**1.0 WHAT DID I DO**

To implement the cybersecurity audit plan, I chose my local church in Tucson, Arizona, where I have an existing connection to ensure a smoother process. The goal was to assess and provide recommendations to improve the church’s cybersecurity, focusing on physical access, security cameras, internet connections, computers, and processes like live streaming and online donation platforms.

The audit began after Sunday service, where I introduced myself to the IT Lead and team. Together, we delved into areas such as password policies, physical entries, security cameras, and online payment security, documenting observations and expected findings. Once completed, a post-audit meeting was held with Pastor Lynn and IT team to discuss initial findings and agree on action plans. Detailed processes for this audit were outlined in a prior assignment for reference.

**2.0 WHAT ARE THE RESULTS**

Below are some of the 5 major findings from the audit, with their severity and discussed in relation to the audit plan. Other findings can be referenced directly in the audit plan.

1. ***Lack of Incident Response Plan (Item #16)***

Severity: High  
The absence of an incident response plan is one of the most critical findings. Without a clear, documented plan for handling security breaches, the church is unprepared to respond to potential incidents, leaving it vulnerable to extended downtime, data loss, or reputational damage in the event of an attack. This issue must be addressed as soon as possible by developing and implementing a comprehensive incident response plan.

**2*. Weak Password Policies (Item #1)***

Severity: High  
Although it was hard for the church to provide me with some of the password’s they have during the audit, what was given me suggested mixed password strength, with some passwords being extremely weak, such as "Marana\_Methodist". Weak passwords increase the risk of unauthorized access to sensitive systems which is easier to guess. Strengthening passwords by introducing complexity helps out to throw off would be attackers.

***3. Insufficient Access Controls for Admin Accounts (Item #2)***

Severity: High  
Several staff members have admin-level access, which goes against the best practice of giving people only the access they need to do their job. Using role-based access control (RBAC) can help by limiting admin access to just the people who really need it such as the IT lead and assistant, lowering the chances of accidental or intentional misuse.

**4*. Lack of Multi-Factor Authentication (MFA) for Key Accounts (Items #14, #20)***

Severity: Medium  
Multi-factor authentication (MFA) was active for financial accounts but not for the church's social media accounts. Without MFA, these accounts are at risk of phishing and unauthorized access, especially since platforms like Facebook is used for streaming services. Adding MFA to all accounts would significantly improve their security.

***5. Outdated Systems and Plugins (Item #7)***

Severity: Medium  
Some systems, like WordPress plugins, were outdated and missing important security updates. Hackers often exploit outdated software, so keeping everything updated regularly is necessary to reduce risks.

**Some Positive Findings**

*Active and Updated SSL Certificate (Item #3)*

The church's website has an active SSL/TLS certificate, guaranteeing secure HTTPS connections for users. This secured connection protects data transmitted between users and the site, including login credentials and payment information.

*Encrypted Payment Data (Item #11)*

Payment data is securely encrypted during transmission, adhering to crucial cybersecurity standards that protect sensitive financial information. This practice means that the church follows secure protocols for handling online donations and payments, which minimizes the risk of financial fraud or data breaches of its congregation.

**3.0 RECOMMENDATIONS AND IMPLEMENTATION PLAN**

***1. Develop an Incident Response Plan (Item #16)***

Recommendation:  
Create a comprehensive incident response plan to guide the church in handling security breaches. The plan should include steps for reporting, containment, recovery, and post-incident analysis. Train the IT team and staff in executing the plan effectively. Plan and training should be completed by the end of February 2025.

Implementation Plan:  
Draft the incident response plan using free templates from reputable cybersecurity organizations or contact the auditor to assist in drafting plan. After drafting the plan, review and finalize the plan with Pastor Lynn and other IT team. Conduct a simulation exercise to test the plan's effectiveness and refine it as necessary

***2. Strengthen Password Policies (Item #1)***

Recommendation:  
Implement a policy requiring strong, complex passwords with at least 12 characters, including a mix of uppercase and lowercase letters, numbers, and symbols. Encourage the use of a password manager for secure and easy password management. Additionally, the IT team should conduct a mandatory one-time password reset for all users with weak credentials. Recommended to have password manager and password change by staff by end of December 2024.

Implementation Plan:  
Communicate the new password policy and provide training on password management tools within. Perform the one-time password reset following the communication ensuring compliance with the new standards. Enforce automated password expiration and complexity checks using built-in system features or free tools.

***3. Limit Admin Access with Role-Based Access Control (RBAC) (Item #2)***

Recommendation:  
Restrict administrative access to lead and assistant personnel only and implement a role-based access control (RBAC) system to ensure permissions are assigned based on job responsibilities. This reduces the risk of unauthorized access.

Implementation Plan:  
Firstly, identify all the IT team with admin privileges and document their access needs. Configure RBAC settings on all systems, ensuring that roles are well-defined. Test the functionality of the new access controls and adjust as necessary. Recommended to have this in place by end of Q1 2025

***4.Provide Multi-Factor Authentication (MFA) for all accounts***

Recommendation:

Enable MFA for all accounts, especially those used for social media, email, and other critical church services. Use widely available tools such as Google Authenticator, Microsoft Authenticator, or built-in MFA features of the platforms to add an additional layer of security.

Implementation

Begin by identifying all accounts that currently lack MFA. Work with the IT team to enable MFA features on these accounts within the next two weeks. Provide step-by-step guidance to account users to ensure smooth implementation. This process requires minimal cost as most MFA tools are free or included in existing services, and it has little impact on ongoing operations.

***5. Recommendation for Outdated Systems and Plugins***

Recommendation:

Develop a routine update schedule to ensure that all systems, plugins, and software are regularly updated. Enable automatic updates wherever possible to address security vulnerabilities promptly. This recommendation should be implemented by the end of November 2024.

Implementation

Assign a team member to monitor update notifications for all critical systems weekly and apply updates during off-peak hours to avoid disruptions. Enable automatic updates for WordPress plugins and other software tools. This plan can be implemented immediately, with most updates completed within one month.

**4. Risk Posture Analysis**

The church’s cybersecurity risk posture is moderately high, with significant vulnerabilities that expose it to potential threats. The greatest risk is the absence of an incident response plan, which leaves the church unprepared to manage security breaches. This could result in data loss, service disruptions, or extended downtime. Additionally, weak password policies and the lack of multi-factor authentication for key accounts increase the risk of unauthorized access.

The greatest vulnerability lies in outdated systems and plugins, which create opportunities for attackers to exploit known weaknesses. Although the church has some strengths, such as SSL encryption and secure payment data transmission, addressing these critical gaps will substantially enhance its security and reduce its exposure to cyber threats.