

## Construction + Contractors

Benefits of a Smart Cyber Insurance® Policy

---



**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.

**What’s New?** As software tools such as cloud-based project management portals, automatic takeoff & estimation programs, and customer relationship management (CRM) systems have proliferated in the construction industry, so has cyber risk. In 2020, [13.2% of all North American Construction firms](#) reported falling victim to a cyber breach.

**Your Solution:** Adequate cyber liability coverage and risk management practices are now essential. Companies in the Construction industry should have cyber liability insurance to cover the cost of a cyberattack, including first- and third-party coverages such as ransomware and social engineering.

## Cyber Claims Examples

---

[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.

[An excavation and construction company](#) noticed their printers acting up one day in April 2021, and soon after, they found themselves locked out of their entire network. The ransom cost \$100K, but they estimate that an extra \$1 million in additional work is needed to recoup their \$100K loss.

[A Canadian construction firm](#) suffered a **Maze** ransomware attack in Dec. 2019. They lost 60 GB of data outlining information on over \$400 million in construction contracts with Canada’s Department of National Defense between 2006 and 2015.

## Smart Cyber + Cyber Excess Policy Highlights

### Coverage for Ransomware Remediation

When a business suffers a ransomware attack, cybercriminals typically encrypt or threaten to delete company data. Cyber coverage helps businesses, such as construction firms, pay for the cost of the ransom to end the threat or unencrypt data.

### vCISO Digital Experience

Policyholders receive on-demand access to actionable advice, advanced IT security recommendations, and resources to help reduce risk and provide a full scope of their business’s IT security posture.

### Risk Mitigation

Through the policy term, we offer a suite of complementary and reduced-cost services aimed at helping our policyholders prevent, prepare for, and respond to any cyber 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 \$5m for primary and excess Cyber policies).

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

Eligibility for such programs is determined when you apply for coverage. Policy quotes, terms and conditions, and premiums are made in accordance with Corvus Insurance’s underwriting guidelines. The policy, not general descriptions or material within this document, will form the contract between the insured and our insurance carrier partners. Coverage may not be available in all jurisdictions.



**Brian Alva**  
**Vice President of Cyber Underwriting**  
 balva@corvusinsurance.com

### Social Engineering & Cyber Crime

Cybercriminals often use social engineering tactics, such as phishing, to gain valuable information from their victims. The information gathered is typically used to gain access to bank accounts, resulting in stolen funds. Cyber coverage helps businesses cover the cost of a social engineering attack.

### Vulnerability Alerting

Policyholders receive notifications of emerging cybersecurity risks and new vulnerabilities on their systems through Corvus email alerts to help proactively prevent future cyber attacks.

### Incident Response

Corvus’s dedicated breach response and cyber claims teams work with you during the entire life cycle of an insurance claim. We also provide assistance with the engagement of trusted partners, including breach counsel and forensics firms to ensure success.

Annual Revenue	Typical Limit Purchased
Up to \$50m	\$1m
\$50m - \$200m	\$2m
\$200m - \$300m	\$3m
\$300m +	\$4m

At Corvus, our mission is to make the world a safer place by helping organizations mitigate or eliminate the impact of adverse events. We’re the leading provider of data-driven Smart Commercial Insurance® products, with offerings in cyber and technology E&O. Our nationally distributed team includes many of the most experienced Cyber Insurance underwriters.

**Contact your insurance broker for a quote today!**