Why Contractors Should Be More Concerned About Cyber Security

9.13.2021

We have all seen news reports of cyber-attacks on a company's information system. According to the World Economic Forum's 2019 Global Risk Report, cyber and data privacy and security threats are the leading risks companies face in North America. Yet, there is a common misconception that small businesses are rarely a target for hackers because of their smaller size and lack of valuable data. However, cyber risk does not discriminate, and any information stored on your systems might be interesting to criminals. The "bots" that many threat actors use to find vulnerabilities on the Internet are just that—small computer scripts. They are just looking for open doors, the easiest access to a potential pay-day. While the healthcare industry continually leads the ranks on targeted cyber-attacks, many businesses outside of healthcare fail to recognize that they, too, may have relevant health information that must be protected from hackers.

Greater Efficiency, Greater Risk

Many contractors do not view cyber risk as a priority, leaving them vulnerable to costly cyber-attacks or technology disruptions that can be devastating to the company's bottom line. Even more problematic, many Contractors don't consider themselves to have the type of information that hackers look for. While many businesses provide healthcare insurance for their workforce through a self-funded health plan, these businesses often fail to recognize that these plans may create obligations under the Health Insurance Portability and Accountability Act ("HIPAA") to protect health information that is received about their work force. Contractors often fail to recognize their mode of operation makes them at-risk targets. With increasing frequency, Contractors are expanding their digitization for project scheduling, payments, payrolls, order processing and communications. Construction equipment and control systems are increasingly becoming automated, and, as a result,

Related People

Eric J. Flessland
Shareholder

Related Services

Cybersecurity and Privacy Specialty Team

increasingly becoming wide-open targets.

Consider further the fluid nature of contractor's workforce; many employees work in the field using laptops, smartphones and tablets rather than sitting at a desk in a traditional office environment. The reliance on subcontractors presents even further security challenges as daily reports are uploaded to a central information system. Dozens of companies frequently share vast quantities of confidential information, including bids, blueprints, employee records, and financial information, all in the name of improved record retention and efficiency. While these technical advancements make the company more efficient, they also make the company more attractive to cybercriminals looking to steal corporate and customer data, ransom operating systems, or otherwise disrupt the company's operations.

Risk Assessment and Prevention

The first step in managing cyber risk is to identify sources of potential risk. First and foremost, Contractors must determine what type of information they have in their system. Once identified, Contractors should conduct a risk assessment to determine employee access to and use of critical and sensitive data, including personally identifiable information, protected health information and proprietary company assets. This risk assessment should determine who has access to such information and critical systems, and assess your company's existing capability for monitoring inappropriate system access and potential security events. If you don't have the expertise to conduct such an assessment internally, consider hiring an expert. Given the importance of this tool as an assessment of your company's risk exposure, this activity should not be left to the internal IT department. Credentialled forensic experts are the best resources.

Once you understand your vulnerabilities and capabilities, the National Security Advisor for Cyber recommends **step up your security game.** Butzel Long recommends companies adopt the following Best Practices:

- Implement multifactor authentication (threat actors thrive when MFA is not deployed)
- Mandate Virtual Private Networks (VPNs) for remote access to company networks (critical for a dispersed and/or work-from-home workforce)
- Deploy endpoint detection and response (EDRs will detect and prevent most incidents automatically and do so 24/7/365)
- Implement Incident Response Plans (without a plan, it can be chaos)
- Encrypt confidential and sensitive data both at rest and in transit (encrypted data is useless to threat actors and a non-event under most data breach laws)
- Back up data (encrypted) and secure that backup off-site (with a good backup available, no ransom payment is necessary)
- Turn on logging (you can't find what you can't see)

- Segment data across IT networks (don't make it easy for threat actors to crawl across your network)
- Control access credentials to need-to-have individuals (threat actors target IT managers with the "keys" to the network)
- Implement periodic training for all (training works and it's simple to do)
- Purchase a comprehensive cyber insurance policy (and pre-vet your cyber counsel and forensic team)
- Maintain physical security controls (lock your doors and lock up your sensitive equipment)
- Conduct periodic external and internal vulnerability scans (security is not a one-and-done effort and requires constant vigilance)

Each point comes with a "lessons learned" story of a data breach. Contractors, like most companies, rely on technology to do business. That can be a source of strength, but any breach or technology interruption disrupts critical workflows and operations, and can lead to substantial losses for the company and its stakeholders. Although it may be difficult to remove that risk, contractors can create effective cyber risk management policies and procedures to reduce the risk. Be the company to avoid the lesson and go with the best practices.

Eric Flessland
313.983.6901
flesslae@butzel.com