Coalition

THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Construction Industry

Construction companies use technology to improve efficiency and productivity, but many can fail to recognize that weak or outdated security controls can make them vulnerable to cyber attacks, as construction is one of the most frequently targeted industries. Attackers often exploit everyday technology, like email and passwords, as well as unsuspecting employees to gain unauthorized access and pursue malicious activities.

Cybersecurity should be a priority for construction companies that depend on technology to operate because a cyber attack can be costly, disruptive, and cause irreparable damage to a business' reputation. While fraudulent payments and data theft are typically the most common cyber threats, many of the technologies used in construction can create additional risk for bodily injury and property damage, underscoring the importance of strong security controls and cyber insurance.

Claims Insights

It's just a little security incident. How bad could it be?

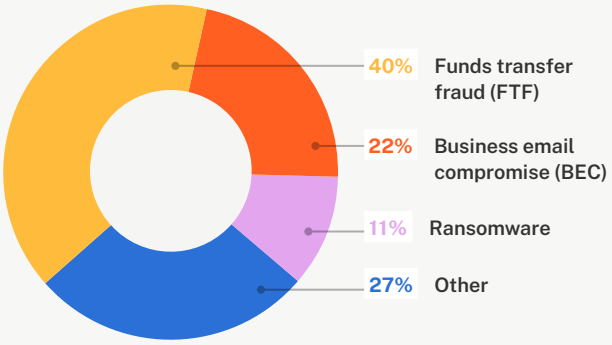
$208,000

Average cost of a cyber insurance claim for construction organizations

Claim Examples

ORGANIZATION	EVENT TYPE	LOSS
Concrete Contractor	Funds Transfer Fraud	$256,000
Car Parking Lifts	Business Email Compromise	$82,000
Chassis Leasing	Ransomware	$603,000

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT — Among all event types experienced by construction businesses, FTF claims are the most expensive with an average loss of more than $290,000.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Unique Exposures

Most construction businesses use data and technology. Why is that risky?

Essential Technologies Can Create Cyber Risk

Building information modeling (BIM) software

This software is used to create 3D models and help with planning, coordinating, and managing project costs. While BIM software can improve efficiency and reduce errors, the data it relies on exposes organizations to cyber risk in the event of a breach.

Document management systems

These software platforms are used to store and handle a large volume of shared files. However, a compromise could expose sensitive data and cause serious disruptions due to the volume and potentially sensitive nature of the information in these systems.

Supervisory control and data acquisition (SCADA) systems

Used to gather and analyze equipment data, SCADA systems can be vulnerable to cyber attacks through outdated software, a lack of encryption, weak passwords, and unsecured wireless networks, which can lead to unauthorized access and data compromise.

Safety management software

Used to manage safety and compliance on construction sites, this software supports employee health and safer working conditions by helping with inspections, incident reporting, and training.

Payment processing software

Funds transfer fraud and invoice manipulation are often major drivers of cyber claims. For construction companies that use electronic payments, even one fraudulent transfer can have dire financial consequences.

CRM systems

Customer relationship management (CRM) systems are used to support business development activities. Containing client data and confidential corporate information, CRM systems could be compromised and leveraged for malicious purposes, resulting in a data breach.

Email & mobile devices

Mobile devices are essential for communication among construction workers, particularly email. However, business email compromise (BEC) is a frequent cause of cyber insurance claims for construction companies, which can trigger data breaches, business interruption and even reputational damage.

End-of-life software & hardware

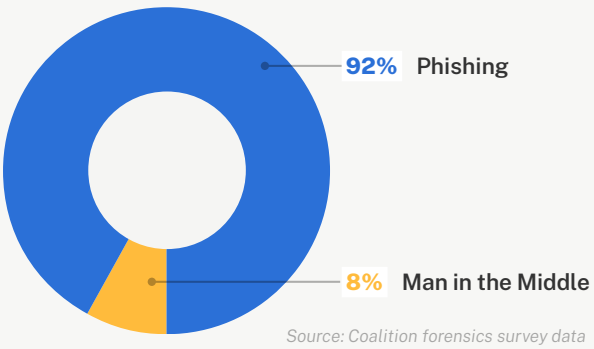
Some organizations may use outdated technologies with the belief that upgrading would be expensive, time-consuming, and disruptive. However, technologies no longer supported by the manufacturer often have known security vulnerabilities and may lack important security features to protect against modern threats.

