RISK IN FOCUS

CYBER + CONSTRUCTION

Proactively Managing Cyber Risk and Insurance in the Construction Industry

Table of Contents

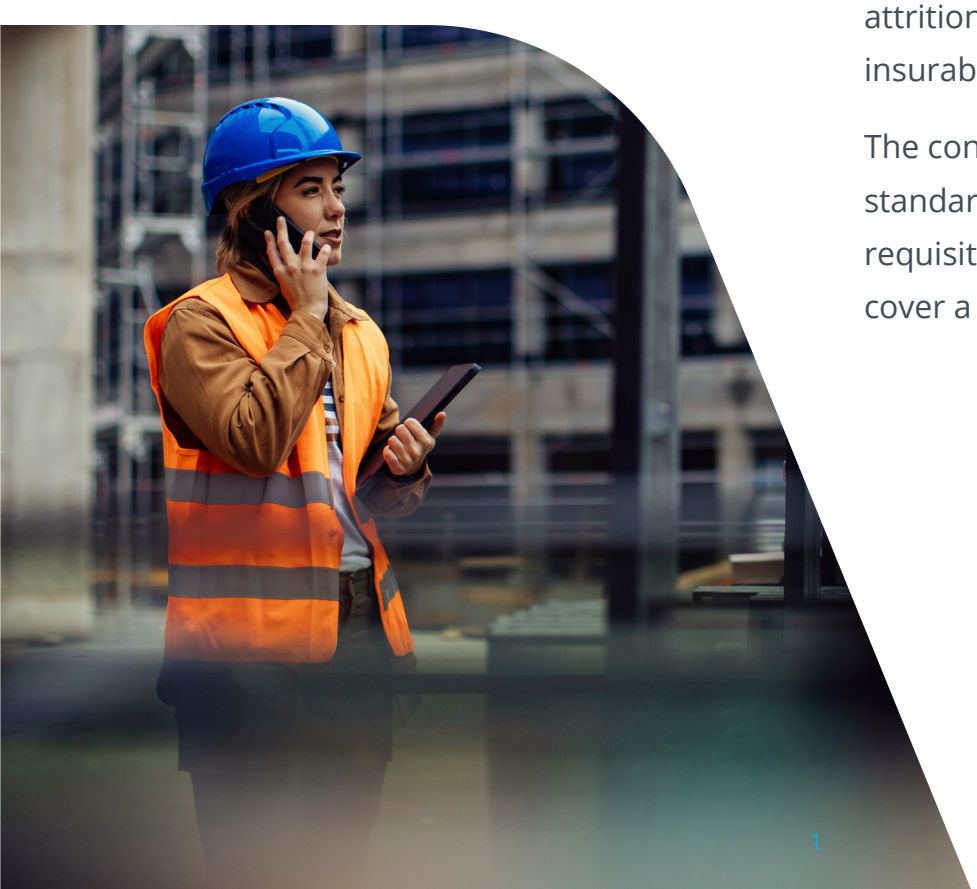
RISK IN FOCUS

Cyber Risk within the Construction Industry

Contractors and tradesmen have always been faced with managing a relatively high-hazard work environment. The adoption of mobile technology, construction software, robotics, and other operating technologies has forced contractors to respond to threats that have historically not been well-addressed in the construction industry. Examples include:

SOCIAL ENGINEERING AND INVOICE MANIPULATION

Business email compromise and subsequent manipulation of employees, clients, and/or vendors, through which the business voluntarily parts with funds.



RANSOMWARE ATTACKS

Threat actors that steal or encrypt personal data and demand a ransom for its release. This risk is more significant as companies become more reliant on technology to administer the business, or utilize operating technology to power equipment in the field.

REPUTATIONAL HARM

Organizations can suffer not only the immediate consequences of a cyber incident, but also the longer term of effects of the incident including customer attrition due to a loss of trust in the business stemming from the cyber incident. The immediate loss of income stemming from a cyber incident and subsequent loss of income due to customer attrition relative to the cyber-attack are both insurable on a cyber policy.

The construction industry is unique, and a standard cyber policy may not have all the requisite coverage features to adequately cover a claim.

