Small Town Family Medicine Security Evaluation and Upgrade

****

Western Governors University

Table of Contents

A. Proposal Overview

A.1 Problem Summary

Small Town Family Medicine (STFM) is a small doctor's office offering general medical care to local patients. The office is owned by the sole physician who is supported by a staff of four employees, two nurses and two front office staff. The doctor is approaching retirement age and has decided to sell the practice to a local hospital to ensure continued care for his patients after he steps away. As part of the preparation for the sale, the office has decided to hire Small Town Security Experts (STSE) to evaluate the current network for security issues and provide upgrades and remediations, particularly around the local server holding the personal health information (PHI) of the office's patients, which is protected under HIPAA. Ensuring that the PHI of the patients is secure will be a critical part of the sale preparations as the hospital will not want to purchase an office that risks HIPAA violations through network insecurities. The upgrades will also provide a more robust network with higher performance and reliability than the current configuration. Currently, the network consists of a store-bought Linksys SOHO router with the office computers and PHI server plugged in directly. The router broadcasts two wireless networks, one for office use with access to the server and one for patient use. The guest network password is printed on a note beside the front desk, and the internal network is not hidden but is protected with a simple WPA2 password.

A.2 IT Solution

After performing a penetration test and vulnerability assessment on the network, STSE will provide the office with a report indicating how the network is vulnerable and what remediations the team will be taking. The report will also contain a list of maintenance the team will perform on current network devices and office computers, as well as which devices will be removed or replaced, what devices and software will be installed, and a diagram explaining how the upgraded network will be laid out and function.

The network will be built using Cisco devices to ensure the reliability, performance, and support coming from an industry leader. A Firepower 1000 Series firewall in front of a 1000 Series Integrated Services Router will provide a secure connection into the office from the ISP, where a Catalyst 1200 Series switch will segment the network into VLANs and provide switching functionality across the network. For Wi-Fi connectivity, a mesh of Business 150AX Access Points will be connected to a VLAN on the switch, then used to provide three separate wireless VLANs to the office, one hidden network for wireless office laptops used by the physician and nurses to access the PHI server in exam rooms, a second for employee personal devices, and a third for patient use during their visit. All wireless networks will be secured with WPA3.

The device choices and configuration will provide the necessary performance and security while keeping in mind the small size of the office and managing upgrade costs.

A.3 Implementation Plan

First, the team will perform a penetration test of the network and attempt to gain access to the PHI server. Given the sensitive nature of the information stored on the server, we will be sure to acquire explicit written permission from the practice and detailed rules of engagement. The test will simulate a realistic type of attack based on the office’s physical location and layout with the attacker in a vehicle parked in front of the building gaining access to the server by moving through the wireless network. Once the server has been accessed, the test will end and the tester will generate a report describing the steps they took and any vulnerabilities they encountered with remediations.

After the test has concluded, the team will perform a vulnerability scan of the network as a whole. The scan results will be combined with the report from the pentester and analyzed to provide further remediations. The team will also physically examine the network devices, office computers, and server to assess any maintenance needs before delivering the overall vulnerability report, a list of remediations, and the plan for the new network layout, which will include a detailed diagram and a list of new equipment to be installed in the next phase.

After obtaining approval from the practice, the team will acquire the new network equipment and schedule an install date. The office will not be able to access the network during the installation, so they will choose a date and close for the day to allow the team to work. After installation, the team will ensure that the network is performing as desired, perform a follow-up vulnerability scan, and repeat the penetration test to verify that the security upgrades were effective at securing the server.

Implementing the plan in this fashion will ensure the team does not miss any critical vulnerabilities, the network is properly secured and returned to functionality, and, other than the installation date, the process will feel almost entirely seamless to the staff. The only changes to the staff's routine will be the day after the installation when a team member will be on-site helping the staff reconnect their personal devices to the new wireless network specifically for those devices. An infographic will be posted by the front desk to explain to patients how to connect to their new network. Having the network properly segmented and configured will limit access to the PHI server to authorized personnel and devices and prevent potential lateral movement and access from potential outside attackers. In addition, the firewall device will prevent malicious traffic from entering the network remotely. Securing the wireless networks with WPA3 will prevent cracking attacks over the air like the one simulated in the penetration test. Overall, the upgraded network will secure the PHI server behind multiple layers of defensive configurations.

