WS&Co. Briefing

December 2017

Cyber Risks & Construction – No Industry Can Hide

With yet another high profile data breach in the news, we are constantly reminded that every company has data that can be compromised and exposed. As businesses become more reliant on internet-connected solutions and remote access systems, we all become more vulnerable to data breaches. Many construction firms have found themselves as targets of such breaches given the valuable data they maintain and their relatively low level of data security. Below are details on what can happen and steps you can take to protect valuable data you maintain for yourself, your clients and your employees.

What could cause an incident:

- Compromised data via a phishing scheme, lost documents (tangible and intangible) or laptops
- A hacker aiming to make money or cause harm to your organization
- System itself – hole in the hardware or security system exploited by a third party

What information could be exposed in an incident:

- Intellectual Property of your customers, such as drawings or specifications
- Financial banking information of your customers and employees
- Other personally identifiable information such as social security numbers, names, addresses
- Log-in credentials in order to access customer systems

What you should be doing about it:

Culture: Engaged Employees

- Beware of phishing schemes – review the sender's address before clicking on links (when in doubt, don't click)
- Encrypt laptops and implement a clean desk policy to ensure safety measures when not around
- Be cautious of allowing entrance to your building

Risk Mitigation Platform

- Proactive IT Department – help educate employees on how to identify phishing schemes and other attempts to gain access to your systems
- Robust data encryption approach – strong password requirements with frequent changes
- Data Assessment and Profiling to ensure you only keep the information you need
- Developing and executing an engaging and thorough security awareness program
- Adhering to industry standard patching cadence for antivirus, operation systems and software

Insurance and Risk Transfer

- Many insurance companies offer cyber coverage that serves as a risk transfer mechanism to help insureds respond to a security or privacy incident and to access free loss prevention tools and training

(continued on page 2)

- Insurance policies should include coverage for the following exposures:
  - Breach Response Costs, including forensics, data breach legal guidance, and notification costs
  - Network and Information Security Liability including defense and indemnity for damages to third parties arising from a breach or hack
  - Regulatory Defense Expense
- Programs could also include coverage for the following exposures:
  - Media Liability
  - Business Interruption
  - Cyber Crime coverage in which an employee is tricked into wiring or sending money to the wrong party can be recovered under a Crime policy or endorsed for a nominal sub-limit to a Cyber policy

Construction Industry

- A recent survey from Forrester's revealed that 75% of construction, engineering and infrastructure firms have experienced a cyber-incident within the last 12 months
- Construction firms tend to believe that tangible products and hard copy documents reduce the threat they face from bad actors
- Technology tools are being implemented into operations and need to be done in tandem with cybersecurity protocols
- Construction companies have just as much data on their servers as any other company including social security numbers, bank documents, blueprints, and other Personally Identifiable Information etc. that need to be kept safe

Overall – All companies have network security and privacy exposure which they should be constantly evaluating and proactively addressing. This can effectively be done through corporate governance, employee training and the procurement of insurance.

Sample Claims

Security Breach

Incident: A construction company had an unencrypted laptop left at a site that was stolen and contained confidential employee and customer information.

Social Engineering

Incident: A large national construction company was the victim of a phishing scheme when an employee forwarded private information to a fraudulent email address which resulted in the exposure of social security numbers of 566 current and past employees across the state.

Contact Us

Woodruff-Sawyer can help address these risks and keep you informed of emerging threats to your business. Contact your Account Executive at Woodruff-Sawyer & Co.

Woodruff-Sawyer is one of the largest independent insurance brokerage firms in the nation, and an active partner of Assurex Global and International Benefits Network. For nearly 100 years, we have been partnering with clients to deliver effective insurance, employee benefits and risk management solutions, both nationally and abroad. Headquartered in San Francisco, Woodruff-Sawyer has offices throughout California and in Oregon, Washington, Colorado, Hawaii and New England.

844.WSANDCO (844.972.6326)
www.wsandco.com.