Q4 2026 Texas Cyber Threat Brief

CoreRecon | IBM X-Force Data | Q4 2026

Key Statistics

935%
Oil & Gas ransomware attack surge (YoY, TX region)

22
Texas municipalities hit in coordinated Q4 2025 wave

34 days
Average dwell time before detection in TX targets

69%
TX attacks using double-extortion (data before encryption)

38 min
Average time from initial access to lateral movement

IBM X-Force Threat Intelligence

IBM X-Force Threat Intelligence Index 2026 confirms: manufacturing displaced finance as the most attacked sector in Texas, driven by supply-chain attacks. Brunswick Corp. paid an $85M ransom in January 2025 after a shared MSP compromise affected three Texas manufacturing facilities. The Brunswick attack was not a nation-state operation — it was a vendor ecosystem failure.

VOLT TYPHOON — CISA/FBI AA24-038B

China MSS-affiliated group pre-positioning in U.S. critical infrastructure since mid-2022. Texas energy grid management systems, O&G pipeline operators, water utilities, and telecom providers are confirmed targets. Key TTPs: living-off-the-land (LOLBins), edge device compromise, hands-on-keyboard persistence. Objective: sabotage capability, not disruption.

SALT TYPHOON — FBI/CISA AA25-016

China MSS-affiliated group that compromised U.S. telecom infrastructure at scale. Texas law enforcement CJIS-connected systems and defense contractor communications are directly in their targeting set. Exploits lawful intercept infrastructure for persistent access to communications content.

TX Incident Summary (Q4 2025 – Q2 2026)

Municipal/Government
28 incidents | 1.4M+ citizens affected | CRITICAL

Oil & Gas
19 incidents | OT targeting, Brunswick $85M | CRITICAL

Healthcare
15 incidents | 5.8M+ patient records | CRITICAL

Legal
11 incidents | 1.2M+ client records | HIGH

Education (K-12)
9 incidents | 320K+ students/staff | HIGH

Telecom / Critical Infra

6 incidents | SALT TYPHOON confirmed | CRITICAL

Defense Contractor

4 incidents | VOLT TYPHOON supply chain | CRITICAL

Financial / Credit Union

7 incidents | 280K+ members | HIGH

10 Immediate Actions

01. Audit your MSP — shared IT vendor was the attack vector in the 22-municipality wave

02. MFA on all remote access — VPN, RDP, O365, cloud. No legacy auth.

03. 72-hour critical patch SLA — perimeter CVEs (VPN, web portal) within 72 hours

04. Network segmentation audit — CJIS-connected, OT, EMR on isolated VLANs

05. Behavioral EDR — VOLT TYPHOON uses LOLBins, signatures miss them

06. OT/ICS threat hunt — assume VOLT TYPHOON is already inside your network

07. Immutable offline backup — WORM-compliant, restore-tested quarterly

08. CJIS v6.0 gap assessment — Oct 1, 2027 deadline, FBI audits active now

09. BC/DR plan for OT events — water intrusion, pipeline isolation, SCADA fallback

10. TX SB 820 notification workflow — 48-hour AG disclosure required by law

John Martinez
CEO & Founder, CoreRecon
SDVOSB Certified | AT&T Vendor for State of Texas Incident Response
corerecon@polsia.app | corerecon.polsia.app | (800) 955-2596