Team Delta

Final Project

Mentor: Caden Jones
Team Lead: Dalvin Cash
Team Members: Vitaly Andrejeus, Christian Matthews, Declan Johnson, Rob Carter
CS 6317 | Spring A 2025 | Dr. Dogdu | Angelo State University
Department of Computer Science

Project Description

This project focuses on assessing and improving cybersecurity practices at Habitat for Humanity of San Angelo. Through interviews, data collection, and a comprehensive cybersecurity evaluation, students will gain hands-on experience identifying vulnerabilities and recommending security enhancements for a nonprofit organization.

The assessment will utilize industry-standard tools such as CISA Vulnerability Scanning, CISA Free Cybersecurity Tools and Services, and CIS Establishing Essential Cyber Hygiene. Additionally, resources like Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Platform Enumeration (CPE), and the Common Vulnerability Scoring System (CVSS 4.0) will be used to evaluate and prioritize security risks.

The two objectives of this project are to help Habitat for Humanity of San Angelo strengthen its cybersecurity posture by identifying weaknesses and implementing best practices and to provide students with real-world experience in cybersecurity assessments. By the end of the project, students will understand how to conduct vulnerability assessments, analyze cyber threats, and apply cybersecurity frameworks to protect organizations from potential attacks. This initiative reinforces the importance of cybersecurity in nonprofit sectors and prepares students for future careers in related fields.

Habitat for Humanity®
of San Angelo

Habitat for Humanity of San Angelo
401 North Chadbourne Street
San Angelo, TX 76903
https://www.habitatsanangelo.org/
Phone: (325) 655-7535

Habitat for Humanity of San Angelo is a locally run affiliate of Habitat for Humanity International, a nonprofit, ecumenical Christian organization, one of over 2100 affiliates that have built more than 1,500,000 homes worldwide WITH families needing safe, decent, affordable shelter. Through volunteer labor and tax-deductible donations, Habitat works WITH partner families to build houses sold at no profit and financed with an affordable zero-interest mortgage. Partner families make no cash down payment but must contribute at least 300 hours of Sweat Equity and then pay a monthly mortgage. These mortgage payments go into a revolving Fund for Humanity to help build even more homes in San Angelo.

Project Plan

Expected project scope

This project aims to assess and improve Habitat for Humanity of San Angelo's cybersecurity practices by identifying vulnerabilities, strengthening security measures, and ensuring compliance with industry best practices. The scope includes evaluating the organization's software applications, IT infrastructure, and data security to protect against cyber threats while providing hands-on learning opportunities for students.

To-do items

1. Identify frameworks that will apply to the client's needs based on the answers to the questions provided during the first meeting.
2. Develop additional questions for the follow-up client meeting to clarify or expand on the provided answers.
3. Update the meeting agenda weekly, before the meeting

Timeline

There will be weekly meetings with the client on Mondays at 4 PM CST 02/03/2025 - 03/13/2025 to gather information and any other data related to their software security and IT needs.

Meeting Agenda

Follow up with the client with additional questions and clarifications

Questions and discussions for the upcoming meetings

1. How does your organization currently approach cybersecurity, and how do you ensure regular updates to address new and emerging threats (e.g., through insurance training modules or other methods)?

- **The organization is currently utilizing cybersecurity insurance through Lockton, and staff are going through training modules. The organization plans to rely on these training resources and may update them periodically as new threats emerge.**

2. What process do you follow to periodically review and adjust access permissions, particularly for users with elevated privileges (e.g., admins or compliance officers), and how will you ensure roles are clearly defined for all employees?

- The organization plans to begin **defining roles** for employees (full-time and part-time). The **admin roles** are under review, with **Mrs. Pam** confirmed as the admin and **Judy** as the possible compliance officer. Access to sensitive data, including the **S: drive**, will be audited, and **roles and privileges** will be clearly defined moving forward.

3. Can you confirm the current access control structure for sensitive data, such as the information stored on the S: drive, and would you be willing to conduct an audit to identify all users, including third-party service providers?

- The **S: drive** contains sensitive financial data that is not encrypted. Currently, **5**

employees have access to the drive. The organization is open to conducting an audit to identify **all users** and their privileges, including those of **third-party service providers**.

