SAMPLE — REDACTED

SECURITY POSTURE ASSESSMENT REPORT

North Texas Regional Law Firm | 45 Endpoints

Assessment Date: %^%^%^%^%^%^%^ | Delivered By: CoreRecon

OVERALL RISK SCORE: 34 / 100

CRITICAL — Immediate Action Required

CoreRecon | SDVOSB Certified | corerecon.polsia.app | (800) 955-2596

EXECUTIVE SUMMARY

Assessment Scope

External attack surface enumeration, internal endpoint posture review, credential exposure check, and compliance gap mapping against Texas State Bar Ethics Opinion 712. 45 endpoints assessed across 2 office locations.

Risk Score Breakdown

External Attack Surface:
28/100 — CRITICAL

Internal Posture:
41/100 — HIGH

Compliance Alignment:
33/100 — CRITICAL

Overall Composite:
34/100 — CRITICAL

Top 3 Findings

1. [CRITICAL] External RDP Exposure on 3 Endpoints — No MFA

Remote Desktop Protocol open to the internet on ports 3389 and %^%^%^%^. No multi-factor authentication. Active brute-force attempts logged from %^%^.%^%^%^.%^%^.%^%^%^ (classified origin). Attorney workstations reachable without credential bypass protection.

2. [CRITICAL] Leaked Credential in Public Breach Dataset

Email %^%^%^%^%^%^%^%^@ntrlawfirm.com with near-plaintext password found in %^%^%^%^%^%^%^%^ breach dump (2024). Password reu
365 tenant %^%^%^%^%^%^%^%^%^%^%^%^%^%^%^%^%^%^. No password rotation policy enforced.

3. [HIGH] No EDR Coverage on 12 of 45 Endpoints

Paralegal workstations and conference room terminals running Windows 10 21H2 (end of support Nov 2025) with only Windows Defender. No centralized telemetry or SIEM alert routing configured.

ATTACK SURFACE FINDINGS

Pages 2–4 | External Scan + Credential Exposure

External Port Scan Results

Port 80 / HTTP [OPEN]
!’ No redirect to HTTPS on all subdomains

Port 443 / HTTPS [OPEN]
!’ TLS 1.0 still accepted — cipher downgrade risk

Port %ˆ%ˆ%ˆ%ˆ / RDP [OPEN &]
!’ Critical — No MFA, active brute-force logged

Port %ˆ%ˆ%ˆ%ˆ / SMB [FILTERED]
!’ Externally filtered but internally exposed

Port %ˆ%ˆ%ˆ%ˆ / SMTP [OPEN]
!’ Relay test: %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ — partial open relay

Exposed Subdomains

%ˆ%ˆ%ˆ%ˆ.ntrlawfirm.com
!’ Staging environment — HTTP only, default credentials not rotated

%ˆ%ˆ%ˆ%ˆ.ntrlawfirm.com
!’ Old client portal — running outdated CMS (CVE-%ˆ%ˆ%ˆ%ˆ-%ˆ%ˆ%ˆ%ˆ)

mail.ntrlawfirm.com
!’ Exchange 2016 — ProxyLogon patched but ProxyShell not confirmed

Credential Exposure — Breach Dataset Check

Domain @ntrlawfirm.com checked against %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ, HIBP, and %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ breach indexes.

3 accounts found in breach datasets:
%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ@ntrlawfirm.com — %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ breach (2024), plaintext password in sample
%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ@ntrlawfirm.com — LinkedIn breach (2023), MD5 hash — crackable
%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ@ntrlawfirm.com — %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ combo list (2025), password reuse confirmed

INTERNAL POSTURE FINDINGS

Pages 5–6 | MFA, EDR, Patching, Privileged Accounts

MFA Enrollment [HIGH]

Status: 31 / 45 endpoints (69%)

Partners enrolled; 14 paralegal + conference accounts not enrolled. O365 tenant allows legacy auth bypass — MFA can be circumvented.

EDR Coverage [HIGH]

Status: 33 / 45 endpoints (73%)

CrowdStrike Falcon on attorney workstations. 12 endpoints (paralegal tier + shared terminals) running Windows Defender only. No telemetry to SIEM.

Patch Cadence [CRITICAL]

Status: Avg. 47 days to Critical patch

7 unpatched Critical CVEs across fleet. Oldest: CVE-%^%^%^%^-%^%^%^%^ (186 days). Windows 10 21H2 EoS on 12 devices.

Privileged Accounts [CRITICAL]

Status: 4 domain admins, 0 with MFA

Domain admin accounts lack MFA. Shared service account password last rotated %^%^%^%^ (>2 years). No PAM solution in place.

Backup Integrity [HIGH]

Status: Offsite backup: unverified

Cloud backup to %^%^%^%^%^%^%^%^. Last restore test: %^%^%^%^ (>18 months). No immutable/WORM copy confirmed. Ransomware could target.

Network Segmentation [HIGH]

Status: Flat network topology

All 45 endpoints on single VLAN. Lateral movement from any compromised endpoint reaches all attorney workstations, file servers, and billing systems.

COMPLIANCE GAP ANALYSIS

Pages 7–8 | Texas State Bar Ethics Opinion 712

Texas State Bar Ethics Opinion 712 requires law firms to implement reasonable safeguards to protect confidential client information from unauthorized access. The following gaps were identified:

Ethics Op. 712 §4.1 [FAIL]

Requirement: Reasonable security measures

Gap: No MFA on all accounts, 12 unprotected endpoints, flat network topology.

