PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

CONSTRUCTION PRACTICE GROUP

DECEMBER 2015

PART 1 OF 3

CONSTRUCTION INDUSTRY RISKS: DATA PRIVACY AND CYBER SECURITY BASICS

Nick Montera | Vice President, Account Executive

Rarely does a week pass when we don't hear about another major cyber breach, computer virus, or social engineering scam. Healthcare, financial institutions, retail, and governmental networks tend to experience the highest frequency of attacks. However, that does not mean that the construction industry is immune to cyber attacks. The truth of the matter is that any business connected to the internet is a potential victim. This is the first in a three part series discussing cyber events as they relate to the construction industry. Below we discuss why contractors need to address the risks associated with cyber exposures. In part two, we will discuss cyber risk management basics: what you can do to prevent a cyber event from occurring and how you can minimize damage if and when they do occur. Finally, in part three, we will discuss risk transfer and how outsourcing, contract management, and insurance can protect your firm from loss.

Why contractors need to be concerned.

It's not just large corporations that get hacked. In fact, Verizon's "Data Breach Investigation Report" states, "85% of targets of opportunity are small businesses."[i] A recent publication by Hartford Financial Services Group goes on to state, "Cyber-related crime incidents affecting small businesses have been increasing since 2004."[ii] There are a number of reasons hackers may want to gain access to your systems including:

- Access to Personal Information. While contractors may not have as much personally identifiable information (PII) as a retailer or financial institution, construction firms still have employee information that could include social security numbers, bank accounts for payroll, as well as healthcare information.
- Access to proprietary corporate assets including privileged contracts, project/bid data, architectural designs (including security designs), and intellectual property.
- Hackers may also target information regarding a construction organization's bank and other financial accounts via social engineering and phishing schemes, and then attempt to entice an employee to unwittingly transfer corporate funds/assets.
- Access to personal information on other organization's servers. One of the most prominent examples of this is the Target breach in which the initial intrusion was traced back to credentials stolen from an HVAC contractor.
- Disgruntled employees or subcontractors may wish to embarrass the organization.
- Extortion (CryptoLocker). CryptoLocker is a ransomware trojan which targets computers running Microsoft Windows. This ransomware is typically propagated as an attachment or link associated with a seemingly innocuous e-mail message. The intent is to breach a corporation's systems spreading malware and encrypting corporate data. The company is then forced to pay a ransom in order to recover/unlock any data that has not been backed up.

Consequence of a breach.

47 states have now passed 47 separate data breach laws each with their own reporting requirements. In addition, there are various federal laws that institute further requirements. While the laws vary, in the event of a breach there are generally three issues a victim needs to address. First, the organization needs to figure out how they were breached and what data may have been accessed. This generally requires the services of an outside IT forensic firm. Once it is discovered what data has been accessed, legal counsel is engaged to determine notification responsibilities in the various jurisdictions. For instance, California notification requirements may require notification within days while other states may allow weeks. Finally, once it is understood what the notification responsibilities are in each of the applicable jurisdictions, affected parties need to be notified and credit monitoring is often offered to potential victims of identity theft.

In addition to these legislative requirements, your organization may face civil suits from parties who may have, or could suffer identity theft. Regulatory fines and penalties are also common when a breach has occurred.

Ponemon Institute's latest report estimates that, "$154 is the cost per lost or stolen record. $3.79 million is the average total cost of a data breach."[iii] This represents a 23% increase from 2013.

With the prevalence of breaches and the high costs associated with combating one, it's easy to understand why all organizations need to be keenly aware of the risks and how to protect themselves from a breach. In the second part of our series, we will discuss some basic risk management controls to help prevent a breach as well as the need for a data breach response plan.

[i] Verizon, "Data Breach Investigations Report," http://www.verizonenterprise.com/resources/reports

[ii] Cyber Exposures of Small An Midsize Business – Adigital Pandemic, exhibit 1

[iii] (May, 2015), 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute

The core of Parker, Smith & Feek's development over the past 78 years has been the construction industry client. Today, this diverse group of more than 300 contractors and subcontractors serves every segment of the industry and represents a third of our firm's total revenue.

We focus on providing best-in-class guidance on client issues, while investing in our customer service team's expertise. Our construction team, including insurance, bonding, safety, and claims specialists, has been recruited for their knowledge and real world experience, which they draw upon to create targeted solutions for the unique needs of our clients. This team includes three executives dedicated solely to builder's risk, and a team of nine claims specialists. Our reputation of advocating difficult insurance claims, crafting cutting-edge insurance coverage, assisting with project safety concerns, and providing exceptional service is unmatched among other brokers. Whether it's investigating alternative risk financing options through self-insurance, captive feasibility or Controlled Insurance Programs (wraps), or securing a surety bond for a multi-million dollar project, PS&F has the experience and know-how to support these unique needs.

SERVICES OFFERED

- Insurance Program Design
- Alternative Risk Management Strategies
- Contract Review
- Surety
- Job Site Safety
- Environmental Risk
- Workers' Compensation
- Builder's Risk
- Claims Management
- Employee Benefits Plans