Addressing Construction Industry Cyber Exposures

Coverage for unique situations includes:

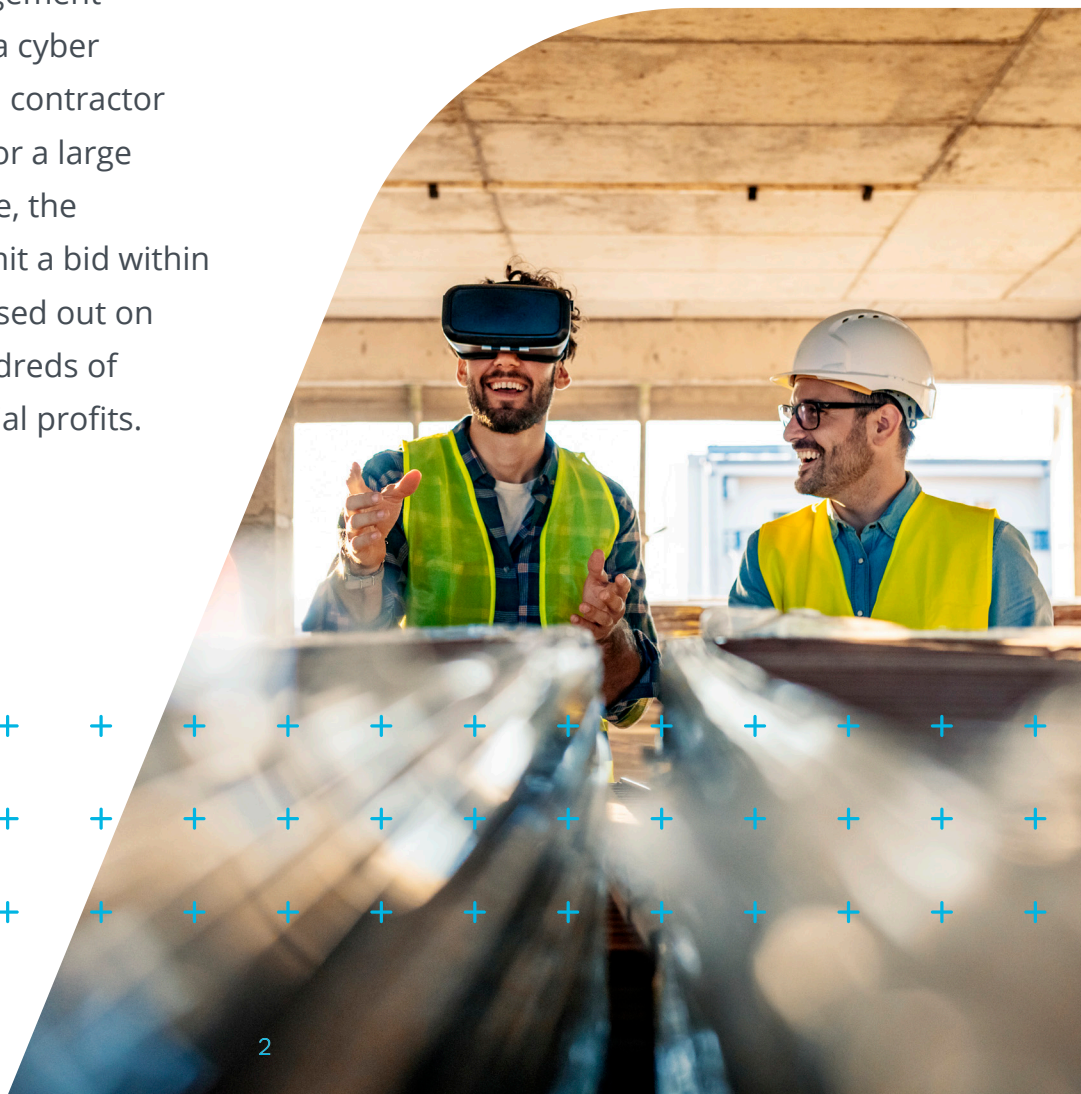
MISSED BID COVERAGE

A work stoppage stemming from a cyber incident is a significant risk. The risk of missing the opportunity to bid and win new business because of a cyber incident is also significant. The loss of speculative income, not having had the opportunity to bid for and win a contract can be as impactful on the bottom line as a work stoppage in some instances.

Contracts and proposal management systems that are impacted by a cyber incident can result in a general contractor being unable to submit a bid for a large multi-year project. For example, the contractor was unable to submit a bid within the required deadline and missed out on several years of work and hundreds of thousands of dollars in potential profits.

