

THE CONSTRUCTION IT & CYBERSECURITY GUIDE

Cybersecurity, Connectivity, Software & Compliance

A Practical Guide from Preactive IT Solutions for Texas General Contractors & Subcontractors

20+ YEARS SPECIALIZING

Construction, Engineering & Manufacturing IT

MSP TITAN 2024

Construction & Engineering

FOUNDED 2003

Houston, Austin, San Antonio & Beaumont

TABLE OF CONTENTS

Executive Summary	3
Cybersecurity for Construction Companies	5
Real-World Cyber Incidents in Construction	6
Project Management & Field Software	9
Network Infrastructure & Job-Site Connectivity	12
Design & Engineering Software	15
IT & Cybersecurity Compliance for Construction	18
Real-World Case Study	21
Next Steps & Resources	22
Sources & Further Reading	24

About This Guide

Developed by Preactive IT Solutions — a process-driven Managed IT provider founded in 2003, specializing in construction, engineering, and manufacturing firms across Texas. Our team includes CompTIA Security+ certified professionals and Bluebeam Certified Professionals, supporting the software, connectivity, and compliance needs of general contractors and subcontractors throughout Houston, Austin, San Antonio, and Beaumont.



EXECUTIVE SUMMARY

TOP 3 Most-Targeted Industries for Ransomware in 2025²	418 Construction Ransomware Victims Tracked in 2025¹	10 Ransomware Groups Tracked Targeting Construction²	90-DAY Action Framework Included in This Guide
--	--	--	---

Construction firms run on more connected technology than ever — project management platforms, cloud-based drawing collaboration, job-site networks, design software, and a growing web of subcontractor relationships. That technology is what keeps modern projects on schedule and on budget. It is also what has made construction one of the most targeted industries for ransomware and cyberattacks throughout 2025.

For general contractors and subcontractors across Texas, IT is no longer a back-office concern — it is a direct input to project continuity, bid competitiveness, and client trust. When a firewall fails, job-site coordination stops. When Procore or Bluebeam access is misconfigured, subcontractors lose the current drawing set. When a ransomware group gets in, bid data and BIM files are exposed to competitors. When compliance documentation cannot be produced on demand, insurance coverage and contract eligibility are put at risk.

This guide addresses the six areas of IT that actually determine whether a construction firm's technology helps the business or works against it — grounded in real deployments Preactive IT Solutions has executed for construction clients across Texas.

What This Guide Covers

- ✓ Cybersecurity: named ransomware groups actively targeting construction, the attack path they follow, and a multi-layered defense framework
- ✓ Project management and field software: getting more out of Procore, Bluebeam, and Autodesk Forma/Forma Build, and the integrations firms overlook
- ✓ Network infrastructure and job-site connectivity: what actually works for temporary and remote job sites, with a real-world case study
- ✓ Design and engineering software: what AutoCAD, Revit, and BIM workflows demand from your infrastructure
- ✓ IT & cybersecurity compliance: CMMC, DFARS, NIST 800-171, and cyber insurance requirements, plus the records IT must preserve for OSHA, bonding, and certified payroll
- ✓ A practical, prioritized next-steps framework any construction firm can start on immediately



“A ransomware attack on a construction firm is not just an IT problem — it stops projects, exposes client data, and threatens relationships that took years to build. Proactive, layered protection is not optional; it is a business imperative.”

Charles Swihart Founder & CEO, Preactive IT Solutions | MSP Titan of the Industry 2024 | Author, On Thin Ice

A construction site at sunset or sunrise. Several large tower cranes are visible, their silhouettes and cables stretching across the sky. In the foreground, a dense network of vertical rebar is visible, suggesting the foundation or early structure of a building. The sky is a mix of orange, red, and purple hues. A vertical red line is positioned on the left side of the image, partially overlapping the text.

CYBERSECURITY: THE THREAT LANDSCAPE CONSTRUCTION ACTUALLY **FACES**

CYBERSECURITY FOR CONSTRUCTION COMPANIES

Construction firms don't think of themselves as a cybersecurity target — they think of themselves as builders. Ransomware groups think differently. Construction remained one of the most targeted industries for ransomware throughout 2025, with hundreds of confirmed victims tracked across the sector for the year.² This isn't a future risk to plan around eventually — it's the present-tense reality of running a construction business on digital tools.

Construction presents a combination of pressure points attackers look for: time-sensitive projects that create pressure to pay quickly, complex subcontractor networks that multiply entry points, uncontrolled field devices and networks, heavy reliance on shared cloud tools like Procore and Bluebeam, and — historically — thinner cybersecurity investment than other industries.

