Real risks!

Bill Smith reports that construction companies are often targets for cyber criminals.

I think it's fair to say that 15 years ago business owners had a relatively good idea of what risks they faced on a daily basis. They knew – to a reasonable degree, at least – where they were vulnerable. Safety measures and programs could be enhanced to limit injuries and incidents, and new processes and procedures could limit the negative effects of the evolving trends in human behavior. But now that technology has permanently rooted itself in our lives and businesses, the areas in which we're vulnerable can sometimes be a little harder to distinguish.

In early January, during the Insurance and Risk Management Committee Meeting held at the Specialized Carriers and Rigging Association's (SC&RA) Board and Committee Meetings, the conversation turned to a hot-button issue that's becoming increasingly more important: cyber security. Two crane and rigging/specialized transportation business owners shared horror stories about their internal computer networks being taken hostage by ransomware – malicious software designed to prohibit access to digital files until a sum of money, usually substantial, is paid to the hacker. In each of their cases, these SC&RA business owners were forced to pay a ransom to recover their networks, and the amounts paid were – take a deep breath here – in the $50,000 range. To say they were frustrated is putting it mildly.

You are a target

As members of a specialized segment of the construction industry, it's easy to think of cyber security as something that should only apply to banks and large retail stores, but as we're starting to see more and more in the insurance industry, that's simply not the case. Construction companies of all sizes are now often targets for cyber criminals who understand that every company, regardless of what industry it operates within, has something of value worth taking.

Last year, the Miami Herald reported that, "Given the increasing popularity of practices such as Building Information Modeling, 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."

Add to that Kim Slowey's article, which was published last year on ConstructionDive.com, where she quoted Jonathan Gossels, president and CEO of security consulting firm SystemExperts: "Construction companies aren't typically focused on cyber security. They tend to be more focused on the task at hand, which is completing their construction projects within budget and on schedule."

Vulnerable industry

That leaves the construction industry vulnerable.

Luca Berni, a cyber security expert and frequent contributor to Forbes.com, who wrote an article appearing on the website January 30, 2017, believes that "2017 will be a year when geopolitical shifts and technological advances by nation-state and criminal actors will combine to create an unprecedentedly complex cyber threat landscape."

Let that phrase sink in for a minute: unprecedentedly complex cyber threat landscape. Sounds ominous, right? Well, it is. In fact, a January 6, 2017 article in ComputerWeekly.com takes a similar position: "…in 2017, experts predict an increase in professional, advanced attacks – including attacks on cloud infrastructure – and the rise of data manipulation attacks, further underlining the need for a fresh approach to data security."

So what does this all mean? Simply put: it means that you need to be ready in case you're attacked, and you need to take steps to protect your business.

Protect, protect, protect

The good news – and there is good news, despite the grave outlook – is that cyber security is nothing new, and one estimate puts the cyber security market at $170 billion by 2020. That means there are a lot of folks investing a lot of money in protecting the digital things we hold dear. But there are certainly a few things you should know, and, according to the cyber experts over at Strongarm, four best practices to protect your system from ransomware:

1 EMAIL SAFETY TRAINING

Email is one of the most notorious ways ransomware gets in, so it's a good idea to educate your company about the basics of email safety. Explain not only the basics like using complex passwords, changing them regularly, having a password management tool and enabling two-factor authentication, but also show your employees what ransomware emails look like and what to do when one comes in.

2 BACKUP YOUR DATA AND REGULARLY TEST THE RESTORE PROCESS

You need to be able to ensure that if an attacker does try to hold your data ransom, you can continue business as usual with a redundant copy. To do this,

>100

THE AUTHOR

Bill Smith is executive vice president of claims and risk management for NBIS.

> “Cyber criminals understand that every company, regardless of what industry it operates within, has something of value worth taking.”

back up both your local data and anything stored in the cloud – everything from customer data to payment details, and financials to other personally identifiable information (PII).

3 STOP RANSOMWARE COMMUNICATION TO KNOWN BAD PLACES

There are databases that keep track of where criminals set up their malware infrastructure. These databases include IP addresses, domains, and other sources that have sent malware in the past.

Using a DNS black hole that leverages these databases can help you to block the known malware strains and prevent them from doing damage to your systems. This can help you automatically stay on top of and protected from the latest malware threats.

4 LOCATE AND REMOVE INFECTIONS QUICKLY

Most security defenses today focus on keeping threats out altogether (which isn't realistic) or just getting rid of them (which isn't enough). The reality is that ransomware will get in at some point. Once it does, you need to know how exactly it got in and who its victims are. Otherwise, even after you remove it, how can you be certain it's gone and won't do further damage? Not to mention you won't be prepared to protect against similar attacks in the future.

I think the reality of cyber-attacks is that we ultimately need to handle them in the same way we handle all the other risks in our industry: through mitigation and risk management techniques. In the same way we continually train our employees to be safer on the jobsite, we should also be continually training our employees to operate more safely when they're connected to the internet. And, perhaps most importantly, you should be absolutely certain you're backing up your information as often as you can by following the "Rule of Three:"

1 Have three copies of all-important data
2 Keep copies in two formats (for example, local hard drive, and Dropbox)
3 Store at least one copy offsite (yes, in the cloud counts)

At NBIS, we take a risk management approach to finding insurance solutions for our clients and we're constantly reviewing the industry for new threats. It's important to understand that the landscape of cyber risk is evolving rapidly for everyone, even and for your insurance provider. So make sure the insurance partner you choose is ready to serve your business in the ways that are right for you. Contact NBIS today to learn more, 877-860-7677 or visit us online www.NBIS.com. ■