**Audit Report by Lana Bracken**

**1. What Did You Do?**

The cybersecurity audit was conducted at Company X, a small chiropractic clinic, on May 2, 2025. The audit followed the structured audit plan that included onsite assessment, vulnerability scanning, interviews, and documentation review.

During the onsite visit, I reviewed the configuration of two computers, a VoIP phone, printer/scanner, Square point-of-sale system, router, and six Amazon Echo smart speakers. The audit also assessed physical security controls, surge protection, password management, software update practices, and access controls.

I conducted vulnerability scanning using Nessus Essentials, which scanned 12 hosts across the network, excluding my own laptop. This provided insight into software vulnerabilities, insecure protocols, and potential misconfigurations. I also used Nmap to perform detailed port scans, operating system detection, and identify hidden or filtered devices (e.g., IoT and mobile).

In addition to technical testing, I researched the clinic’s cloud-based electronic health record (EHR) and practice management software, Jane (<https://jane.app/>). This involved reviewing Jane’s published security documentation, privacy practices, service-level agreements, data retention policies, and procedures for user access control, backups, and patient data deletion. I specifically examined:

* Encryption and privacy practices (data in transit and at rest)
* Responsibility for system backups and breach incidents
* User account role management and access segregation
* Jane’s alignment with HIPAA/PIPEDA compliance
* Policies for third-party vendors and data retention/deletion

These findings were incorporated into the completed audit plan, and they inform the recommendations and risk posture assessment that follow.

**2. What Are the Results?**

The audit of Company X revealed several areas for improvement in cybersecurity posture, particularly in relation to password practices, device management, and cloud software configurations. A total of 29 audit items were evaluated, with observations and pass/fail designations recorded in the completed audit plan. Below are the top findings, each referencing the applicable item(s) in the audit plan:

**1. Presence of Always-Listening Smart Devices (Item 17)**

The clinic operates six Amazon Echo smart speakers throughout the facility. According to Amazon's official documentation, these devices continuously listen for wake words and, once triggered, send voice recordings to Amazon's servers. As of March 28, 2025, Amazon has removed the “Do Not Send Voice Recordings” option, meaning all user-triggered interactions are now automatically uploaded and stored in the cloud. This presents a significant privacy risk in healthcare settings, especially if such devices are located in exam rooms or other spaces where sensitive patient information may be discussed.  
**Severity**: High

**2. Two-Factor Authentication Not Enabled on Jane Accounts (Items 28–29)**

While Jane—the clinic's cloud-based practice management system—supports two-step verification for user accounts, this feature is not currently enabled for any staff. Without this added layer of security, user accounts are more vulnerable to unauthorized access, especially if passwords are compromised.  
**Severity**: High

**3. Weak Passwords on Critical Systems (Items 1, 20, 19)**

The audit found that multiple systems, including both front and back office computers and the Wi-Fi network, are protected by 4-digit PINs. In addition, the Square payment platform and VoIP phones use passwords that include dictionary words, making them more susceptible to brute-force attacks or credential stuffing attempts.  
**Severity**: High

**4. VoIP Configuration Gaps and Update Uncertainty (Items 18–19)**

The VoIP phone system is configured and accessed via a VPN, which is a good practice; however, administrative access credentials are not known by staff, preventing verification of firmware updates or advanced security configurations. Additionally, user passwords on the VoIP system are weak and shared between staff.  
**Severity**: Medium

**5. Lack of Local Computer Backups (Item 4)**

Although most of the clinic’s critical data resides in Jane’s cloud infrastructure (which has robust backup procedures), there are no backup systems in place for the local computers themselves. While this poses minimal risk to patient records, a local hardware failure could still result in significant productivity loss.  
**Severity**: Medium

**6. Shared User Accounts on Computers and VoIP Phone (Items 5, 19)**

Computers and VoIP systems are being accessed via shared credentials rather than individual user accounts. This undermines accountability and makes it impossible to determine which user performed specific actions, a critical gap in environments handling sensitive data.  
**Severity**: Low  
**Additional Nessus/Nmap Findings**

In addition to the top findings, network scans using Nessus and Nmap identified several medium-risk vulnerabilities. These include:

* Use of self-signed SSL certificates on the router (192.168.20.1), VoIP phone (192.168.20.89), and wireless bridge (192.168.20.194), which weakens the trustworthiness of encrypted communications and may allow man-in-the-middle attacks.
* Exposure of the SMB service (port 445) on the router, which is a known vector for malware and lateral movement.
* ICMP timestamp responses from multiple hosts (including the VoIP phone and router), which can aid attackers in fingerprinting devices and estimating system uptime.