Ransomware Groups Frequently Targeting Construction in 2025²

Group	Observed Activity & Tactics	Construction Relevance
Play	Double extortion — data exfiltration followed by encryption; intermittent encryption to speed up attacks	Named by Rapid7 among groups frequently hitting construction firms in 2025
Akira	Frequently gains initial access through unpatched VPN and remote-access appliances	Higher risk for firms with field/remote access into office systems that isn't tightly managed
Qilin	Cross-platform (Windows, Linux, VMware ESXi); grew rapidly after other groups' 2025 disruptions	Broad, opportunistic targeting that includes mid-size project-based firms
SafePay	Exfiltrates data before encrypting; extortion-first negotiation posture	Elevated risk for firms holding sensitive bid, budget, or project data
RansomHub	Was the most active RaaS operation into early 2025; its leak-site infrastructure went dark starting April 2025 and affiliates dispersed to other groups	Included for 2025 context — no longer an active, ongoing operation as of this guide's publication
Lynx	Double-extortion RaaS model with an active public leak site through 2025	Reported construction-sector activity alongside other mid-market industries
DragonForce	Cartel-style RaaS model; absorbed some activity from 2025's RansomHub disruption	Targets mid-market firms; publishes stolen project data on leak sites
Medusa	Long dwell times using living-off-the-land techniques to avoid early detection	Extended undetected access increases the chance project and financial systems are touched before an attack triggers
WorldLeaks	Extortion-focused, with stolen data published on dedicated leak sites	Direct exposure risk for bid, contract, and personnel records
INC Ransom	Frequently leverages stolen or compromised third-party credentials for initial access	Elevated risk from subcontractor and vendor account compromise

Group list and 2025 construction-sector activity per Rapid7 threat research.² RansomHub is included for context on 2025 activity levels; it is not an ongoing threat as of publication.

REAL-WORLD CYBER INCIDENTS IN CONSTRUCTION

Ransomware attacks on construction firms follow a recognizable pattern. Here is how that pattern played out for three real organizations, and the general sequence attackers typically follow to get there.

Initial Access	Credential Compromise / Lateral Movement	Data Exfiltration	Encryption / Extortion
Bird Construction <i>Toronto — Canadian federal contractor · 2019 · Maze ransomware</i> Hit by Maze ransomware with a \$9M demand. Employee financial and health records were leaked after the firm did not pay. ³	Skender Construction <i>Chicago — General contractor · March 2024 · Double extortion</i> Discovered a double-extortion attack that exfiltrated roughly 600GB, including architectural drawings and personal data for over 1,000 people. Because of its preparedness, Skender did not pay. ³	MasTec <i>Publicly traded infrastructure firm · 2025 · Clop / third-party zero-day</i> Disclosed that the Clop group exploited a third-party software zero-day, exposing data for more than 25,000 individuals. ³	

See the full case study on page 21 for how this plays out for a Texas contractor, and page 24 for source references.

What Ransomware Groups Are After

- ✓ BIM models, Revit, AutoCAD, and SolidWorks design files
- ✓ Project bids, cost estimates, and RFI responses
- ✓ Schedules, progress reports, and change orders
- ✓ Subcontractor agreements and compliance documentation
- ✓ Client and vendor databases — financial and contact data

A Multi-Layered Defense: Prevention, Detection, Recovery

No single tool stops ransomware. Preactive IT builds construction clients' security around three layers that work together — prevention reduces the attack surface, detection catches breaches early, and recovery limits the damage when something gets through.



Identity & Access Control

Identity & Access Control

MFA and Conditional Access across Microsoft 365, Microsoft Entra ID, Procore, Bluebeam, and VPNs, with SSO and Intune-managed device compliance for laptops, tablets, and field devices. Fast provisioning and deprovisioning — including guest access — keeps permissions clean as employees and subcontractors move on and off projects.



Network Segmentation

Network Segmentation

Office and job-site systems shouldn't share a flat network. Segmentation means a compromised field laptop can't become a company-wide incident.



24/7 Monitoring & Detection

24/7 Monitoring & Detection

Ransomware doesn't wait for business hours. Continuous monitoring and vulnerability scanning catch breaches before ransomware deploys.



Ransomware Protection

Ransomware Protection

Modern EDR with ransomware-specific rollback on every device, including field laptops and tablets — standard antivirus is not sufficient.



Backup & Disaster Recovery

Backup & Disaster Recovery

Backups ransomware cannot reach, modify, or delete — tested with real restoration drills, not just left running.



Incident Response

Incident Response

Defined roles and protocols for who decides restore vs. negotiate, and who talks to the client — documented before a crisis, not during one.

A construction worker wearing a yellow hard hat and a high-visibility safety vest over a dark jacket is looking down at a tablet computer. The background shows a blurred construction site with orange machinery.

**BUILT FOR THE FIELD: IT SUPPORT
FOR PROCORE, BLUEBEAM & FIELD
SOFTWARE**

PROJECT MANAGEMENT & FIELD SOFTWARE

Ask any project manager what would bring their job site to a halt fastest, and the answer usually isn't a broken excavator — it's Procore going down during a submittal deadline, or a Bluebeam Studio session that won't sync during a bid walkthrough. Construction runs on a specific stack of software, and that software has become as operationally critical as the tools on the job site itself.

Procore: Support Beyond Software Training

Procore centralizes RFIs, submittals, budgeting, scheduling, and document control from preconstruction through closeout, integrating with over 500 other tools. That breadth is exactly why Procore support is an IT function, not just a training question. A misconfigured permission structure can expose bid data to the wrong subcontractor. A poor integration with your accounting platform creates job-costing errors that surface weeks later. Preactive IT audits and optimizes how Procore fits into a client's broader environment — access controls, integrations, and connectivity — so the platform works the way it's supposed to.

