Construction Industry Cyber Risk Exposures and Risk Transfer Solutions

AON
Empower Results®

Technological advancements are changing the way that business is conducted in the construction industry. The use of hydraulic modeling software, the introduction of "wearable technology" into hardhats, safety vests and tools, and collaborative 3D design techniques are just a few examples of how technology is transforming the way that projects are completed. As companies use these technological advancements to enhance efficiency, facilitate communication, and decrease the time it takes to complete a project, the use of these tools is also changing organizations' risk profiles, adding new or increased cyber risk exposures

Cyber risk exposures in the construction industry

For many years construction companies have allocated significant resources to ensuring the physical safety of their projects, but the same attention and resources have not been devoted to information and electronic systems security. While many companies in the industry may not believe they have a real cyber risk exposure, the fact is that most possess confidential information that could make them an attractive target for hackers. In 2016, Construction Dive, a U.S. based news and analysis company, reported a 400% increase in ransomware attacks on the construction industry over the previous year. Relatedly, a recent U.S. survey by Forrester Research, Inc. revealed that more than 75% of respondents in the construction, engineering & infrastructure industries had experienced a cyber-incident within the last 12 months. While these statistics are U.S. focused, trends observed south of the border frequently serve as early predictors of Canadian experiences to follow.

Many construction companies store large amounts of employee payroll and health information, which some experts believe is more valuable to hackers than third-party payment-card data. In addition, information related to high-profile, large-scale projects might be targeted for politically motivated reasons or, in some cases, used to gain access to valuable corporate data that can be exploited to obtain a competitive advantage. Hackers may also seek to capitalize on vulnerabilities in shared procedural or structural models, design and construction software systems (such as BIM, Procor and Revit), Smart Building monitoring systems or other systems that have internet-connected capabilities or can be accessed remotely. If cyber criminals are able to obtain access to the data in these systems, they can create operational issues, alter or destroy data and possibly delay a project's completion.

Organizations that have a high degree of dependency on electronic processes or computer networks are also potentially vulnerable to cyber extortion attacks. Hackers seeking a ransom have used distributed denial of service (DDoS) attacks to swamp a system with traffic from botnets, preventing access to company servers, websites and client web portals until payment is received. Extortionists have also targeted employees, causing them to unknowingly download malware sent through a seemingly innocent email that encrypts files and demands a ransom in order to have them unlocked.

Real threats to construction organizations

All too often organizations take a back seat to addressing cyber risk, reasoning they will never be a target due to scale, geographic location or otherwise. However, today's reality is such that small and mi-sized businesses are actually more frequently targeted than large organizations, as criminals are preying on the unsuspecting, unprotected small business owner. Given the tangible financial, reputational and legal severity of cyber incidents, it is prudent for every construction firm to implement a cyber risk management program to mitigate the effects of cyber incidents such as these:

- A concrete contractor's CEO opened a phishing email that infiltrated the company's computer network, undetected by anti-virus software. The malicious code exposed names, addresses, social security numbers and healthcare records of 50 employees. The company was fined $218,797 by a regulatory investigation committee for "failure to protect personally identifiable information."
- Turner Construction was the victim of a spear phishing scam in 2016 when an employee sent tax information on current and former employees to a fraudulent email account. The information included full names, Social Security numbers, states of employment and residence as well as tax withholding data for 2015.
- In 2016, Whiting-Turner Contracting was notified by an outside vendor that prepared W-2 and 1095 tax forms for the company's employees about suspicious activity on that vendor's systems. Around the same time, employees of Whiting-Turner were reporting fraudulent tax filings being made in their names. In addition to employee information, it is also possible that personal information on children and beneficiaries of employees who received healthcare insurance coverage through Whiting-Turner was compromised.

Cyber liability insurance coverage

A cyber liability insurance solution can provide coverage for an insured's first and third-party costs that result from a cyber or privacy breach. A summary of the coverage provided by this insurance is below:

First-party coverage

- Privacy/cyber breach (actual or alleged) response costs, including:
  - Dedicated breach response team of experts, including legal counsel, providing 24/7 on-call support
  - Breach notification expenses, including the cost of hiring legal counsel and public relations consultants
  - Credit monitoring/protection costs
  - Notification and establishment of a call centre
  - IT forensic investigation costs
  - Identity theft resources
  - Proactive crisis management initiatives in the event of a suspected cyber breach
- Business interruption costs resulting from a network security failure (i.e. lost income, expenses to get system back up and running, etc.)
- Data restoration costs in the event of damage or alteration of intangible property (i.e. cost to restore/recreate data or software that is altered/destroyed by a network security failure)
- Cyber extortion costs (i.e. the amount of any ransom paid; cost to hire experts to assist in resolving the situation)
- Third-party coverage

Third-party coverage

- Defence costs, judgment and/or settlement amounts for actions seeking damages as a result of wrongful disclosure of personally identifiable information or confidential corporate information in the firm's care, custody or control via a computer network or off-line (e.g. via laptop, paper, records, disks)
- Defence costs, judgment and/or settlement amounts for actions seeking damages as a result of a failure of the insured's computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks
- Defence costs, judgment and/or settlement amounts for content liability perils such as actions alleging defamation and infringement of intellectual property rights arising out of website, marketing and advertising activities
- Defence costs for regulatory proceedings arising out of a security or privacy breach and coverage for administrative fines and penalties, where insurable

Aon's integrated approach

The cyber liability insurance market is one of the most specialized in the world of commercial liability. Appropriately incorporating this coverage into a comprehensive insurance program is a complex task that requires a sophisticated understanding of numerous policy forms.

As such, we recommend working with a broker that has extensive experience and a good understanding of the risk transfer solutions that are available. In addition to having a dedicated Construction Services Group, Aon is the only Canadian brokerage with an integrated national cyber and privacy practice composed of specialized brokers, account executives, lawyers and information technology professionals. Our brokers understand that few privacy and security risks are alike, and construction firms have unique needs depending on their size, location, use of technology, and the type of projects performed.

We take the time to consider the unique exposures of each construction company and work with our clients to customize a comprehensive and effective insurance program.

Contacts

Sean Hoare
Manager, Construction Services Group
+1.416.868.5593
sean.hoare@aon.ca

Katie Andruchow
Vice President and National Cyber and Privacy Broking Practice Leader
+1.416.868.5526
katie.andruchow@aon.ca

Jessica Foster J.D.
Legal Consultant
+1.416.868.5651
jessica.foster@aon.ca

About Aon in Canada

Aon Reed Stenhouse
For more than 150 years, in one form or another, Aon Reed Stenhouse has been a major force in the Canadian insurance industry.

Aon Reed Stenhouse is Canada's leading insurance brokerage and risk management services firm. We serve an extensive client base, handling more than $2 billion in annual premiums on behalf of our clients.

- Insurance brokerage
- Risk management
- Employee health and benefits

Our 1,600 professionals serve clients from 23 offices located across Canada. We provide our clients with a wide range of innovative solutions. Each day, Aon professionals work to deliver the best solutions to our clients.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Empower Results®