Construction Executive

http://constructionexec.com/article/trust-but-verify-why-cybersecurity-is-so-important-for-a-construction-contractor?

Trust but Verify: Why Cybersecurity Is Important for Construction Contractors

By Robert Coro | Tuesday, February 25, 2020

A contractor had not yet received payment on a multi-million-dollar project, which was unusual for that particular client. He was relying on timely payment in order to meet payment obligations to employees, subcontractors and other expenses. But upon checking with the client, he discovered payment had been made—but not to him.

Another contractor emailed personnel files and other confidential information in response to a customer request. After a quick call to the client to follow up, the contractor realized the request didn't come from the client.

These are just two examples of the many ways hackers can and do use technology to disrupt the construction industry.

According to Knowbe4's 2019 Phishing by Industry Benchmarking Report, 38% of small- to mid-sized construction companies are at risk of falling victim to a phishing scam. The percentage decreases slightly (37%) for large construction companies. Overall, across all industries and company sizes, one out of three employees is likely to fall victim to a phishing scam.

Contractors, construction companies and owners are not immune to these attacks, resulting in downtime, reputational and financial impact, as well as significant efforts to address breach notification requirements. Educating staff and taking appropriate precautions to prevent cybersecurity attacks is essential, as no company is off limits to enterprising hackers. In fact, the construction industry is an ideal target for cybersecurity disruption, given the prevalence of remote worksites, small or inexperienced IT staff and frequent lack of security training.

REMOTE WORKFORCE

For construction contractors, setting up a small office on the jobsite is a common practice. The remote office is typically established within a physically secured location with a wireless access point. As with any remote worker, there is a risk that the employee may bypass the security protocol of the company's wireless network and connect to an unsecured wireless network, which could allow hackers to intercept the employee's password credentials and access confidential data. With the increased use of mobile devices (laptops, phones, tablets and drones) for the remote workforce, businesses need to understand

and assess the risks and vulnerabilities that come with that and implement controls to mitigate these vulnerabilities.

SMALL OR INEXPERIENCED IT STAFFS

While the dangers of insecure IT networks are now well understood, CEOs of smaller companies may not always recognize the threats to their businesses, believing that hackers are looking for larger targets with potentially bigger pay-offs. This is a patently false assumption that can be potentially crippling, particularly to an enterprise with limited resources to fend off an attack or to rectify damage resulting from a hack of their mission-critical systems.

In addition, IT personnel in smaller operating environments are often stretched thin in their day-to-day responsibilities—keeping the network running, addressing support tickets, and maintaining printers. They might not have the bandwidth or skill set to analyze logs that can identify whether a hacker has gained access to the network.

According to a FireEye Mandiant Frontline investigation report, the average hacker spends 78 days inside a system before being discovered. Once inside the network, hackers can traverse the network, analyzing network traffic and reading emails received and/or sent by key people in the organization in order to accumulate just enough data to leverage for malicious intent. Just as project managers, designers and engineers are trained on the newest construction techniques, IT personnel should also be trained on the continually evolving techniques and strategies for combating cybersecurity threats. Awareness and preventive training need to be at the forefront of any company's strategic plan.

SECURITY AWARENESS TRAINING

Proper training and education must be reinforced annually to refresh and update employees' awareness of common threats they are potentially exposed to daily. Training can be conducted in person or via modules providing real life scenarios and examples to test employees' cyber knowledge and level of safety. The cost of cybersecurity training can range from $1,000 for a business with 50 employees up to $5,000 or more for enterprise-level training. Hackers are becoming more and more sophisticated and trends are changing, so relevant education is key to staying abreast of how to identify and address potential threats.

Another training technique is conducting simulated phishing attacks, in which someone posing as a legitimate sender issues simulated phishing emails to employees--enticing them to click on a link, download a file, reveal their user name or password, respond to the email or obey a fraudulent request. These simulated phishing attacks gauge the actions of employees and help understand the risks to the organization. These techniques can enhance regular training and education efforts. The KnowBe4 Benchmarking Report found that construction companies experienced a drastic reduction to the percentage of employee prone to phishing attacks. After scoring over 30% on the baseline test, they dropped between to 13% and 15% after 90 days of training.

Is the company prepared to recover after a security incident? According to a report issued by a research collaboration between Cisco and the National Center for the Middle Market, based on data from 1,377 CEOs of small- and mid-sized businesses, 6% of firms don't have an up-to-date or active cybersecurity strategy. And according to the National Cyber Security Alliance, 60% of small- and mid-sized business that experience a substantial cybersecurity incident go out of business within six months.

Technology is helping businesses achieve new efficiencies, improve cost effectiveness and pursue innovation. But businesses need to develop proper protocols, including technology governance parameters, and strengthen systems and employee skill sets to minimize—and properly respond to—cybersecurity events.

Always trust but verify. Providing the tools for employees to remain educated and informed is mission-critical to the company's cybersecurity health for the future.

Written by Robert Coro - Director, Marcum LLP

Contact Info: Robert.coro@marcumllp.com

Robert Coro, CPA, CISA, CISM, PCI QSA, is an information technology audit director in Marcum LLP's New Haven, CT, office and is a member of the Firm's IT Risk and Assurance Services Practice group. He has extensive experience with internal and external audits as well as specialized projects for application reviews, firewalls, intrusion detection systems, network security, Sarbanes-Oxley 404, SSAE 16/AT 101 audits, PCI Assessment, internal and external vulnerability assessments, wireless assessments, and penetration testing. Marcum LLP's Construction Services group provides audit, consulting and taxation services to clients ranging from start-ups to multi-billion-dollar enterprises.