Bluebeam: A Platform We Know From the Inside

Bluebeam Revu is the industry standard for PDF markup, digital takeoffs, and drawing review — and it's a platform Preactive IT knows firsthand as a Bluebeam Certified Professional shop. Estimators use it for precise quantity takeoffs; project teams use Bluebeam Studio sessions for real-time collaborative markup, including subcontractors without full platform access. Our support covers role-based Studio permissions, encrypted cloud storage for master CAD and BIM files rather than local shared drives, and workstation performance tuning so large drawing sets don't choke a laptop mid-review — the same controls referenced in this guide's cybersecurity section, because Bluebeam security and Bluebeam performance are the same conversation.

Field Devices & Mobile Access on the Job Site

Procore and Bluebeam are only as reliable as the phones, tablets, and rugged devices project teams actually carry into the field. A superintendent needs current drawings and RFI responses to load instantly on a job-site tablet with spotty cellular service, not stall on a stale local copy. Preactive IT enrolls field devices in mobile device management so a lost or stolen tablet can be remotely wiped, personal devices accessing project data meet minimum security requirements, and app updates roll out without someone standing at a desk. That device layer rarely gets attention until a lost iPad turns into a data-exposure conversation.

Signs Your Procore or Bluebeam Environment Needs an IT Review

- ✓ Subcontractors keep Studio or Procore access long after their scope of work ends
- ✓ Job-costing figures between Procore and your accounting platform don't reconcile without manual correction
- ✓ Large BIM or drawing sets routinely time out or fail to sync from job-site connections
- ✓ Field tablets and laptops accessing project data aren't enrolled in any device management
- ✓ No one can say who currently has admin-level permissions in Procore or Bluebeam Studio

How Procore and Bluebeam Work Together

Procore and Bluebeam aren't competing platforms — most construction firms run both. Procore manages the project as a whole: budgets, schedules, RFIs, and team communication. Bluebeam handles the drawings themselves: markup, takeoffs, and plan review. Since 2025, Bluebeam has expanded its native integrations with Procore's Documents and Submittals tools specifically to reduce the data silos between the two — getting that integration configured correctly, rather than leaving teams to manually shuttle files, is exactly the kind of support gap Preactive IT closes.

Procore Handles	Bluebeam Handles
Budgets, schedules, and RFI tracking	Drawing markup and redlines
Submittal logging and document control	Digital quantity takeoffs
Subcontractor and vendor management	Real-time Studio collaboration sessions
Daily logs and field reports	Plan review and version comparison

PlanGrid, Forma Build & the Back-Office Connection

PlanGrid — Autodesk's original field-access app — is now in maintenance mode, with Autodesk Forma / Forma Build (formerly Autodesk Construction Cloud / Autodesk Build) as its designated successor for net-new customers. Existing PlanGrid environments continue to work, but firms are increasingly migrating to Forma Build for field-level access to current drawings, punch lists, and issue tracking from a mobile device on-site. Preactive IT supports the connectivity and mobile device management that make field access reliable, whatever stage of the PlanGrid-to-Forma-Build transition a client is in.

The Layer Underneath the Software

Procore, Bluebeam, and Autodesk Forma/Forma Build all ultimately depend on the same underlying layer: identity, device management, connectivity, and permissions. A platform outage is rarely the platform itself — it's usually an identity, network, or device problem showing up as a software problem.

Project management and field software rarely operate in isolation from a firm's accounting and ERP systems — Sage 300 CRE, Viewpoint Vista, and similar platforms. Job costing, WIP reporting, and certified payroll depend on clean data moving between the field platform and the back office without manual re-entry — an integration layer Preactive IT treats as part of the same support scope as Procore and Bluebeam themselves.

Frequently Asked

How easy is it to integrate Procore with other construction software?

Procore supports hundreds of integrations natively, but correct configuration — particularly with accounting/ERP platforms and design software — is where most firms need support to avoid duplicate data entry and reconciliation errors.

How does Procore work alongside tools like Bluebeam?

They're complementary, not competing — Procore manages the project as a whole while Bluebeam handles the drawings themselves, with native integrations now connecting the two directly.

What is Bluebeam used for in construction?

Digital takeoffs during estimating, real-time collaborative markup through Studio sessions, and plan review across project teams and subcontractors, with version history and audit logging documenting every change.



**ALWAYS CONNECTED: NETWORK
INFRASTRUCTURE FOR EVERY JOB
SITE**

NETWORK INFRASTRUCTURE & JOB-SITE CONNECTIVITY

A construction company's network doesn't live in one building. It stretches from a permanent office to a job-site trailer that might exist for six months and then disappear, across cellular dead zones, through weather that takes down power and internet at the worst possible moment. Office IT and job-site IT are genuinely different problems, and treating them the same way is why so many construction firms end up with a network that's reliable in the office and a liability everywhere else.

