Cyber Wise Corp

Cybersecurity Assessment Report

Expert-reviewed by CISSP-certified security professionals

Prepared for: Desert Sun Veterinary Clinic

[Address withheld for privacy], Scottsdale, AZ, 85251

OVERALL SECURITY POSTURE

D

Needs Attention

Score: 12/20 (60.0%)

Report ID: DEMO-BIZ

Generated May 03, 2026

Executive Summary

D

Needs Attention - Score: 12/20 (60.0%)

Your security has significant weaknesses that put your data, devices, and accounts at real risk. Treat the recommendations in this report as urgent - most can be done in a weekend.

Your Top Priorities

> **Device Security (2/5)**

1) Upgrade or replace the Windows 10 22H2 machine within 30 days - it is no longer receiving security updates and represents your single...

> **Network Security (3/5)**

1) Delete the unnamed open SSID immediately - this is broadcasting an unauthenticated entry point to your network.

> **Data Security (3/5)**

1) Audit and remove the 23 external 'anyone with link' shares - 3 of those contain customer payment data and could trigger PCI/state breach...

What You Are Doing Well

\+ **User Awareness (4/5)**

Training: company subscribes to KnowBe4 and runs monthly phishing simulations.

! CRITICAL FINDINGS - Address Within 7 Days

! Open WiFi SSID (no encryption, no captive portal) is broadcasting from the office router. Anyone in the parking lot or adjacent suite can join and reach internal resources. Disable in the UDM-Pro admin within 24 hours.

! Two former employees (departed in 2024 and 2025) still have active SSH keys on the office router. Revoke these immediately - departed-employee credentials are the source of an estimated 20%% of small-business breaches.

! Three SharePoint files containing customer payment records (credit card last-4, billing addresses) are shared 'with anyone who has the link'. This creates exposure under state breach notification laws and PCI DSS. Revoke today.

Report Information

Report ID	DEMO-BIZ
Client	Desert Sun Veterinary Clinic
Service Address	[Address withheld for privacy], Scottsdale, AZ, 85251
Service Type	Business Assessment
Assessor	Priya Shah - Arizona State University
Expert Reviewer	Chad Freese, CISSP, CCSP, CRISC, AIGP
Generated	2026-05-03 09:10 UTC

Assessor's Full Summary

This 8-person business has a security culture significantly above its peers - the ownership clearly invests in training, has selected appropriate tools (1Password Business, M365 Business Standard, Ubiquiti), and the team uses them well. Where the assessment found gaps, they reflect under-configured tools rather than missing tools, which is a much easier remediation posture. The two areas requiring near-term attention are (a) network segmentation - everything currently shares one VLAN including the POS terminal, which expands PCI scope unnecessarily and creates lateral movement risk - and (b) device security on the unencrypted Windows machines, particularly the bookkeeper's laptop. The Critical Findings should be addressed within 7 days; the unsegmented network and unencrypted disks within 30. With those changes plus the third-party M365 backup, this business would move from an Adequate posture to Strong. Consider a follow-up engagement in 6 months to verify segmentation work and re-baseline.

Detailed Category Breakdown

Each category is scored on a 5-point scale. The 'industry baseline' shows the average score for households or small businesses we have assessed - use it to gauge where you stand relative to your peers.

Network Security — 3/5 - D (Needs Attention)

4% below industry baseline (64%)

What this measures

Your home or office WiFi, router, and how cleanly your network is segmented.

Why it matters

Your network is the front door. A poorly configured router or weak WiFi password lets attackers onto your network without ever touching your devices, where they can intercept traffic, attack other devices, or use your bandwidth for illegal activity.

Threats this protects against

* Wardriving and unauthorized WiFi access
* Router admin compromise
* Lateral movement between devices

Assessor's findings at your location

Office network is built around a Ubiquiti UDM-Pro running current firmware. Three SSIDs configured: corporate (WPA3), guest (WPA2 with captive portal), and an unnamed open network with no encryption that appears to be left over from a former IT vendor's testing. Site-to-site VPN is configured but uses an outdated IKEv1 profile. Network segmentation: production servers, employee workstations, and IoT devices (printers, conference room equipment) all share VLAN 1. The point-of-sale terminal at the front desk is also on VLAN 1. Firewall rules are largely default - no egress filtering, port scanning is allowed outbound. No intrusion detection. The router admin password is strong but two former employees still have admin SSH keys.

Recommendations

1) Delete the unnamed open SSID immediately - this is broadcasting an unauthenticated entry point to your network. 2) Remove SSH keys for the two former employees (their names are in the appendix delivered separately). 3) Migrate the VPN to IKEv2 with modern crypto (AES-256-GCM, SHA2-384). 4) Implement basic VLAN segmentation: VLAN 10 for production servers, VLAN 20 for workstations, VLAN 30 for IoT/printers, VLAN 40 for the POS terminal (PCI scope). The UDM-Pro supports this natively. 5) Add basic egress filtering blocking known C2 destinations (Cisco Talos publishes free lists).

Device Security 2/5 - F (Action Required)

18% below industry baseline (58%)

What this measures

Operating system patching, endpoint protection (antivirus/EDR), disk encryption, and IoT device hygiene.