4. What measures are you planning to implement for protecting sensitive data, such as using encryption software or full disk encryption (e.g., BitLocker), and how will these measures be maintained over time?

- The organization is willing to **evaluate encryption software** (including open-source solutions and BitLocker for full disk encryption) to protect sensitive data. They plan to assess the available tools and implement encryption to secure data stored on the **S: drive**.

5. How will you work with your service providers, such as Computer Bytes and Allen Young, to ensure they are conducting necessary security testing (e.g., vulnerability scans or penetration tests), and what is the scope of support they provide?

- The organization has spoken with **Kevin Green** from **Computer Bytes**, who clarified that their services are primarily focused on **component computer alerts**, and they are willing to help with **cyberattack response,** but this is not part of the **SLA**. The organization will continue engaging with **Computer Bytes** to understand their **security testing methodologies** and to request more comprehensive testing if needed. They also intend to reach out to **Allen Young** for further clarification on their security testing protocols.

6. What steps will you take to ensure your organization meets the cybersecurity requirements for insurance claims with Lockton, and are there any specific protocols or practices required for compliance?

- The organization has been provided with **training modules** from **Lockton**, but they need to further clarify what specific cybersecurity protocols or practices are required to meet the standards for filing claims. The organization plans to contact Lockton to ensure compliance with the insurance policy's requirements.

7. How often will you provide cybersecurity training (including phishing simulations and password security practices) to your employees, and how will you ensure the program is updated regularly to stay aligned with new threats?

- The organization is committed to providing **cybersecurity training every 4 months**, which will include **phishing simulations** and **password security** practices. The program will be updated as needed, with reference to **insurance-provided training modules** and any **new emerging threats**.

Frameworks considered for software assessment report

- CIS Establishing Essential Cyber Hygiene
- Common Vulnerability Scoring System SIG
- Free Cybersecurity Services & Tools: CISA.
- Vulnerability Metrics

Cybersecurity recommendations

1. Cybersecurity Training Every 4 Months

- **Recommendation**: Conduct cybersecurity training every 4 months, as research indicates that this frequency ensures better retention of security knowledge.
- **Action**:
    - Design a **cybersecurity training program** that includes phishing simulations, password security practices, and other critical areas.
    - Use **CISA Free Cybersecurity Tools** for free training resources or third-party providers for more comprehensive training.
    - **Protocol**: Align your training program with **NIST CSF** and **CIS Control 17** to ensure all employees are up-to-date on essential security measures.
    - Regularly test security knowledge with simulated phishing campaigns or quizzes to measure training effectiveness.
- **Best Practice**: Implement **Security Awareness Training** (SAT) with quarterly updates, using real-world attack scenarios based on **CAPEC** (Common Attack Pattern Enumeration and Classification) to tailor the training to the latest threats.
- **Reference:** CISA Free Cybersecurity Tools and Services - Security Training Resources; CAPEC - Phishing and Social Engineering Techniques (CAPEC-98)

2. Access Control and User Roles

- **Recommendation**: Identify all users with access to the **S: drive** and ensure you have clear visibility into who has administrator rights and role-based access control (RBAC) policies in place.
- **Action**:
    - **Perform an audit** of the **S: drive** to identify users and their associated permissions. Ensure that **third-party service providers** are included in the audit.
    - Use **CISA Vulnerability Scanning** to review access configurations and identify any insecure or misconfigured permissions.
    - **Protocol**: Implement **Least Privilege Access** and ensure **RBAC** is properly enforced, following **NIST SP 800-53** and **CIS Control 4** for access control.
- **Best Practice**: Regularly review user permissions and maintain an **audit trail** of all access changes using tools like **CIS Cyber Hygiene** to track role assignments and adjustments. Use **Multi-Factor Authentication (MFA)** for users with elevated access.
- **Reference:** NIST SP 800-218 - Section 3.2 (Role-based Access Control); CIS Essential Cyber Hygiene - Control 4 (Access Control Management)

