Texas CPA Firms: Tax Season Target.

2026 Cybersecurity Reality for Texas Accounting & CPA Firms

800K	Landmark Admin TX TPA records exposed (2024 ransomware)
207d	Median dwell time for accounting & FS firms (IBM X-Force 2024)
$300K	Avg. BEC wire loss per CPA firm incident (FBI IC3 2024)
14	IRS Pub 4557 WISP elements — every PTIN holder required

SECTION 1 | EXECUTIVE SUMMARY

The 90-Day Tax Season Kill Zone

Landmark Admin 800K exposed. Whitley Penn + Lane Gorman Trubitt confirmed. IRS Pub 4557, FTC §314, TDPSA, PCAOB flow-down.

!’ Landmark Admin TX TPA: 800,000+ claimant records exposed via ransomware (2024)

!’ Whitley Penn (Oct 2023) and Lane Gorman Trubitt (Jan 2024) — both confirmed ransomware, TX AG notified

!’ Median dwell time for accounting & financial services: 207 days (IBM X-Force Threat Intelligence Index 2024)

!’ IRS Publication 4557 (Rev. 11-2021) — every PTIN holder required to maintain a WISP, ~14 mandatory elements

!’ FTC Safeguards Rule 2023 (16 CFR §314) classifies tax preparation firms as financial institutions — MFA + Qualified Individual + 30-day breach reporting

!’ TDPSA §541 enumerates taxpayer data (SSN, EIN, account numbers) as "sensitive data" — $7,500/violation civil penalty

!’ PCAOB AS 1000 / QC 1000 / AS 1215 — firms with PCAOB audit clients inherit flow-down for audit workpaper integrity

!’ Average BEC wire transfer loss across accounting firms: $300K per incident (FBI IC3 2024 Annual Report)

SECTION 2 | TX CPA THREAT LANDSCAPE 2024–2026

Four TX Accounting-Firm-Sector Breaches

01 Whitley Penn — Oct 2023

Top-20 Texas CPA firm. Operations, file shares, and tax-prep environment encrypted. Forensic investigation coordinated with IRS Office of Safeguards. TX AG breach notification followed.

02 Lane Gorman Trubitt (Dallas) — Jan 2024

Dallas-based 80+ year CPA firm. Practice management, tax-prep, and document management systems affected. Client return data exfiltrated before encryption. State notification followed.

03 Landmark Admin (TX TPA) — 2024

Texas third-party administrator handling claims, payroll, and HR data. 800,000+ claimant records exfiltrated. Ransomware encrypted servers; exfiltrated before encrypt. Many TX CPA firms have TPA-adjacent clients.

04 BST & Co. (CPAs touching PHI) — OCR Settlement

Illustrative OCR exposure for CPA firms whose audit or assurance clients handle PHI. $28K HHS OCR settlement for inadequate safeguards — defines the CPA-touching-PHI pathway.

SECTION 3 | FTC SAFEGUARDS RULE COMPLIANCE GAPS

Why Most TX CPA Firms Fail §314

The 2023 FTC Safeguards Rule amendment (16 CFR §314) explicitly classifies tax preparation firms as financial institutions. CPA firms handling more than 5,000 consumer records now face the same regulatory machinery as banks and credit unions. The Final Rule's eight elements — Qualified Individual, written infosec program, MFA, encryption, monitoring, training, vendor oversight, IR plan — are checked against the firm's actual program during an FTC examination.

No Qualified Individual named

§314.4(a) requires a single "Qualified Individual" to oversee the information security program and report to the board. Most firms have no name in writing — the default is "the managing partner handles it."

MFA not enforced on tax-prep SaaS

§314.4(c)(5) requires MFA on any access to nonpublic customer information. QuickBooks Online, UltraTax CS, Drake, and Lacerte logins rarely have MFA enforced at the firm identity layer.

No 30-day breach report workflow

§314.4(j) requires notification to the FTC within 30 days of discovery for any breach involving "e500 consumers. The workflow is not designed; counsel is engaged after the fact.

