An important message to Construction Companies

Did you know you are one of the next big targets for Cyber-attacks?

Febuary 10, 2020
by AJ Rodriguez

Construction professionals are experts at what they do. They understand how to build beautiful architectural buildings and landscapes and they know how to illustrate the vision of their customers' imaginations. However, some construction companies never imagine how they are exposing themselves and their customers' most important assets to criminals. It's not hard for cyber criminals known as hackers to find out which construction companies are most lucrative and vulnerable. They form a way to attack, then they gather information like confidential data (bids, blueprints, financials, employee records). Some of these hackers are local, some are government sponsored by China or Iran, and some can even be rival competitors looking to steal your secrets.

These criminals are looking to destroy and steal data and post to the internet to expose names and seek to damage your reputation in a form of extortion.

The link below is to an article (**"Construction Cybercrime is on the rise"**) that gives two examples of breaches to Construction companies **.** The article addresses two construction companies that were the victim of cyber crimes due to inadequate security controls around financials**.**

https://www.enr.com/articles/46832-construction-cybercrime-is-on-the-rise

Threat Landscape is the landscape (vectors) where threats actors can access your data. Below is a list of some of the vectors that top 10 breaches worldwide occurred. We will dive deeper into some of them in this article.

1. Social engineering (cleverly getting information from a person unaware)
2. Vendor and Providers (networks that you connect to or connect to you)
3. Email phishing (click on a file attachment that has a malware virus)
4. Web page API (Access Program Interface) (Web pages code vulnerabilities)
5. Mobile Devices used by employees
6. Companies Office Network
7. IoT (Internet of Things)

The construction company **Threat Landscape** is constantly growing in this new digital age since many have field employees where most use laptops, tablets, and smartphones which expands the safety of their customers' data security far past the main office. The mobile devices to access financial interactions is the new frontier for hackers. Android phones and IPhone malware has quadrupled in the last couple years and continues to grow.

The construction industry uses merging technology and "smart devices" (IoT - Internet of Things) on the jobsite to become more efficient, profitable and to combat the ongoing worker shortage. Today, construction equipment runs on IoT (Internet of Things) such as computers systems, sensors, GPS, and more advanced things like application in concrete curing. IoT gives companies advantages like real-time site maps, updated risk matrix's so managers can monitor and measure progress and react to real time environments on the site.

IoT allows for the creation of a digital real-time job site map works together to update risks associated and notifies every worker when getting closer to a risk or entering a dangerous environment. For example, monitoring the air quality in an enclosed space is critical for a safe workplace environment. IoT technologies will not only prevent staff from being exposed to dangerous conditions but can also detect those conditions before or as they happen. However these IoT devices themselves expose dangerous conditions by allowing a vector for hackers!

Now that we know how complicated the Treat Landscape can be, let's take time to understand some of your risks:

Top 3 Cybersecurity Risks in Construction:

- **Backend Office –** As construction companies grow from small to medium to large organizations, the safeguards protecting their assets should grow as well. Many companies don't understand the risks that increase as they grow. Ransomware is a popular trend where the criminal will encrypt (virtually lock) your data and hold it hostage until you pay a ransom.

- **Not knowing you already have been infiltrated - Park and Stay –** APT (Advanced Precedent Threat) A criminal can slowly steal your data without you knowing. For example, Malware can reside within your system for a long time without you knowing. 75% of all security breach victims do not have the staff to identify, detect, protect, respond and recover.

- **Can't protect what you don't know –** The expanding perimeter forces IT Security to understand personal user habits, education of employees, and to understand the growing risks which require more resources to protect the expanding Threat Landscape.

Common mistakes:

- Companies find out the Hardaway that PCI (Payment Card Industry Data Security Standard) compliance and others is not adequate security.

- Attitude mistake - it won't happen to me.

- Hacking is hard and you really need to spend a lot of time and money to get my information and mine is not worth it.
    - HaaS (Hacking as a Service) Hacking is easier than you think. If I wanted a "custom designed malware" to infiltrate your network I can hire a hacker to write a custom malware and hide it in an email invoice document then send it to someone that is apt to open it. It's that easy!

What can you do to Minimize Cybersecurity Risks?

- Data Risk Assessment - Benchmarking
    - What is your risk level and likelihood?
- Know your unique vulnerabilities
    - Every company does business differently; they work with different vendors and technologies.
- Know IT Security best practices
    - Do you handle credit cards or personal information?
- Cyber security needs to be one of the highest priorities in any organization
    - Cyber security should come from the top down and a bottom up approach.
    - Cyber security must get C level executive support as well as buy in from the team. IT security should be a line item within your budget to ensure your assets are protected.

Helpful hint:

- "Did we spend enough?" How do you know how much you should spend on a "Safeguard Cost" such as IT Security Technology Systems and Consulting? The answer is simple:

    ✔ **Safeguard Cost = Annual Loss Estimate - Annual Loss Estimate after implementing safeguard - Annual cost of Safeguard.**

The most valuable thing you can do to minimize your risk is to partner with a security consulting company. **STAR,LLC** offers the full range of **STAR IT Security Services** in all security domains. We can help you with understanding the risk and likelihood of critical threats, in addition to help you understand the vulnerability level of your assets, and then help you protect those assets in your unique environment.