3. Find Good and Free Encryption Software

- **Recommendation**: Research encryption software that is both affordable and effective, such as:
    - **VeraCrypt**: Open-source disk encryption software.
    - **AxCrypt**: This offers both free and paid versions for file encryption.
    - **BitLocker**: Built into Windows for full disk encryption.
- **Action**:
    - Evaluate the tools and select one that fits your organization's needs, with a focus on **AES-256 encryption** for data at rest.
    - **Protocol**: Ensure all sensitive data is encrypted using **AES-256** and that **SSL/TLS** is used for data in transit. Regularly review encryption protocols to maintain high standards.
- **Best Practice**: Integrate **Key Management Systems (KMS)** to manage and store encryption keys securely. This is critical for ensuring long-term protection of sensitive data.
- **Reference:** Common Vulnerability Scoring System (CVSS 4.0) - Data Encryption Impact Scoring

4. Security Testing by Computer Bytes and Allen Young

- **Recommendation**: Investigate the security testing practices of **Computer Bytes** and **Allen Young** to ensure they align with industry standards.
- **Action**:
    - Contact **Computer Bytes** and **Allen Young** to ask about their testing methodologies, including whether they perform vulnerability scans, penetration tests, and code analysis.
    - Ensure they use **CISA Vulnerability Scanning** and **CVSS 4.0** to assess vulnerabilities and prioritize based on risk.
    - **Protocol**: Align with **OWASP Testing Guide** and **NIST SP 800-115** for security testing, ensuring it covers all vulnerabilities, including web applications and network infrastructures.
- **Best Practice**: Perform **penetration testing** at least quarterly and use **CVE**, **CWE**, and **CVSS 4.0** to evaluate discovered vulnerabilities and assign appropriate risk scores.
- **Reference:** CISA Vulnerability Scanning - Automated Security Scanning; OWASP Software Security 5D Framework - Security Testing Strategies

5. Lockton Cybersecurity Insurance Requirements

- **Recommendation**: Find out whether **Lockton Cybersecurity Insurance** has specific requirements to file claims.
- **Action**:
    - Contact **Lockton** to inquire about specific requirements for filing claims, focusing

    on the need for security controls, incident response plans, and vulnerability management.
  - **Protocol**: Review your **Incident Response Plan (IRP)** and ensure it aligns with **Lockton's** expectations. Implement **CIS Control 17** for incident response preparedness.
- **Best Practice**: Establish a **Security Incident Response Team (SIRT)** and conduct **Tabletop Exercises** regularly to ensure readiness for filing insurance claims in case of a security incident.
- **Reference:** CIS Essential Cyber Hygiene - Cyber Insurance Compliance Guidelines

6. Security Scanning Frequency (Internal and External Systems)

- **Recommendation**: Industry standards advise scanning internal and external systems at least quarterly. However, it is recommended to perform security assessments **monthly**.
- **Action**:
  - Set up a monthly schedule for **vulnerability scans** using tools like **CISA Vulnerability Scanning**.
  - Use **CIS Cyber Hygiene** to implement continuous vulnerability management practices.
  - **Protocol**: Apply **CISA Vulnerability Scanning** to both internal and external systems at least monthly. Use **CVSS 4.0** to evaluate and prioritize vulnerabilities based on their risk level.
- **Best Practice**: Establish an ongoing **patch management** and **vulnerability remediation** process, ensuring that vulnerabilities are addressed within the timeframe dictated by their risk score.
- **Reference:** CISA Vulnerability Scanning - Continuous Monitoring Best Practices; CVSS 4.0 - Vulnerability Prioritization Framework

7. Regular Security Awareness Training

Action:

- Conduct quarterly security training focused on:
  - Phishing awareness
  - Password security
  - Safe file-sharing practices
  - Proper use of MFA
- Use **CISA Free Cybersecurity Training** modules for cost-effective training.
- **Best Practice:** Simulate **phishing attacks** to test employee awareness and provide feedback.
- **Reference:** CISA Free Cybersecurity Tools and Services - Phishing Awareness Training; CAPEC - Social Engineering Attacks Overview

8. Implement an incident response plan

- **Recommendation**: Even though the client stated they never experienced any incidents, it is important to have a program in place for when an incident happens. Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
- **Action**:
  - Designate Personnel to Manage Incident Handling Designate one key person and at least one backup who will manage the enterprise's incident-handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually or when significant enterprise changes occur that could impact this Safeguard
  - Establish and Maintain Contact Information for Reporting Security Incidents Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date
  - Establish and Maintain an Enterprise Process for Reporting Incidents Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually or when significant enterprise changes occur that could impact this Safeguard.
- **Best Practice**: Align the organization with **CIS Control 17** of the **Establishing Essential Cyber Hygiene** guide by CIS for incident response.
- **Reference:** NIST SP 800-218 - Section 3.4 (Incident Response Preparedness); CIS Essential Cyber Hygiene - Control 17 (Incident Response Management)

9. Implement cybersecurity tools and enable account security in day-to-day software applications

- **Recommendation**: Research what steps can be taken to secure Canva and Facebook accounts.Research encryption software that is both affordable and effective, such as:
  - **Windows Defender**: Free Windows built-in antivirus.