Encryption "to make unreadable" missing

§314.4(c)(8) requires encryption at rest and in transit. Many firms rely on SaaS provider encryption alone — the firm cannot demonstrate the control.

Vendor risk assessments skipped

§314.4(d) requires continuous monitoring of service providers. Vendor questionnaires are not sent; SOC 2 reports are not reviewed.

SECTION 4 | IRS WISP + PUB 4557 BREAKDOWN

The 14 Elements of a Compliant WISP

IRS Publication 4557 — "Safeguarding Taxpayer Data" — is the IRS Office of Safeguards guidance for every PTIN holder. Last revised November 2021. The WISP must be "appropriate to the size and complexity of the data." IRS examiners, breach counsel, and cyber insurance carriers all read the WISP when a taxpayer-data breach occurs.

01. Designated Qualified Individual

Named in the WISP; oversees the program; reports to firm leadership

02. Risk assessment

Annual written assessment; identifies reasonably foreseeable threats

03. Access controls

Unique user IDs; MFA on remote access; least-privilege review

04. Encryption

Taxpayer data encrypted at rest and in transit; key management

05. Monitoring

Logging of access to taxpayer information; review of logs

06. Background checks

Pre-employment screening for staff with data access

07. Training

Annual awareness training; phishing simulation; WISP acknowledgment

08. Incident response plan

Documented IR plan; roles; communications; post-incident review

09. Vendor (Firm/contractor) oversight

Due diligence on third parties with taxpayer data; written agreements

10. Periodic review & testing

Annual WISP review; tabletop exercises; control testing

11. Notification procedures

Internal escalation; IRS notification per Pub 4557 §4

12. Record retention

Documentation of safeguards; WISP history; breach records

13. Physical security

Workstation controls; secure record storage; disposal

14. Reporting & improvement

Executive reporting; program updates from lessons learned

SECTION 5 | TOP 5 ATTACK VECTORS

The Five Patterns CPA Firms Face in 2026

01 BEC During Tax Season

IRS e-file window Jan 1 – Apr 15. Phishing + credential stuffing peak during compressed workload. FBI IC3: $2.77B BEC losses 2024 with $300K average per CPA firm wire-fraud incident. Attackers time campaigns to IRS e-file deadlines.

02 Ransomware on Tax Software

QuickBooks, UltraTax CS, ProSeries, Drake, Lacerte, TaxAct, CCH Axcess — each with private credentials and EFIN/PTC e-file auth tokens. One compromised preparer workstation = full client base e-fileable. LockBit + BlackCat target the tax-prep stack specifically in Q1.

03 Credential Theft (Acct. takeover)

Preparer credentials are harvested via phishing, reused passwords, and token theft. With EFIN credentials, attackers can file amended returns on the actual taxpayer. Identity theft + IRS Form 14039-B filings + class-action exposure on the firm that lost them.

04 Supply Chain via ProSeries/UltraTax/Lacerte

Wolters Kluwer (ProSeries, Lacerte), Intuit (UltraTax CS, Drake), Thomson Reuters — vendor compromise flows down to every firm using the software. Patch cadence, vendor access credentials, and outbound integrations are the supply-chain surface.

05 Insider Risk

Departing preparers, frustrated staff, seasonal contractors with elevated access. 207-day median dwell time (IBM X-Force 2024) means attackers are inside the network for months. Insider + external persistence = the modern CPA-firm breach.

