CYBERSECURITY ASSESSMENT REPORT

Business: Cornerstone Dental
Industry: Healthcare
Employees: 8
Date: {{Insert Today's Date}}
Consultant: Timothy Corrado, Cybersecurity Analyst

Executive Summary

This assessment provides a high-level evaluation of **Cornerstone Dental**'s cybersecurity posture.
Several high-severity risks were identified, including default router credentials, lack of network segmentation, exposed RDP services, absence of MFA, and local-only backups.
These issues significantly increase exposure to ransomware, unauthorized access, and potential HIPAA violations.

Immediate corrective actions are recommended to reduce risk and improve business continuity.

Security Snapshot

Category	Score
Overall Security Score	**42 / 100**
Network Security	38
Access Controls	40
Device Security	45
Business Processes	45

Severity Legend

- 🔴 **High Severity** – Immediate attention required
- 🟠 **Medium Severity** – Important, address soon
- 🟡 **Low Severity** – Hardening / best-practice improvements

---

Top Risks

1. 🔴 Default router admin password
2. 🔴 No guest Wi-Fi network
3. 🔴 RDP enabled on 2 PCs
4. 🟠 Backups stored locally only
5. 🔴 No MFA on email

Quick Wins (Complete Within 72 Hours)

- Change default router admin password to a long, unique passphrase
- Create an isolated **Guest Wi-Fi** network
- Disable **RDP** on all machines not requiring remote access
- Enable **MFA** on all staff email accounts
- Begin using **secure cloud/offsite backups**

Detailed Findings

Network / Wi-Fi

- Router still uses default admin credentials (critical exposure)
- No guest network; patients share same SSID as staff systems
- Wi-Fi uses only WPA2; not configured for WPA3
- Router's firmware status unknown; likely outdated

Workstations

- RDP enabled on 2 workstations — common ransomware entry point
- Shared "FrontDesk" login; no user accountability
- BitLocker disk encryption not enabled
- Patch/update status requires review

Server / Backups

- Backups stored locally only; no offsite redundancy
- Local backup device vulnerable to ransomware wipe
- No documented backup testing or recovery process

Business Processes & Human Factors

- No MFA on email accounts
- No employee phishing/security awareness training
- No documented incident response plan
- No quarterly access review process

Recommendations

Short-Term (0–30 Days)

- Change router admin password; verify firmware is current
- Create segmented **Guest Wi-Fi** network
- Disable RDP on all non-admin machines
- Enable MFA across all email and cloud accounts
- Begin offsite/cloud backup solution
- Enforce unique user accounts for all employees

Long-Term (30–180 Days)

- Implement a formal **Incident Response Plan**
- Deploy BitLocker encryption on all workstations
- Conduct quarterly access and permission reviews
- Provide basic cybersecurity training to staff
- Replace ISP-provided router with a business-grade firewall/router

---

Contact

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