    - **ZoneAlarm Free Firewall** – If you want extra protection beyond Windows Firewall.
    - **Malwarebytes Free** – Great for scanning and removing malware.
    - Research Canva and FB
- **Action**:
    - Take steps to secure your organization’s data while using Canva and FB accounts. Use the maximum recommended security settings in both.
    - Evaluate already available tools such as Windows Defender and implement them in your organization
    - **Protocol**: Ensure all systems are protected with recommended cybersecurity tools at all times.
- **Best Practice**: In addition to the above-mentioned tools, use a password manager to store and manage your organization’s passwords.
- **Reference:** CISA Free Cybersecurity Tools and Services - Endpoint Security Tools

10. Ensure third-party vendors comply with your security standards

- **Recommendation**: Review the security measures provided by third-party vendors you use. Ensure they fit within your organization's software security and password control requirements.
- **Action**:
    - Ensure that third-party vendors use the same encryption your organization uses.
    - Review your access controls and make sure third-party vendors adhere to your rules.
    - **Protocol**: Read third-party user agreements and contracts to ensure they fit within the standards of your organization.
- **Best Practice**: Conduct a periodic (quarterly) audit of third-party vendors and any changes to their end-user agreements or contracts. Conduct quarterly audit logs on your systems to see if third-party vendors comply with your access controls.
- **Reference:** NIST SP 800-218 - Section 4.1 (Third-Party Risk Management)

11. Use a secure web hosting platform

- **Recommendation:** It is recommended to use a secure web hosting platform like Cloudflare, AWS (with AWS WAF), or Google Cloud Armor. These tools provide built-in cybersecurity, including DDoS protection, bot mitigation, and automated security updates.
- **Action**:
    - **Choose a Secure Hosting Provider –** Opt for a hosting service that offers automated security updates, SSL/TLS encryption, and DDoS protection.
    - **Implement a WAF –** Deploy a Web Application Firewall to block malicious traffic before it reaches your website.
    - **Use Multi-Factor Authentication (MFA) –** Secure admin access with MFA to

    prevent unauthorized logins.
  - **Regularly Update Software –** Keep CMS, plugins, and dependencies up to date to patch security vulnerabilities.
  - **Enable Automated Backups –** Set up daily backups in case of cyberattacks or accidental data loss.
- **Best Practice**: Follow the Principle of Least Privilege (PoLP) – Ensure users and services only have access to the resources they need. This minimizes the risk of compromised accounts leading to full system breaches.
- **Reference:** CIS Essential Cyber Hygiene - Secure Cloud & Web Services Implementation

12. Register Similar Domain Names and Monitor for Fraudulent Websites

- **Recommendation:** It is recommended to register similar domain names and monitor for fraudulent websites. This prevents cybercriminals from creating deceptive lookalike sites to trick donors or members.
- **Action**:
  - **Secure Similar Domain Names –** Purchase common misspellings, variations, and different domain extensions (e.g., .org, .com, .net) to prevent this issue.
  - **Set Up Domain Monitoring –** Use services like Google Alerts, Whois Lookup, or domain monitoring tools (e.g., GoDaddy Domain Monitoring, Namecheap's Domain Watch) to detect fraudulent sites.
  - **Report Impersonation Websites –** If a fake site is found, report it to Google Safe Browsing for takedown.
  - **Educate Your Audience –** Inform supporters to always check the official domain name before donating or entering personal information.
- **Best Practice**: Implement **DMARC (Domain-based Message Authentication, Reporting, and Conformance)** to prevent phishing emails that appear to come from your nonprofit. These security measures help ensure that scammers cannot send emails impersonating your organization.
- **Reference:** Common Vulnerability Scoring System (CVSS 4.0) - Domain Spoofing Risk Assessment

13. Regular Software and Security Patch Management

Recommendation: Regularly update and patch software to fix vulnerabilities and prevent cyberattacks.

