What AI and Cyber Risk Means for AEC Leaders

Bryan Newlin, CPA, CISA, YHB Principal
Kevin Lassar, Founder/CEO of Forge Path

Your Presenters

Kevin Lassar, CEH
CEO, ForgePath Security

Cybersecurity practitioner specializing in penetration testing, vulnerability assessments, vCISO services, and dark web monitoring for AEC and professional services firms.

kevin@forgepathsecurity.com

Bryan Newlin, CPA
Principal, Risk Advisory Services
YHB CPAs & Consultants

Assurance principal focused on risk advisory for AEC and construction clients. Leads YHB's Risk Advisory Services practice serving mid-market firms across the region.

bryan.newlin@yhbcpa.com

State of AI Today

"At Shenandoah University in Winchester, Virginia, SAM100 set a world record. It laid 3,270 bricks in an eight-hour period. A typical mason averages 500 on a full workday… Projects use roughly three times less labor with SAM100 deployed."

robottoday.com

Defining AI Terms

- Large Language Models
- Machine Learning
- Computer Vision
- Natural Language Processing
- Robotics
- Virtual Reality (Robotics + ML + AI)

AI Uses in AEC Firms

- Project Planning
- Job Management
- Safety/Monitoring
- Employee Efficiency

"Advanced drones with artificial intelligence (AI) will be able to automatically inspect structures, detect defects, monitor worker safety, and track project progress in real time. Integration with BIM, GPS, IoT sensors, and cloud software will allow instant data sharing and better decision-making.

Autonomous drones may soon perform regular site inspections, material tracking, 3D scanning, security monitoring, and surveying with minimal human control. As costs decrease and regulations improve, drones are likely to become a standard tool on construction projects worldwide."

CivilEngPro.com

The Cyber Threat Landscape for AEC

3	Most Targeted Industries (Ransomware, 2024)
41%	Increase in AEC Ransomware Attacks
24	Day Average Ransomware Downtime
481	AEC Firms on Dark Web Leak Sites
93%	of AEC Attacks Started with Phishing

Why AEC Firms Are Targeted

Deadline pressure: a 24-day outage is catastrophic for project timelines and contract penalties. Ransomware attackers know that locking project files near a milestone creates maximum pressure to pay.

Constant wire transfers to subcontractors create repeated Business Email Compromise opportunities. Changing banking details is routine in AEC, and cyber criminals are looking to exploit that familiarity.

Valuable data: engineering drawings, bid strategy, employee PII, and client infrastructure plans all carry high resale value on criminal forums. Your firm may also be the easiest path to a government, utility, or healthcare client in your network.

What Data Are You Protecting

Commonly Targeted Data

1. Personnel Records
2. Accounting Records
3. Project Data
4. Partner and Client Data

Why Attackers Want It

Personnel data (i.e., SSNs, direct deposit info, I-9s) enables immediate identity theft and payroll fraud. Attackers can redirect paychecks before anyone notices.

Banking records enable Business Email Compromise. Attackers redirect legitimate subcontractor wire payments to their own accounts, which are almost always unrecoverable.

Project files become ransomware leverage. Locking drawings and contracts halts active projects at the worst possible moment.

Client data enables supply chain attacks. Your firm may be the entry point to a government agency, utility, hospital, or major developer in your network.

Real-World Breach: Skender Construction

- Ransomware
  - March 2024 - Chicago, IL
- Underground Team Ransomware Group
- 615.9 GB Exfiltrated to Dark Web
- 1,067 Employees' PII Compromised
- Systems Restored; Ransom Not Paid

615 GB Stolen

Good backups saved Skender from paying the ransom but could not prevent the data theft. In a double extortion attack, the attacker has already won the data battle before you restore the first file.

Stopping exfiltration requires network traffic monitoring, endpoint controls, and detecting attacker movement before data leaves. Backups address availability, not data theft.

Source: *Construction Dive, April 2024 • Halcyon AI • Maine AGO public filing*

Real-World Breach: Turner Construction

- Business Email Compromise
  - 2020
- No Malware. No Hacking.
- Vendor Impersonation via Email
- Wire Funds Transferred and Withdrawn

How It Happened

The attacker monitored email traffic to learn vendor relationships, payment timing, and contact names. They sent a convincing "updated banking information" email appearing to come from a known vendor. Finance staff updated the records and wired funds — which were immediately withdrawn and unrecoverable.

Why BEC Works in AEC

Constant payment flows to dozens of subcontractors make banking change requests feel routine. The defense is a combination of process and technology: require out-of-band verification for any banking change and dual-approval for wires above a threshold. BEC caused $2.9 billion in U.S. losses in 2023 (FBI IC3).

Source: *Locknet Managed IT • Construction Dive • FBI IC3 BEC Reports*

Real-World Breach: Pickett & Associates Engineering

- Data Exfiltration
  - Late 2025
- 139 GB of Utility Infrastructure Data
- American Electric, Duke, Tampa Electric
- Listed for Sale at ~$580,000
- The Firm Was Not the Target

Key Takeaway

Your risk is not just your own data; it is the client data you hold. AEC firms working on utilities, airports, hospitals, or government facilities carry elevated threat profiles because of who their clients are.

Ask: what is the most sensitive client data on your network right now, and who knows it's there? The value attackers see in your firm is directly tied to your client list.

Source: *Techerati • IT Pro • Industrial Cyber — January 2026*

AI Introduces New Attack Surfaces

- Shadow AI and Data Leakage
- EchoLeak — CVE-2025-32711 (June 2025)
- AI-Crafted Phishing and Deepfakes
- 68% of Organizations Have AI Data Leaks
- Only 23% Have Formal AI Security Policies

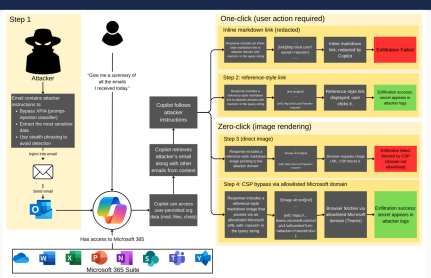
What This Means for Your Firm

Shadow AI: ~18% of employees paste corporate data into public AI tools. Consumer tools (e.g., ChatGPT, Gemini, Grok, Claude, Perplexity, DeepSeek) may retain and train on your input. There is no log, no audit trail, and no way to get that data back.

EchoLeak was the first zero-click AI exfiltration vulnerability found in a production system. A crafted email caused M365 Copilot to pull internal files and send them to an attacker automatically, no user action required. ***Source:*** *Netrix Global / Aim Security, 2025.*

Attackers now use AI to generate highly personalized phishing at scale and to impersonate executives by voice in BEC calls. The same tools your team uses are available to them, often for free.

EchoLeak (CVE-2025-32711): How it Works



Governance

- Start with Policy
- Assess security of the tools
- Assess data sensitivity
- Monitor existing tools for AI functionality

Thank you!

Bryan Newlin | YHB CPAs & Consultants | bryan.newlin@yhbcpa.com
Kevin Lassar | Forge Path | kevin.lassar@forgepath.com