NEWMEYER & DILLION LLP

Be Proactive Now: Commercial Construction Quickly Joining List of Industries Vulnerable to Cyber Attacks

By: Jeffrey M. Dennis & J. Nathan Owens

Jeffrey M. Dennis

Contact

949.271.7316
jeff.dennis@ndlf.com

Practice Areas

Business Litigation
Construction Litigation
Cybersecurity
Insurance Law
Real Estate Litigation

Nathan Owens

Contact

702.777.7505
nathan.owens@ndlf.com

Practice Areas

Business Litigation
Business Transactions
Construction Litigation
Cybersecurity
Eminent Domain & Real Estate Valuation
Insurance Law
Real Estate Litigation

Commercial contractors have long faced their own unique business risks - labor and material shortages, delay claims, bonding issues, and defects in workmanship. But, in today's ever-evolving cyber world, it is imperative that contractors understand they are vulnerable to risks beyond finishing a project on time and on budget. As we are seeing more and more each day, cyber threats impact all businesses, including the construction industry, and the failure to protect against these threats will cost your company millions in damages and reputational harm.

UNDERSTANDING CYBER THREATS

Traditionally, cyber threats are thought of as the theft of employee and customer information over the internet. Given the construction industry is the largest employer in the world, the need to protect this information is obvious. The release or loss of personnel or consumer data could lead to extensive liability under a variety of potential claims, including statutory fines. In addition to securing confidential information, companies have to protect against outside agents accessing control of a company's security protocols, equipment or encrypting files using malicious software. The recent "WannaCry" attack demonstrates that no business is immune from cyber attacks.

EXAMPLES OF RELATED BREACHES

For those that think these scenarios do not happen, here are two examples of these types of breaches:

- In May 2013, Chinese hackers stole floor plans, server information, and security system designs from an Australian prime contractor. Fearing the risks of compromised physical and network security, the contractor incurred additional costs of $132.6 million in project delays and costs to rework the various components that had been stolen.

- Then, in December 2014, a German governmental office reported that a steel mill suffered massive damage when malware prevented a blast furnace from being properly shut down. Hackers gained access to key technology within the company, which eventually allowed them to control the production line.

THE NEW WORLD OF THE IoT

In addition to these types of "traditional" hacking threats, cybersecurity risks continue to evolve and become more complicated every day. Some of these new threats are driven by the development of a phenomenon known as the Internet of things, or IoT. The IoT is most basically defined as the interconnection of devices with on / off

switches to the Internet and each other. Since the IoT is estimated to be 20 billion or more devices within 3 years, and can be combined with malicious software, IoT poses one of the most challenging risks for contractors to protect against.

The technology included in today's commercial buildings clearly opens this avenue of risk. A centralized computer control center, typically employed in new buildings, controls and maintains the systems that are vital to the operation of the building, e.g., power, elevators, HVAC, lighting, and security. What happens if a hacker gains control to one of these systems, let alone all of them? What if a hacker simply utilizes an IoT attack to overwhelm a building's computer systems? In either scenario, at a minimum, significant disruption would occur. Worse, the health and safety of those within the building could be jeopardized. A hacker may utilize ransomware in combination with an IoT attack to take over control of the building and hold it and possibly the occupants "hostage" until a ransom is paid.

The first significant IoT attack happened in October 2016 when a major web hosting company was attacked through the IoT, causing the host site to crash. The attack did not steal information, it simply caused the site to crash. But, that crash caused world-wide disruption across the Internet. Hackers used malicious software to access a hundred thousand common household devices — web cameras, fitness trackers, DVR's, smart TVs and even baby monitors — to flood the hosting company's servers with incredibly high internet traffic. This attack showed that everyday items can be hacked and controlled by cyber criminals and then used against anyone else.

As we have all seen in recent news, the WannaCry cyber attack impacted businesses across the globe. Days after the attacks, hospitals were still left feeling its impact with continued appointment and planned operation cancellations, and delays in service. We should expect to see these types of attacks increasing in frequency.

PAY ATTENTION OR FACE THE CONSEQUENCES

Make no mistake about it, the stakes are incredibly high in the realm of cyber security protection. By 2021, the annual worldwide cost attributable to cyber attacks is estimated to reach the trillions of dollars. If any of these potential attacks occur, a contractor faces significant exposure, in many forms, including:

- **Monetary.** Cybersecurity events result in direct monetary losses in the form of notification costs, data recovery costs, and, of course, legal and public relations fees. States are also starting to impose strict standards on companies which will result in significant regulatory punishment in the cases of cyber breaches, including the added costs associated with agency investigations, regulatory fines and consumer redress funds.

- **Reputation.** Perhaps more important than the monetary risk, a contractor may incur substantial reputational harm if such a breach or attack is successful. Recent data has shown that small to medium-sized companies that experience a significant cybersecurity breach go out of business within six months of the breach – due to not only high monetary costs, but severe reputational damage.

- **Criminal.** The recently passed New York cybersecurity regulations place potential criminal penalties on compliance personnel. Other states are likely to follow New York.

As a business leader and commercial builder, the time to act is now. While the purchase of specific cyber insurance is an important part of protecting against the risks of a cyber attack, many cyber policies contain exclusionary language embedded in the policy making coverage potentially illusory. Additional steps can and need to be taken immediately, including an honest discussion of internal cybersecurity protections, examination of risk management strategy, and the training of employees. Failure to take these important steps could result in a disastrous cybersecurity breach and the loss of millions of dollars.

Jeffrey M. Dennis currently serves as Newmeyer and Dillion's Managing Partner and, as a business leader, advises his clients on cybersecurity related issues, introducing contractual and insurance opportunities to lessen their risk. You can reach Jeff at jeff.dennis@ndlf.com.

J. Nathan Owens is the Managing Partner for Newmeyer & Dillion's Las Vegas office. With more than 10 years in the construction industry as a former contractor himself, Nathan understands the complex issues builders and developers face in all aspects of development and construction. You can reach Nathan at nathan.owens@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.