Why it matters

Devices are where attackers actually do damage - installing ransomware, stealing data, or pivoting to other systems. An unpatched OS or default-password IoT device is the most common entry point in residential breaches.

Threats this protects against

* Ransomware
* Credential theft via malware
* IoT botnet recruitment (Mirai-style)

Assessor's findings at your location

Eight employee endpoints assessed - mix of Windows 11 (5) and macOS (3). Patch status: 4 of 5 Windows machines current, 1 still on Windows 10 22H2 (out of mainstream support since October 2025). All 3 Macs current. Endpoint protection: Microsoft Defender on Windows (acceptable baseline), no third-party EDR. Disk encryption: BitLocker NOT enabled on 3 of 5 Windows machines, FileVault enabled on all 3 Macs. The unencrypted machines include the bookkeeper's laptop which holds QuickBooks files locally. Two employees admitted to using their personal phones to access the company Microsoft 365 tenant - one of those phones (Android) has not been updated since 2024. The POS terminal at the front desk is running Windows 10 IoT Enterprise LTSC, which is supported through 2032 (good). One server in the back office runs Windows Server 2019 with patches current.

Recommendations

1) Upgrade or replace the Windows 10 22H2 machine within 30 days - it is no longer receiving security updates and represents your single largest endpoint risk. 2) Enable BitLocker on all 5 Windows endpoints. The bookkeeper's machine is the priority - QuickBooks files contain financial PII that triggers breach notification laws if lost unencrypted. 3) Implement basic MDM (Microsoft Intune is included with M365 Business Premium) and enforce a policy that company data only accessible from managed devices. This addresses the personal-phone-with-company-data risk. 4) Consider upgrading from Defender baseline to Defender for Business (part of M365 Business Premium) for better detection and response.

Data Security 3/5 - D (Needs Attention)

8% above industry baseline (52%)

What this measures

Backup strategy, where files are stored, and how data is shared with others.

Why it matters

If something goes wrong - hardware failure, ransomware, theft - your backup is the only thing standing between an inconvenience and a catastrophe. The 3-2-1 rule (3 copies, 2 different media, 1 offsite) remains the gold standard.

Threats this protects against

* Ransomware encryption (no recovery without backup)
* Hardware failure / theft
* Accidental data exposure via misconfigured cloud sharing

Assessor's findings at your location

Microsoft 365 Business Standard tenant in use. OneDrive for Business is deployed for all 8 employees. SharePoint document libraries hold the bulk of business records. Backups: Microsoft handles M365 retention (good), but no third-party backup of the M365 tenant exists - if a malicious or accidental deletion is not caught within Microsoft's retention window, data is gone. The on-premise server has nightly backups to a NAS in the same room as the server (single-site failure risk). External sharing audit: found 23 SharePoint files shared externally with 'anyone with the link', including 3 that contain customer payment records. Records retention policy is undocumented. No DLP (Data Loss Prevention) rules configured.

Recommendations

1) Audit and remove the 23 external 'anyone with link' shares - 3 of those contain customer payment data and could trigger PCI/state breach notification obligations if discovered by an auditor. 2) Add a third-party M365 backup (Veeam, Datto SaaS Protection, Spanning) - Microsoft retention is not a backup. Ransomware that encrypts a OneDrive folder syncs the encryption to all employees' machines. 3) Move the on-prem server backup to an offsite destination (Azure Backup vault is included with M365 Business Premium). 4) Enable basic M365 DLP policies for credit card numbers and SSNs - out-of-the-box templates exist.

User Awareness 4/5 - B (Strong)

19% above industry baseline (61%)

What this measures

Password practices, multi-factor authentication adoption, and ability to recognize phishing.

Why it matters

Over 80% of breaches start with a human element - reused passwords, falling for a phishing email, or skipping MFA prompts. The strongest technical controls fail if a single account gets compromised through social engineering.

Threats this protects against

* Phishing and credential theft
* Account takeover via password reuse
* SIM-swap attacks bypassing SMS-only MFA

Assessor's findings at your location

Training: company subscribes to KnowBe4 and runs monthly phishing simulations. Most recent simulation (March 2026) had a 12% click rate, which is significantly better than the small business industry average (28%). Two employees clicked: both have completed remedial training. Password practices: all employees use 1Password Business; password reuse audit shows zero reused passwords across business accounts. MFA: enabled on all M365 accounts (mandatory via conditional access). No SMS-based MFA - all authenticator app or hardware token. The owner uses a YubiKey. One gap: the two contractors who have M365 guest access do not have MFA enforced. Incident reporting: clear written process exists, posted on the kitchen board. One employee reported a suspicious email last month and it turned out to be a real phishing attempt - the team handled it well.

Recommendations

1) Enforce MFA on the two contractor accounts via conditional access policy. Contractors are a frequent attack vector because their security posture is outside your control. 2) Schedule a quarterly tabletop exercise (30 minutes) walking the team through 'what if our M365 tenant got compromised tomorrow' - free tabletop scenarios are at cisa.gov. 3) Consider migrating the entire team to YubiKeys (phishing-resistant) given the demonstrated culture of taking security seriously.