- **Action**: Implement a routine schedule for reviewing software updates and patches for all operating systems, software applications, and devices.
- **Protocol**: Ensure all updates are installed within a specified window (e.g., within 72 hours of release).
- **Best Practice**: Use automated patch management tools to track and apply patches

efficiently and avoid delays. Evaluate patch effectiveness and the potential risks associated with any security flaws using the CVSS 4.0 system.

- **Reference:** CISA Vulnerability Scanning - Patch Management Guidelines; CVSS 4.0 - Risk-Based Patch Prioritization

14. Backup and Disaster Recovery Planning

Recommendation: Ensure that Habitat for Humanity of San Angelo has a solid backup and disaster recovery plan in place.

- **Action**: Set up automated backups of critical data (documents, donor information, financial records) on a daily, weekly, or monthly basis, depending on its importance.
- **Protocol**: Follow the 3-2-1 backup rule (3 copies of data, 2 different media types, 1 offsite copy).
- **Best Practice**: Regularly test the backup system and recovery process to ensure it works as intended in case of a cyberattack or other disaster.
- **Reference:** CIS Essential Cyber Hygiene - Data Backup & Recovery Protocols

15. Incident Reporting Mechanism

Recommendation: Establish an easy-to-use mechanism for employees to report security incidents, suspicious activities, or potential breaches.

- **Action**: Create an accessible, centralized reporting system (either through a dedicated email, ticketing system, or internal platform) where employees can submit alerts regarding security concerns.
- **Protocol**: Ensure that the process aligns with NIST Incident Handling procedures and includes steps for escalating and resolving reported incidents.
- **Best Practice**: Provide anonymity for employees who report security issues, encouraging transparency and ensuring the company can react quickly to threats.
- **Reference:** NIST SP 800-218 - Section 3.5 (Security Incident Reporting)

16. Multi-Factor Authentication (MFA) Implementation Across All Critical Systems

Recommendation: Enforce MFA across all systems that handle sensitive data, especially for accounts with administrative privileges.

- **Action**: Implement MFA solutions such as Google Authenticator, Microsoft Authenticator, or hardware tokens for critical systems like email, databases, and file-sharing services.
- **Protocol**: Ensure that MFA is applied to both internal and third-party access points, including remote workers and cloud services.
- **Best Practice**: Review MFA coverage annually and adjust for new services or technologies introduced to the organization.

- **Reference:** NIST SP 800-218 - Section 2.3 (MFA Implementation); CIS Essential Cyber Hygiene - Control 5 (MFA Security Enforcement)

17. Data Minimization and Retention Policies

Recommendation: Implement strict data minimization and retention policies to limit the exposure of sensitive data.

- **Action**: Identify and categorize all sensitive data held by the organization. Establish retention periods based on business and legal requirements and safely delete unnecessary data when it no longer serves a purpose.
- **Protocol**: Ensure that data is encrypted during storage and transmission.
- **Best Practice**: Regularly audit data retention policies and practices to ensure that they comply with industry regulations (e.g., GDPR, HIPAA if applicable) and maintain only necessary data.
- **Reference:** CIS Essential Cyber Hygiene - Data Protection & Retention Framework

18. Phishing and Social Engineering Prevention

Recommendation: Strengthen defenses against phishing and social engineering attacks.

- **Action**: Conduct simulated phishing exercises using tools like CISA's Phishing Campaign Toolkit or third-party services to train employees on recognizing phishing attempts.
- **Protocol**: Implement email filtering tools that detect and block malicious links, attachments, and other phishing-related content.
- **Best Practice**: Encourage a culture of skepticism, where employees are encouraged to verify suspicious emails and communications before clicking links or sharing sensitive information.
- **Reference:** CISA Free Cybersecurity Tools and Services - Phishing Prevention Guides; CAPEC - Social Engineering Attack Patterns (CAPEC-166)

19. Cybersecurity Risk Assessment and Business Continuity Planning

Recommendation: Perform regular risk assessments and integrate them into the organization's business continuity planning.

