2022 CLM Construction Conference
September 21-23, 2022
San Diego, CA.

Evolving Cybersecurity Threats to the Construction Industry

I. Cybersecurity Threats Continue to Plague the Construction Industry.

The prevalence and severity of cybersecurity attacks continue to dramatically increase affecting industries across the country. The construction and engineering industry is particularly susceptible to attacks, especially due to heightened vulnerability of automated and control systems. The Colonial Pipeline attack and other ransomware attacks targeting critical infrastructure have prompted the U.S. Government to enact regulations requiring heightened cybersecurity protections and immediate reporting of cyber incidents. The panel will provide an overview of the latest cyber threats facing the industry and the evolving governmental, law enforcement and industry response, and will discuss best practices on how to ensure your cyber house is in order.

This significant increase in cyber-attacks presents a fact of life that can no longer be ignored by any industry. Recent FBI statistics reveal notable increases in cyber-attacks across all industries over the past two years, with some of the more dramatic events causing economic disaster. The cyber insurance market has evolved with the changing risk landscape and successfully helps businesses shift financial risk from company ledgers and public coffers to insurance reserves. Payouts of millions of dollars in ransomware payments have caused chaos in the cyber insurance marketplace as well as for construction companies dealing with this stealthy threat.

Ransomware demands are exhausting cyber policy limits faster than ever before, and the evolution of sophisticated spear fishing and fraudulent transfer schemes have forced cyber claims handlers and cyber insurance underwriters to stay one step ahead of the next threat. As a result, cyber insurance premiums have skyrocketed and shifts in coverages in claims handling strategies have reverberated through the global cyber insurance industry.

II. Scope of Cyber Coverage for Losses under Construction Industry Cyber Policies.

The earliest form of cyber insurance was focused on network security and virus-related claims. In 2003, California enacted the nation's first data breach statute which required notification of individuals affected by data breach events, and more states rapidly followed. Cyber insurance coverage evolved to cover first-party breach response expenses including IT forensics, legal response and credit monitoring and notification. Followed by the enactment of the HIPAA breach notification rule in 2009, first-party cyber

claims grew in response to the increasing regulatory pressure on industries to safeguard personal information.

Business interruption service is now recognized as vital part of any cyber insurance policy. Any company can be brought to its knees as the result of one employee's click of a mouse, from factories remaining idle to frozen computer systems preventing progress on a construction site, business losses can quickly morph into a monumental cost. The further interconnectedness of companies, including those using cloud services and data storage, have generated an increasing need for contingent business interruption coverage. Many companies rely on these third-party vendors, the breach of which can just as significantly affect a company's operations as if it were attacked directly, and coverage for these losses has grown in response.

Third-party cyber claims have existed since the inception of cyber insurance policies, but changes in statutes and evolving case law have created an environment ripe for data breach related claims. Third-party coverage protects companies from claims arising out of a data breach or similar cyber incident, including those brought by vendors, clients, customers, or regulatory and administrative bodies. Those claims have increased in prevalence, especially data breach class actions, and have dramatically affected the scope and breadth of coverage. From Illinois enactment of the Biometric Information Privacy Act in 2008, to California's Consumer Privacy Act of 2018 to the most recent Strengthening Cybersecurity Act of 2022 passed by the U.S. Congress this past March, the law is moving towards greater regulation of personal information and courts have given plaintiffs greater leeway in asserting third-party claims related to a data breach. This reality has produced greater demand for more expansive third-party cyber claim coverages, and the cyber insurance industry has responded accordingly.

While the take up rate for cyber insurance policies has been increasing, there is still a significant share of companies in the construction industry and beyond, which do not have cyber insurance policies and rely on non-cyber policies to try and cover losses of cyber incidents. The insurance industry has been moving to address this "silent cyber" threat, by specifically excluding cyber claims from non-cyber policies, and the uncertainty of these coverages and potential exposures has prompted the need for further change.

