CYBERSECURITY ASSESSMENT REPORT

Business: TimmyDental
Industry: Teeth
Employees: 10
Date: 12/23/2025
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 **TimmyDental**'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	**57 / 100**
Network Security	7 / 10
Access Controls	7 / 10
Device Security	7 / 10
Business Processes	2 / 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)
- Strong password practices are in place
- Automatic system and security updates are being maintained
- Networking equipment is physically secured
- Workstations are configured with basic security hardening (auto-lock)

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

Severity Legend

- ● **High Severity** – Action recommended soon
- ● **Medium Severity** – 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** Firewall enabled on router
- ● **High Severity** Windows Update current
- ● **High Severity** Antivirus active
- ● **High Severity** Unique accounts per employee
- ● **High Severity** Backups occur regularly
- ● **High Severity** Backups stored offsite
- ● **Medium Severity** Backup integrity tested

> 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.

- Create **unique accounts** per employee and remove shared logins
- Configure **offsite backups** (cloud or rotated external drive stored offsite)
- 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: **Yes**
  ✔ **Secure / In Place**
- Guest Wi-Fi exists: **No**
  ● **Medium Severity**
- Guest Wi-Fi isolated: **Yes**
  ✔ **Secure / In Place**
- SSID names recorded: **Yes**
  ✔ **Secure / In Place**
- Wi-Fi password complexity strong: **Yes**
  ✔ **Secure / In Place**
- WPS disabled: **Unknown**
  ○ **Unknown**
- UPnP disabled: **Yes**
  ✔ **Secure / In Place**

- Firewall enabled on router: **No**
  ● **High Severity**

Devices / Workstations

- Windows Update current: **No**
  ● **High Severity**
- Antivirus active: **No**
  ● **High Severity**
- Local admin disabled: **Unknown**
  ○ **Unknown**
- *Why it matters:* Admin rights increase blast radius if a workstation is compromised.
- BitLocker enabled: **Yes**
  ✔ **Secure / In Place**
- Auto-lock screen enabled: **Yes**
  ✔ **Secure / In Place**
- Shared accounts in use: **No**
  ✔ **Secure / In Place**
- *Why it matters:* Shared logins reduce accountability and make investigations and compliance harder.
- RDP enabled anywhere: **No**
  ✔ **Secure / In Place**
- *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: **No**
  ● **Medium Severity**
- MFA on email: **Yes**
  ✔ **Secure / In Place**
- MFA on critical systems: **Yes**
  ✔ **Secure / In Place**
- Inactive accounts removed: **Yes**
  ✔ **Secure / In Place**
- Default accounts disabled: **Yes**
  ✔ **Secure / In Place**

Backups & Data Protection

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

○ Unknown

Business Processes & Human Factors

- Incident Response Plan exists: **Yes**
  ✔ Secure / In Place
- Cybersecurity training done: **No**
  ● Medium Severity
- Onboarding documented: **Unknown**
  ○ Unknown
- Offboarding documented: **Unknown**
  ○ Unknown

Physical Security

- Networking equipment secured: **Yes**
  ✔ Secure / In Place
- Server room restricted: **Yes**
  ✔ Secure / In Place
- Workstations not publicly exposed: **Yes**
  ✔ Secure / In Place

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:
- WPS disabled - Local admin disabled - Everyone permissions found - Onboarding documented - Offboarding documented

---

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
Email: TimothyCorrado@gmail.com
LinkedIn: https://linkedin.com/in/timothy-corrado

END OF REPORT