Review of Other Works

Review of work 1

To perform the penetration test at the beginning of the project, the pentester will be using the aircrack-ng suite of tools to crack the WPA2 password and gain access to the internal office network. Aircrack-ng.org has a helpful tutorial on cracking WPA and WPA2. The tutorial provides a walkthrough of the actions taken to crack the network by capturing the authentication handshake when a client authenticates to the network, either passively or actively. According to the tutorial, "“actively” means you will accelerate the process by deauthenticating an existing wireless client," while "“passively” means you simply wait for a wireless client to authenticate to the WPA/WPA2 network" (Aircrack-ng, 2022). The tutorial covers several of the different tools included in the suite, including airodump-ng for the handshake capture, aireplay-ng for the deauthentication, and aircrack-ng for making use of the captured handshake to crack the pre-shared key. There is a troubleshooting section at the bottom in case the tester has trouble and even links to other articles explaining how to properly set up aircrack-ng and what type of environment it is best run in.

Review of work 2

In designing the new network, the team will be reviewing data sheets on several different network devices to choose the one that best suits the needs of the practice while keeping costs low. After exploring several options, the Cisco Business 150AX Access Point stood out as the choice for providing the office with wireless access. The datasheet, found on the Cisco website, opens with, "Ideal for smaller networks, the Cisco® Business 150AX Access Point brings a full slate of Cisco high-performance functionality to the business environment at an affordable price point" (Cisco, 2023). It goes on to lay out the specifications and features of the access point, as well as highlight the benefits that such an access point can provide to a small business. Of particular importance to the team, the sheet states that the access point supports Wi-Fi 6, wireless mesh technology, WPA3, up to 16

VLANs, and a guest network that can even authenticate against Google and Facebook logins (Cisco, 2022). This access point meets all of the needs of the office and will be the clear choice for the project.

Review of work 3

The HIPAA Journal is an online provider of news and advice relating to HIPAA, the Health Insurance Portability and Accountability Act, which governs how healthcare professionals and companies can use and store patient health information. As part of the Journal's efforts to increase HIPAA compliance, it published an article titled "How to Secure Patient Information (PHI)." The article first distinguishes what is and is not considered PHI, providing examples and drawing the distinction between patient information and patient *health* information, the latter being protected by HIPAA while the former is not. The article then provides a list of recommended defense-in-depth controls that experts recommend for protecting PHI against data theft, including things such as:

- A firewall to prevent unauthorized access to networks and data
- Data encryption on all workstations and portable devices
- An intrusion detection system that monitors for irregular network activity
- Physical controls to prevent data and equipment theft (Alder, 2025)

The rest of the article suggests that informing patients that their information is properly secured can improve patient willingness to provide full health details and facilitate better health outcomes, then provides a simple FAQ related to the topics covered. This article will be a great starting point for the team in determining what security controls need to be in place on the finished network.

Review of work 4

According to the article "Waterfall Model – Software Engineering" on GeeksforGeeks.org, the Waterfall Model is a classical software development methodology introduced in 1970 as a linear and sequential approach to software development consisting of several phases to be completed in a specific order (GeeksforGeeks, 2024). While this project is not specifically related to software development, the methodology can be applied in a general sense and provides a fitting framework for the project's progress. The article describes the model as being sequential and document-driven while placing "a high emphasis on quality control and testing at each phase of the project to ensure that the final product meets the requirements and expectations of the stakeholders" (GeeksforGeeks, 2024). It then lays out the six phases of the model as follows:

1. Requirements: The first phase involves gathering requirements from stakeholders and analyzing them to understand the scope and objectives of the project.
2. Design: Once the requirements are understood, the design phase begins. This involves creating a detailed design document that outlines the software architecture, user interface, and system components.
3. Development: The Development phase include implementation involves coding the software based on the design specifications. This phase also includes unit testing to ensure that each component of the software is working as expected.
4. Testing: In the testing phase, the software is tested as a whole to ensure that it meets the requirements and is free from defects.
5. Deployment: Once the software has been tested and approved, it is deployed to the production environment.
6. Maintenance: The final phase of the Waterfall Model is maintenance, which involves fixing any issues that arise after the software has been deployed and ensuring that it continues to meet the requirements over time. (GeeksforGeeks, 2024)

The article continues to further elaborate on each phase and the common goals and activities found during the phases then provides a real-life example for reference. Before concluding, the article discusses the advantages and disadvantages of the methodology, when to use the model, a few examples of typical applications for using a waterfall model, and an FAQ. This article will help the team lay out a plan for how to progress through the various phases of the project and keep track of project expectations to ensure the project is completed in a timely and successful fashion.

