Building a Strong Cybersecurity Foundation in the Construction Industry

ARTICLE 10.26.21 DEAN DORTON

Recent and highly visible ransomware attacks such as the one on Colonial Pipeline should serve as a wakeup call for organizations that do not see themselves as “typical” targets of cyber-attacks.

The size and industry of the organization often does not matter for cyber criminals who are always looking for opportunities.

According to the 2020 Verizon Data Breach Investigations Report (*), 67% of all breaches come from three attack types: credential theft, errors, and social attacks. The average cost for a data breach is $2.64 million for organizations under 500 employees. Phishing and ransomware remain two of the top Cyber risks for most industries, including the Construction industry.

The first thing that organizations can do is to perform a Security Assessment to ensure that they understand where their vulnerabilities are and to assess their resilience against cyber attacks.

Key controls to consider are:

- Multifactor authentication (MFA) – for all remote access to systems and information (including emails) to mitigate credential theft attacks.
- Strong password policy – making sure weak passwords cannot be used and that users cannot reuse passwords.
- Endpoint security – many cyber attacks start with a user clicking on a bad link from their devices. Having a strong endpoint detection and response software on all endpoints is critical.
- Vulnerability management – the “cyclical (never-ending) practice of identifying, classifying, prioritizing, remediating, and mitigating” software vulnerabilities.
- Logging monitoring – this detective control can allow organizations to quickly react to suspicious activities and can provide information after an attack to determine what was accessed by the threat actors.
- Security Awareness – employees and business partners need to understand how to identify and report potential security issues. Security Awareness is especially important if you are working with a workforce that might not be totally comfortable with computers.
- Resilient backup – employ a “3-2-1 strategy” which means having at least three total copies of your data, two of which are local but on different mediums (or devices), and at least one copy off-site.
- Incident Response and Business Continuity Plans – contain specific information and playbooks on how to react when an incident occurs and how to quickly resume operations.

Having cyber insurance coverage is critical, but this is becoming more complex: organizations have to be careful to make sure that they have the appropriate coverage for common attacks scenarios. We often see sublimit in coverages specific to ransomware and even no at all coverage for email frauds. Insurance companies are also asking for more

assurance that security controls to be in place during the underwriting process.

Many organizations have transitioned to a hybrid remote work since the pandemic started and the security controls need to be reviewed and tested for this new environment.

Of course, these measures should apply to contractors and subcontractors working with organizations. If their companies do not have the level of sophistication needed to mitigate these risks, they put their customers and partners at risk.

Construction organizations must improve their security posture and implement measures to mitigate cyber risks.

Gui Cozzi | Cybersecurity Practice Lead
gcozzi@ddaftech.com
859.425.7649