**3. What are My Recommendations?**

**1. Remove or Relocate Amazon Echo Devices**

**Related Finding**: Item 17  
**Issue**: Always-on microphones present privacy risks in a healthcare setting.  
**Recommendation**: Immediately unplug all Amazon Echo devices to eliminate the risk of unintended recording. Then, assess each device's purpose and determine whether it should be permanently removed or replaced with a non-listening alternative (e.g., Bluetooth speaker with no microphone). Echo devices should not be used in any location where confidential conversations, protected health information (PHI), or staff discussions occur.  
**Implementation Notes**: Unplugging requires no cost or technical skill. Replacement options include simple, non-smart speakers for music or announcements.  
**Timeline**: Unplug immediately; assess and replace within 1–2 weeks.

**2. Enable Two-Factor Authentication (2FA) for All Jane Users**

**Related Finding**: Items 28–29  
**Issue**: Jane supports 2FA, but it is not currently enabled for any user accounts.  
**Recommendation**: Enable 2FA for all staff accounts, particularly those with access to clinical or billing data. Jane’s built-in 2-Step Verification feature uses SMS and is free to activate.  
**Implementation Notes**: Requires staff to update login credentials and link a mobile device. Training may be helpful.  
**Timeline**: Within 2 weeks.

**3. Replace Weak Passwords Across All Systems**

**Related Finding**: Items 1, 19, 20  
**Issue**: 4-digit PINs and passwords containing dictionary words are in use for Wi-Fi, Square, and VoIP access.  
**Recommendation**: Replace all passwords with strong, complex alternatives. For example, use a minimum of 12 characters with a mix of upper/lowercase, numbers, and symbols. Avoid dictionary words.  
**Implementation Notes**: Use a password manager (like LastPass) to ease management.  
**Timeline**: Within 1–2 weeks.

**4. Implement Independent Jane Data Backups Using the 3-2-1 Rule**

**Related Findings**: Items 4, 25, 26  
**Issue**: While Jane provides secure cloud storage and backups, complete reliance on any single provider (no matter how secure) exposes the clinic to risks such as cloud outages, account lockouts, ransomware, or third-party breaches.  
**Recommendation**: Perform regular exports of clinic data from Jane and store the files using the 3-2-1 backup method:

* Keep 3 copies of your data
* Store it on 2 different media types (e.g., local computer + external USB drive)
* Keep 1 copy off-site or in the cloud

Exported files should be compressed (zipped) to reduce file size and support long-term storage. This protects the clinic's operational resilience and ensures access to critical records even if Jane becomes unavailable.  
**Implementation Notes**: Use Jane’s built-in export features to download reports, schedules, and patient data in CSV or PDF formats. Store these files securely, with password protection if applicable.  
**Timeline**: Begin weekly or monthly exports within 2 weeks and automate/standardize the process within 1 month.

**5. Create Individual User Accounts for Computers and VoIP Phones**

**Related Finding**: Items 5, 19  
**Issue**: Shared credentials make accountability and auditing impossible.  
**Recommendation**: Set up separate user accounts for each employee who uses a computer or VoIP phone. Each account should have a unique, strong password.  
**Implementation Notes**: Minimal cost; requires administrator access to reconfigure systems.  
**Timeline**: Within 2–3 weeks.

**6. Implement Local Backups for Non-Cloud Devices**

**Related Finding**: Item 4  
**Issue**: While Jane handles cloud data, no local backup exists for clinic computers.  
**Recommendation**: Implement local or external drive backups for important documents, configurations, or locally stored data (e.g., browser bookmarks, app settings).  
**Implementation Notes**: Use Windows File History, Time Machine (Mac), or an external USB backup drive.  
**Timeline**: Within 1 month.

**7. Regain Administrative Access to VoIP System**

**Related Finding**: Items 18–19  
**Issue**: Admin credentials for the VoIP system are not available, preventing firmware checks or changes.  
**Recommendation**: Contact the VoIP provider (Ama TechTel) to retrieve or reset administrative access. Ensure the device firmware is up to date and change the admin password.  
**Implementation Notes**: Requires provider coordination; no software/hardware changes needed.  
**Timeline**: Within 2 weeks.

**8. Address Network-Level Vulnerabilities (Nessus/Nmap)**

These additional findings suggest areas for further network hardening to reduce the organization’s attack surface:

* Replacing self-signed SSL certificates on key devices.
* Disabling unused services (e.g., SMB) on the router if not required.
* Filtering ICMP timestamp replies via firewall rules.