- **Action**: Conduct a risk assessment every six months or after any major system change. This will identify new threats and vulnerabilities that could impact operations.
- **Protocol**: Align risk assessments with NIST SP 800-30 for risk management and adjust business continuity plans based on the latest assessment.
- **Best Practice**: Develop and test business continuity scenarios that include both cyberattacks (e.g., ransomware, data breaches) and physical disasters (e.g., fire, flood), ensuring comprehensive disaster recovery strategies.

- **Reference:** NIST SP 800-218 - Section 5.2 (Risk Management Strategies)

20. Security Hardening of Hardware and Connected Devices

Recommendation: Ensure that all hardware and connected devices are secured against vulnerabilities.

- **Action:** Disable **unnecessary services, ports, and default accounts** on servers and workstations. Remove **end-of-life (EOL) software** that no longer receives security updates. Regularly audit **printers, IoT devices, and network hardware** to ensure proper security configurations.
- **Protocol:** Apply **CIS Benchmarks** for system hardening, ensuring that all IT assets meet best-practice security configurations.
- **Best Practice:** Conduct **quarterly security reviews** of all devices and software used by the organization to ensure continuous compliance with cybersecurity standards.
- **Reference:** CIS Essential Cyber Hygiene - Hardware Security & Endpoint Protection

21. USB & External Device Security Policy

Recommendation: Prevent unauthorized USB devices from introducing malware or stealing sensitive data.

- **Action:** Disable auto-run features for USB devices to prevent malware infections. Implement Data Loss Prevention (DLP) tools to monitor and restrict file transfers to external devices. Require approval before allowing employees to use external USB storage on work computers.
- **Protocol:** Enforce endpoint security policies to restrict the use of unauthorized USB devices and log any data transfers.
- **Best Practice:** Provide organization-approved encrypted USB drives for employees who need to transfer data securely.
- **Reference:** NIST SP 800-218 - Section 2.6 (Device Security & Endpoint Control); CIS Essential Cyber Hygiene - Removable Media & USB Security Policies

22. Endpoint Detection and Response (EDR) Implementation

Recommendation: Deploy an Endpoint Detection and Response (EDR) solution to monitor and mitigate threats on all endpoints, including workstations, servers, and mobile devices.

- **Action:** Implement a robust EDR tool such as Microsoft Defender for Endpoint, CrowdStrike Falcon, or SentinelOne.Monitor endpoint activity for suspicious behavior, including unauthorized software installations and lateral movement attacks.
- **Protocol:** Ensure EDR solutions are integrated with existing security logging and monitoring tools for real-time alerts and automated response.
- **Best Practice:** Conduct periodic security assessments on endpoints to identify vulnerabilities and track compliance with cybersecurity policies.
- **Reference:** CISA Free Cybersecurity Tools and Services - Endpoint Threat Detection

23. Email Security and Spoofing Protection

Recommendation: Strengthen email security to prevent phishing, email spoofing, and business email compromise (BEC) attacks.

- **Action:** Implement Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM) to prevent spoofed emails. Use email filtering and anti-phishing solutions such as Proofpoint, Mimecast, or Google Workspace Security to scan inbound emails for threats.
- **Protocol:** Enforce email authentication policies using DMARC monitoring tools.
- **Best Practice:** Conduct phishing simulation training at least twice a year to improve employee awareness of social engineering tactics.
- **Reference:** CISA Free Cybersecurity Tools and Services - Email Security Measures; CAPEC - Business Email Compromise Attack Patterns (CAPEC-163)

Scorecard

Scores: 1- Not implemented, 2 - Needs improvement, 3 - Partial Implementation, 4 -Fully implemented, needs monitoring, 5 - Fully implemented and optimized

Recommendation	Current Status	Reference Frameworks	Score (1-5)	Explanation
Cybersecurity Training Every 4 Months	Partial Implementation	CISA Free Cybersecurity Tools, CAPEC	3	Training is conducted but lacks structured regularity and effectiveness.