Core Technologies for Reliable Job-Site Networks

Satellite connectivity

- ✓ Starlink has quickly become the default answer for temporary job-site connectivity in areas without reliable cellular coverage — fast to deploy and increasingly standard equipment in a job-site trailer setup.

Cellular boosters and private 5G

- ✓ Where cellular coverage exists but is inconsistent, signal boosters and increasingly private 5G extend usable bandwidth to the parts of a site standard coverage doesn't reach.

Mesh Wi-Fi

- ✓ A single access point rarely covers an active site. Mesh networks extend coverage across trailers, staging areas, and structures as the site itself changes shape over the project.

Rugged devices & MDM

- ✓ Beyond hardware selection, mobile device management ensures every field device running Procore, Bluebeam, or email is secured, tracked, and recoverable if lost or damaged.

Equipment tracking & telematics

- ✓ GPS asset tracking and equipment telematics increasingly run on the same network infrastructure as everything else on-site.

Network segmentation

- ✓ Office systems and job-site systems shouldn't sit on a flat network — segmenting field devices from core office servers contains a compromised device before it becomes a company-wide incident.

Dual-WAN failover & SD-WAN

- ✓ Two independent connections with automatic failover — and SD-WAN to intelligently route traffic between them — keep a site online when one connection drops instead of going dark.

VLANs, QoS & redundant power

- ✓ VLANs keep office, field, and telematics/IoT traffic properly separated; QoS prioritizes VoIP and video calls over less time-sensitive traffic; and redundant power paired with automated monitoring means an outage gets caught and alerted on, not discovered the next morning.

Weatherproof, ruggedized equipment

- ✓ Job-site networking gear lives in trailers and enclosures exposed to heat, dust, and moisture that office equipment never sees. NEMA-rated enclosures and temperature-tolerant hardware keep switches and access points running through a Texas summer instead of failing at the worst time.

Guest & subcontractor network segmentation

- ✓ Subcontractors, vendors, and site visitors need internet access without touching company systems or project data. A separate guest network with its own credentials keeps that access convenient without becoming an open door.

No single technology on this list solves job-site connectivity on its own — a site with dual-WAN failover and mesh Wi-Fi but no segmentation is still one compromised laptop away from a company-wide incident. Preactive IT designs each job-site network as a complete system, then supports it for the life of the project instead of walking away once it's turned on.

Choosing the Right Connection for the Job

Connection	Best For
Fiber / cable	Long-duration, established sites and permanent offices
5G / LTE	Sites with strong existing carrier coverage
Starlink	Remote or temporary sites without reliable cellular coverage
Dual connections	Sites where connectivity is operationally critical and downtime isn't acceptable
Cellular bonding (multi-carrier)	Sites needing more bandwidth or redundancy than a single carrier connection can reliably provide

Starlink is a connectivity component, not an entire job-site network strategy — it solves the "can this site get online" problem, but segmentation, failover, and monitoring are what make that connection usable and secure.

Case Study Preview: Eliminating Recurring Firewall Failures

G&G Enterprises, a family-owned general contractor building across South Texas since 1986, had a firewall that repeatedly failed with no warning, no visibility into their own network, and IT support handled by a single overwhelmed in-house generalist. Preactive IT replaced the firewall with a high-availability pair, added redundant load-balanced UPS power protection, and onboarded G&G onto a full managed services model — turning a network reliability fix into a complete foundation for how their team works day to day. See the full story starting on page 21.

The Preactive IT Process: **Audit** — **Prioritize** — **Plan** — **Execute** — **Review** — Applied consistently, this cycle builds resilience without disrupting the projects that drive revenue.

Frequently Asked

Is Starlink good for construction sites?

Yes, for the specific problem it solves — fast, carrier-independent connectivity for temporary or remote job sites without reliable cellular coverage. Works best as one piece of a broader network plan, not a standalone solution.

