THREE PRACTICAL STEPS TO PROTECT YOUR CONSTRUCTION BUSINESS AGAINST CYBERATTACKS

by **J. CHRISTOPHER SELMAN & ERIN ILLMAN**

EVERY DAY, NEW INSTANCES OF DATA BREACHES, ransomware attacks, and cybercrimes affect companies around the world. Many of these companies are in the construction industry. For some, the thought of protecting one's organization from cyberattacks may seem overwhelming or cost and time prohibitive. However, any company that is connected to the internet faces risks and potential liability for failing to implement proper cybersecurity policies.

With the right team of experts, strengthening a company's baseline cybersecurity can be both inexpensive and relatively simple. Below are three practical and affordable measures to do so:

1. **Enhance Security.** Institute appropriate security measures. Not only is this a pragmatic step to deter cyberattacks, but it can also be a legal requirement. For example, the new Alabama Data Breach Notification Act requires certain companies, including those in the construction industry, to "implement and maintain reasonable security measures." Accordingly, companies should start analyzing what security measures may need to be in place. This can present unique challenges for construction companies. For example, the increased use of design and modeling applications and multi-user collaborative platforms create additional data and access points that are sometimes difficult to manage. Easy security measures that should be implemented include updating antivirus software and installing firewalls and patches regularly. Companies should also safeguard WiFi networks, use VPNs, employ data purging policies, and require multi-factor authentication for all devices.

   Additionally, construction companies should consider including data privacy and security provisions in all contracts. These may include notification requirements, cybersecurity insurance, training, retention policies, limiting access, and establishing data tiers.


CHRIS SELMAN

J. Christopher Selman is an attorney in Bradley's Construction and Procurement, Government Contracts, and Litigation Practice Groups. Chris has represented owners, general contractors, subcontractors and engineers throughout the United States and abroad, advising clients at every stage of a construction project from initial contract negotiation and preparation to close-out and dispute resolution.


ERIN ILLMAN

Erin Jane Illman is a partner in and co-chair of Bradley's Data Privacy and Cybersecurity Practice Group. Erin is an ANSI certified information privacy professional with over a decade of experience representing corporate entities, technology companies and e-commerce clients in a wide variety of regulatory compliance, litigation and contract matters.

2. **Perform Training and Monitor Compliance.** Educating employees at all levels of the organization on risks, threat actors, attack vectors, and prior incidents involving construction companies is critical. It is equally important to ensure compliance through consistent monitoring and testing of company cybersecurity policies.
3. **Prepare for the Inevitable.** It is essential to develop a cyberattack response plan now so that damages can be mitigated and actions taken immediately. Key components in a plan may include identifying critical systems and assets that would prevent the company from doing business, employing the use of backup systems, gathering forensic data from affected systems, and notifying law enforcement and legal counsel.

All construction companies should recognize the potential harm of cyberattacks and implement appropriate practices. While each organization's needs vary, these steps can help provide a baseline of protection against cybercrime.

Bradley

Bradley Arant Boult Cummings LLP

Birmingham Office
Phone: 205.521.8000
Email: cselman@bradley.com
eillman@bradley.com