30 / 60 / 90 Day Remediation Roadmap

A practical sequence for addressing the items in this report. Most items can be done in well under the suggested timeframe - the windows are deliberately generous so progress feels achievable. If you only do the THIS WEEK items, you will close the highest-impact gaps.

THIS WEEK - Critical Findings (P0)

! Open WiFi SSID (no encryption, no captive portal) is broadcasting from the office router. Anyone in the parking lot or adjacent suite can join and reach internal resources. Disable in the UDM-Pro admin within 24 hours.

! Two former employees (departed in 2024 and 2025) still have active SSH keys on the office router. Revoke these immediately - departed-employee credentials are the source of an estimated 20%% of small-business breaches.

! Three SharePoint files containing customer payment records (credit card last-4, billing addresses) are shared 'with anyone who has the link'. This creates exposure under state breach notification laws and PCI DSS. Revoke today.

THIS MONTH - High-Risk Categories (P1)

> Device Security

1) Upgrade or replace the Windows 10 22H2 machine within 30 days - it is no longer receiving security updates and represents your single largest endpoint risk.

THIS QUARTER - Medium-Risk Improvements (P2)

> Network Security

1) Delete the unnamed open SSID immediately - this is broadcasting an unauthenticated entry point to your network.

> Data Security

1) Audit and remove the 23 external 'anyone with link' shares - 3 of those contain customer payment data and could trigger PCI/state breach notification obligations if discovered...

NEXT 6 MONTHS - Optimization (P3)

> User Awareness

1) Enforce MFA on the two contractor accounts via conditional access policy. Contractors are a frequent attack vector because their security posture is outside your control.

Appendix: Glossary

MFA / 2FA

Multi-Factor Authentication. Requires a second proof of identity (app code, hardware key, biometric) beyond just a password. Use an authenticator app (Authy, Google Authenticator, 1Password) over SMS when possible - SMS can be intercepted via SIM swapping.

WPA3 / WPA2

WiFi encryption standards. WPA3 is current and strongest (mandatory on devices sold after 2020). WPA2 is acceptable if WPA3 is not supported. WEP and "Open" are obsolete and easily cracked.

Endpoint Protection

Software that detects and blocks malicious activity on a device (antivirus, anti-ransomware). Modern operating systems have decent built-in options (Microsoft Defender, XProtect on macOS) - third-party tools add features but built-in is far better than nothing.

IoT

Internet of Things - smart devices like thermostats, doorbells, smart bulbs, voice assistants. They run software, connect to the internet, and often have weak default security. Treat each one as a tiny computer that could be hijacked.

Phishing

Fraudulent emails, texts, or calls designed to trick you into revealing credentials or clicking malicious links. Modern phishing is highly convincing - always verify unexpected payment, login, or "urgent" messages through a separate channel.

Password Manager

Software that generates and stores unique strong passwords for every account, protected by one master password. Examples: 1Password, Bitwarden, Apple Keychain. Eliminates the #1 weakness: password reuse.

Backup Rule (3-2-1)

3 copies of important data, on 2 different types of media (local drive + external), with 1 copy offsite (cloud or physically remote). Protects against device failure, theft, fire, and ransomware.

NIST CSF

National Institute of Standards and Technology Cybersecurity Framework. The U.S. government standard for security practices, organized around five functions: Identify, Protect, Detect, Respond, Recover. CWC assessments align with this framework.

Free + Low-Cost Tools We Recommend

CWC has no financial relationship with any of these vendors.

Have I Been Pwned (haveibeenpwned.com)

Check if your email or password has appeared in a data breach. Sign up for notifications to get alerted to future breaches.

Bitwarden (bitwarden.com)

Free, open-source password manager with cross-device sync.

Authy (authy.com)

Free authenticator app for MFA codes - works across devices with encrypted cloud backup.

Microsoft Defender (Built into Windows 10/11)

Solid baseline antivirus and ransomware protection - already on your Windows PC. Just keep it enabled.

Tailscale (tailscale.com)
Free for personal use - secure WireGuard-based VPN for remote access to your home network.

CIS Benchmarks (cisecurity.org/cis-benchmarks)
Free hardening guides for Windows, macOS, routers, and more. Not light reading but authoritative.

When to Reassess

Schedule a fresh assessment whenever any of the following happens:

- It has been 12 months since your last assessment.
- You moved to a new home or office (new network, new threat surface).
- You added significant new technology - smart home system, business server, IoT cluster.
- You experienced a security incident, even a small one (suspicious email, unauthorized login alert, lost device).
- A family member or employee left the household / business with shared access to accounts or devices.

About This Report

This assessment was performed in person by a Cyber Wise Corp assessor and reviewed for accuracy and completeness by a CISSP-certified security professional before delivery. Our methodology aligns with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) and the CIS Critical Security Controls.

No assessment can identify every possible vulnerability, and no recommendation guarantees protection against all threats. This report reduces your risk - it does not eliminate it. For questions about any finding or recommendation, contact us through cyberwisecorp.com/contact.