The Case for Cyber Coverage in the Construction Industry

Construction companies are not exempt from the dangers of cybercrime.

Construction may be one of the few industries today that is not data production driven. Most construction firms don't have large IT departments and the majority have little expertise in managing information security. However, access to clients' confidential information and an increased dependence on technology have exposed construction companies to a host of new threats, making the need for cybersecurity a critical risk management consideration.

It is projected that cybercrime will cost businesses approximately $6 trillion per year on average through 2021. There's a belief among construction companies that they aren't a target, which only makes the industry easier prey for attackers. And it's not just large companies that are susceptible. In 2016, nearly half of cyber hacks targeted small businesses. A recent Forrester survey revealed that more than 75 percent of respondents in the construction, engineering and infrastructure industries had experienced a cyber-incident within the last 12 months.

A recent Forrester survey revealed that more than 75% of respondents in the construction, engineering & infrastructure industries had experienced a cyber-incident within the last 12 months.

Like all businesses, construction companies must adopt a robust cyber security risk management strategy and take the time to understand the exposures including:

Access to client's confidential information – Although your company may not store the type of personal information hackers find desirable (e.g., credit cards or financial records), you may still have access to your clients' confidential information. Compromised intellectual property such as building specifications and architectural drawings can provide a roadmap for criminals to gain access to valuable personally identifiable information (PII), including financial accounts and employee data. Just like any other company, if you have access to this type of confidential information, you're vulnerable to phishing, ransomware, and other common forms of cyber-attack.

Business interruption exposure – As in any industry, cyber-attacks can result in costly business interruptions for construction companies. A delay in construction projects can be quite costly. This potential disruption must be built into a risk management plan. If a breach occurs, construction companies should have a contingency plan in place to make sure projects are not delayed and if so, they are back up and running as soon as possible.

Mobile dependency – The construction industry poses a unique cyber security challenge in that it is highly decentralized. There are many stakeholders involved in construction projects that are highly dependent on mobile devices and laptops, offering multiple access points to networks and creating vulnerability if they are not all adequately trained on cyber security. Adding another layer of exposure, valuable technology such as laptops are often stored on jobsites in unsecured trailers, making this information an easy target for thieves.

Increased reliance on technology – In addition to a reliance on mobile devices such as smart phones and laptops, the construction industry is increasingly adopting new technologies to improve safety and efficiency. Wearables and drones provide real-time monitoring and data collection, while virtual reality can create simulations of building designs. These technologies open a world of safety, training and efficiency opportunities, but also give malicious actors potential access to valuable information.

Third party liability – As third-party vendors to clients, who also use third party suppliers and subcontractors themselves, construction companies are exposed to stakeholder breach liability risk on all sides. Perhaps the most well-known example of this exposure came in the 2013 cyber-attack on a large, national retailer, in which a small HVAC contractor providing services suffered a data breach. The hackers gained access to the network credentials that the contractor used to remotely access the retailer's network, resulting in a breach of credit and debit card information for tens of millions of customers in the U.S. This HVAC contractor could have been held liable for the damages customers sustained.

Claims findings – Claims arising out of breaches are as a result of various types of attacks including ransomware, phishing and social engineering where criminals send emails purporting to be employees or trusted business partners in order to get confidential information or steal money. These attacks can be from criminals with a pure profit motive, competitors attempting to steal information, or criminals seeking to create chaos for other reasons.

The bottom line?

Construction companies are not exempt from the dangers of cybercrime. Our increased dependency on technology exposes all stakeholders to increased risk. Companies can mitigate this risk by developing mobile device security and cyber breach plans, and by providing adequate training for all employees on cyber security measures and responsibilities. Recognizing that construction companies tend to be more focused on completing projects on time and within budget, some cyber policies offer proactive, value-added risk management support. This added level of support can serve as a tremendous resource, especially for companies that lack expertise in information security. Working with an insurance agent who has proven expertise in cyber security and familiarity with the unique risks posed to this industry is the best way for construction companies to ensure that they are adequately covered.

By: Allied World | June 6, 2018

Orbis Solutions, Inc /Volume 10 / Issue 7/ JULY 2019

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

The Shocking Truth Behind The Growing Cybercrime Threats You Face... And What You Can Do NOW To Protect Your Company

Are businesses losing the war on cybercrime? One recent article on *ZDNet* says yes. The number of security breaches has risen by 11% just in the last year. This is costing businesses even more in lost revenue dealing with these kinds of attacks. It's wasting their time and resources.

In 2016, Cybersecurity Ventures stated that by 2021, digital crime will cost businesses a total of $6 trillion. So far, this projection seems on point as hackers continue to chip away at businesses around the world. They don't care about the damage they're doing.

Right now, the Internet is flooded with sensitive data. From passwords to financial information – it's out there. Some of it is secure, some of it isn't. Either way, because of the sheer amount of data floating out there, cybercriminals have a greater chance to get what they want. And over time, it becomes harder to protect that data.

