jerry's Beverage Company. Little Jerry's Beverage Company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Little Jerry's Beverage 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 Little Jerry's Beverage 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 Little Jerry's Beverage Company network.

3. Scope

All employees, contractors, consultants, temporary and other workers at Little Jerry's Beverage Company, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Little Jerry's Beverage Company must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Little Jerry's Beverage Company network or reside on Little Jerry's Beverage 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 Little Jerry's Beverage Company site and connect to a Little Jerry's Beverage Company network, or provide access to information classified as Little Jerry's Beverage Company Confidential, or above must:
4.1.1 For securing the tunnel we need to implement the authentication protocol need to be used which are EAP-FAST, PEAP.
4.1.2 TKIP Must be used as the encryption protocol. The length of the key should be 128 bits.
4.1.3 SSP need to be implement the Bluetooth devices also encryption need to be done at end users.
4.1.4 Use Little Jerry's Beverage Company approved encryption protocols.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to Little Jerry's
Beverage 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 Little Jerry's Beverage Company must:
4.2.1 Identify, Analyze, Implement and Develop the SSD for device network which is connected to different production devices.
4.2.2 Configuration of SSID need to be done manually by its unique ID instead of using predefined Network.

4.3 Home Wireless Device Requirements

4.3.1 Enabling the authentication we are using PSK, EAP-FAST methods.
4.3.2 Disabling the SSID instead we configure the secret key from the two end wirelessly.

5. Policy Compliance

5.1 Compliance Measurement
The Infosec team will verify compliance to this policy through various methods, including but not limited to, 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

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/

- AES
- SSID
- WPA-PSK
- PEAP
- EAP-TLS
- EAP-FAST

8. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
October 2022	SANS Policy Team	Converted to new format.
February 2023	SANS Policy Team	Updated and changed to nev

Challenge Exercises

Part 1: Conduct Additional Research

Conduct additional research about the Critical Security Controls. What is another name commonly associated with this same set of controls?

The Critical Security Controls are provided controls measures which can defend against known attacks and reduce risk of data loss. The policy guidelines has provided by center for information security.
The CSC is also known as CIS controls both of these are developed by center for information security.
The controls has divided into three categories:

1. Basic: which address the prevalent and most damaging attacks.

2. Foundation: It more emphasize on advance protection.

3. Organization: focuses on risk assessments, compliance and governance.

To advancement in technology we need to monitor patches and update the threat landscape. All sector uses this framework for developing the effective security programs not only that it also includes remediation, benchmarking, security best practices.

Part 2: Draft a Wireless Communication Policy

Download the Wireless Communication Policy template from http://www.sans.org/security-resources/policies/. **Customize** the policy components for Little Jerry's Beverage Corporation, then **paste** your completed policy here.

4.1 General Requirements All wireless infrastructure devices that reside at a Little Jerry's Beverage Corporation site and connect to a Little Jerry's Beverage Corporation network, or provide access to information classified as Little Jerry's Beverage Corporation Confidential, or above must: 4.1.1 Abide by the standards specified in the Wireless Communication Standard. 4.1.2 Be installed, supported, and maintained by an approved support team. 4.1.3 Use Little Jerry's Beverage Corporation approved authentication protocols and infrastructure. 4.1.4 Use Little Jerry's Beverage Corporation approved encryption protocols. 4.1.5 Maintain a hardware address (MAC address) that can be registered and tracked. 4.1.6 Not interfere with wireless access deployments maintained by other support organizations.