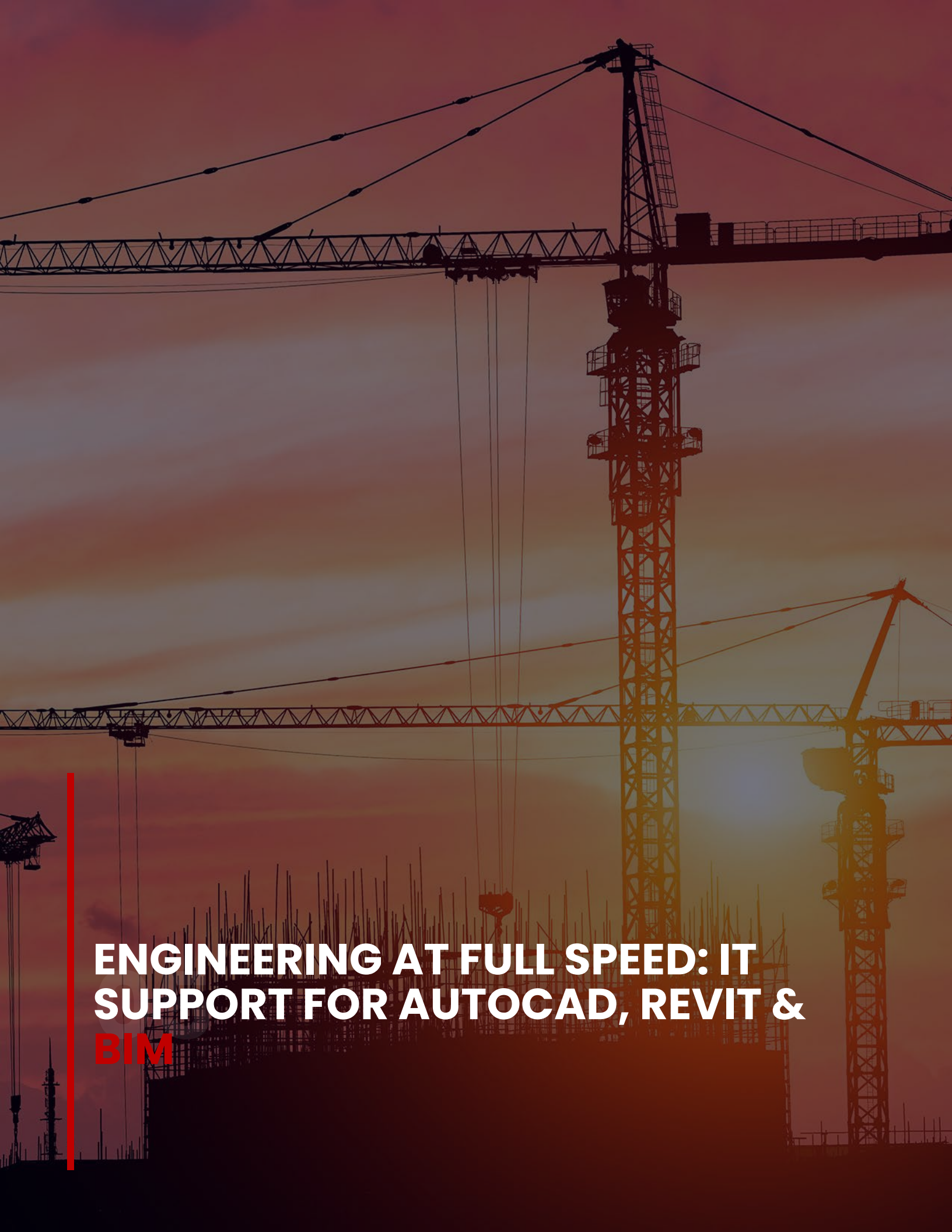
What is the best network setup for a construction job site?

It depends on site duration and location, but the common elements are reliable primary connectivity (cellular, satellite, or both), mesh Wi-Fi for site-wide coverage, network segmentation from office systems, and automated outage alerting.

How much internet bandwidth does a typical job site actually need?

It depends on headcount and use case, but a site running cloud-based project software, VoIP, and a few security cameras typically needs more bandwidth than most contractors budget for upfront — an assessment of actual usage patterns, not a generic recommendation, is what prevents a connection from becoming a bottleneck.

A reliable job-site network is also what makes everything in the next chapter possible — large BIM models, Revit Cloud Worksharing, and multi-gigabyte drawing sets all depend on the same connectivity and infrastructure decisions covered here.

A construction site at dusk or dawn, featuring several large tower cranes and a building under construction with visible rebar. The scene is overlaid with a semi-transparent orange-red gradient. A vertical red line is positioned to the left of the text.

**ENGINEERING AT FULL SPEED: IT
SUPPORT FOR AUTOCAD, REVIT &
BIM**

DESIGN & ENGINEERING SOFTWARE

Design and engineering software occupies a strange position in most construction firms' IT environments: it's often the single most demanding software on the network, running on the most expensive workstations, generating the largest files — and it's frequently supported with the same generic approach as email and office productivity tools. Building Information Modeling has changed what "a drawing" means: a BIM model carries geometry, scheduling, cost, and increasingly IoT data through a project's entire lifecycle, not a static file that becomes outdated the moment it's issued.

What Preactive IT Supports

Workstation performance

- ✓ Revit performance is driven primarily by CPU single-core clock speed, with RAM, storage speed, model complexity, and network connectivity all playing a role — GPU matters far less than most hardware guidance assumes. Autodesk's 2026 guidance recommends 32GB+ RAM for a balanced Revit configuration and 64GB+ for large, complex models.

Large file management & backup

- ✓ BIM models and CAD drawings generate enormous file sizes that standard backup routines aren't built to handle — encrypted, access-controlled storage sized correctly for this data.

Version control & PDM

- ✓ Revit Cloud Worksharing and Autodesk Docs (part of Forma) handle version control and rollback for most AEC teams; SolidWorks PDM remains relevant where Preactive IT also supports engineering-side file management for clients running it.

Navisworks, Model Coordination & Desktop Connector

- ✓ Clash detection and multi-discipline coordination run through Navisworks Clash Detective and Autodesk Model Coordination, not Revit itself — Preactive IT supports the infrastructure and integration work (including Desktop Connector) that determines whether that coordination actually functions smoothly across a project team.

