# Texas Law Firms: Under Siege.

2026 Cybersecurity Reality for Texas Law Firms

| | |
|---|---|
| **45** | Ransomware attacks on law firms in 2024 — record high |
| **$2.77B** | FBI IC3 BEC losses 2024 — 12% from attorney impersonation |
| **$8M** | Orrick settlement — largest law firm data breach recovery |
| **12 Steps** | Action checklist for TX law firm security posture |

## SECTION 1 | EXECUTIVE SUMMARY

# The Threat Is Accelerating

45 ransomware attacks on law firms in 2024. $2.77B BEC losses. ABA Rule 1.6(c) formally enforceable.

!’ 45 ransomware attacks on law firms in 2024 — record high (Black Fog Annual Report 2026)

!’ $2.77 billion in BEC losses from 21,442 FBI IC3 complaints in 2024

!’ Attorney/law firm impersonation = 12% of all BEC attack types (FBI IC3)

!’ ABA Model Rule 1.6(c) makes cybersecurity a formal ethical obligation — cost is a factor, not an exemption

!’ TX SB 2610 safe harbor (Sept 1, 2025): implement NIST CSF / CIS Controls to eliminate punitive damages

!’ Orrick $8M, HPMB $200K NY AG fine, Gunster $8.5M — leading precedents that define "reasonable efforts" in 2026

!’ 1.5M+ records compromised via legal tech vendor breaches alone (2024)

SECTION 2 | ATTACK VECTORS

# Four Attack Patterns Hitting TX Law Firms

## 01 Ransomware — Exfil First, Encrypt Second

Modern groups exfiltrate the highest-value client data before encryption, then threaten to publish on dark web leak sites. ALPHV/BlackCat, INC Ransom, and Silent Ransom Group (SRG) all use this model. Attorney-client privilege ends the moment privileged files appear on an extortion site.

## 02 Business Email Compromise — Wire Fraud Kill Zone

FBI IC3 $2.77B losses. Law firms move large wire transfers (closings, settlements, escrow) on predictable schedules. Crimson Kingsnake used 92 malicious domains targeting 19 law firms. Strikes at the exact moment wire is expected. Funds move irreversibly through mule accounts.

## 03 Vendor Supply Chain Attacks

ABA Formal Opinion 483 requires vendor due diligence. Clio/Cleo (Cl0p, Oct–Dec 2024): Hertz legal department and Western Alliance Bank confirmed compromised. iManage on-prem vulnerability. DocketWise 116,666 immigration records exposed. Your vendor breach is your breach.

## 04 E-Discovery Exfiltration

Litigation holds and discovery productions create extended network access windows. Opposing counsel strategy accessed via compromised firm email before critical depositions is a recurring pattern. Privileged communications, settlement positions, and M&A strategy are the primary targets.

## SECTION 3 | REGULATORY EXPOSURE

# ABA Rule 1.6(c) Is No Longer Optional

### ABA Model Rule 1.6(c)

"A lawyer shall make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment [18]: cost is a factor, not a blanket exemption. HPMB $200K NY AG fine — small firm, failure to apply available patch.

### TX Disciplinary Rule 1.05

Mirrors ABA Model Rule 1.6(c) for Texas attorneys. State Bar of Texas Ethics Opinion 712 requires due diligence on cloud vendor security, reasonable safeguards, and documented IR plan.

### TX SB 2610 Safe Harbor

Effective Sept 1, 2025: implement NIST CSF, CIS Controls, or ISO 27001 !' eliminate punitive damages. Safe harbor only applies to programs already in place when breach occurs. No grace period.

### HIPAA (if PHI involved)

Law firms handling healthcare litigation, insurance disputes, or elder law often process Protected Health Information. A breach involving unencrypted PHI is both a HIPAA breach notification event and a state bar disciplinary matter.

**KEY PRECEDENT**

HPMB case: NY AG fined firm $200,000 for failure to apply an available security patch. The size of the firm didn't matter. The absence of basic controls did. "Reasonable efforts" under Rule 1.6 requires documented, proactive security — not reactive IT.

