

CYBERSECURITY ASSESSMENT REPORT

Business: Chiropractic01
Industry: Healthcare
Employees: 7
Date: 12/19/2025
Prepared by: Timothy Corrado — Cybersecurity Analyst

Important Context for This Report

This assessment is **not a pass/fail audit**.

Most small businesses of similar size have comparable gaps.

The purpose of this report is to **identify practical, prioritized improvements** that reduce risk without disrupting daily operations.

Executive Summary (Plain English)

This report provides a high-level snapshot of **Chiropractic01's** cybersecurity posture.

Overall, the business demonstrates **several strong security practices already in place**, particularly around staff processes and basic device protection.

However, a small number of **high-priority risks** were identified that could increase exposure to ransomware, data loss, or operational downtime if left unaddressed.

The good news:

Most recommended improvements are **low-cost configuration changes**, not major technology purchases.

Security Snapshot (At-a-Glance)

Category	Score
Overall Security Score	68 / 100
Network Security	5 / 10
Access Controls	6 / 10
Device Security	6 / 10
Business Processes	10 / 10

How to read this:

Scores reflect current risk exposure, not effort or intent.

Improving a few high-priority areas can raise the overall score quickly.

What You're Doing Well

- The following controls are **configured correctly** and help reduce overall risk:
- Account cleanup practices are in place (inactive/default accounts handled correctly)
 - File sharing permissions are controlled (no broad public access)
 - Data-loss risk is reduced through removable media controls (USB restrictions)
 - Workstations have antivirus protection enabled
 - Basic network protection (router firewall) is enabled
 - Employee onboarding and offboarding procedures are documented
 - Strong password practices are in place
 - Automatic system and security updates are being maintained
 - Networking equipment is physically secured
 - Staff cybersecurity awareness training has been completed

- Workstations are configured with basic security hardening (auto-lock)

These are **foundational controls** many small businesses lack — keep these in place.

Severity Legend

- **High Priority Risk** – Action recommended soon
 - **Improvement Opportunity** – Address as time allows
 - **Unknown** – Needs verification
 - **Secure / In Place** – No action required
-

Top 5 Priority Risks

The items below represent the **most impactful risks** to address first.

- **High Severity** WPA2 or WPA3 in use
- **High Severity** Local admin disabled
- **High Severity** Shared accounts in use
- **High Severity** Unique accounts per employee
- **High Severity** MFA on email
- **High Severity** MFA on critical systems
- **High Severity** Backups stored offsite
- **High Severity** Server room restricted
- **High Severity** Workstations not publicly exposed

> Additional findings are documented later in this report.

Quick Wins (Can Usually Be Completed Within 72 Hours)

These actions provide **meaningful risk reduction** with minimal disruption.

- Enable **WPA2/WPA3** on all Wi-Fi networks
- Enable **MFA** for all email accounts
- Create **unique accounts** per employee and remove shared logins
- Eliminate **shared accounts** and assign per-user credentials
- Configure **offsite backups** (cloud or rotated external drive stored offsite)
- Restrict **server/networking access** (locked closet/room, limited key access)
- Verify all **Unknown** configurations (router settings + backup checks)

Estimated effort: Low

Estimated cost: Low (primarily configuration changes)

Detailed Findings (Reference Section)

The following pages document all reviewed areas for transparency and future planning.

Unknown items are treated as **potential risk until confirmed**.

Network / Wi-Fi

- Router firmware updated: **Yes**
✓ **Secure / In Place**
- Router admin password strong: **Yes**
✓ **Secure / In Place**
- WPA2 or WPA3 in use: **No**
• **High Severity**
- *Why it matters:* Wi-Fi encryption protects traffic from interception. Weak/legacy Wi-Fi settings increase risk of unauthorized access.

