Construction Industry Cyber Exposures

How technology advancements are evolving risk

Technological advancements are changing the way that business is conducted in the construction industry. The use of Smart Grid technology, the introduction of "wearable technology" into hardhats, safety vests and tools, and collaborative 3D building information modelling are just a few examples of how technology is transforming the way that projects are completed. However, 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 a new or increased cyber and technology risk exposure.

As a result, we have seen increased government regulation around cybersecurity compliance in many industries and more frequent use of contractual protections with respect to cyber risk exposures, including contractual requirements for the purchase of cyber and technology insurance products being imposed on contractors and other service providers. In addition, many companies in the construction industry are taking proactive steps to explore the available options for mitigating and transferring cyber and technology risk through insurance.

Cyber and technology risk exposures for 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 actually do possess confidential information that could make them an attractive target for hackers. A lot of construction companies store large amounts of employee payroll and health information, which some experts believe is actually 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 used to obtain a competitive advantage.

Hackers may also seek to exploit 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 they are able to get access to the data being used 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 potentially vulnerable to another disruptive tactic used by hackers: 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 they are paid. They 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.

Standard insurance policies are not enough

Even though some insurance policies may offer limited coverage for cyber and technology risk exposures, most have not been drafted with the intention of providing coverage for the types of losses that might arise from a cyber attack or privacy breach:

- General liability: covers bodily injury and property damage, not economic loss and may contain exclusions for data and privacy breaches
- Errors and omissions: covers economic damages resulting from a failure of defined services only (not broad enough to pick up additional technology services rendered), and may contain exclusions for data and privacy breaches. Absence of insuring agreements to respond to first party crisis management costs during a cyber breach.
- Property insurance: covers tangible property, which data is not. Loss must be caused by a physical peril while perils to data are viruses and hackers.
- Crime: covers employees and generally only money, securities and tangible property. No coverage for third party property such as customer/client data.
- In addition, there may be situations where standard insurance policies are not sufficient for contractual reasons:
  - A construction company retained by a third party may be contractually required in some cases to purchase cyber and/or technology errors and omissions insurance.
  - Insurance may be needed to adequately address its cyber exposure when a third party storing its electronic data refuses to retain the liability for a cyber breach with respect to that data.

Cyber liability and technology errors and omissions insurance coverage

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

Third party coverage

- Defence costs, judgment and/or settlement amounts for actions seeking damages as a result of wrongful disclosure of personally identifiable information, protected health information or confidential corporate information in the client'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, whether or not these threats occur in the context of the insured's provision of professional services
- Defence costs, judgment and/or settlement amounts for actions alleging an error, omission or negligence in performing data analytics or in the provision of technology products or services
- 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

First party coverage

Network business interruption costs due to a network security failure, including lost income and extra expenses to get the system back up and running

- Costs related to damage or alteration of intangible property, including the cost to restore or recreate data or software that is altered or destroyed because of a network security failure
- Cyber breach response costs, including:
  - Breach notification expenses, including the cost of hiring legal counsel and public relations consultants
  - Credit monitoring/protection
  - Notification and establishment of a call centre
  - IT forensic costs
  - Identity theft resources
- Costs to deal with cyber extortion including the amount of any ransom paid and the cost to hire experts to help resolve the extortion situation

Effectively transferring cyber and technology risks

The insurance marketplace in the cyber realm is rapidly evolving and many insurers are now providing an insured with access to data breach coaches, loss control resources, dedicated claims resources, and pre-approved panels of breach response vendors and service providers, when they purchase cyber insurance. However, the quality of the insurance products in the cyber liability realm varies greatly, so it is important to work with an insurance broker that is familiar with the nuances of this coverage and the additional breach resources that insurance carriers can offer.