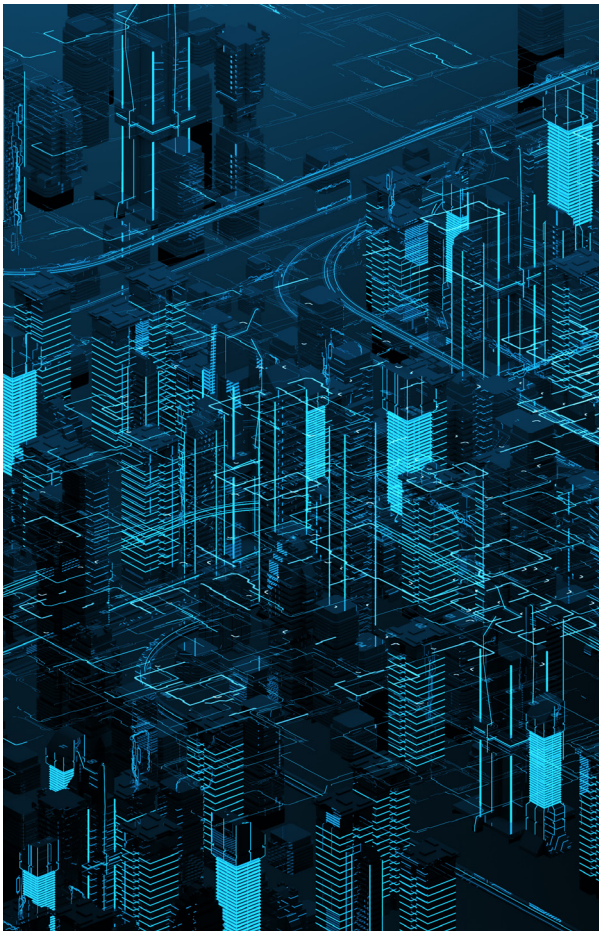
MARSH

INSIGHTS | OCTOBER 2018

Why Cyber Should be Higher on Contractors' Risk Agendas

Rarely does a week go by without a cyber incident making headlines. According to the World Economic Forum's *2018 Global Risks Report*, cyber and data privacy and security threats are the leading risks facing companies operating in North America. The simple truth is that cyber risk is industry agnostic and any business that relies on technology can suffer a loss.

Yet many construction risk professionals do not view cyber risk as a priority for their organizations, leaving them vulnerable to costly cyber-attacks or technology disruptions that can devastate their bottom lines. However, contractors can take action to reduce their risk through a combination of robust internal practices and the purchase of insurance coverage.



Greater Efficiency, Greater Risk

Contractors are different than many other businesses in that they collaborate in a digital environment with many project stakeholders to bid on and perform work. Through design-build and other alternative contract delivery methods, contractors — rather than professional service firms — hold ultimate responsibility for the source of systems and software that is incorporated into a building or other form of infrastructure.

More broadly, the construction industry is embarking on a period of rapid digitization, with technology increasingly being embraced both for project modeling and day-to-day operations. A 2016 survey by PwC found that construction companies planned to invest 5% of their annual revenue into digital operations solutions in the coming years. Three specific technologies — building information modeling, geographic information systems, and integrated project delivery — are quickly becoming cornerstones of the industry. And construction equipment and control systems are expected to become increasingly automated in the years ahead.

These and other technological advancements will help the industry become increasingly efficient, but can also make construction companies more attractive targets for cyber criminals looking to steal data, ransom systems, or otherwise disrupt companies' operations. Virtually all companies in the construction industry rely on IT networks, software applications, and data to maintain general business activities, from payroll and order processing to marketing and communications.

Other industry characteristics can present risks as well. For example, the construction industry's workforce is fluid; many construction industry employees work in the field — using laptops, smartphones, and tablets — rather than traditional office environments. The reliance on subcontractors can also present unique challenges, including training. Moreover, the completion of any project typically involves dozens of companies and their employees and the sharing of vast quantities of confidential data, including bids, blueprints, employee records, and financial information.

These and other factors translate to several potential cyber risks for contractors, including:

- Business interruption stemming from technology disruptions, via ransomware and other forms of malware. Such attacks, as seen in the WannaCry and NotPetya attacks of 2017, can have devastating effects and typically do not spare companies in any industry. A multinational manufacturer of construction materials, for example, lost approximately €250 million in sales and €80 million in operating income as a result of nearly one month of downtime following the NotPetya attack.
- Theft, loss, or unauthorized disclosure of corporate personal information. While they are not likely to collect and hold as much data as retailers or other businesses, construction companies have been targeted for their financial assets and the information they retain about employees. In 2014, for example, a multinational engineering company suffered a breach of approximately 52,000 employees' names, addresses, social security numbers, and personal bank account information. The costs stemming from such data breaches are often high, and can be complicated by rigorous data privacy laws that exist in many jurisdictions.
- Theft of proprietary corporate assets. This could include privileged contracts, confidential project/bid data, architectural designs (including security designs), and intellectual property. In 2013, a prime contractor's computers were breached by hackers tied back to a foreign government; floor plans, communication-cable layouts, server locations, and security system designs for a government building project were stolen.
- Theft of customer information.
- Access to personal information on other organizations' servers. A 2014 data breach of a retailer's systems, for example, was traced back to credentials stolen from an HVAC contractor via a phishing scam perpetrated against an employee of the contractor.
- Theft or other damage by disgruntled employees, subcontractors, vendors, or competitors.

Health care organizations, financial institutions, retailers, and public entities have long considered cyber risk among their most critical exposures, but the same is not true of the construction industry. Relatively few contractors have thoroughly identified and quantified their cyber exposures or developed plans to mitigate and/or transfer that particular risk.