Ethics Op. 712 §4.2 [PARTIAL]

Requirement: Encryption of client data in transit

Gap: HTTPS enforced on primary domain. Email encryption not configured. File transfers via unencrypted %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ.

Ethics Op. 712 §4.3 [FAIL]

Requirement: Incident response capability

Gap: No documented IR plan. No breach notification workflow. No designated incident coordinator.

Ethics Op. 712 §4.4 [FAIL]

Requirement: Vendor / third-party access controls

Gap: IT vendor %ˆ%ˆ%ˆ%ˆ%ˆ%ˆ%ˆ has standing admin access — no just-in-time provisioning. No vendor risk assessments on file.

Ethics Op. 712 §4.5 [PARTIAL]

Requirement: Employee security training

Gap: Annual training completed by %ˆ%ˆ%ˆ%ˆ of %ˆ%ˆ%ˆ%ˆ staff. Phishing simulation: last run %ˆ%ˆ%ˆ%ˆ (>14 months). No tabletop exercise

Ethics Op. 712 §4.6 [FAIL]

Requirement: Data retention and destruction

Gap: No formal data retention policy. Client files on shared drives without classification. No secure deletion procedures.

REMEDIATION ROADMAP

Pages 9–10 | Prioritized Effort / Impact Matrix

Sorted by impact vs. effort. Quick Wins are executable this week with no additional budget. Near-Term items require planning and vendor coordination. Strategic items address root-cause architecture gaps.

[QUICK WIN] Enable MFA on all O365 accounts

Owner: IT | Timeline: 2–4 hours

Eliminates credential-based breach risk for 45 accounts immediately. No cost with existing O365 E3 license.

[QUICK WIN] Block legacy authentication on O365 tenant

Owner: IT | Timeline: 1 hour

Closes MFA bypass via legacy protocols (IMAP, POP3, SMTP auth). Low disruption risk.

[QUICK WIN] Rotate all domain admin passwords + remove stale accounts

Owner: IT | Timeline: 4 hours

Eliminates standing compromise risk on 4 elevated accounts.

[NEAR-TERM] Deploy EDR to remaining 12 endpoints

Owner: IT + Vendor | Timeline: 1–2 weeks

Closes visibility gap on paralegal tier. Requires CrowdStrike license expansion or equivalent.

[NEAR-TERM] Patch 7 critical CVEs — prioritize %^%^%^%^-%^%^%^%^ (186 days)

Owner: IT | Timeline: 1 week

Eliminates known exploit vectors. Windows 10 EoS devices require upgrade plan.

[NEAR-TERM] Implement network segmentation — attorney vs. staff VLANs

Owner: IT + Network Vendor | Timeline: 2–4 weeks

Limits lateral movement. Requires switch/firewall configuration change.

[STRATEGIC] Develop and test Incident Response Plan

Owner: CISO / Partner | Timeline: 60–90 days

Required for Ethics Op. 712 §4.3 compliance. CoreRecon Command tier includes IR playbook and tabletop facilitation.

[STRATEGIC] Implement immutable backup solution

Owner: IT + Vendor | Timeline: 30–45 days

Ransomware resilience. Offline or WORM-compliant copy required. Current backup target is reachable from network.

[STRATEGIC] Vendor access control review + PAM implementation

Owner: IT + Legal | Timeline: 60 days

Ethics Op. 712 §4.4 gap. Requires JIT provisioning for %^%^%^%^%^%^%^%^ admin access and formal vendor risk assessment process.

HOW CORERECON CLOSES YOUR GAPS

SENTINEL — $89/endpoint/month

24/7 SOC monitoring, SIEM correlation, threat detection, 30-min incident response SLA. Closes: EDR coverage gaps, SIEM visibility, alert routing, breach detection.

- Finding 1 — RDP brute-force detection + block
- Finding 3 — EDR telemetry centralization
- Finding 5 — Patch tracking and alert baseline

FORTRESS — $109/endpoint/month

Everything in Sentinel + EDR managed deployment, vulnerability management, automated patch orchestration, phishing simulation. Closes: EDR gaps, patch cadence, training compliance.

- Finding 2 — Credential exposure monitoring
- Finding 4 — Patch cadence (47-day avg !' <7 days)
- Finding 6 — Phishing simulation program

COMMAND — $129/endpoint/month

Everything in Fortress + vCISO layer, IR plan authoring and testing, compliance mapping, Ethics Op. 712 / CMMC / CJIS documentation, executive reporting. Closes: all compliance gaps.

- Compliance Gap §4.3 — IR plan and tabletop
- Compliance Gap §4.4 — Vendor access review
- Compliance Gap §4.6 — Data retention policy

NEXT STEPS

You now have a complete picture of your security posture.

This report is yours regardless of what you decide next. Here are your options:

1. Take it to your current IT vendor
Share the findings and ask for a remediation timeline. We've structured the roadmap so any competent vendor can act on it.

2. Share with firm leadership
The executive summary and risk score are designed for the managing partner or administrator. No technical background required to understand the priority.

3. Engage CoreRecon for one or more tier
No contract required to start. Month-to-month. Cancel any time. We earn continued engagement through the work.

4. Do nothing
We'll follow up once. After that, the decision is yours. We don't chase. We publish our findings so you have a record regardless.

Contact

John Martinez — CEO & Founder
corerecon@polsia.app | (800) 955-2596
corerecon.polsia.app/assessment