LIQUIDATED DAMAGES / DOWNSTREAM CONTRACTUAL PENALTIES COVERAGES

Owners and operators of construction companies may be subject to liquidated damages, assuming they fail to meet certain deadlines or performance standards stipulated in their contracts. Cyber policies can provide coverage for liquidated damages (i.e., downstream contractual penalties) stemming from a covered cyber incident.



PRIVACY LIABILITY STEMMING FROM DRONE OPERATIONS

Companies are frequently deploying new and innovative monitoring technology including drones to scope and manage projects in the field. However, using drones creates the opportunity for claims alleging violation of privacy stemming from their operations near private residences or other commercial establishments.

ADDITIONAL INSURED STATUS FOR OWNERS OF PROPERTY MANAGED BY THE INSURED

The owners of any property managed by the named insured can be named as an additional insured on the cyber policy automatically. Assuming the Contractor suffers a breach for which they and the owner of the property are named in a suit, the cyber policy would respond to cover both parties.

Market Expectations

Overall, the **market for cyber insurance remains stable** for those with current insurance programs, and for new entrants in the market with strong IT security controls. Underwriters have solidified their approach to underwriting and expectations from a technical security perspective have become more standardized from carrier to carrier.

Market data indicates that a new capacity for cyber insurance continues to come online, likewise Reuters reports that worldwide cyber insurance premiums are expected to continue to increase from $12B in 2022 to $50B in 2030. Year-over-year renewal rates have consistently decreased over the past 12 months considering these factors. Cyber insurance rates saw a drop of 10% in June 2023.[1]

Rates in the cyber insurance market may be 'bottoming out' as the volume of ransomware attacks has increased over the past quarter, which will impact carrier loss ratios over the next 12 months. Many in the industry theorize this is due to professional criminal organizations. Specifically, those in Ukraine and Eastern Europe coming back online after having been displaced by the War in Ukraine and deploying more resources to focus on disrupting war-related operations.

Cyber Risk Management and Insurance Market Guidance

PARTNER WITH INDUSTRY EXPERTS

IMA maintains a practice group 100% dedicated to cyber insurance and risk management. Our team is focused on assisting clients in coverage analysis, financial loss exposure benchmarking, contract language review, cyber threat analysis, and finally placing high-value cyber insurance programs.

REVIEW CYBER SECURITY PROTOCOLS WITH YOUR BROKER

To ensure you're able to procure the broadest insurance coverage for cyber risk available in the current marketplace.

CONTRACT REVIEW

Review critical IT providers in your business and ensure you have strong contractual risk transfer and indemnity provisions. IMA's contract review teams add value to our clients' overall risk management program by making sure the indemnity language is favorable.

LOSS CONTROL - LEVERAGE CARRIER RESOURCES

Many carriers offer free or cost-effective cyber security and risk management solutions that can help a client improve their security posture, or access to professionals that can advise on best practices.

MORE THAN JUST **INSURANCE**

Based in North America, IMA Financial Group, Inc. is an integrated financial services company focused on protecting the assets of its widely varied client base through insurance, risk management, employee benefits and wealth management solutions. As an employee-owned company, IMA's 2,000-plus associates are empowered to provide customized solutions for their clients' unique needs.

CONTACT THE **IMA TEAM**

For additional questions regarding this content or the resources that our carrier partners offer, please reach out to our Construction Practice Leader.

MICHAEL CAMPO
EVP, National Construction Practice Leader
303.615.7546
michael.campo@imacorp.com

JIM MILLAR
Construction and Cyber Practice Liaison
303.615.7711
jim.millar@imacorp.com

RISK IN **FOCUS** | **CONTRIBUTORS**

MICHAEL CAMPO, *National Construction Practice Leader*

JIM MILLAR, *Construction and Cyber Practice Liaison*

ANGELA THOMPSON, *Marketing Specialist*

SOURCES

[1] Reuters. (2023, July 5). Cyber insurance rates drop 10% in June, report says. Reuters. reuters.com/technology/cyber-insurance-rates-drop-10-june-report-2023-07-04/

[2] CyberMaxx. (2023). CyberMaxx Q2 Ransomware Research Report [Infographic]. CyberMaxx.com. https://www.cybermaxx.com/ransomware-research-report/thank-you-asset-download-ransomware-research-report-q2/?submissionGuid=4f85bc1e-5e19-45fa-85f5-29ae35451a12

NPN 1316541 | IMA, Inc dba IMA Insurance Services | California Lic #0H64724

IMACORP.COM/RIF