DHG | views

March 2016

A Cybersecurity Risk in the Construction Industry

Rick White, Partner | DHG Assurance Services

Rodney Murray, Principal | DHG IT Advisory

Connected devices, social media and the cloud are altering the ways companies' process, share and store information. These advances allow staff to access company data from remote locations while traveling, on a job site, or from their home. As new communications mediums, currencies and storage options continue to emerge, attackers see even more opportunity to steal valuable information. It is becoming more imperative for management to focus on responding to cybersecurity risk to prevent these attacks.

Why It Matters to Your Company

Failure to address cybersecurity threats increases exposure to a host of risks to a company's brand and bottom line. Negative press has become commonplace in relation to publicized cybersecurity incidents in recent years. It causes reputational damage and can result in unplanned costs. Further, it can decrease a company's market valuation, create new legal complexities and may give rise to fines from some regulatory bodies for noncompliance. All of these are possibilities when breach prevention and notification practices have not been managed or properly handled.

How Attackers Penetrate Your Company and Information

There are multiple ways in which your company's confidential information can be compromised. Some of the various methods of attacking your system require a high level of skill and time on behalf of the intruder, while others require little to no effort and can be performed by relatively inexperienced attackers. Examples of attack methods include:

- **Malware** – A computer program with malicious intent. These programs often appear as harmless files that are designed to trick users to click on the file, yet cause them to reveal sensitive information.

- **Keyloggers** – These invisible applications often silently install themselves after unsuspecting users open a malicious email attachment or web link. They allow intruders to collect passwords, credit card numbers and other confidential data as they are being typed on the keyboard.
- **Password attacks** – This includes obtaining and determining ("cracking") a username and password. This can allow unauthorized users to access information via your "secured" system.
- **Denial of service** – These attacks occur when attackers disrupt or impair valid user's ability to access your company's networks.
- **Unpatched software** – A patch is an update to a computer program (e.g. Java or Adobe software) intended to close vulnerabilities that could be exploited by attackers. Unpatched applications provide an entry opportunity for these attackers allowing them into your computer and network.

Why is it Important to the Construction Industry?

Limited regulation and guidance for construction companies result in less focus on cybersecurity relative to other industries. Yet, construction companies face the same threats, given reliance upon IT systems and Internet connectivity for business operations. The reduced attention on security risks – combined with a common belief that they aren't a target – often make construction companies low hanging fruit for attackers.

Has your business assessed the impact on operations if an intruder gained access to your proprietary bidding model and sold it to your competitors, or stole bank account credentials to conduct fraudulent transactions? Would your business be able to recover and remain competitive?

Ask Yourself the Right Questions

Thwarting cybersecurity threats is challenging, as intruders are using more sophisticated and always-evolving techniques to avoid detection. But, it is imperative for your business that you ask yourself and your IT advisors the right questions regarding the security of your company's critical systems and data. Some questions to consider include:

- Is our company heavily dependent on third parties to support our IT systems or process financial transactions?
- Does our company have the capability to monitor for inappropriate use of the system or potential security events that might arise?
- Does our company have a documented formal policy regarding use of company networks and data to limit potential of exposure to unauthorized individuals?
- Has access to critical systems and data been limited to appropriate individuals?
- Have our employees been trained how to avoid exploits and how to report potential malicious activity on the network?

Finding the answers to these questions could highlight the need to consider establishing additional cybersecurity controls within your organization.

What are the Steps You Can Take?

Here are a few simple actions you can take to reduce cybersecurity risks immediately:

- Identify your company's most valuable information and where that information is located on your network.
- Establish internal controls and cybersecurity procedures that consider both internal and external threats.
- Prioritize cybersecurity procedures to protect the most valuable information. You need to place the highest levels of protection around your most valuable information.
- On a regular basis, evaluate your cybersecurity controls and procedures for their effectiveness with thorough audits and technical assessments by resources with cybersecurity experience.
- Establish a plan of action in the event that you must respond to an adverse cybersecurity incident. Test the plan by conducting a simulation at least once a year.
- Establish procedures to evaluate your third party service providers (if applicable) and assess their cybersecurity processes.
- Communicate cybersecurity measures to the entire organization and help every employee within your organization understand the threats your organization faces, and their role in protecting the company's assets.

What Can You Do if Your Company Lacks These Resources?

The suggestions provide a high level first step in assessing your company's IT preparedness. Should additional resources be necessary to improve the IT security infrastructure, we recommend you consult a trusted third party service provider to do an assessment of your IT structure and risks. Knowledgeable IT advisors can provide you the tools and counsel you need to help protect your company from cybersecurity breaches or other IT related issues. When searching for a trusted third party advisor, you may consider individuals holding established certifications in the industry, such as CISSP, CCE, CISA, CRISC and GCIH certifications.

In Conclusion

In today's evolving information technology world, addressing security risks can be critical to sustaining a strong brand in the industry. Don't let your business be impaired by theft of sensitive information or fraudulent financial activity as a result of a data breach. Take the steps necessary to protect your information and future and avoid damaging interruption of operations, or worse – becoming the next headline.

Rick White
Partner
DHG Assurance Services
703.226.0098
rick.white@dhgllp.com

Rodney Murray
Principal
DHG IT Advisory
704.367.7062
rodney.murray@dhgllp.com