Remote & hybrid design work

- ✓ Virtual workstations and optimized remote access configured specifically for CAD/BIM performance, not a standard VPN connection that can't keep up with graphics demands.

Rendering, visualization & VR walkthroughs

- ✓ Client-facing renderings, fly-through animations, and VR walkthroughs are GPU-bound workloads — the opposite profile from Revit's CPU-bound modeling. A workstation strategy built around only one of these use cases usually underserves the other.

Point cloud & reality capture data

- ✓ Laser scanning and drone-based reality capture generate enormous point cloud datasets that need dedicated storage, processing power, and a clear workflow for aligning captured conditions against the design model.

Autodesk licensing & seat management

- ✓ Named-user licensing makes it easy to pay for more seats than are actually in use, or too few during a project's peak. Preactive IT audits license allocation across office and field so budget matches actual usage.

These workloads share a common thread: none of them perform well on infrastructure sized for email and spreadsheets. Getting workstation, storage, and licensing decisions right up front costs less than fixing a design team's performance complaints after the fact.

A Quick Primer

BIM (Building Information Modeling) is a process and set of tools for creating and managing digital representations of a building's physical and functional characteristics — combining 3D geometry with scheduling, cost, and operational data in a single evolving model.

Revit is Autodesk's BIM authoring and coordination software, used to create and manage building models across disciplines. Clash detection itself runs through Navisworks Clash Detective and Autodesk Model Coordination — Revit is the environment the models come from, not the clash-detection tool.

AutoCAD is Autodesk's foundational computer-aided design software, widely used for 2D drafting and 3D design work, often run alongside Revit or BIM-specific tools.

Revit Cloud Worksharing, part of Autodesk Docs within Forma, lets multi-discipline teams collaborate on a shared central model in real time. Autodesk publishes specific bandwidth recommendations for reliable Cloud Worksharing performance — one more reason the network chapter on page 12 and this chapter are really the same conversation.

Point cloud data is a dense collection of 3D coordinate points captured by laser scanners or drones, used to document existing conditions and verify that as-built construction matches the design model.

Frequently Asked

Why does Revit or AutoCAD run slowly even on a relatively new computer?

Most performance problems trace back to a hardware-to-software mismatch — a machine specced for general office work will struggle regardless of its age. The fix is usually a workstation audit against the actual demands of the models being run.

How should construction firms manage and back up large CAD and BIM files?

Encrypted, access-controlled cloud storage rather than local shared drives, paired with a backup approach sized for file volume and version control that allows rollback without losing a day of collaborative work.

Can design teams work effectively on Revit or AutoCAD remotely?

Yes, with purpose-built infrastructure — virtual workstations or optimized remote access configured for CAD/BIM performance — rather than a standard VPN connection to a local machine.

How do I know if our Autodesk licensing is set up efficiently?

The most common sign is a mismatch between purchased seats and actual usage — either paying for licenses that sit idle most of the year, or field staff sharing a login because there aren't enough seats during a project's peak. A licensing audit compares assignment against real usage patterns.

The same design files this chapter covers — BIM models, CAD drawings, point cloud data — are also exactly what the next chapter's compliance and data-security requirements are built to protect.

A construction site at dusk or dawn, featuring a large yellow tower crane on the right. In the foreground, two men wearing hard hats and safety vests stand with their backs to the camera, looking out over the site. The ground is covered with rebar and construction materials. The sky is a mix of blue and orange hues from the low sun.

BUILT BEFORE THE AUDIT: IT & CYBERSECURITY COMPLIANCE FOR CONSTRUCTION

IT & CYBERSECURITY COMPLIANCE FOR CONSTRUCTION COMPANIES

Preactive IT doesn't provide OSHA, building-code, employment-law, or bonding compliance consulting — those belong to safety consultants, code officials, attorneys, and sureties. What Preactive IT supports is the technology underneath all of it: the security controls, access management, backups, and documentation systems that make compliance possible to prove, on demand, when an auditor, underwriter, or general contractor asks for evidence.

Where IT Carries the Compliance Burden

Area	What It Means for IT
Cyber Insurance	The fastest-growing compliance category — underwriters increasingly require documented MFA, endpoint protection, and tested backups as a condition of coverage, not a suggestion.
DFARS / CMMC	Firms on federal or defense-adjacent projects may need to meet DFARS or CMMC standards — specific, auditable IT security controls beyond general best practice.
NIST 800-171 / CUI	Where a project involves Controlled Unclassified Information, NIST 800-171 controls — access management, encryption, monitoring, incident response — become contractual requirements, not optional hardening.
Contractual Security Requirements	General contractors increasingly flow down security requirements to subcontractors — MFA, incident response plans, and vendor access controls are now bid qualifiers on some projects.
OSHA Records	Safety programs, training records, and inspection reports are OSHA's requirement to keep — IT's role is making sure those records are accessible, current, backed up, and defensible.
Certified Payroll	Davis-Bacon requirements on federally funded projects mean accurate, auditable wage records tied directly to project data — an accounting/field-software integration point IT supports.
Bonding & Building-Code Documentation	Bonding, insurance, and code-approval paperwork depend on producing accurate records on demand — and protecting them, since project and financial documentation is exactly what ransomware groups target.
Texas Building Codes	Texas establishes baseline building-code requirements through the state-mandated adoption of the International Building Code, while municipalities can adopt local amendments and more stringent provisions. Firms working across Houston, Austin, San Antonio, and Beaumont manage jurisdiction-specific requirements and documentation as a result.

