Under Attack

HACKERS FIND CONSTRUCTION DATA ATTRACTIVE TARGET

There is an old adage concerning timely action about the uselessness of locking the stable after the horse is gone. It is, unfortunately, the story of many construction companies confronting the issue of cybersecurity. They never considered themselves a target until it was too late.

Many are surprised by how fast the future has arrived, but it is here now. From payroll and tool-tracking to 3D building models and as-built laser scans, a construction company's network is the conduit for increasing portions of its activities and is hosting an increasing number of outsiders and their devices. That is an attractive target for thieves, especially since the number of vulnerabilities in the network is growing. If the 'stable' in the old adage is your computer network with 250 doors instead of one and strangers going in and out, locking it up is not a simple task. To avoid becoming a victim, cybersecurity must be considered a top issue.

THE THREATS

A construction company's computer network is unlike the networks of many other types of businesses. It's not located in a single building, but often physically dispersed over a number of locations, including jobsite trailers. There are many mobile devices on the network. There are many devices from outside the company coming and going on the network, and bringing with them data in a broad variety of formats. It handles business information, financial information, communications, construction documents, the cameras monitoring the jobsite and laser scanners checking floor flatness. The company's day-to-day operations are deeply dependent on the network and the data to which it gives access.

According to James McGibney, senior director of cyber security and compliance for Bay Area electrical giant Rosendin Electric, a member of multiple AGC chapters, construction data can be an especially attractive target for hackers. "We deal with a lot of hacking attempts that come from China or Russia, and these hackers assume that because we're a large electrical contractor, that we would have the blueprints for the power grid in San Jose (which we don't), for example," McGibney says. McGibney is a cybersecurity veteran, literally, having entered the field while serving in the U.S. Marines, including a stint at Marine Security Battalion in Quantico, Va.

From a hacker's point of view, the company's own data can be worth stealing, too, such as financials or employees' personal information (think identity theft). Ransomware doesn't care, it's trying to infect as many people as possible. If a hacker gains access to your system and locks it down under its control, you can't use your data. Then, its value to you becomes the issue. Companies have paid hundreds of thousands of dollars to get back into their own computer systems. increasingly, there are hackers who simply steal the use of the network itself. They don't have to steal information, they can steal resources. Hackers can use your network's computing power for activities like bitcoin mining. As the number of bitcoins in the world has grown, the amount of computing necessary to make new bitcoins – called mining – has increased so much that the cost of the electricity can be greater than the value of the bitcoin. Bitcoin mining is much more profitable if you steal the computing resources. The computer's owner is probably unaware of the bitcoin mining activity, but it can slow down a system enormously. While the threats are varied, they have one thing in common for a construction company. It's impacting their ability to do the job, to finish the job on time, and that's what matters to construction companies.

THE VULNERABILITIES

"The human element is what I worry about the most," confesses McGibney. "You get an email that appears to come from the CEO, and it says 'Hey, I need you to read this right away, click here.' You click on that link, and up comes a prompt for the username and password, and you're thinking, 'OK, I just need to re-authenticate for whatever reason,' and they put in that password, not knowing that they just gave that to a hacker. Now that a hacker has your user name and password on our network, they can easily see your entire email structure, and now they can start specifically targeting users like executives." Hackers use human error to gain access to a network:

By getting someone in the network to reveal their login credentials (username and password). It is often done via email, which might link to an app or website that appears to be legitimate and collects the information. By getting someone in the network to download/activate a malicious program that communicates with the hacker. This might happen from opening an attachment to an email, clicking a link in an email or text, downloading an app or other file from the web, or plugging in an infected memory device. Physical security is also an issue. "If they can get access to your building where you have your servers," McGibney relates, "they can put a pi device on your network, and that device just sits there listening on your network. A hacker can create a clone wireless access point on your network: I see I have an access point, I connect to it, I log in thinking, 'it's in my building so it's got to be one of mine,' and then come to find out a hacker has put it there, and they have been harvesting credentials for the past few months."

Even if your network is secured to stop email phishing and physical hacking, people can bring in trouble from outside. "They have a laptop at work, everything's fine. Then they go home and their child uses it to play games online, and they download something... When they come in the next day with that laptop that is how a lot of companies get breached."

THE REMEDIES

Protecting a network and the data that's on it requires securing it against intrusion, detecting intrusion, and blocking it. Each step involves both technology and live humans.

"There are so many pieces," McGibney says. "You have to worry about the server side, the network, the end user computers, mobile, iPads, iPhones... Think about thermostats in a building, or lighting that is now controlled via software. A hacker can hack into your lighting environment which, for some companies, just happens to be on the same network as your servers." McGibney recommends putting those devices on a separate subnet.

Many of the endpoints have human beings connected to most of them. Securing the human element *requires training*. McGibney starts when an employee first comes to the company. "Day 1, the very first thing they do is they take a cybersecurity training course. If they are compromised later on down the line, we have them take an advanced cyber security course, more in depth, so they can see the anatomy of what happened when they clicked on that link and put in their credentials. That has helped curtail successful phishing attempts by 65 percent or more." McGibney even stress-tests the human elements of his network. "We send out simulated phishing campaigns. I'll send one out that will look very realistic. I'll even spoof the Rosendin domain. It'll say, 'Your password is expiring within 24 hours. Click here to change your password now.' We then collect those statistics and we then reach out directly and have them take an advanced refresher course. It's gotten to the point where people won't click on anything — even legitimate emails that come in."

There are also a range of options to harden the network technologically, which will almost inevitably mean turning to third-party vendors. Security is all about limiting access. Networks are designed to enable access and generally include only the most basic functionality for limiting it. To detect and prevent today's cyber threats requires software and/or hardware add-ons and ongoing active human scrutiny.

BUILDING THE SECURITY SYSTEM
Should a construction company bring that expertise in-house? McGibney and Hoban both recommend having IT/cybersecurity professionals if a company is big enough to afford it. That team will take the lead in creating and maintaining a security culture within the company, will be able to determine the security requirements, will identify and vet third-party vendors and will be the resource to respond to any threats or breaches that are detected.

The next step is to buy more expertise from third-party vendors, starting with a security audit of the company. Once you have found out where the holes are, you can look for security providers who can solve those issues. This could include software and hardware that screens email and downloads, watches all the traffic on your network and looks for unusual or suspicious activity. The software might learn the network habits of individuals in the company so it can detect anomalies. Human monitoring and human intervention to block attacks proactively is critical.

These types of protection are available in pieces or in packages. A company with an in-house security professional might have the expertise to shop around and put together effective protection from multiple providers. The other option is to buy a complete solution from a single IT service provider, an especially attractive route for a construction company that is too small to have its own security team. An IT service provider will take the responsibility for managing and monitoring the security of a customers' network. It goes beyond just providing technology and software, to having experts that are watching over customer networks, doing investigations, and responding to threats. They need to monitor all of the events that happen on the network.

HIRING HELP
Selecting the right third-party help is a job in itself, one that a security director or chief information security officer (CISO) is in a better position to tackle.

McGibney strongly recommends asking for customer references. "That's what Rosendin did. We went for the bigger players in the space, but even then, we asked for customer references. We reached out to those customers, and then to customers of those customers (they didn't know we were going to do that) just to see the trials and tribulations that they had. He also admits that nothing is bulletproof. "We block millions of phishing attempts that come in on a monthly basis, but you can't block every single one. In my opinion, hackers are some of the smartest people in the world, and if they want in, they'll try and figure out the best way to do so."

Security is a moving target, and a company that does not stay focused on it is more likely to become a victim.

BY STEVEN H. MILLER
Constructor - AGC