Risk Assessment and Prevention

The first step in managing cyber risk is to identify sources of potential risk. Contractors should conduct audits that gauge employee access to and use of critical and sensitive data, including personally identifiable information and proprietary corporate assets. This audit should determine who has access to such information and critical systems and take stock of existing capabilities for monitoring inappropriate system access and potential security events.

Once complete, businesses should develop formal, written policies regarding the use of corporate networks, and ensure that access to sensitive data is restricted only to parties that require it. Organizations should also:

- **Encrypt or otherwise secure critical technologies.** Laptops, smartphones, tablets, and portable media devices — along with emerging technologies that are often present on construction sites, such as wearable devices — can present significant data security threats if lost, stolen, or hacked.
- **Train employees and others on how to identify, avoid, and report potentially malicious activity on corporate networks.** The construction industry is heavily decentralized and involves a number of stakeholders. Without thorough and regular training and buy-in from all personnel, even the most robust cyber risk management plans can be rendered ineffective. Businesses should also implement strong internal controls, including resetting of passwords every 90 days.
- **Regularly review and update firewalls and security patches.** Despite the added expense, investing in a robust set of firewalls that require user authentication can be beneficial. Businesses should also institute secure file sharing, advanced email and web filtering, and separate WiFi networks for subcontractors, architects, and engineers.

- **Closely monitor third-party risk.** Assess the cybersecurity processes of any third parties that access or retain critical data. And seek to build favorable hold harmless agreements into contracts with third-party vendors. Also establish procedures to evaluate any third-party service providers (if applicable) and, as discussed, review their agreements, limiting as much liability to your company as possible, and assess their cybersecurity processes.
- **Develop detailed data breach response plans.** Advance planning can enable an organization to act swiftly, decisively, and effectively to minimize damage from a breach and any resulting claims or regulatory actions.

Insurance Considerations

Although all businesses should plan for and take steps to prevent potential cyber-attacks and technology disruptions, the reality for many businesses is that it's not a question of "if" a cyber-loss will occur but rather "when" one will. To prepare for that eventuality, insurance should be a part of any construction company's risk management program.

The continual evolution of privacy and computer security risks has left traditional forms of insurance largely unable to adequately cover cyber exposures. For example:

- General liability (GL) policies typically require bodily injury and/or physical damage to property to trigger coverage. Insurers have frequently argued that GL policies do not provide coverage for electronic data loss because data does not constitute tangible property.
- Property policies typically limit coverage to tangible property as a result of a covered physical peril, and several insurers have specifically excluded damage or theft of data. Business interruption coverage also does not usually include losses stemming from the unavailability of critical applications, data, and networks, unless the root cause is a physical damage event.
- Commercial crime policies often limit coverage to theft of assets, fraudulent electronic fund transfers, and the cost of recollecting, replicating, or restoring lost or corrupted data
- Similarly, professional liability policies often limit coverage to liability arising from an act, error, or omission in the course of an insured's professional duties and are principally designed to provide coverage for third-party claims; a contractor's own first-party cyber exposures would not be adequately addressed under such policies. Some architects and engineers (A&E) policies expand the scope of coverage for professional services to include any activities that involve the use of technology. This typically provides coverage for third-party claims, but most cyber risks — including first-party claims — are not included.

Given the limitations of these and other forms of coverage, contractors should consider purchasing standalone cyber insurance coverage. While cyber insurance policies have historically been most often associated with data and privacy breaches, today's cyber policies cover the failure of technology and the resulting interruption or loss of revenue. Cyber policies can also be designed to cover:

- Damage to computers or servers caused by malware rather than a physical event.
- Forensic investigations into the nature and cause of a data breach.
- Legal expenses associated with the release of confidential information and intellectual property, legal settlements, and regulatory fines.

In addition to coverage for these specific risks, many cyber insurers offer additional services to help manage the effects of a cyber loss and prevent future losses. For example, many insurers can provide data breach "coaches" to help insured businesses better manage their risk. Such coaches are often attorneys who specialize in the unique legal and regulatory issues surrounding breaches, and can help insured businesses navigate the response process and better ensure compliance with state and federal privacy laws. Most insurers also have pre-negotiated rates with IT forensics specialists, who can spearhead investigations into what has occurred, what data has been compromised, and how to fix any identified vulnerabilities.

As they attempt to address a range of potential cyber risks, especially the growing threat of ransomware, organizations should seek to optimize their cyber insurance programs, coordinating and aligning cyber, property, and casualty insurance coverages. Working with their insurance advisors, risk professionals should review these policies to determine current levels and areas of coverage, identify any gaps or exclusions — with close attention to potential implications of "other insurance" clauses — and tailor insurance solutions to their organizations' cyber risk profiles. Organizations should also update policies as needed to provide coverage for new types of risks, including business interruption and cyber extortion, and reevaluate program limits in the face of catastrophic scenarios.

Contractors, like most all other organizations, rely on technology to do business. That can be a source of strength, but any breach or technology interruption that disrupts critical workflows and operations can lead to substantial losses for contractors and other project stakeholders. Although it's difficult to remove that risk, contractors can create effective cyber risk management programs to reduce it and secure robust cyber insurance coverage to protect against potential losses.

This briefing was prepared by Marsh with support from Thomas Tripodianos, a partner at Welby, Brady & Greenblatt, LLP.

For more information, visit marsh.com, contact your Marsh representative, or contact:

NICK MONTERA
Vice President, Construction Practice
Marsh
+1 212 345 4044
nick.montera@marsh.com

MATT MCCABE
Senior Vice President and Cyber Risk Adviser, FINPRO
Marsh
+1 212 345 9642
matthew.p.mccabe@marsh.com