- Guest Wi-Fi exists: **Yes**
✓ **Secure / In Place**
 - Guest Wi-Fi isolated: **Unknown**
 - **Unknown**
 - SSID names recorded: **Unknown**
 - **Unknown**
 - Wi-Fi password complexity strong: **Yes**
✓ **Secure / In Place**
 - WPS disabled: **Unknown**
 - **Unknown**
 - UPnP disabled: **Unknown**
 - **Unknown**
 - Firewall enabled on router: **Yes**
✓ **Secure / In Place**
-

Devices / Workstations

- Windows Update current: **Yes**
✓ **Secure / In Place**
 - Antivirus active: **Yes**
✓ **Secure / In Place**
 - Local admin disabled: **No**
 - **High Severity**
 - *Why it matters:* Admin rights increase blast radius if a workstation is compromised.
 - BitLocker enabled: **Unknown**
 - **Unknown**
 - Auto-lock screen enabled: **Yes**
✓ **Secure / In Place**
 - Shared accounts in use: **Yes**
 - **High Severity**
 - *Why it matters:* Shared logins reduce accountability and make investigations and compliance harder.
 - RDP enabled anywhere: **Unknown**
 - **Unknown**
 - *Why it matters:* Exposed remote access is frequently targeted for ransomware intrusion.
 - Unsupported OS present: **No**
✓ **Secure / In Place**
 - USB ports restricted: **Yes**
✓ **Secure / In Place**
-

Accounts & Access Control

- Unique accounts per employee: **No**
 - **High Severity**
- *Why it matters:* Unique logins support accountability, least privilege, and safer offboarding.
- Password complexity enforced: **Yes**
✓ **Secure / In Place**
- Password expiration policy active: **Yes**
✓ **Secure / In Place**
- MFA on email: **No**
 - **High Severity**
- *Why it matters:* Email is a common entry point for phishing and ransomware; MFA blocks most account takeover attempts.
- MFA on critical systems: **No**
 - **High Severity**
- Inactive accounts removed: **Yes**
✓ **Secure / In Place**
- Default accounts disabled: **Yes**
✓ **Secure / In Place**

Backups & Data Protection

- Backups occur regularly: **Unknown**
 - **Unknown**
 - Backups stored offsite: **No**
 - **High Severity**
 - *Why it matters*: Offsite backups protect against ransomware, theft, and disasters affecting on-site systems.
 - Backup integrity tested: **Unknown**
 - **Unknown**
 - Shared folders restricted: **Yes**
 - ✓ **Secure / In Place**
 - Everyone permissions found: **No**
 - ✓ **Secure / In Place**
-

Business Processes & Human Factors

- Incident Response Plan exists: **Yes**
 - ✓ **Secure / In Place**
 - Cybersecurity training done: **Yes**
 - ✓ **Secure / In Place**
 - Onboarding documented: **Yes**
 - ✓ **Secure / In Place**
 - Offboarding documented: **Yes**
 - ✓ **Secure / In Place**
-

Physical Security

- Networking equipment secured: **Yes**
 - ✓ **Secure / In Place**
 - Server room restricted: **No**
 - **High Severity**
 - *Why it matters*: Physical access can bypass many cybersecurity controls.
 - Workstations not publicly exposed: **No**
 - **High Severity**
-

Items Requiring Verification

Any field marked with

◦ **Unknown**

indicates a configuration that could not be confirmed during the assessment.

Unknowns should be treated as **potential vulnerabilities** until verified.

Recommended Action for ALL Unknowns:

Status unknown — recommend verification with IT, router settings review, or a future on-site configuration check.

Unknown items for this assessment:

- Guest Wi-Fi isolated - SSID names recorded - WPS disabled - UPnP disabled - BitLocker enabled - RDP enabled anywhere - Backups occur regularly - Backup integrity tested

Short-Term Recommendations (0–30 Days)

- Enable WPA2/WPA3 Wi-Fi encryption

- Enforce unique user accounts and remove shared logins
 - Enable MFA on email and any critical systems
 - Implement offsite backups and define backup frequency
 - Restrict physical access to networking/server equipment
 - Verify and resolve all Unknown items
-

Long-Term Improvements (30–180 Days)

- Deploy full-disk encryption (BitLocker) on all workstations
 - Centralize identity and access management (least privilege)
 - Establish monthly backup test/restore checks
 - Perform quarterly account access reviews and annual security review
 - Document remote access policy and restrict/monitor any RDP usage
-

Closing Note

Cybersecurity improvements are **most effective when approached incrementally**.

Addressing the top priority items in this report will significantly reduce risk without requiring major changes to daily workflows.

Consultant

Timothy Corrado

Cybersecurity Analyst

✉ TimothyCorrado@gmail.com

🌐 <https://linkedin.com/in/timothy-corrado>

END OF REPORT