III. The Evaluation of Cybersecurity Claims Handling & Insurance Underwriting Guidelines for the Construction Industry.

The first construction cyber claims involved online security breaches and virus remediation, and claims handling procedures. In the current landscape, immediate triage is often required to properly deal with a security breach. Cyber insurance carriers have responded to the unpredictability of cyber-attacks by establishing 24/7 cyber breach hotlines and deploying breach response teams at a moment's notice. Such attacks can occur at all hours of the night, especially during holiday weekends, and require an immediate and comprehensive response from cyber insurance carriers including the deployment of legal counsel, forensics, and ransomware negotiators. Whether it is a ransomware attack with an impending deadline to respond, or a complete lock up of a construction company's systems, businesses are at the mercy of these criminals and look increasingly to the claims handling services provided by cyber insurance carriers.

The measurement of cyber risk to the construction industry continues to be a challenge for the cyber insurance industry given its evolving nature which renders historical cyber claim data nearly obsolete on an ongoing basis. Additionally, in comparison to other types of insurance, there is relatively limited cyber loss data to pull from as not all cyber incidents are publicly disclosed or reported. Furthermore, while there are some recognized information security standards, the lack of a universally accepted and implemented information security protocols across industries or jurisdictions makes assessing policyholder vulnerabilities rocky terrain for insurers.

With the increasing sophistication and frequency of ransomware and other cyber-attacks, claims handlers need to be possess the ability to quickly adjust and pivot. From immediate triage to protection of reputational harm and increased coordination with law enforcement, the protection of a company's cyber assets proves complicated. Couple that with the changing regulatory protections on the national, state, and local level and adjusters are faced with the daunting task of keeping up.

Construction industry professionals are confronting increased ransomware demands, heightened scrutiny from federal and state regulators, and spiking third-party claim exposure due to class actions and other litigation initiated by these cyber incidents. Courts across the country have trended towards allowing such claims. Data breach class actions and other data breach claims are growing across jurisdictions.

The increase in the volume and severity of ransomware claims have also required cyber insurance carriers to reevaluate underwriting standards which now nearly universally require increased security controls including multi-factor authentication and endpoint protection. Some cyber insurance policies are now bundled with software which continually monitors for vulnerabilities so they can be identified and remediated before the next attack occurs.

Cyber insurance policies have been adjusting to the rapidly changing cyber risk environment, though aggregation of such risk is unlike any other insurable risk out there. The attack vectors, scope, and manner of cyber-attacks constantly evolve and practically render risk modelling ineffective. However, advances in analytics and other technologies have helped cyber insurance companies attempt to stay ahead of the curve. The hardening of the cyber insurance market reflects the fact that cyber risk has generally been underpriced and under mitigated.

IV. Looking Ahead: The Future of Cyber Risks in the Construction Industry and the Cyber Insurance Market Response.

Comprehensive data privacy statutes, which typically establish requirements for the handling and processing of personal information, and provide for regulatory, and increasingly private, enforcement of data breaches, are trending as top priorities for legislative bodies across the country as well as around the world. These laws have resulted in more exposure to the construction industry from potential third-party cyber claims. As more states and municipalities are at various stages of enacting similar regulations; statutory allowance for private claims can easily result in overwhelming exposure to regulatory enforcement actions. Cyber claims teams will have to continually monitor legislative developments along with legal counsel to ensure the proper and appropriate handling of claims.

Cyber insurance policies are also taking a proactive approach to minimizing risk by offering pre-breach services such as regulatory compliance advice and training for construction executives and employees on cyber risks, as well as the development of incident response plans. Additionally, cybersecurity risk assessments as well as ongoing cyber risk monitoring through end point protection and other tools may be covered. The increase in these pre-breach services in the construction industry, especially better training for employees who inadvertently pose the greatest risk in a company's cybersecurity defense systems, can significantly reduce a company's cyber risk.

In a growing trend, many jurisdictions, governments, and insurance carriers are prohibiting the payment of ransoms. Should this trend continue, or be enacted on a more global scale such as through legislation through the U.S. Congress, no one can be sure how cyber criminals will adapt. Revenge attacks by hackers have been launched in the recent past against some insurance carriers after an announcement that it would no longer cover ransomware payments. These revenge attacks may become more commonplace if more carriers follow suit, or if regulations are passed prohibiting such payments. One thing is for certain, cyber risks in the construction industry will generate demand for cyber coverage for construction companies and their partners.