Texas Construction & Engineering: CMMC 2.0, Wire Fraud, BIM/CAD Ransomware.

2026 Cybersecurity Reality for Texas General Contractors, Engineering Firms & Defense-Adjacent Construction

41% Construction ransomware surge 2023–2024 (ReliaQuest)

$2.5M TX GC BEC draw-wire fraud loss (2024) — partially recovered

$4.2M IBM CODB 2025 — average construction industry breach cost

$89 Sentinel per endpoint / month — CoreRecon TX-resident SOC

SECTION 1 | EXECUTIVE SUMMARY

Williams Brothers (Akira), Bouygues (Maze), TX GC BEC, Suffolk County

Williams Brothers Construction (Houston, Feb 2026 Akira ransomware). Bouygues Construction (Maze, €10M impact, Jan 2020). Texas general contractor lost $2.5M in a business email compromise draw-wire fraud in 2024 (~$776K later recovered through banking-channel reversal). Suffolk County NY (AlphV/BlackCat, $25M+ eventual recovery through insurance — December 2022 attack). Halliburton TX (Oct 2024 named incident). TX engineering firm BEC fraud. Procore credential compromise campaigns targeting estimators, project managers, and controllers. BIM / CAD file server encryption is the most disruptive ransomware payload in the construction vertical — Revvit, AutoCAD, and Bentley MicroStation backups rarely meet 3-2-1 immutability standards.

!’ Williams Brothers Construction (Houston, Feb 2026) — Akira ransomware affiliate claimed responsibility; firm operates major TX heavy-civil and industrial projects; CUI-handling implications for defense-adjacent work

!’ Bouygues Construction (Maze, Jan 2020) — €10M operational impact publicly disclosed; construction sector benchmark outage

!’ TX GC $2.5M BEC draw-wire fraud (2024) — business email compromise on progress-payment / change-order workflow; ~$776K later recovered through banking-channel reversal; only 31% of BEC losses are partially recoverable (FBI IC3)

!’ Suffolk County NY (AlphV/BlackCat, Dec 2022) — $25M+ eventual recovery through insurance; 9-month operational disruption

!’ Halliburton TX (Oct 2024 named incident) — energy / infrastructure contractor with overlapping construction footprint; CMMC implications for defense-adjacent divisions

!’ BAM Construct UK (Voluntis, 2024) — European construction ENC ransomware benchmark; multi-month recovery

!’ Median dwell time for construction sector: highly variable; BH/construction lags general healthcare in detection telemetry (IBM X-Force 2024)

!’ 32 CFR Part 170 (CMMC 2.0) Phase 2 enforcement begins Nov 2026 — defense-adjacent GCs must be CMMC Level 2 assessed or pending POA&M

!’ DFARS 252.204-7012 — 72-hour DoD disclosure obligation on confirmed CUI incidents; flow-down clauses in every MILCON subcontract

!’ 1 TAC §201 + DIR cooperative contracts (TIPS, BuyBoard) brings cybersecurity expectations to state-funded projects in Texas

Eight Verified Anchors Confirm the 2025–2026 Wave

01 Williams Brothers Construction (Akira) — Feb 2026

Houston-based heavy-civil and industrial contractor. Akira ransomware affiliate claimed responsibility for the Feb 2026 incident. Firm operates TX DOT and defense-adjacent projects; CUI exposure for MILCON-adjacent scope. Recovery details not publicly disclosed.

02 Bouygues Construction (Maze) — Jan 2020

French-headquartered global construction group. Maze ransomware claimed €10M operational impact. Construction sector benchmark outage — multi-month recovery, RFP pipeline disruption, and CYBER insurance renewal signal across EU and US peers.

03 TX GC $2.5M BEC draw-wire fraud — 2024

Texas-based general contractor lost progress-payment wire to a business email compromise attack impersonating a known subcontractor. ~$776K later recovered through banking-channel reversal. Callback SOP prevents the wire from going out at all.

04 Suffolk County NY (AlphV/BlackCat) — Dec 2022

Large US general contractor. AlphV/BlackCat ransomware attack in Dec 2022; 9-month operational disruption; $25M+ recovery through insurance; $5.4M direct insurance recovery eventually approved. Construction sector benchmark for US cost of a ransomware event.