## SECTION 4 | COST OF A BREACH

# When Ransomware Hits a Law Firm

**Settlement / Class Action**

**$8M**

Orrick (2024) — 638,000 individuals, SSNs, medical records, financial accounts

**Regulatory Fine**

**$200K**

HPMB — NY AG fine for failure to apply available security patch

**Settlement / Class Action**

**$8.5M**

Gunster Yoakley & Stewart (2024) — ~10,000 individuals data exposed

**Avg. BEC Wire Loss**

**$347K**

Per law firm incident. Recovery rate after wire leaves firm: <15%

**Malpractice Exposure**

**Unlimited**

Exfiltrated M&A strategy, litigation positions, and settlement discussions reaching opposing parties

**Bar Discipline**

**Active**

ABA Formal Opinion 483 post-breach obligations — monitoring, stopping, remediation, client notification

SECTION 5 | WHY TRADITIONAL IT FAILS

# The Gap That Kills: No 24/7 Monitoring

Most small and mid-size Texas law firms rely on daytime IT support — a managed services provider (MSP) that handles helpdesk, network maintenance, and server management. This model works perfectly for keeping the lights on. It is catastrophically inadequate for security operations.

THE DWELL TIME PROBLEM

## 26 days

= average time between initial access and detection across all industries (IBM 2025)

For law firms, which often have lower security maturity, dwell times can be significantly longer. A firm that relies on its daytime IT provider detects breaches at step 4 of the ransomware playbook — when the ransom note appears, not when the exfiltration begins. Standard EDR stops step 4 — but steps 1–3 have already destroyed privilege.

**Daytime-only coverage**

No detection between 6pm Friday and 9am Monday — exactly when ransomware detonates

**No behavioral analytics**

MSP tools flag known-bad, not anomalous behavior. LOLBin activity, RDP brute-force, and credential stuffing are invisible

**Flat network assumption**

MSPs design for uptime, not segmentation. Attorney workstations share VLAN with file servers

**No IR retainer**

When ransomware hits, the firm scrambles to find a response contact. Every minute of delay costs data

**No BEC-specific monitoring**

DMARC enforcement, impersonation detection, and anomalous wire transfer alerts are not standard MSP deliverables

## SECTION 6 | CORERECON APPROACH

# 30-Minute IR SLA. TX-Native. SDVOSB.

### SENTINEL — $89/endpoint/month

Best for: Solo/small firms (1–10 attorneys)

- 24/7 SOC monitoring + SIEM correlation
- Email security with BEC impersonation defense
- MFA deployment on practice management SaaS
- Security awareness training + bar-compliant attestation
- Monthly TX legal sector threat digest
- Documented security program (satisfies Ethics Op. 712)

### FORTRESS — $109/endpoint/month

Best for: Mid-size firms, M&A/litigation practice

- Everything in Sentinel

' EDR deployment with behavioral + exfil detection

' Encrypted immutable offsite backup + monthly restore test

' Wire fraud BEC detection + email anomaly monitoring

' TX SB 2610 safe harbor compliance support

' Vendor due diligence for legal tech stack

---

## COMMAND — $129/endpoint/month

Best for: Large firms, multi-office, high-value data

' Everything in Fortress

' Advanced exfil detection (SRG defense)

' Continuous compliance monitoring (ABA 1.6, TDRPC 1.05)

' Red team / penetration testing annually

' Bar notification workflow + client comms templates

' Annual security assessment + board-level incident reporting

SECTION 7 | 12-STEP ACTION CHECKLIST

# 12 Steps Every TX Law Firm Should Take Now

01

02

03

04

05

06

07

08

09

10

11

12

YOUR NEXT MOVE

## Book Free Assessment !’

https://corerecon.polsia.app/assessment | (800) 955-2596

---

' SDVOSB Certified | ' 30-Min IR SLA | ' TX SOC — Corpus Christi | ' AT&T TX State Vendor



Sources: FBI IC3 2024 Annual Report ($2.77B BEC); Black Fog Annual Ransomware Report 2026 (45 attacks on law firms 2024); Baker & Hostetler DSIR 2026; Reuters (Orrick, Gunster); ABA Formal Opinions 477R, 483, 498; Texas Legislature 89(R) SB 2610; Halcyon (INC Ransom legal sector targeting); FBI IC3 CSA 2025/250523 (SRG); Abnormal Security (Crimson Kingsnake); CertifID.