Construction Cybersecurity Playbook

Protecting Bids, Blueprints, and Vendor Payments

A practical field guide for construction owners, controllers, estimators, project executives, operations leaders, and accounts payable teams.

24,768	$3.046B
BEC complaints reported to IC3 in 2025	Reported BEC losses in 2025

Source: FBI Internet Crime Complaint Center, 2025 IC3 Annual Report.

Five controls to put in place first

- **Protect accounts:** Require MFA for email, finance, project platforms, cloud storage, and remote access.
- **Control project data:** Use an authoritative repository, named accounts, project-level permissions, and version control.
- **Verify payment changes:** Call a previously validated number and require a second authorized reviewer.
- **Manage devices:** Encrypt, patch, inventory, lock, and rapidly revoke access to office and field devices.
- **Test recovery:** Restore a representative bid or project file and practice first-hour incident decisions.

Where construction wire fraud enters

Vendor setup	**Pay applications**	**Lien waivers**
Joint checks	**Retainage release**	**Final payment**

Computerbilities supports construction businesses across Raleigh, Cary, Durham, and the North Carolina Triangle from its Cary office.

Vendor Payment Verification Checklist

Use this checklist for every new vendor and every request to change bank details, payment method, remittance address, payee identity, joint-check arrangement, or retainage destination.

- ☐ Flag the request as a high-risk change before editing the vendor record.
- ☐ Review the full sender address and domain for subtle changes.
- ☐ Call a previously validated number from the vendor master record or an independent official source.
- ☐ Confirm the authorized vendor representative, bank name, account details, effective date, and affected invoices.
- ☐ Match the request to the contract, approved pay application, schedule of values, lien waiver, joint-check agreement, and retainage status as applicable.
- ☐ Require a second authorized employee to review the change and supporting evidence.
- ☐ Separate vendor-record maintenance from payment approval whenever staffing permits.
- ☐ Document the callback, number used, vendor contact, details confirmed, date, time, and approver.
- ☐ Send confirmation through the established vendor contact channel.
- ☐ Monitor and promptly reconcile the first payment to the new account.
- ☐ Escalate urgency, secrecy, duplicate invoices, unusual credits, or conflicting documents before releasing funds.

Stop and verify when

- An executive or project leader asks to bypass the normal approval process.
- A pay application and lien waiver point to different payees or accounts.
- A vendor requests a last-minute joint check or retainage change.
- A permit or planning fee email threatens delay and discourages a phone call.
- A familiar voice, phone number, or email account makes an unusual request.

Rule: Never verify a payment change with the phone number, reply address, or link supplied in the same request.

Protect Bids and Blueprints

Construction teams may work across Procore, Bluebeam, Autodesk Construction Cloud (ACC), Sage 300 CRE, Microsoft 365, and other platforms. Apply controls to the workflow and confirm which systems are covered by each provider agreement.

Workflow	Risk	Minimum controls
Bids and estimates	Account takeover, unauthorized sharing, altered submission	MFA; named accounts; approved sharing; version history; recoverable copies; final release review
Drawings and project files	Stale drawing, stolen device, excessive access, outage	Authoritative repository; project permissions; encryption; managed devices; tested recovery
Jobsite access	Shared credentials, unmanaged device, weak remote access	Named identity; screen lock; patching; secure remote access; rapid revocation
Project closeout	Lingering access, lost records, unclear retention	Access removal; archive ownership; retention decision; vendor offboarding

Lost-device response

- Report the loss immediately through the approved support route.
- Revoke active sessions and protect affected accounts.
- Lock or wipe managed business data when appropriate.
- Record the device, user, last known location, and potentially exposed data.
- Decide whether clients, insurers, counsel, or other parties must be notified.

Recovery check

Choose one current bid or project data set. Restore it to an isolated location, record the recovery time, confirm that an authorized employee can open it, and document the next improvement. A backup is not a recovery plan until the process has been tested.

First Hour After Suspected Wire Fraud

- **1. Call the bank.** Ask the originating financial institution about a recall or reversal and required indemnification documents.
- **2. Call the intended vendor.** Use a previously verified number and confirm what changed.
- **3. Protect accounts.** Review sign-ins and mailbox rules, revoke suspicious sessions, reset credentials as appropriate, and preserve logs.
- **4. Preserve evidence.** Keep messages, headers, attachments, timestamps, payment details, phone numbers, and related communications.
- **5. Report the incident.** File a detailed complaint with IC3.gov and follow legal, insurance, client, and regulatory notification requirements.
- **6. Warn relevant partners.** Attackers may continue the same conversation or target the next payment.

30-Day Action Plan

Week 1	Map owners, systems, vendors, authoritative files, and high-risk transactions.
Week 2	Enforce MFA, remove dormant access, and publish the callback and dual-approval rule.
Week 3	Run a wire-fraud scenario, a lost-device scenario, and one representative restore.
Week 4	Assign remaining risks to owners with due dates and a 90-day review cadence.

Book a Construction Cybersecurity Review

Computerbilities serves construction businesses in Raleigh, Cary, Durham, and the North Carolina Triangle. Review scope, covered users, platforms, locations, and responsibilities in the written proposal.

Sources: FBI IC3 Business Email Compromise guidance and 2025 Annual Report; FBI construction-material and 2026 planning-and-zoning alerts; CISA MFA guidance; NIST SP 1305; FTC small-business scam guidance; Computerbilities construction IT, service-plan, and disaster-recovery pages.

This playbook provides general operational guidance and is not legal, banking, insurance, or compliance advice.