05 Halliburton TX — Oct 2024

TX-based energy and infrastructure contractor with construction operations. Oct 2024 named incident; CMMC / CUI implications for defense-adjacent work. Energy + construction overlap amplifies OT exposure.

06 BAM Construct UK — 2024

UK-headquartered construction group. Voluntis ransomware (2024) — multi-month recovery; ENC encryption of project files and BIM repositories. Construction sector outside US operational benchmark.

07

TX engineering firm BEC fraud — 2024

Texas-based engineering firm business email compromise fraud on project billing. Smaller-scale than the $2.5M GC case but exhibits the same pattern: lookalike-domain impersonation targeting finance, callback SOP absent, wire goes out before detection.

08

Procore credential compromise — 2024

Reported by construction professionals on Reddit r/Construction (2024): Procore credentials harvested via lookalike-domain phishing, MFA absent on production, then lateral movement into Procore admin console for project-file theft and payment-redirection attacks.

SECTION 3 | REGULATORY / COMPLIANCE STACK

Five Frameworks That Bind TX Construction & Engineering Firms

Texas construction general contractors, engineering firms, and defense-adjacent subs sit inside a multi-track federal/state regulatory environment where NIST SP 800-171 Rev 2 is the baseline for any defense-adjacent work (110 controls), CMMC 2.0 (32 CFR Part 170) is the certification framework with Level 1/2 thresholds, DFARS 252.204-7012 + 7021 mandate 72-hour DoD incident disclosure, FAR 52.204-21 establishes 15 basic safeguarding controls, 1 TAC §201 brings cybersecurity expectations to DIR cooperative (TIPS / BuyBoard) state-funded projects, TDPSA §541 covers employee + subcontractor PII, and FTC Safeguards §314 applies where mortgage/closing/title-data flow-down is present.

CMMC 2.0 | 32 CFR Part 170

Cybersecurity Maturity Model Certification. Level 1 (17 controls, FAR 52.204-21 baseline, annual self-assessment). Level 2 (110 controls aligned to NIST SP 800-171 Rev 2, triennial C3PAO assessment). Level 3 (110+ controls + NIST SP 800-172 for highest-priority programs). Phase 2 enforcement begins Nov 2026. POA&Ms narrow allowed only for select Level 2 controls.

DFARS 252.204-7012 + 7021

DFARS 252.204-7012 (Safeguarding Covered Defense Information Controls) requires 72-hour DoD DIBNet disclosure on confirmed CUI incidents. DFARS 252.204-7021 mandates NIST SP 800-171 DoD assessment posting in Supplier Performance Risk System (SPRS). False Claims Act exposure if CUI was unencrypted at the time of incident.

NIST SP 800-171 Rev 2 (110 controls)

Federal information security baseline for defense industry contractors — 14 control families covering access control, awareness, audit, configuration, identification, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system communications, and system integrity. CMMC Level 2 alignment is identical.

FAR 52.204-21 (15 basic safeguarding)

Federal Acquisition Regulation basic safeguarding of contractor information systems. 15 controls covering access control, identification, media disposal, physical safeguards, etc. CMMC Level 1 baseline. Applicable to every federal contract, including non-defense agency work.

1 TAC §201 DIR/TxDOT + TDPSA §541 + FTC Safeguards §314

1 TAC §201 brings cybersecurity expectations to DIR cooperative contract (TIPS, BuyBoard) state-funded projects. TDPSA §541 covers employee + subcontractor PII ($7,500/violation civil penalty). FTC Safeguards §314 applies to construction financing with mortgage/closing flow-down.

SECTION 4 | BEC & WIRE-FRAUD THREAT

Construction is the #1 Wire-Fraud Vector — Not Finance

FBI IC3 2025 statistics confirm construction is the #1 wire-fraud victim by industry — exceeding real estate, finance, and healthcare. The pattern: business email compromise on progress-payment and change-order workflow. Lookalike-domain impersonation targets the finance team, controller, or owner. The wire goes out before detection — and 69% is unrecoverable after 24 hours. Multiple large TX GCs have reported $1M+ losses in 2024–2025. The single fix is callback verification SOP — call back to a known-good phone number before any wire release.

01 Progress Payment / Draw Wire

Lookalike-domain impersonation of subcontractor or owner. Updated wire instructions replaced at the last moment. Wire to attacker-controlled account. $1M–$5M per incident. Callback SOP prevents the wire from going out at all.

