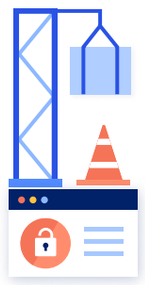
Construction/Contractors

Benefits of a Smart Cyber Insurance Policy

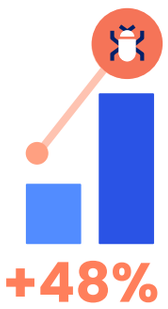
CORVUS BY TRAVELERS

1 The Big Picture



In years past, professionals in the construction industry may have felt that their businesses were safely “off-line” and out of reach of cyber threats. With the adoption of web-connected tools, that’s changed.

2 What’s New?



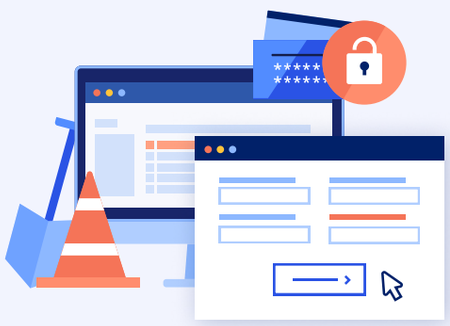
Ransomware attacks in the construction industry surged by 48% from 2022 to 2023, and 80% of industry respondents in 2024 said they believed having proper cybersecurity controls in place is critical.

3 The Risk Management Solution

Cyber liability coverage and proactive risk management practices are now essential. Companies in the construction industry should carry insurance to cover the cost of a cyberattack, including first- and third-party coverages such as ransomware and social engineering attacks.

Cyber Claims Examples

Phishing Email Scam



A large construction firm placed an order with one of their go-to suppliers ahead of a new project. The firm received an email from the billing representative informing them that the supplier’s bank information had changed. New instructions for payment were attached.

The construction company sent the payment (approximately $2,000,000). Two days later, their supplier called to inquire about the payment status, and it was quickly discovered that the firm had been defrauded by threat actors who had impersonated the billing representative.

Corvus worked with the construction firm to respond to the fraudulent transfer of funds, connecting them with several vendors to investigate the wire transfer and their IT system. Since the construction company quickly notified Corvus of the fraudulent charge, we were able to help claw back a majority of the stolen funds.

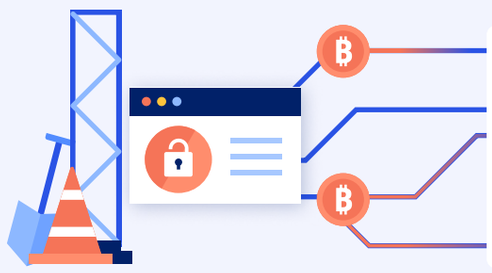
Vendor Data Breach on Construction Management Platform

A leading construction management firm that handles large-scale projects through a centralized vendor management system suffered a data breach that exposed hundreds of subcontractors' payment and personal information.

After a forensic investigation, it was determined that the attacker had infiltrated the firm’s system over a four-month period, exfiltrating subcontractor names, bank details, tax IDs, and confidential project-related documents. This allowed the attacker to gain access to sensitive financial and operational data without detection for months.

State regulations required the firm to notify all affected subcontractors and suppliers and offer a year of credit monitoring. The construction firm incurred significant costs for legal fees and compliance requirements and hired a public relations team to manage communication with stakeholders and mitigate reputational damage. Additionally, the firm invested in upgrading its security infrastructure to prevent future breaches.

Ransomware Attack and System Vulnerability



A construction management company was hit with a ransomware attack demanding $60K in bitcoin. Their network security, along with their data backup/disaster recovery system, was left vulnerable, and as a result, 30 employees were unable to access company files for ten days. This cost the company an additional $100K in lost productivity & business, totaling $160,000 in losses.

Smart Cyber and Cyber Excess Policy Highlights

Missed Bid Coverage

Coverage under business income loss is expanded for a missed bid or request for proposal (RFP) due to a total, partial, intermittent interruption or degradation in service of an Insured's computer system resulting from a privacy breach, security breach, administrative error, or power failure.

Coverage for Third-Party Risk

Construction and contractor institutions increasingly transfer or entrust data to third-party vendors such as cloud storage companies. Third-party cyber coverage can respond when construction institutions face a breach, regardless of which organization's system was breached, or where the data resided at the time of the compromise.

Risk Prevention Services

Through tailored threat alerts and partnership with in-house cyber experts, we're here to help policyholders reduce the likelihood of a cyber attack at their organization — and at no additional cost beyond their policy premium.

In-house Claims Handling

When a security breach happens, every minute matters. Our in-house incident response and claims teams are available through the entire breach response process — before, during, and after an incident.

Industry Benchmarks

Limit Benchmarks

While recommended limits will vary by the specifics of each risk, these benchmarks approximate the Smart Cyber Insurance coverage purchased by organizations grouped by gross annual revenue. (Corvus offers limits of up to $10m for primary and excess Cyber policies)

Annual Revenue	Typical Limit Purchased
Up to $50m	$2m
$50m - $200m	$4m
$200m - $300m	$4m
$300m+*	$5m

**Data reflects Corvus primary policies only. Policyholders may be achieving aggregate limits greater than $5 million through excess policies.*

About Corvus

Corvus Insurance, a wholly owned subsidiary of The Travelers Companies, Inc., is building a safer world through insurance products and digital tools that reduce risk, increase transparency, and improve resilience for policyholders and program partners.

Our market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance® and Smart Tech E+O®.

Brian Alva
Senior Vice President
Cyber TEO Underwriting