**Implementation Notes**: May require coordination with your IT provider or ISP.  
**Timeline**: Within 1–2 months.

**9. Formalize BYOD and Remote Work Policies for International Staff**

**Related Finding**: Remote employee in Brazil using a personal device and internet connection.

**Issue**: The clinic's remote worker in Brazil accesses sensitive systems, such as the VoIP platform, using a personal (BYOD) device over a non-corporate internet connection. While this arrangement offers advantages, it also introduces potential security and compliance risks.

**Recommendation**: Develop and implement a formal BYOD and remote work policy tailored for international staff. This policy should:

* **Acknowledge Benefits**: Recognize the cost savings, flexibility, and increased productivity that come with remote work and BYOD arrangements.
* **Address Security Risks**: Mitigate risks such as data leakage, device loss, malware infections, and unauthorized access by:
  + Requiring the use of up-to-date antivirus software.
  + Implementing strong password policies and, where possible, multi-factor authentication.
  + Ensuring regular software and system updates.
  + Restricting access to sensitive data based on user roles.
* **Comply with Brazilian Data Protection Laws**: Ensure adherence to Brazil's General Data Protection Law (LGPD), which mandates specific obligations for companies processing personal data of individuals located in Brazil, even if the company itself is based elsewhere. This includes:
  + Obtaining clear consent for data processing activities.
  + Implementing measures to protect personal data.
  + Providing mechanisms for data subjects to exercise their rights under the LGPD.
  + Being prepared for potential audits or inquiries by Brazilian data protection authorities.

**Implementation Notes**:

* Collaborate with legal counsel familiar with Brazilian labor and data protection laws to draft compliant policies.
* Provide training sessions for international staff to ensure understanding and adherence to the new policies.

**Timeline**: Draft and review the policy within 4 weeks, with full implementation and training completed within 8 weeks.

**4. What is Risk Posture?**

Company X demonstrates a moderate overall cybersecurity posture. The organization benefits from several positive security elements, including:

* The use of a secure cloud-based platform (Jane) for the majority of its sensitive data, which reduces local exposure to threats like ransomware or data loss.
* The routine use of a VPN for remote VoIP access.
* Updated operating systems on workstations.
* The presence of working antivirus software.

However, the clinic's overall risk posture is significantly elevated by several key vulnerabilities, including: insecure smart device usage, inadequate account security, weak password practices, and a lack of comprehensive endpoint protection. A detailed examination of the vulnerabilities reveals the following:

* The presence of Amazon Echo devices throughout the facility represents a high privacy risk, particularly given the potential for unauthorized recording and transmission of Protected Health Information (PHI).
* Failure to enable two-factor authentication (2FA) on Jane accounts leaves the clinic highly vulnerable to account compromise, especially if a weak password is reused or leaked. This is the greatest technical vulnerability identified in the audit.
* The use of weak passwords (4-digit PINs) on critical systems like computers, Wi-Fi, Square, and VoIP exposes the clinic to brute-force attacks and credential stuffing.
* VoIP configuration gaps, including unknown administrative credentials and weak, shared user passwords, hinder security management and increase the risk of unauthorized access.
* The lack of local computer backups, while posing minimal risk to patient records, creates a vulnerability to productivity loss in the event of hardware failure.
* Shared user accounts on computers and VoIP phones undermine accountability and auditability, creating a significant gap in security best practices.
* Reliance on a remote employee using a BYOD device from another country introduces international compliance risks under Brazil’s LGPD and highlights the need for a formalized remote access policy.

While not presenting immediate critical risks, network-level vulnerabilities such as self-signed SSL certificates and open SMB ports expand the organization's attack surface and should be addressed as part of a continuous security improvement process. Beyond the immediate technical vulnerabilities, the clinic must also consider the broader context of data security and regulatory compliance. Reliance on cloud providers like Jane introduces systemic risks, and the clinic retains ultimate legal responsibility for protecting patient data under HIPAA and LGPD. To mitigate these risks, the clinic should:

* Regularly export its own copies of critical data and store them using the 3-2-1 backup strategy.
* Establish a written breach notification protocol aligned with U.S. Department of Health & Human Services (HHS) guidance.

In conclusion, while Company X demonstrates some positive security practices, addressing the identified vulnerabilities, particularly concerning smart device usage, account security, and remote work controls, is essential to significantly improve its overall risk posture. Furthermore, the clinic must adopt a holistic approach to data security, encompassing both technical safeguards and robust compliance measures, to ensure the long-term protection of its patients and the sustainability of its operations.