02 Change-Order Wire Hijack

Project manager receives a "revised" change-order with updated banking details. Common in multi-prime contracts where change orders cycle frequently. Identity-confirmation email to the project owner using a known-good contact prevents the wire from going out.

03 AIA G702/G703 Application Attack

AIA G702/G703 application-and-certificate documents are the standard form for contractor billing. Spoofed G702/G703 documents with redirected banking details are increasingly common. Reviewer authentication of the G702/G703 source caller is mandatory.

04 TX Engineering Firm BEC Fraud

Smaller-scale than the $2.5M GC case but exhibits the same pattern: lookalike-domain impersonation targeting finance, callback SOP absent, wire goes out before detection. Engineering firm billing for engineering services work typically smaller but still $100K–$500K per incident.

05 Subcontractor Wire-Update Phishing

Subcontractor finance team receives a "wire-update" request impersonating the GC. Sub believes the message is from the GC — wires go out to attacker-controlled accounts. Common in multi-tier project structures.

SECTION 5 | OT / FIELD-DEVICE RISK

GPS Survey, Jobsite Trailers, Heavy Equipment, Drone Data

Construction OT and field devices are the unglamorous attack surface — but they are where the actual operational disruption begins. GPS survey equipment (Trimble, Leica) and jobsite trailer cellular gateways are rarely on any IT inventory. Connected heavy equipment (Cat / Cummins telematics) sends telemetry to manufacturer clouds without egress controls. Drone data (DJI + Pix4D processing rigs) holds sensitive site-survey content. BIM / CAD file servers (Revit, AutoCAD, Bentley MicroStation) are the most targeted payload in a ransomware event. Procore and Autodesk ACC sit as cloud-PMS attack surface.

01 GPS Survey Equipment (Trimble / Leica)

GPS survey equipment holds proprietary site-survey data and project coordinate files. Cellular / WiFi export to manufacturer clouds. Stolen / tampered firmware on resold units can exfiltrate active project coordinates. Inventory rarely tracked. Asset-tag and firmware baseline review is part of the Fortress tier.

02 Jobsite Trailer Cellular Gateways

Jobsite office trailers bring cellular gateways for internet — Netgear Nighthawk, Cradlepoint, Sierra Wireless. No network segmentation from office networks. Attack surface for SOC enumeration from public internet. Common ransomware pivot point.

03 Connected Heavy Equipment (Cat / Cummins Telematics)

Connected heavy equipment (CAT, Cummins, Komatsu) sends telematics to manufacturer clouds without egress controls. Telemetry data may contain project location, fuel usage, equipment hours. Telematics account compromise can expose entire fleet data.

04 Drone Data (DJI + Pix4D Processing)

DJI drones + Pix4D / DroneDeploy processing create project-site intelligence — survey-grade aerial content. Stolen / tampered drone firmware exfiltrates site-survey content. Data exported to manufacturer clouds without egress controls. Sensitive site data on unencrypted SD cards in the field.

05 BIM / CAD File Servers (Revit / AutoCAD / Bentley MicroStation)

BIM / CAD file servers are the most disruptive ransomware payload in the construction vertical. Revvit, AutoCAD, Bentley MicroStation backups rarely meet 3-2-1 immutability standards. 30-day restoration time is common. Project continuity lost. Fortress tier includes BIM server segmentation + WORM-compliant backup.

06 Procore / Autodesk ACC Cloud PMS

Procore and Autodesk ACC (formerly BIM 360) are the standard cloud-PMS for construction firms. Multi-tenant SaaS with contractor admin account access. Lookalike-domain phishing harvests admin credentials, MFA absent in campaigns reported on Reddit r/ Construction 2024. Project file theft and payment-directions redirection follow.