Access Control and User Roles	Needs Improvement	NIST SP 800-218, CIS Hygiene	2	Access control policies exist but need stronger role-based enforcement.
Find Good and Free Encryption Software	Not Implemented	CVSS 4.0	1	Encryption practices are not in place for sensitive data.
Security Testing by External Vendors	Needs Improvement	CISA Scanning, OWASP 5D	2	Security testing is conducted but lacks comprehensive third-party assessments.
Cyber Insurance Compliance	Not Assessed	CIS Cyber Hygiene	0	Cyber insurance requirements are unclear or unassessed.
Security Scanning Frequency	Partially Implemented	CISA Scanning, CVSS 4.0	3	Security scans occur but are not conducted frequently enough.
Regular Security Awareness Training	Needs Improvement	CISA Training, CAPEC	2	Awareness training is sporadic and lacks phishing simulations.
Incident Response Plan	Not Implemented	NIST SP 800-218, CIS Hygiene	1	An incident response plan is missing or underdeveloped.

Cybersecurity Tools & Account Security	Partial Implementation	CISA Cyber Tools	3	Some security tools are in place but not fully configured.
Third-Party Security Compliance	Not Assessed	NIST SP 800-218	0	Third-party vendors' security compliance has not been evaluated.
Secure Web Hosting	Not Implemented	CIS Hygiene	1	Web hosting lacks essential security measures like WAF and DDoS protection.
Domain Monitoring & Fraud Prevention	Not Implemented	CVSS 4.0	1	No domain monitoring strategy to prevent fraudulent sites.
Patch Management	Needs Improvement	CISA Scanning, CVSS 4.0	2	Software updates are applied inconsistently, leaving vulnerabilities.
Backup & Disaster Recovery	Partial Implementation	CIS Hygiene	3	Backup processes exist but need testing and better redundancy.
Incident Reporting System	Not Implemented	NIST SP 800-218	1	Employees lack a clear system for reporting security incidents.

Multi-Factor Authentication (MFA)	Needs Improvement	NIST SP 800-218, CIS Hygiene	2	MFA is partially implemented but not enforced across all critical systems.
Data Minimization & Retention	Not Implemented	CIS Hygiene	1	Data minimization policies are weak or non-existent.
Phishing & Social Engineering Prevention	Needs Improvement	CISA Training, CAPEC	2	Basic phishing training exists, but more frequent simulations are needed.
Risk Assessment & Business Continuity	Not Implemented	NIST SP 800-218	1	Risk assessments are conducted irregularly and not integrated with business continuity plans.
Security Hardening of Devices	Partial Implementation	CIS Hygiene	3	Hardware security lacks systematic audits and hardening procedures.
USB & External Device Security	Not Implemented	NIST SP 800-218, CIS Hygiene	1	No clear policies to prevent unauthorized USB device usage.
Endpoint Detection & Response (EDR)	Not Implemented	CISA Tools	1	No endpoint detection and response tools are deployed.

Email Security & Spoofing Protection	Needs Improvement	CISA Tools, CAPEC	2	Email security measures exist but lack DMARC, SPF, and DKIM enforcement.

Conclusion

This cybersecurity assessment of Habitat for Humanity of San Angelo has provided a comprehensive evaluation of the organization's security posture, identifying key vulnerabilities and recommending measures to enhance its resilience against cyber threats. Through the application of industry-standard tools, frameworks, and methodologies, this study has yielded several critical findings that underscore the importance of robust cybersecurity practices within nonprofit organizations.

The key findings of this assessment include:

- **Enhancement of Access Control Mechanisms**: The implementation of Role-Based Access Control (RBAC), regular audits of user permissions, and the enforcement of multi-factor authentication (MFA) are essential in mitigating unauthorized access risks.
- **Strengthening Cybersecurity Awareness and Training**: Regular cybersecurity training sessions, simulated phishing exercises, and awareness programs will improve staff preparedness and reduce susceptibility to social engineering attacks.
- **Implementation of Data Protection and Encryption Measures**: Ensuring that sensitive data is encrypted both in transit and at rest, utilizing secure web hosting platforms, and adopting stringent data retention policies are fundamental in minimizing data exposure risks.
- **Development of a Comprehensive Incident Response Framework**: Establishing a well-defined incident response plan, conducting periodic security testing, and aligning with established cybersecurity frameworks such as CIS, NIST, and CISA will enhance the organization's ability to detect, respond to, and recover from cyber incidents.
- **Evaluation of Third-Party Security Compliance**: Ensuring that external service providers adhere to security policies, conducting regular audits, and assessing third-party risk management strategies will help mitigate supply chain security vulnerabilities.
- **Sustained Cybersecurity Maintenance and Risk Mitigation**: Implementing continuous vulnerability scanning, timely software patching, and adherence to cybersecurity insurance requirements will contribute to the long-term effectiveness of the organization's security infrastructure.