Field operations platforms

This technology is used to keep track of workers' progress, help coordinate delivery of supplies, and manage devices used on-site. The platform typically holds crucial data that can be vulnerable to cyber attacks, especially when connected to insecure networks in the field.

Cyber Claims in the Construction Industry by Attack Vector

KEY INSIGHT —— Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue many malicious activities, which is why **phishing is the leading attack vector for nearly every cyber claim in the construction industry.**



Source: Coalition forensics survey data

Coalition

Sensitive Data Can Increase Business Liability

Financial data

Collecting and processing financial data, such as tax information, credit card numbers, or payment history, requires adherence to industry standards. If compromised, data can cause harm to clients and trigger regulatory investigations.

Legal and contractual data

Construction companies may have access to contracts, legal agreements, and disputes, including settlements, judgments, and court orders. Mishandling confidential data can cause significant damage to the data owner.

Non-sensitive personal information

Some data on clients, prospects, and other third parties may be publicly available and not considered protected. However, a breach of this data can still impact trust and public image if handled improperly.

Sensitive employee information

Every organization collects and stores information about its employees. Unauthorized access or disclosure of this data — whether PII, PHI, financial, or otherwise — can cause direct harm to employees.

Corporate confidential data

To perform work and access job sites, construction firms and contractors often need access to sensitive corporate data, such as blueprints, architectural/electrical drawings, and change orders. Governance of this data may be addressed in contracts, and breach implications can be significant.

Personally identifiable information (PII)

PII is any data that can potentially identify a specific person. PII can be used to launch cyber attacks or gain access to networks to initiate attacks. Organizations that mishandle PII or fail to respond to a data breach appropriately can be subject to fines, penalties, and other financial damages.

Protected health information (PHI)

Some construction firms may have access to health-related information, such as disabilities or injuries, for the purposes of accommodation and compliance. All PHI must be protected to ensure medical privacy and comply with Health Insurance Portability & Accountability Act (HIPAA) regulations.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- HIPAA & business associate agreements
- International data privacy and consumer protection regulations
- State data privacy & consumer protection laws
- State notification requirements
- Payment Card Industry Data Security Standard (PCI DSS)

$4.47 million

Average total cost of a **data breach** for construction companies[1]

1. IBM Security, Cost of a Data Breach Report 2022

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **coalitioninc.com**

Coalition

Business Impacts

What can construction companies expect after a cyber incident?

Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, most commonly first-party expenses. If a construction business experiences BEC and sensitive data is involved, it can trigger a need for additional legal counsel, forensic investigation, victim remediation, and notification. Simple investigations can cost tens of thousands of dollars, while more complex matters can increase costs exponentially. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 1st Party
- Breach Response
- Crisis Management
- Cyber Extortion

Liability to others

Many construction companies face new and unexpected exposures after a cyber event. Though most do not collect large amounts of sensitive personal information, they may have access to corporate confidential data and systems; some must also comply with industry standards or government requirements for protecting data. This type of information and access is typically addressed in contracts and often carries strict information security and disclosure requirements in the event of a breach, exposing firms to cyber liability they may not anticipate. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 3rd Party
- Multimedia Content Liability
- Network and Information Security Liability
- PCI Fines and Assessments
- Pollution
- Regulatory Defense and Penalties

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on a construction business' ability to operate and can be highly visible to clients, customers, and other stakeholders. Even short periods of disruption can lead to direct loss of revenue and inhibit the ability to support clients, negatively impacting client retention and acquisition. Relevant insuring agreements may include:

- Business Interruption & Extra Expenses
- Reputation Repair

Cybercrime

Beyond ransomware and data breaches, cyber events can result in financial theft for a construction company or its clients — often without an actual breach. If an attacker dupes someone in the billing department to alter payment instructions, a business can lose tens or hundreds of thousands of dollars almost instantly. Attackers can also gain access to email accounts and send fraudulent invoices or payment instructions to clients, customers, and other third parties. Relevant insuring agreements may include:

- Funds Transfer Fraud
- Invoice Manipulation
- Phishing (Impersonation) and Proof of Loss Preparation Expense Endorsement
- Service Fraud

Recovery and restoration

After a cyber event, resuming operation is no easy task. If an attacker damages or destroys essential technology, data, or physical equipment, a construction business may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require purchasing new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