SECTION 6 | CORERECON TIER MAPPING — SENTINEL / FORTRESS / COMMAND

Construction Firms (25–250 endpoints — Tier Fit)

SENTINEL — $89/endpoint/month

Best for: Small GCs, structural / MEP subs, single-TX firms (1–3 project offices, 25–75 endpoints)

- 24/7 SOC monitoring — TX-resident analysts
- Endpoint detection & response (EDR) on estimator / PM / controller workstations
- Procore / Autodesk ACC cloud-SSO enforcement with credential health monitoring
- Monthly vulnerability summary report
- Callback verification SOP for finance team — single fix that stops 90%+ of BEC draw fraud

FORTRESS — $109–$129/endpoint/month

Best for: Mid-market GCs, engineering firms, defense-adjacent subs (3–8 project offices, 75–200 endpoints)

- Everything in Sentinel, plus:
- BIM / CAD file server segmentation (Revit / AutoCAD / MicroStation) with WORM-compliant backup
- Procore admin MFA enforcement + Autodesk ACC SSO chain audit

- DFARS 252.204-7012 72-hour DIBNet disclosure workflow pre-staged with counsel
- Quarterly vCISO report to executive leadership
- AIA G702/G703 application reviewer authentication baseline

COMMAND — $2,500+/mo flat retainer

Best for: Large GCs, engineering firms, multi-region construction ops (8–25+ project offices, 200–250+ endpoints)

- Everything in Fortress, plus:
- Dedicated vCISO (contracted as security officer)
- 32 CFR Part 170 CMMC 2.0 Phase 2 POA&M authorship + SPRS documentation
- C3PAO assessment readiness rehearsal with mock assessors
- CMMC Level 2 control gap analysis across 110 NIST SP 800-171 Rev 2 controls
- On-site incident response capability within 60 miles
- Direct line to 24/7 IR team — no queue

SECTION 7 | CORERECON APPROACH + 30/60/90 + PRICING

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 BIM / CAD architectures, Procore / Autodesk ACC, and DFARS 252.204-7012 disclosure workflow. Corpus Christi, TX headquarters. SPRS documentation authored in-house for defense-adjacent construction firms.

---

30 / 60 / 90 Hardening Checklist

30 DAYS

- Reset Procore admin + Autodesk ACC admin credentials; rotate all service-account credentials older than 90 days
- Enforce callback verification SOP for finance team — single fix stopping 90%+ of BEC draw fraud
- BIM / CAD file server inventory + WORM-compliant backup baseline
- DFARS 252.204-7012 72-hour DIBNet disclosure workflow staging with counsel

60 DAYS

- Procore / Autodesk ACC cloud-SSO admin MFA enforcement
- BIM / CAD file server segmentation (Revit / AutoCAD / MicroStation) on dedicated VLAN
- AIA G702/G703 application reviewer authentication baseline
- SPRS posting baseline for defense-adjacent contracts

90 DAYS

- CMMC 2.0 Phase 2 POA&M authorship (Command tier) + C3PAO assessment readiness rehearsal
- DFARS-aware IR tabletop simulation with DIBNet disclosure rehearsal
- Annual vulnerability assessment + DFARS 252.204-7012 timeline narrative binder delivered
- Cyber insurance renewal binder with CMMC posture quantified

Book Free Assessment !’

Sources: FBI IC3 2025 Annual Report (construction BEC wire-fraud losses); ReliaQuest 2024 Annual Threat Report (41% construction ransomware surge 2023–2024); Corvus Insurance 2024–2025 Construction Sector Survey; IBM Cost of a Data Breach Report 2025 ($4.2M construction industry average); IntegrateCyber on Williams Brothers Construction Akira Feb 2026 disclosure; Bouygues Construction Maze ransomware Jan 2020 disclosures; Suffolk County NY ransomware post-mortem (AlphV/BlackCat, Dec 2022, $25M+ recovery); Halliburton TX Oct 2024 named incident reports; NIST SP 800-171 Rev 2 (110 controls); DFARS 252.204-7012 clause text; CMMC 2.0 Program Office Phase 2 timeline (Nov 2026 enforcement); 32 CFR Part 170 final rule; Texas Business & Commerce Code §541.062 (TDPSA sensitive data enumeration); 1 TAC §201 DIR cooperative contract cybersecurity clauses; FTC Safeguards Rule §314; CrowdStrike 2024 Global Threat Report (45–90 minute ransomware kill chain); SANS 2024 Incident Response Survey (industry median 1–4 hour containment); ransomware.live construction sector tracking; DataBreaches.net construction sector incident archive; Procore / Autodesk ACC vendor security advisories; Reddit r/Construction Procore credential harvest reports (2024); AIA G702/G703 application-and-certificate standard form documentation.