Compliance as a Byproduct, Not a Scramble

Compliance support isn't a separate service line at Preactive IT — it's the natural output of the same process behind everything else we do: Audit, Prioritize, Plan, Execute, Review. For G&G Enterprises (see the case study on page 21), that meant a dedicated backup and disaster recovery solution and company-wide security monitoring — antivirus, email filtering, endpoint intrusion detection and prevention — deployed where none existed before. Those aren't just cybersecurity improvements; they're exactly the documented controls a cyber insurance underwriter or a security-conscious general contractor now expects to see.

The Preactive IT Process: **Audit** — **Prioritize** — **Plan** — **Execute** — **Review** — Applied consistently, this cycle builds resilience without disrupting the projects that drive revenue.

What Auditors and Underwriters Actually Ask For

Compliance requirements rarely get evaluated through a conversation — they get evaluated through documentation requests. Knowing what that documentation needs to look like before it's requested is the difference between a same-day response and a scramble.

- ☒ Documented MFA enforcement across email, VPN, and cloud platforms — not just a policy stating it's required
- ☒ Backup restoration test logs showing data actually recovers, not just that backups completed
- ☒ A written incident response plan naming who makes the call to restore, negotiate, or notify
- ☒ Access control records showing who can reach project and financial data, and why
- ☒ Security awareness training completion records for employees and, where required, subcontractors

Frequently Asked

What compliance standards apply to construction companies?

It depends on the work: OSHA applies broadly, local building codes vary by municipality, bonding and insurance apply to most commercial work, Davis-Bacon applies to federally funded projects, and cyber insurance and contractual security requirements increasingly apply across the board.

Do construction companies need cyber insurance, and what does it require?

Cyber insurance is close to standard for firms handling sensitive bid data and client information — and insurers increasingly require documented controls like MFA, endpoint protection, and tested backups as a condition of coverage, not just a recommendation.

Does Preactive IT handle CMMC, DFARS, or NIST 800-171 compliance directly?

Preactive IT implements and documents the underlying IT security controls — access management, encryption, monitoring, incident response, and audit evidence — that CMMC, DFARS, and NIST 800-171 require. Formal certification and legal compliance determinations remain the client's responsibility, typically with a specialized assessor.

How often should compliance documentation be reviewed?

At minimum annually, and after any material change — a new cyber insurance policy, a new federal contract, or a security incident all reset the clock on what needs to be current.



**PROOF IN PRACTICE: NETWORK
RELIABILITY AND FULL-SERVICE
MANAGED IT FOR A SOUTH TEXAS
GENERAL CONTRACTOR**

REAL-WORLD CASE STUDY

HIGH-AVAILABILITY NETWORK & MANAGED IT DEPLOYMENT

G&G Enterprises — General Contractor, Beaumont, Texas

THE CHALLENGE	THE SOLUTION	THE RESULTS
A family-owned general contractor with nearly four decades building across South Texas needed to replace a failure-prone firewall and close major gaps in visibility and support. • Recurring firewall failures with no advance warning • No notification when the firewall, power, or internet went down • No visibility into their own WiFi and switch environment • Entire IT function — help desk included — handled by one in-house generalist • No formal ticketing, SLAs, or dedicated security monitoring	Preactive IT redesigned G&G's network and power infrastructure around redundancy and visibility, then onboarded the company onto a full managed services model. • High-availability firewall pair with automatic failover • Redundant, load-balanced UPS power protection • Proactive offline alerting for firewall, power, and internet • Client-facing, read-only network visibility portal • Company-wide managed services onboarding: help desk, BDR, and security monitoring	Operational improvements in network reliability, visibility, response, and day-to-day IT support across G&G's organization. • Single point of failure eliminated with automatic failover • Immediate, automated outage alerts replace “wait and see” • Real-time network visibility for G&G's own team • Full help desk team with formal ticketing replaces one-person IT • Company-wide security monitoring and BDR in place for the first time

KEY TAKEAWAY

This engagement shows what happens when a construction firm's IT stops being reactive: redundant infrastructure that fails over automatically, monitoring that catches problems before anyone notices, and a support team sized to match the business rather than one person absorbing everything by default. For G&G, that shift came from the same structured process behind every Preactive IT engagement — Audit, Prioritize, Plan, Execute, Review — applied first to the network, then to the business as a whole.

“

Have you ever heard the saying, ‘Everything is fine, we’re fine... meanwhile everything is on fire’? That perfectly describes our very first day onboarding with Preactive IT Solutions. Without missing a beat, their team jumped in, troubleshooted the issue, and had us fully back up and running by the end of the day. Our experience with Preactive IT Solutions has been nothing short of great, and we are confident we made the right choice partnering with them.

