



No Industry is Safe from the Threat of CYBER FRAUD

No Industry Is Safe From the Threat of Cyber Fraud

by David R Leng, CPCU, CIC, CBWA, CWCA, CRM

The internet is an informational super-highway, tethered to how business is conducted. But like any heavily-traveled road, it can also be a place fraught with danger. Just when companies think all is well and are cruising along without a worry, with anti-virus seatbelts securely fastened, they suddenly get slammed by a big rig with the words “cyber fraud” on the side.

Some companies survive the wreck, while others aren’t so lucky, but the ensuing damage is devastating.

According to an article in *Forbes*, cyber crime costs are projected to top \$2 trillion by 2019. IBM Corp.’s Chairman, CEO and President, Ginni Rometty, recently stated that cyber crime is the “greatest threat to every profession, every industry, every company in the world.”

Every industry that relies on the Internet to conduct business is at risk, and the construction industry is one of those industries with a large bulls-eye on its back. In a recent article, the *Miami Herald* pointed out that “given the increasing popularity of practices such as Building Information Modeling (BIM), Integrated Project Delivery and file sharing between participants in a construction project, contractors may be at increased risk of

liability in the event of a data breach. A hacker may be able to access architectural designs, including the designs of security systems and features, financial information, confidential project-specific information and personal information of employees.”

Case in point, in November 2013, hackers gained access to credit and debit card information for tens of millions of Target customers in the U.S. The source of the data breach was a small HVAC contractor that provided services to Target. The HVAC contractor had suffered a data breach from which the hackers were able to obtain the network credentials that the contractor used to remotely access Target’s network.

It’s likely that the breach was initiated by a process called “spear phishing,” where an employee gets an email he believes is from a legitimate source. But once the email is opened, it unleashes a Pandora’s Box that allows the hacker access to valuable information. For example, it was reported that 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."

According to an article in *Forbes*, cyber crime costs are projected to top \$2 trillion by 2019. IBM Corp.'s Chairman, CEO and President, Ginni Rometty, recently stated that cyber crime is the "greatest threat to every profession, every industry, every company in the world."

Every industry that relies on the Internet to conduct business is at risk, and the construction industry is one of those industries with a large bulls-eye on its back. In a recent article, the *Miami Herald* pointed out that "given the increasing popularity of practices such as Building Information Modeling (BIM), Integrated Project Delivery and file sharing between participants in a construction project, contractors may be at increased risk of liability in the event of a data breach. A hacker may be able to access architectural designs, including the designs of security systems and features, financial information, confidential project-specific information and personal information of employees."

Case in point, in November 2013, hackers gained access to credit and debit card information for tens of millions of Target customers in the U.S. The source of the data breach was a small HVAC contractor that provided services to Target. The HVAC contractor had suffered a data breach from which the hackers were able to obtain the network credentials that the contractor used to remotely access Target's network.

It's likely that the breach was initiated by a process called "spear phishing," where an employee gets an email he believes is from a legitimate source. But once the email is opened, it unleashes a Pandora's Box that allows the hacker access to valuable information. For example, it was reported that 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."

The level of cyber crime has morphed to the point that hackers can steal information simply by walking by a mobile phone, which is as prevalent on a construction job site as a hammer or a nail.

According to information from Travelers Insurance, here are six trending cyber threats to be aware of:

1. **Ransomware** - maliciously installed malware where the hacker holds company data hostage until a ransom is paid;
2. **Vendors** - vendors and business partners are additional risks to a company's data security;
3. **Negligent Employees** - workers create breaches by mistakenly sending emails containing confidential information;

4. **Hackers** - cyber criminals attack computers to obtain data;
5. **Hacktivists** - hackers attack a company's website to promote a social or political cause; and
6. **Social Engineering** - employees get tricked into providing financial information.

As long as the construction industry has access to floor plans and other valuable information, it will always be susceptible to cyber fraud. It could be a bank, a government office, a hospital or any type of structure where valuable information is stored. So the important question is how to protect the company and its clients? According to the construction website *iSqFt*, here are some ways to head off a cyber attack:

- install security software on company servers and computers that can provide real-time protection and automatically receive the most up-to-date malware definitions;
- make sure firewalls are enabled and updated regularly with security patches;
- train employees on security policies and practices. Employees should be required to change their passwords every three months. It is estimated that 70 percent or more of cyber fraud could be prevented through better education of the technology user;
- if employees are using mobile devices to access the company's network, they should be equipped with hardware and software data encryption and passwords or PIN locks should be used;
- secure the Wi-Fi network, both at the office and at the jobsite, by encrypting the wireless signal, securing the router with a password and filtering MAC addresses of devices so only employees and authorized personnel can access the network; and
- regularly backup data offsite or with a trusted cloud storage provider.

Unfortunately, when it comes to devising technology to battle cyber fraud, it's a constant struggle to come up with new anti-virus software that's one step ahead of the bad guys trying to sneak in the back door. This only makes preventing cyber fraud through better education even more important.

There is never a 100 percent certainty that a company won't be hacked, no matter what defenses are implemented. But at the very least, through consistent training of employees and vendors on how to stay password protected and be leery of any email, even if it looks friendly, enjoy the satisfaction of knowing that it won't be easy for the hackers to break through the company system.



This article by David Leng appeared with various industry alterations in *Construction Executive*, *Commercial Construction & Renovation*, *EHS Today*, and the *Working Parts*, among others.

*David R. Leng, CPCU, CIC, CBWA, CRM, CWCA, is a best-selling author of **The 10 Laws of Insurance Attraction**, and **Turning Premiums Into Profits**, as well as **Stop Being Frustrated & Overcharged**. David is Executive Vice President & Executive Partner of the Duncan Financial Group in Irwin, PA. He is a 30+-year veteran of the Risk Management and Insurance industry and is regarded as one of the brightest minds in the industry. Since 2004, David has saved his clients well over \$50,000,000 in premiums and overcharges, and was named Advisor of the Year for 2008 by the Institute of WorkComp Professionals.*