3 CRITICAL CYBERSECURITY MEASURES EVERY CONSTRUCTION BUSINESS MUST IMPLEMENT NOW!

CONTINUOUS

FIRST LET'S UNDERSTAND... HOW ARE CONSTRUCTION BUSINESSES EXPOSED TO CYBER RISK?

CONTINUOUS

#1 MOBILE WORKFORCE

RISK

- Jobsite Trailers
- Work from Home
- Traveling Personnel

Workers connect to business networks and systems from temporary locations (ex: jobsite trailers) using laptops, tablets, and smartphones. Security in these temporary locations is often much weaker than in the main office, especially when using worker-owned devices.

This represents a significant risk for a data breach as systems and processes are usually not in place to protect workers properly from the threat of a cyber-attack.

CONTINUOUS

#2 SHARING FILES WITH 3RD PARTIES

RISK

- Blueprints
- Bids/other Financial Info
- Employee Records

Collaboration with 3rd parties is often critical to meeting project requirements and client demands. When this happens, data is often shared and transmitted using unsecured methods that open construction businesses to a significant risk of a data breach. These types of data breaches can result in reputation, clients, and revenue loss.

CONTINUOUS

#3 PERSONNEL TRAINING & AWARENESS

RISK

- High Turnover of Subcontractors
- Changing Jobsites
- Lack of Internal Staff Training

New jobs often require new subcontractors. These subcontractors are separate from the existing company culture, leading to a high level of human risk from data breaches. Personnel must be consistently and regularly trained on changing cybersecurity risks to remain vigilant against these human-based attacks. Additionally, full-time personnel must also be consistently and regularly trained to detect and prevent cyber attacks.

CONTINUOUS

HERE ARE 3 WAYS CONSTRUCTION BUSINESSES CAN PROTECT THEMSELVES.

CONTINUOUS

#1 SECURE BACKUPS

PROTECT

- Follow 3-2-2 Backup Rule
- Encrypt Backups
- Regularly Perform Test Recoveries

3-2-2 Backup Rule
- Keep 3 copies of your data
- Store 2 backup copies locally but on different devices
- Store 2 copies offsite (1 copy remote location +1 cloud)

All backups are encrypted with AES-256-bit encryption ciphers to protect confidentiality and integrity.

Backup recovery tests are performed at least quarterly.

CONTINUOUS

#2 CONSISTENT EMPLOYEE CYBERSECURITY TRAINING

PROTECT

- Bi-Weekly Micro-training
- Regular Phish Testing
- Build a Culture of Security

If you want to build a culture of security, all company employees should receive bi-weekly cybersecurity micro-training. Here's why...

- Employees are less likely to retain information when training is infrequent and more time-consuming.
- Training should be fun (even funny!), engaging, and short (no more than 3-5 minutes).
- Employees should be tested on the knowledge they are gaining regularly (bi-weekly).

CONTINUOUS

#3

CYBERSECURITY DOCUMENTATION & MANAGEMENT

PROTECT

- Implement IT Policies & Procedures
- Create Incident Response Plan
- Create Business Continuity Plan

You wouldn't buy materials to build a house without having a blueprint, so why would you install cybersecurity tools without having a technology plan? Cybersecurity documentation and management guarantees that you make the best technology decisions that protect your company, control your costs, and deliver for your clients.

CONTINUOUS

WANT MORE INFORMATION?

CONTACT US FOR A

FREE CHECK

OF YOUR NETWORK AND CYBERSECURITY.

CONTINUOUS

WE MAKE IT PERSONAL

success@continuous.net
Tel. (201) 579-2086

Call us or email us and say "I want my FREE CyberSCORE!"