SECTION 6 | 30/60/90-DAY HARDENING CHECKLIST

What to Do — and When

30 DAYS

- Enforce MFA on QuickBooks Online, UltraTax CS, Drake, ProSeries, Lacerte, TaxAct, CCH Axcess, and all firm email — by policy, not by individual opt-in
- Audit vendor access credentials; rotate any service-account credentials older than 90 days
- EOL-of-day culture: patch perimeter devices, VPN concentrators, file servers, RDP gateways within 72 hours of CVE publication
- Document and circulate the IR plan to managing partners; assign roles (decision-maker, comms, forensics, breach counsel)

60 DAYS

- Achieve FDIC-style network segmentation — tax-prep workstations isolated from file servers and bank-integration endpoints
- Outbound ACH batch monitoring with dual-control callback enforcement on all wires over a threshold ($25K default)
- Network-wide behavioral EDR across preparer workstations, file servers, and the e-file submission path
- Phishing awareness training + IRS Pub 4557 WISP acknowledgment distributed and tracked to all PTIN-bearing staff

90 DAYS

- Quantified gap assessment against the 14 IRS Pub 4557 elements; written WISP binder delivered; Qualified Individual named in the document
- Annual vulnerability assessment + IR tabletop with breach counsel present; results in writing
- Annual review of FTC §314 compliance: encryption, monitoring, vendor oversight, 30-day breach-report workflow
- Cyber insurance binder renewal with current WISP, IR plan, and SOC evidence; coverage reviewed against ransomware BEC tactics

SECTION 7 | CORERECON APPROACH

Sentinel / Fortress / Command for CPA Firms (10–100 endpoints)

SENTINEL — $89/endpoint/month

Best for: Small firms (1–10 CPAs, 10–25 endpoints)

- 24/7 SOC monitoring — TX-resident analysts
- Endpoint detection & response (EDR)
- Email threat analysis + BEC monitoring
- Monthly vulnerability summary report
- IRS Pub 4557 / FTC Safeguards §314 mapped

FORTRESS — $109–$129/endpoint/month

Best for: Mid-size firms (11–50 CPAs, 25–75 endpoints)

- Everything in Sentinel, plus:

- EDR on QuickBooks / UltraTax / Drake workstations
- ACH batch wire-fraud kill-chain detection
- Dual-control callback enforcement on wires
- Quarterly vCISO report to firm leadership
- IRS Pub 4557 WISP authorship & annual review

COMMAND — $2,500+/mo flat retainer

Best for: Larger firms (50+ CPAs, 75–100+ endpoints)

- Everything in Fortress, plus:
- Dedicated vCISO (contracted as security officer)
- On-site incident response capability
- Full WISP library + named Qualified Individual
- FTC §314 compliance documentation package

' Direct line to 24/7 IR team — no queue

30-MIN SLA • SDVOSB • TEXAS-RESIDENT SOC

Industry median time from detection to containment is 1–4 hours (SANS 2024 IR Survey). CrowdStrike 2024 Global Threat Report: ransomware completes kill chain in 45–90 minutes. CoreRecon's contractual 30-minute IR SLA measures against the actual attacker speed — not the MSSP industry average. SDVOSB-certified (CVE-verified); USMC veteran-led; SOC staffed with TX-resident analysts familiar with multi-office CPA firm topologies. Corpus Christi, TX headquarters.

Book Free Assessment !'

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

' SDVOSB Certified | ' 30-Min IR SLA | ' TX SOC — Corpus Christi | ' USMC Veteran-led | ' IRS Pub 4557 WISP Authored

CoreRecon | SDVOSB | 30-Min IR SLA | https://corerecon.polsia.app | (800) 955-2596

Sources: IRS Publication 4557 (Rev. 11-2021, Cat. No. 35579B); 16 CFR §314 (88 Fed. Reg. 60250, Nov 7, 2023); FTC Safeguards Rule Final Rule; Texas Business & Commerce Code §541 (TDPSA); PCAOB Auditing Standards AS 1000, QC 1000, AS 1215; FBI IC3 2024 Annual Report ($2.77B BEC); IBM X-Force Threat Intelligence Index 2024 (207-day median dwell); TX Attorney General breach notification portal (Landmark Admin, Whitley Penn, Lane Gorman Trubitt); HHS OCR enforcement actions 2023–2024; Sentinel/Forrester 2024.