C. Project Rationale

This project is necessary to facilitate the sale of the practice to the hospital. While the likelihood of an attack on a small practice like STFM is relatively low, a large organization like the local hospital presents a much more enticing target for potential attackers looking to steal information. As such, the hospital is much less likely to consider purchasing an insecure practice that represents a higher risk of legal trouble in the form of HIPAA violations resulting from PHI exfiltration. The hospital will also likely incorporate the office network as a satellite location with access to the organization's primary network, meaning an insecure office network could grant an attacker access to the organization as a whole. Executing this project before presenting the practice for sale will make the practice a more presentable product and help secure the deal, ensuring continued medical care for the doctor's loyal patients.

D. Current Project Environment

The practice's current network consists of a store-bought Linksys SOHO router with two front-office desktop computers and a PHI server plugged in directly. The router broadcasts two wireless networks, one for office use with access to the server and one for patient use. The guest network password is printed on a note beside the front desk, and the internal network is not hidden but is protected with a WPA2 password. The doctor and nurses each have a laptop that they use to access the patients' medical records while in exam rooms. The doctor's laptop can also access the network remotely through a VPN so he can continue his work at home. The front office computers are used by the front office staff for scheduling, handling payments, processing insurance claims, and other miscellaneous office tasks. The desktops are connected directly to the multifunction printer that does not have wireless capabilities. Employee personal devices are allowed to access the internal wireless network, but there is no policy covering what types of devices are allowed or what security features the devices must have.

The current network situation presents several security threats that this project will rectify. First, the lack of network segmentation means that the only thing standing between an attacker and the PHI server is a WPA2 password on a wireless network that is not hiding its broadcast. An attacker with a laptop and Aircrack-ng could simply drive up, crack the password, and access the patients' PHI. This highlights the second serious weakness, the network's router configuration. WPA2 is less secure than WPA3, and having a visible internal network signal makes an attacker's job that much easier. Using a simple SOHO router for both networks can also present a problem, particularly since the guest network password is displayed openly by the front desk. An attacker could gain access to the router itself through the guest network and move into the internal network from there, no password cracking required.

STSE's plan resolves these security issues in several ways. By isolating the PHI server in its own VLAN and only providing access to specific pre-authorized computers, an attacker will be unable to access the server even if they gain access to the network. To prevent the attacker from accessing the network in the first place, the wireless network will be secured with WPA3 and its broadcast will be hidden. Also, by upgrading to a more robust business router from Cisco, it will be more difficult for the attacker to access the router through the guest network and gain access to an internal network. Finally, providing a separate network for employee devices will remove another vector of potential attack through the potentially insecure employee devices.

At Small Town Family Medicine, the patients' health and safety are the top priority. This project aligns with this culture and strategy by ensuring that patient data and information are kept securely. The project also aims to work within the existing environment to provide the necessary upgrades and ensure a seamless transition for the staff and patients.

E. Methodology

This project will use a waterfall methodology. This methodology makes the most sense as this is a one-time project with a straightforward endpoint. The phases are as follows:

1. Requirements: The first phase involves gathering requirements from stakeholders and analyzing them to understand the scope and objectives of the project.
2. Design: Once the requirements are understood, the design phase begins. This involves creating a detailed design document that outlines the software architecture, user interface, and system components.
3. Development: The Development phase include implementation involves coding the software based on the design specifications. This phase also includes unit testing to ensure that each component of the software is working as expected.
4. Testing: In the testing phase, the software is tested as a whole to ensure that it meets the requirements and is free from defects.
5. Deployment: Once the software has been tested and approved, it is deployed to the production environment.
6. Maintenance: The final phase of the Waterfall Model is maintenance, which involves fixing any issues that arise after the software has been deployed and ensuring that it continues to meet the requirements over time. (GeeksforGeeks, 2024)

The phases of our project will be as follows:

1. Requirements: our penetration test and vulnerability scans will make up the bulk of our requirements phase. These will inform the team of the security weaknesses our project needs to address specifically.
2. Design: for the design phase, we will create the list of new network devices to be acquired and produce the remediation report and new network diagram.