But the cyber security industry has also grown in response. People are fighting back. In 2018, the investment into cyber security totaled $37 billion. However, it seems like it's just not enough. When you look at small and medium-sized businesses – the targets of nearly 70% of cyber-attacks, according to SMB Group – cyber security isn't taken as seriously as it should be.

In 2017, *Harvard Business Review* looked at the reasons behind why many businesses don't take cyber security seriously. The results were interesting. It turned out, businesses don't treat cyber security as "the ongoing process that it is." Instead, it's typically treated as a "finite problem that can be solved." In other words, if you do the

In this Issue:

This monthly publication provided courtesy of Sean Connery, President of Orbis Solutions (OSI).

OSI, a virtual IT Department, focusing on solutions to promote companies Productivity, Profitability & Security. OSI provides all the support & services that you would expect from a large full-service IT department.

Orbis Solutions, Inc.
Total IT Service Professionals

bare minimum for security today, the thinking goes, you'll be protected tomorrow.

The problem is as the Internet changes and evolves, so do the threats against its users. It's pretty much impossible to set up a one-and-done security solution. If you were to set up something like an SMB "quick fix" and walk away, there's a good chance your business would be the successful target of an attack within a matter of months.

This kind of thinking is far more costly than many business owners realize. A study by Akouto and Alpha Logistics found that businesses that underinvest in cyber security end up spending more on cyber security in the long run as they deal with attacks – up to 58% more. These costs don't even include downtime or lost wages caused by data breaches. In short, recovering from an attack is FAR more expensive than investing in security now.

So what can you do to protect your business? You can start with changing the way you think about cyber security. You have to accept that the threats are out there and will always be out there. But there are things you can do to minimize those threats.

Start with your people. For many businesses, especially those smaller than Fortune 500 companies, your biggest threat is right inside your organization. For those of us who are Internet-savvy, most would never dream of clicking on a scammy link or responding to a phishing e-mail. We've been around the cyber block and we know what to look for.

However, people still fall for even the most basic scams. There will always be someone on your team who isn't informed about these kinds of threats, or those who use obvious passwords. *ZDNet* points out that "only 26% of workers know what to do in the event of a breach" and that "7% openly acknowledge that they ignore or go around security policy."

It pays to invest in a thorough and ongoing training program. It's crucial to outline clear and firm security protocols so your team knows EXACTLY what to do. No one's left guessing or clicking on anything they don't recognize.

It's also crucial to not go it alone. The single best way to stay on top of all things cyber security is to hire a highly experienced managed services provider who is up-to-date on the threats you're facing. Having a partner means you don't have to assume your business is protected. You'll *know* your business is protected.

> **"It's also crucial to not go it alone. The single best way to stay on top of all things cyber security is to hire a highly experienced managed services provider ..."**

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

Claim your FREE copy today at
https://www.orbissolutionsinc.com/cloudreport

Shiny New Gadget Of The Month:

Logitech's Circle 2 Home Security Camera

The Internet age has made home security a straightforward affair, and with Logitech's popular Circle 2 home security camera, it's easier than ever to get in on the action. Equipped with 1080p livestreaming, a wide 180- degree viewing angle, free 24- hour event -based cloud storage and rated for both indoor or outdoor use, it's a powerful tool for keeping your home safe, whether you're there or not.

The device works seamlessly with all the popular smart home platforms, including Amazon Alexa, Apple HomeKit and Google Assistant, and it is easy to set up. It offers crystal-clear video night or day and is easily viewable from your phone wherever you are. If you're in the market for a smart home security system, this is the place to start.

5 Underrated Habits Of Super-Successful People

1. Asking Questions. Successful people are also the most curious. They're more interested in finding answers than they are worried about appearing to not know everything.

2. Analyzing Feelings And Emotions. The strongest people understand that they're still human and learn to monitor, manage, and understand their inner workings.

3. Standing Up To Their Inner Critics. It's easy to beat yourself up and hard to practice self-compassion. But the latter will lead you to great things, while the former will stop progress in its place.

4. Saying No. The best of us respect their own boundaries.

5. Leaving The Office. Seriously, do it – even working from home for 20% of the workweek has been shown to increase productivity, not to mention sanity. *Inc.com, 3/29/2019*

SURROUND YOURSELF WITH POSITIVE SUCCESSFUL PEOPLE

TECH FACTS

1. 90% of the world's data has been created in the last couple years.

2. We are currently preparing students for jobs that don't exist using technologies that haven't been invented; in order to solve problems that we don't even know are problems yet.

Have you heard about our Referral Program?

We want to reward you for your business connections! Refer us to your network, and if AFTER their initial meeting they are a qualified prospect you get a $25 gift card. If they become a client, you or your favorite charity will receive $50 per user.

What makes a good Referral?

- 20 –1000 computers
- Unhappy with their current provider
- Relocating
- Growing/Adding new employees
- Concerned with their security

Submit your referral to referrals@OrbisSolutionsInc.com or simply visit www.orbissolutionsinc.com/about-us/referral-program/ and fill out the form.