CORERECON THREAT INTELLIGENCE | TX LAW FIRMS | AUGUST 2026

Texas Law Firms: Privilege Under Siege.

A concise, source-backed field brief for small and mid-market Texas firms protecting privileged work product, client funds, and case data.

$2.77B — FBI IC3-reported 2024 BEC losses across the U.S.

4 — Attack paths mapped: identity, systems, funds, and vendors

5 — Compliance lenses: ABA, Texas, TDPSA, HIPAA, and CMMC

90 days — Prioritized action plan for a small or mid-market firm

SECTION 1 | THREAT SNAPSHOT

Why Texas firms are a high-value target

Law firms concentrate privileged records, identity-rich case files, settlement instructions, and access to client systems. The practical question is not whether a firm has a policy; it is whether the firm can detect, contain, restore, and explain a material incident.

!’ State Bar of Texas — INC Ransom incident publicly confirmed in 2025: the institution governing Texas lawyers became a visible target.

!’ Bryan Cave Cadence Capital Group — INC Ransom reporting in 2024 demonstrated that large-firm M&A, litigation, and cross-border matter data is a target set.

!’ Mossing & Navarre — reported ransomware exposure of privileged client data and employee information shows the same risk reaches mid-market firms.

!’ Orrick Herrington & Sutcliffe — reported $8M OCR settlement precedent for a firm handling healthcare-client PHI; HIPAA may follow the matter data.

!’ Gunster Yoakley & Stewart and HPMB — reported settlements show that client-record exposure can create parallel regulatory, malpractice, and insurance pressure.

Decision rule Treat every privileged file store, trust-account workflow, and vendor connection as an incident-response boundary—not just an IT asset.

Selected source base: ABA Formal Opinions 477R and 483; FBI IC3 2024 Annual Report; Texas Business & Commerce Code Chapter 541; HHS OCR HIPAA Security Rule and resolution materials; State Bar of Texas notices and incident reporting.

SECTION 2 | FOUR ATTACK PATHS

Where the first compromise becomes a firm-wide event

Use these four paths to organize a tabletop, a managed detection scope, and the evidence a managing partner or insurer will ask for.

01 Identity + email

M365, SSO, and attorney mailboxes are the launch point for credential theft, mailbox-rule abuse, partner impersonation, and privilege-bearing file access. Require phishing-resistant MFA, conditional access, impossible-travel alerts, and mailbox-rule monitoring.

02 Document + practice-management systems

iManage, NetDocuments, Clio, MyCase, PracticePanther, and similar systems hold matter files, client lists, billing data, and trust-account context. Scope their logs and identities separately; protect immutable backups and test restoration.

03 IOLTA + BEC workflows

A lookalike domain or compromised billing account can redirect a settlement or trust disbursement. Use dual approval, a known-number callback for every bank-change request, and SOC monitoring for high-risk messages.

04 Vendors + portals

eDiscovery, file-transfer, opposing-counsel, MSP, cloud, and contractor access can expose client data outside the firm perimeter. Keep a vendor inventory, security addendum, least-privilege access, offboarding proof, and an incident-notice path.

The control that connects all four

A named incident commander with authority to isolate accounts, preserve evidence, call the bank, engage counsel and the carrier, and start client-matter triage.

SECTION 3 | COMPLIANCE CROSSWALK

Five lenses, one evidence file

The exact legal duty depends on the matter, data, client, and contract. This crosswalk is an operational starting point, not legal advice.

ABA 1.6(c) / 1.4 / 477R / 483

Confidentiality, competent safeguards, and reasonable client communication after a material breach.

Evidence: Risk assessment, MFA scope, vendor review, incident plan, client-notice decision log.

Texas DR 1.05 / 1.15 + IOLTA

Confidentiality and safekeeping of client property, including trust-account and disbursement workflows.

Evidence: Callback SOP, dual approval, monthly reconciliation, role access, call and approval records.

TDPSA Ch. 541 / Ch. 521

Applies based on the firm and processing activity; requires reasonable security practices and may create AG/breach-notice work.

Evidence: Data inventory, privacy/security practices, request workflow, breach decision tree, processor terms.

HIPAA Security Rule

Where the firm acts as a business associate or otherwise handles PHI for a healthcare matter, contractual and regulatory duties may attach.

Evidence: BAA review, risk analysis, access/audit controls, safeguards, incident and breach-notice playbook.

CMMC / NIST SP 800-171

Where defense-adjacent work brings controlled unclassified information into scope; not a blanket requirement for every firm.

Evidence: Boundary map, CUI handling rules, SSP/POA&M evidence, contract flow-down review, 72-hour reporting path.

Crosswalk sources: ABA Formal Opinion 483 (2018) and 477R (2017); Texas Disciplinary Rules of Professional Conduct; Texas Business & Commerce Code Chapters 521 and 541; 45 C.F.R. Parts 160 and 164; 32 C.F.R. Part 170 and NIST SP 800-171.

SECTION 4 | 30/60/90-DAY CHECKLIST

Turn the brief into a defensible program

Assign one owner per item and preserve evidence as you go. The goal is a tested operating rhythm, not a binder that only exists for renewal.

30 DAYS

- Inventory privileged repositories, trust-account users, email admins, and external vendors.
- Enforce MFA and session-risk controls on email, DMS, practice-management, and remote access.
- Ship the dual-approval and known-number callback rule for every bank-change request.
- Verify an offline or immutable backup and document a restore owner.

60 DAYS

- Centralize high-value identity, mailbox, DMS, and practice-management alerts for monitoring.
- Run a vendor access and contract review; remove stale accounts and document incident contacts.
- Write the ABA 1.4 client-communication decision tree and matter-impact triage process.
- Map TDPSA and HIPAA applicability by data set; identify any CMMC/CUI boundary.

90 DAYS

- Tabletop a mailbox takeover, DMS exfiltration, and IOLTA wire-fraud scenario with the managing partner.
- Restore a representative matter repository and record actual recovery time and gaps.
- Package the control evidence for counsel, the carrier, clients, and—where applicable—CMMC or contract review.
- Choose the next operating model: internal owner, assessment, or managed detection and response.

Measure it Track MFA coverage, time to contain, backup restore time, callback adherence, vendor offboarding, and open high-risk findings.

SECTION 5 | NEXT STEP

Make the first 90 days accountable

CoreRecon helps Texas law firms turn the four attack paths into an operating program: managed detection, incident response, evidence, and partner-ready reporting. Start with the path that fits your firm size and matter mix.

1. Get a law-firm compliance assessment

Review your privileged data, IOLTA/BEC workflow, vendor exposure, and applicable ABA/Texas/TDPSA/HIPAA/CMMC obligations.

https://corerecon.polsia.app/assessment?industry=Law+Firms

2. Explore managed cybersecurity for Texas law firms

Right-size monitoring and response for small and mid-market firms, including identity/email, case systems, trust-account workflows, and vendor risk.

https://corerecon.polsia.app/verticals/tx-law-firms-tx

30-minute incident-response SLA | SDVOSB certified | Texas-based SOC