Makenzie Coplen Director of Human Resources, G&G Enterprises

NEXT STEPS & RESOURCES

Immediate Actions — Start Today

1	Complete a self-assessment Across your critical systems — network, software, security, and compliance — using this guide’s checkpoints.
2	Enable MFA on every account Highest-impact, lowest-cost step if it isn’t in place already.
3	Test your backups Schedule a restoration test within two weeks.
4	Audit user permissions In Procore, Bluebeam, and cloud storage.
5	Schedule a job-site connectivity review Before your next new site setup.

A 90-Day Path Forward

DAYS 1–30	Quick wins
✓ Complete the risk assessment and identify your top three gaps ✓ Enable MFA everywhere, starting with email, VPN, and cloud tools ✓ Verify backups and test one restoration ✓ Audit Procore, Bluebeam, and cloud storage permissions	
DAYS 31–60	Strengthen the foundation
✓ Deploy or upgrade endpoint protection on every device, including field equipment ✓ Document a patch management process covering OS, firmware, and design software ✓ Implement network segmentation between office and job-site systems ✓ Review job-site connectivity gaps before your next site setup	
DAYS 61–90	Mature the program
✓ Run a tabletop incident response exercise ✓ Implement immutable or air-gapped backup for critical project data ✓ Apply Zero Trust access controls for remote and cloud access ✓ Schedule your first compliance/audit-readiness review	

Ongoing Maintenance

Frequency	Activity
Monthly	Review security logs and alerts, apply available patches, run a phishing simulation
Quarterly	Test backup restoration, audit vendor/subcontractor access, review the incident response plan
Annually	External security assessment or penetration test — based on risk, contractual, insurance, or compliance requirements — plus a tabletop incident response exercise and formal risk assessment update

MSP Titan 2024 Construction & Engineering	Founded 2003 Houston · Austin · San Antonio · Beaumont	20+ Years Specializing in Construction & Engineering IT
---	--	---

Ready to Assess Your Construction Firm's IT?

Schedule a no-obligation consultation — we will identify your highest-priority gaps across cybersecurity, software, connectivity, and compliance, and provide a practical roadmap at no cost. Serving construction companies in Houston, Austin, San Antonio, and Beaumont.

preactiveit.com/bookcall · (832) 944-6250 · info@preactiveit.com



About Preactive IT Solutions

Preactive IT Solutions is a process-driven Managed IT provider founded in 2003, with offices in Houston and Austin, Texas. We specialize in serving construction and engineering firms with enterprise-level IT tailored to the way your teams work.

Our team includes CompTIA Security+ certified professionals and Bluebeam Certified Professionals. Founder and CEO Charles Swihart literally wrote the book on cybersecurity for SMBs — *On Thin Ice* (Amazon Best-Seller, 2020) — and was recognized as MSP Titan of the Industry in 2024.

Awards & Recognition

- Houston Business Journal Best Places to Work 2024
- MSP Titan of the Industry 2024 — Construction & Engineering
- Channel Futures NextGen 101 — 2022
- Houston Fast 100 — 2017, 2019, 2021
- Channel Futures MSP 501 — 2018, 2021

SOURCES & FURTHER READING

This guide draws on the following public research and reporting. Statistics and group activity reflect the sources and time period cited; readers should confirm current figures before citing them independently.

Cited Sources

1. Black Kite, 2025 Ransomware Report — construction-sector victim count (418 tracked victims, third-highest sector for the year).
2. Rapid7, Threat Landscape of the Building and Construction Sector (ransomware research series, 2025) — construction industry targeting trends and the 2025 ransomware group list.
3. Public incident reporting: Bird Construction (2019 Maze ransomware disclosure); Skender Construction (March 2024 double-extortion disclosure); MasTec (2025 SEC/public disclosure of a Clop-linked third-party zero-day incident).
4. Autodesk, official product documentation and hardware guidance — Revit 2026 system requirements and RAM recommendations, Revit Cloud Worksharing bandwidth guidance, and the Autodesk Construction Cloud / Autodesk Build to Forma / Forma Build rebrand (effective March 2026).
5. Procore and Bluebeam, official product documentation — platform capabilities and native integrations referenced in this guide.
6. U.S. Department of Defense CMMC program documentation, DFARS clauses, and NIST SP 800-171 — federal contract security requirements referenced in the compliance chapter.
7. OSHA (osha.gov) — safety program and recordkeeping requirements referenced as examples of records IT systems must preserve and secure.
8. Texas Department of Licensing and Regulation and Texas Municipal League — statewide I-Code adoption baseline and municipal amendment authority referenced in the compliance chapter.

Continue Reading on PreactiveIT.com

[IT Services for Construction Companies — pillar overview](#)

[Cybersecurity for Construction Companies](#)

[Procore, Bluebeam & Construction Software Support](#)

[Network Infrastructure & Job-Site Connectivity](#)

[AutoCAD, Revit & BIM Support for Construction](#)

[IT & Cybersecurity Compliance for Construction Companies](#)

[G&G Enterprises Construction IT Case Study](#)

[Schedule a Free Consultation](#)