# CYBERSECURITY ASSESSMENT REPORT

**Business:** Riverbend Chiropractic
**Industry:** Healthcare (Chiropractic)
**Employees:** 6
**Date:** 2024-12-XX (Simulated)
**Consultant:** Timothy Corrado — Cybersecurity Analyst

## Executive Summary

Riverbend Chiropractic exhibits several high-severity cybersecurity weaknesses including no MFA, shared accounts, weak network security, and inadequate backup practices.
These issues significantly increase the risk of ransomware, data breaches, credential compromise, and unauthorized access.

Immediate corrective action is required in the areas of authentication, Wi-Fi security, and backups.

## Security Snapshot

| Category | Score |
|---|---|
| **Overall Security Score** | **42 / 100** |
| Network Security | 4 / 10 |
| Access Controls | 3 / 10 |
| Device Security | 5 / 10 |
| Business Processes | 1 / 10 |

## Severity Legend

- ● **High Severity** – Immediate action required
- ● **Medium Severity** – Needs timely improvement
- ● **Low Severity** – Hardening / best practice
- ○ **Unknown** – Requires verification

# Top Risks

- ● No MFA on email or administrative accounts
- ● Shared "FrontDesk" Windows login used by multiple employees
- ● Backups stored onsite only and never tested
- ● Router admin password never changed
- ● Weak Wi-Fi password and unknown WPA2/WPA3 mode

# Quick Wins (Complete Within 72 Hours)

These items provide the biggest security improvement with minimal effort:

- **Enable MFA on all email accounts immediately.**
- **Change the router admin password to a long, unique passphrase.**
- **Replace Wi-Fi password with a strong passphrase (14+ characters).**
- **Enable automatic screen lock after 5–10 minutes on all Windows PCs.**
- **Eliminate the shared "FrontDesk" account — create individual accounts for each employee.**
- **Move the router into a restricted or locked area to prevent tampering.**

# Detailed Findings

## Network / Wi-Fi

- Router admin password changed: **No** ●
  → **Action:** Change the router admin password immediately.
- WPA2/WPA3 encryption: **Unknown** ○
  → **Action:** Verify Wi-Fi is running WPA2 or WPA3. Older modes must be disabled.
- Guest Wi-Fi exists: **Yes**
- Guest Wi-Fi isolation: **Unknown** ○
  → **Action:** Enable guest network isolation to prevent access to business devices.
- Wi-Fi password strength: **Weak** ●
  → **Action:** Replace with a long passphrase immediately.
- Router firmware updated: **Unknown** ○
  → **Action:** Contact ISP or check router UI to confirm and apply updates.

### WPS & UPnP Security Notes

- ○ **Unknown** WPS status
  → **Action:** Disable WPS. It allows brute-force attacks against the Wi-Fi network.
- ○ **Unknown** UPnP status
  → **Action:** Disable UPnP. Malware can automatically open firewall ports if UPnP is enabled.
- Router physically secured: **No** ●
  → **Action:** Move router into a locked cabinet or restricted office.

---

## Devices / Workstations

- Total PCs: **4**
- Windows updates current: **Unknown** ○
  → **Action:** Verify updates are enabled and install all pending updates.
- Antivirus: Windows Defender (baseline only)
  → **Action:** Ensure Defender is active and updated automatically.
- Local admin restricted: **No** ●
  → **Action:** Remove unnecessary admin rights immediately.
- BitLocker enabled: **No** ●
  → **Action:** Enable BitLocker encryption on every workstation.
- Auto-lock enabled: **No** ●
  → **Action:** Configure auto-lock timer on all PCs.
- Shared Windows accounts: **Yes** ●
  → **Action:** Remove shared accounts and create unique user accounts.
- RDP status: **Unknown** ○
  → **Action:** Verify RDP is disabled unless explicitly required.
- USB unrestricted: **Yes** ●
  → **Action:** Restrict USB drive usage or implement an acceptable-use policy.

---

## Accounts & Access Control

- Unique logins (computers): **No** ●
  → **Action:** Assign each employee their own Windows login.

- Password complexity: **No** ●
  → **Action:** Enforce strong password rules (minimum 12 characters).
- MFA on email: **No** ●
  → **Action:** Enable MFA immediately for all accounts.
- Inactive accounts removed: **No** ●
  → **Action:** Remove all unused or stale accounts now.
- Default accounts disabled: **Unknown** ○
  → **Action:** Verify Guest and built-in Administrator accounts are disabled.

---

## Backups & Data Protection

- Backups performed: **Manual only** ●
  → **Action:** Replace manual backups with automated daily backups.
- Offsite/cloud backups: **No** ●
  → **Action:** Implement cloud/offsite backup immediately.
- Backup restore tested: **No** ●
  → **Action:** Perform a full backup recovery test.
- “Everyone” permissions likely present
  → **Action:** Remove “Everyone” access and apply role-based permissions.

---

## Business Processes

- Cybersecurity training: **No** ●
  → **Action:** Begin staff cybersecurity/phishing training.
- Incident response plan: **No** ●
  → **Action:** Create a written incident response plan.
- Onboarding process: **No** ●
  → **Action:** Document account creation and access procedures.
- Offboarding process: **No** ●
  → **Action:** Create a written account removal checklist.

---

## Physical Security

- Router/network gear secured: **No** ●
  → **Action:** Move equipment to a locked or restricted location.
- Front desk workstation exposed: **Yes** ●
  → **Action:** Add privacy filters or reposition monitors.

---

# Unknown Items (Requires Verification)

These settings could not be confirmed and may represent hidden vulnerabilities:

- WPA2/WPA3 encryption status
- Guest Wi-Fi isolation
- Router firmware status
- WPS enabled/disabled
- UPnP enabled/disabled
- RDP enabled or disabled
- Windows update configuration
- Default admin/guest account status

**Action:** Verify and correct all unknown configuration items. Treat them as risks until confirmed secure.

---

# Short-Term Recommendations (0–30 Days)

- Enable MFA on all accounts
- Replace shared logins with individual accounts
- Strengthen Wi-Fi password
- Verify WPA2/WPA3 and disable WPS/UPnP
- Enable auto-lock and BitLocker
- Secure router physically
- Verify RDP is disabled

---

# Long-Term Improvements (30–180 Days)

- Implement automated offsite/cloud backup solution
- Develop a written incident response plan
- Build documented onboarding/offboarding procedures
- Conduct annual cybersecurity training
- Review permission structure for shared folders

---

## Consultant

**Timothy Corrado**
Cybersecurity Analyst
Email: **TimothyCorrado@gmail.com**
LinkedIn: https://linkedin.com/in/timothy-corrado

---

# END OF REPORT