3. Development: this phase will be the installation date. The team will install and implement the new network devices and configurations, including the new VLANs and wireless networks. They will also configure a white list to allow only specific devices to access the server.
4. Testing: testing will take place on the installation day to avoid any further interruption of business for the office. Tests will be focused on ensuring proper performance across the network and that the new security features are properly functioning.
5. Deployment: this phase will be the day after the installation date when a team member is on-site helping office staff connect devices to the new network, familiarize themselves with any relevant changes, and observing the network during an actual work day to discover any issues that were not apparent during testing.
6. Maintenance: any issues that arise during the deployment phase that the on-site team member cannot resolve will be addressed during maintenance, in addition to any issues that come up in the near future. The team at STSE stands by their work and will offer support when needed during a warranty window.

F. Project Goals, Objectives, and Deliverables

F1. Relationship Table

	Goal	Supporting objectives	Deliverables enabling the project objectives
1	Evaluate the network’s security	1.a. Perform a penetration test/attack simulation	1.a.i. Vulnerability report from the pentester
		1.b. Perform vulnerability scans and provide remediations	1.b.i. Vulnerability scan report
			1.b.ii. List of remediations created from combined vulnerability reports
2	Improve network security	2.a. Design a secure network based on the office’s needs	2.a.i. Diagram of new, secure network
			2.a.ii. List of network devices to be acquired and new security configurations
		2.b. Acquire new devices	2.b.i. New network devices
		2.c. Install and configure new devices	2.c.i. New network installed and configured
			2.c.ii. New network tested and confirmed secure and functional
			2.c.iii. Staff familiarized with changes and production functionality confirmed

F.2 Goals, Objectives, and Deliverables Descriptions

The project's first goal is to evaluate the network's security with a penetration test in the form of an attack simulation and a full vulnerability scan of the network. The deliverables for this goal will be the report detailing the network vulnerabilities and the list of remediations that the team will be implementing during the project. The second goal of improving network security starts with designing a secure network. The team will deliver a diagram of the new network and a list of the new network devices that will be acquired and installed to form the new network. The team will then complete the second objective by acquiring and delivering the new network devices, and the third objective will encompass the actual installation, configuration, testing, and deployment of the new devices and network setup.

G. Project Timeline with Milestones

Milestone or deliverable	Duration (hours or days)	Projected start date	Anticipated end date
Penetration test and vulnerability scan completed	1 day	3/3/2025	3/3/2025
Vulnerability and remediation reports, new network diagram, and list of devices for acquisition finished and delivered	1 week	3/4/2025	3/11/2025
New devices acquired	2 weeks	3/12/2025	3/26/2025
Network installation	1 day	3/27/2025	3/27/2025
Staff familiarization and follow-up	1 day	3/28/2025	3/28/2025

H. Outcome

Small Town Family Medicine needs its network security evaluated and upgraded in preparation for selling the practice to the local hospital. Our team has proposed a project involving evaluating the network's current security status and then upgrading the network to provide a proper level of security for the stored patient information on the practice's server. We expect the project to require a single day of downtime on the part of the office for the network installation, but the upgrades provided will properly secure the server and prevent attackers from accessing patient information. The project will be a success when the network is properly segmented and protected against the attacks simulated by the team's penetration tester and major weaknesses discovered by the vulnerability scans. The team will evaluate these metrics during testing after installation by repeating the attack simulation and vulnerability scans. If the attack simulation can no longer access the server or any vital parts of the network, the project will be considered a success.

I. References

Alder, S. (2025, January 8). *How to Secure Patient Information (PHI).* The HIPAA Journal. https://www.hipaajournal.com/secure-patient-information-phi/

Cisco Business 150AX Access Point Data Sheet. (2023, October 3). Cisco. Retrieved February 7, 2025, from https://www.cisco.com/c/en/us/products/collateral/wireless/business-100-series-access-points/business-access-point-ds.html

Tutorial: How to Crack WPA/WPA2. (2022, January 1). Aircrack-ng.org. Retrieved February 7, 2025, from https://www.aircrack-ng.org/doku.php?id=cracking_wpa

Waterfall Model – Software Engineering. (2024, October 18). GeeksforGeeks.org. Retrieved February 7, 2025, from https://www.geeksforgeeks.org/waterfall-model/