HORNE
CPAs & BUSINESS ADVISORS

CAN A CYBERSECURITY BREACH HAPPEN TO ME?

As a contractor, if you think that cyber attacks "will never happen to me," it's time to reconsider your stance. Construction companies are an attractive target for a wide variety of cyber criminals, and the attackers are becoming more active and aggressive.

Despite what you read in the news, hacking is not limited to political scandals and major retailers. It's no longer a question of "if" you will be breached—the question is "when?"

Today, cyber crime is less about stealing credit cards and other personal financial information. Attackers today focus on stealing valuable information such as intellectual property, contract pricing and trade secrets. There's much more at stake today. Cyber crime poses risks to your operations and reputation.

So now, the question becomes: *what should you be doing to secure yourself?* Most contractors do not have a large IT staff which can support operations as well as security efforts. However, here are a few things you can do with limited resources to make your organization more secure:

1. **Keep all software and applications up to date.** Hackers will quickly identify any known vulnerabilities in your system. Out of date software, plug-ins and applications are easily identifiable and a simple way to gain access to your network.
2. **Limit access to sensitive information.** Evaluate your sensitive information. Who all has access to it? Why? How many ways can it be accessed?
3. **Educate employees.** Hackers prey on the oversight and vulnerabilities of your employees. Encourage them to take caution and be more aware of malicious attacks.
4. **Practice good password management.** As cyber criminals become more sophisticated, it is important to practice good password management.

THE BOTTOM LINE

It's no longer a question of "if" you will be breached - the question is "when?"

5. **Conduct routine advanced penetration testing.** The only way to truly know if your system can be hacked is to have a team of "hackers" try to hack your system. Advanced penetration testing will uncover all vulnerabilities in your system which adversaries could leverage to gain access to your network.

6. **Monitor your network.** Security service providers now offer the ability to outsource your security team. Cybersecurity Operations Center services allow for 24/7/365 monitoring of your network for real-time threat detection. The value in these types of services include: access to security expertise (which is not easily obtained in today's security talent shortage), around the clock monitoring and log management, and the ability to do this for less than the cost of a full-time security professional on your payroll.

7. **Know what's on your network and the security implications of growing your attack surface.** Your company and its network will continuously grow and evolve. The "Internet of Things" can create improved productivity and increased operational efficiency, but can also decrease your level of security. Check out my latest blogs on securely integrating the Internet of Things and securing a mobile work force for our insights on these topics.

BE PREPARED

It's no longer a question of "if" but "when?" It's no longer just about your data, but also your business partners' data. Be sure you are taking the proper steps to secure yourself and your organization today.

ABOUT THE AUTHOR.

Dr. Wesley McGrew serves as the director of cyber operations for HORNE Cyber. Known for his work in offensive information security and cyber operations, Wesley specializes in penetration testing, network vulnerability analysis, exploit development, reverse engineering of malicious software and network traffic analysis.