1.87%
Coalition 2022 overall claims frequency

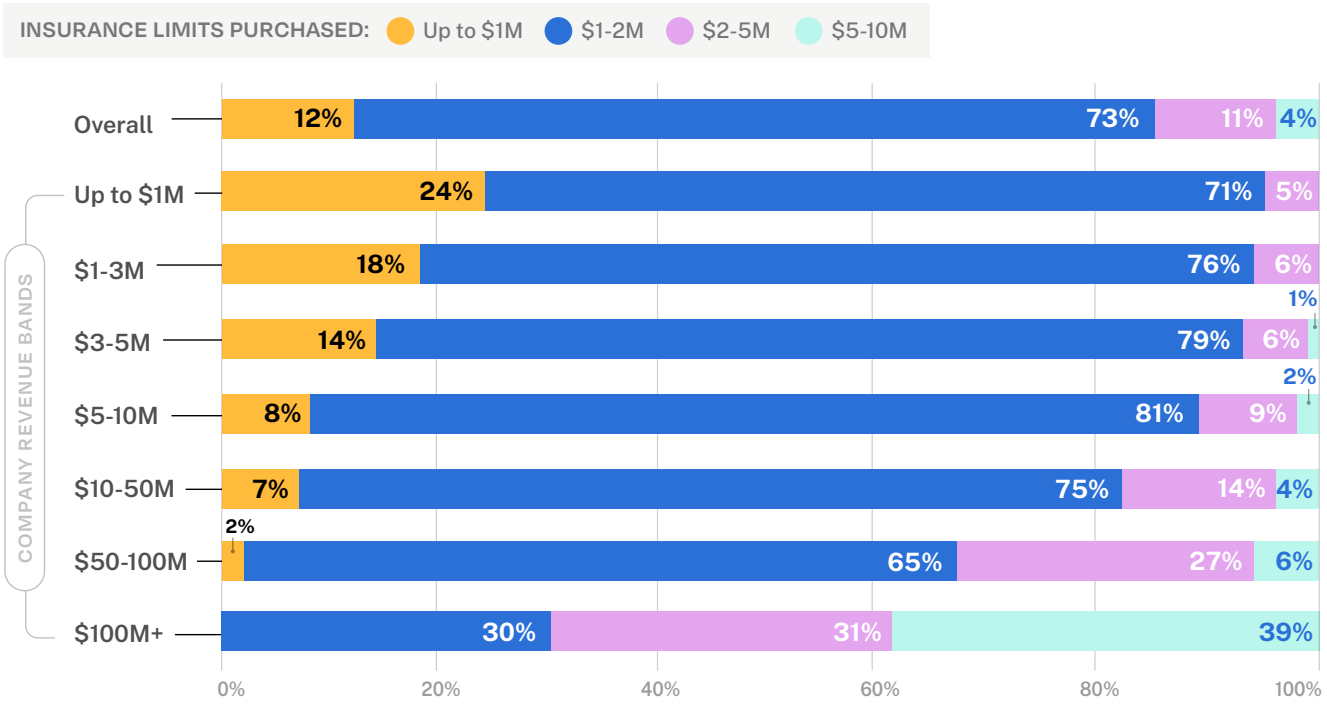
↓ 22%
Year-over-year decrease in Coalition claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the construction industry

PEER PURCHASING HABITS BY REVENUE



Source: Coalition policyholder data

KEY INSIGHT — Most small and medium-sized businesses in the construction industry purchase $1M-2M in limits, as do many mid-market organizations. For those needing more than $10M in limits, Coalition offers primary and excess terms for businesses up to $5B in revenue.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

The Power of Active Insurance

Why do construction companies choose Coalition?

47%	43%	5 minutes
Reported cyber events handled with no cost to policyholder	Reduction in critical vulnerabilities among policyholders in 2022	Average response time to a cyber incident

Active Insurance* is designed to help prevent digital risk before it strikes.
Our new approach to managing digital risk provides **three layers of support**:

Insurance as active as digital risk

In the digital economy, Coalition wants to ensure that all organizations can thrive by helping to protect them from the threat of emerging risks. We've built an expert team across incident response, claims, and our panel vendors. In the event of a claim, Coalition helps organizations respond and recover so they can get back to business.

Brokers
Get appointed today at
signup.coalitioninc.com

Construction businesses
Get a free risk assessment at
control.coalitioninc.com

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **coalitioninc.com**