This study has not only contributed to the enhancement of the cybersecurity framework of Habitat for Humanity of San Angelo's cybersecurity framework but has also provided participating students with practical experience in conducting security assessments. By applying industry-recognized standards and methodologies, students have gained critical skills in vulnerability assessment, risk analysis, and the development of cybersecurity strategies, thereby preparing them for future careers in cybersecurity and information security management.

Moving forward, the organization is encouraged to implement the proposed recommendations to strengthen its security posture and safeguard its operational integrity. The findings of this assessment highlight the necessity for ongoing vigilance, proactive security measures, and a culture of cybersecurity awareness to ensure the protection of digital assets and sensitive information against emerging threats.

Future Considerations and Next Steps:

While this assessment provides a strong foundation for improving cybersecurity at Habitat for Humanity of San Angelo, maintaining a secure environment requires ongoing commitment. Moving forward, the organization should focus on the following:

- **Continuous Security Monitoring**: Implement automated monitoring tools to detect and respond to threats in real time.
- **Policy Enforcement and Compliance**: Regularly update cybersecurity policies to align with evolving threats and industry standards.
- **Annual Security Audits**: Conduct yearly cybersecurity audits to reassess vulnerabilities and ensure compliance with best practices.
- **Expanding Cybersecurity Awareness**: Foster a culture of security by integrating cybersecurity awareness into daily operations and leadership decision-making.
- **Technology Upgrades and Investments**: Evaluate and adopt emerging cybersecurity technologies that align with organizational needs and budget constraints.

By taking these steps, Habitat for Humanity of San Angelo can strengthen its long-term resilience against cyber threats, ensuring the protection of critical data and the trust of its stakeholders. This project serves as a crucial step in enhancing the organization’s security framework, but the journey toward robust cybersecurity is an ongoing process.

References

U.S. Department of Defense. “Assured Compliance Assessment Solution (ACAS).” DISA, www.disa.mil/Services/Cybersecurity/ACAS. Accessed 9 Mar. 2025.

Sochia, E., Franklin, J., & Scarlotta, T. “Establishing Essential Cyber Hygiene.” CIS Center for Internet Security, 22 Apr. 2022, https://learn.cisecurity.org/Establishing-Essential-Cyber-Hygiene.

Cybersecurity and Infrastructure Security Agency (CISA). “Free Cybersecurity Services & Tools.” CISA, www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools. Accessed 9 Mar. 2025.

Cybersecurity and Infrastructure Security Agency (CISA). “CISA Vulnerability Scanning.” CISA, www.cisa.gov/vulnerability-scanning. Accessed 9 Mar. 2025.

MITRE. “Common Attack Pattern Enumeration and Classification (CAPEC).” CAPEC, capec.mitre.org. Accessed 9 Mar. 2025.

National Institute of Standards and Technology (NIST). “Common Platform Enumeration (CPE).” NIST, nvd.nist.gov/products/cpe. Accessed 9 Mar. 2025.

MITRE. “Common Vulnerabilities and Exposures (CVE).” CVE, cve.mitre.org. Accessed 9 Mar. 2025.

First.org. “Common Vulnerability Scoring System (CVSS) Version 4.0: Specification Document.” FIRST, www.first.org/cvss/. Accessed 9 Mar. 2025.

MITRE. “Common Weakness Enumeration (CWE).” CWE, cwe.mitre.org. Accessed 9 Mar. 2025.

National Institute of Standards and Technology (NIST). “Secure Software Development Framework (SSDF) Version 1.1.” NIST SP 800-218, 2022, csrc.nist.gov/publications/detail/sp/800-218/final. Accessed 9 Mar. 2025.

Open Web Application Security Project (OWASP). “OWASP Software Security 5D Framework.” OWASP, owasp.org/www-project-software-security-5d-framework. Accessed 9 Mar. 2025.

sentinelone. “Domain Spoofing: Definition, Impact, and Prevention.” SentinelOne, 16 Jan. 2025, www.sentinelone.com/cybersecurity-101/threat-intelligence/domain-spoofing/.