



PARKER | SMITH | FEEK

COMMERCIAL INSURANCE

EMPLOYEE BENEFITS

PERSONAL INSURANCE

RISK MANAGEMENT

SURETY

CONSTRUCTION PRACTICE GROUP

MARCH 2015

PART 2 OF 3

CONSTRUCTION INDUSTRY RISKS: DATA PRIVACY AND CYBER SECURITY RISK MANAGEMENT AND RISK TRANSFER

Nick Montera | Vice President, Account Executive

DATA SECURITY RISK MANAGEMENT BASICS

The risks associated with the collection, transfer, and retention of data are real and significant. For a construction company, it is of paramount importance to identify areas of exposure and develop adequate risk management programs that address data privacy and security. To help you get started, here is a list of questions to ask yourself when developing your corporate risk management plan. These should include, but not be limited to, identifying and inventorying your corporate data.

What personal identifiable information (PII), employee, and/or client confidential information is stored on computers or in paper files on premises? If this is the case, where specifically is the data stored, how is it secured, who has access, and how many PII data files are there?

- PII is often defined as unique information that can be used to identify, contact, or locate a single person. In Washington state, PII is defined as an individual's first name (or initial) and last name combined with one of the following: social security number, bank account number, credit or debit card number (including security code, access code or password), driver's license number, or a Washington identification card number.
- Track personal data throughout your entire information infrastructure and identify all parties that have access to this data. Conduct an audit that gauges employee access to and use of personal data.

- Make information security a written workplace policy.

What data does the corporation have? Where is the data stored? What is the data connected to?

- Having a detailed inventory of the data held by the company, as well as knowledge and control over where the data is stored, is an essential step in minimizing the chances of data being lost or stolen. In addition, in the event that data is compromised, having a detailed data inventory will expedite and minimize cost in conjunction with forensic processing.

Are all company laptops encrypted? Are portable media devices like thumb drives prohibited, or at the very least, encrypted?

- Devices such as laptops, smart phones, external hard drives, and flash drives all present possible data security threats if lost, stolen, or hacked. While most people assume that system hackers are the greatest threat, recent studies show that lost or stolen portable devices are the most common cause of data breaches.

Has your construction company implemented strong internal password controls and employee training?

- Make sure passwords are strong. It is also a good practice to reset passwords every so often (90 days is a good timeline) and never duplicate passwords. It's also a good idea to reset default passwords.





Are the company's firewalls current and all security patches regularly updated?

- A firewall can be the best defense when trying to isolate and contain breaches. Despite the expense, it is beneficial to invest in a robust set of firewalls that require user authentication.
- Subscribing to annual support and maintenance with the firewall vendor is also a good idea from a risk management perspective. This should include 24/7 monitoring and support.

Does the company outsource any services to third party vendors that may involve a client's information? If so, do these vendors provide hold harmless and indemnification agreements with regards to any data breach involving personal identifiable information?

- It is a common misconception that outsourcing automatically transfers liability for data breaches to the vendor. It is vital that you have favorable hold harmless agreements in place because data owners can still be held responsible for compromised information. If you are storing data in the cloud, be sure to go over your agreement with your cloud vendor and limit your liability as much as possible.

Does the company have in force a detailed plan in case of a data breach?

- When a cyber-breach is discovered, the actions taken in the immediate aftermath are critical. Getting the response coordinated properly from the start can help minimize damage. On the flip side, missing key issues early on can give rise to collateral problems upstream. With advanced planning a company stands the best chance of being able to act swiftly, decisively and effectively, to minimize the risk from the breach itself and any resulting claims or regulatory action.
- Transferring risk via an insurance carrier should be a consideration taken when developing and implementing the cyber risk management plan.

Our next, and final, article in this series will discuss risk transfer and the insurance products available in the marketplace today.

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