Cybersecurity: Where do you start?

BLOG | FEBRUARY 29, 2016

Cybersecurity has become a topic that is increasingly present in headlines. The risk of a company being affected by a data breach increases significantly as business information is shifted to cloud computing services and mobile devices are used to store and transmit confidential data. As data breach incidents become more frequent, the need for businesses of all types and sizes to consider how to prepare for and address these potential threats is imperative.

While the idea of protecting your business from potential data breaches may seem daunting, there are some initial steps you can take to create and implement a plan for cybersecurity threats.

1. Do You Have Coverage for a Data Breach?

The cost of responding to a data breach can be extremely high. In fact, a data breach without adequate insurance can devastate a business. Many insureds have turned to their commercial general liability ("CGL") policies for coverage when they have been affected by a data breach, but courts have continued to rule that CGL policies do not provide coverage.

Companies are increasingly purchasing stand-alone policies. These stand-alone policies generally provide options for first-party and third-party liability costs. First-party coverage may cover costs related to forensics, business interruption, notification, and public relations among others. Third-party coverage may cover costs related to litigation and regulatory fines. Individual companies should work with their brokers to determine which type of coverage is best tailored for their business.

2. What Are Your Reporting Obligations?

Many states, including North Carolina, have data breach notification statutes that set out specific requirements in the event of a data breach. *See* N.C. Gen. Stat. § 75-65. Additionally, there may be international and federal regulations implicated by a breach. These regulations will determine to whom notification is required, and on what timeline. Taking the time to educate your company on the specific reporting obligations it may be subject to ahead of time can help ensure those obligations are fulfilled in the event a breach actually occurs.

3. Do You Have a Plan In Place?

Having an action plan in place can mitigate both the effects and repercussions of a data breach. A plan of action will help to communicate clearly and effectively with regulators to comply with reporting requirements, employees to

identify and mitigate risks, and customers to advise and inform of potential security concerns. An organized response can aid in both shutting down a data breach and cutting costs associated with mitigating the breach and dealing with regulatory fines. The best practice is to have a detailed plan in place ahead of time that can be immediately put into action at the first sign of trouble.

While the complexities of cybersecurity continue to grow as data breach becomes more prevalent and additional federal and state regulations are implemented, there are many steps businesses can take to manage those risks and protect themselves and their clients.

About the author: Sarah Beth's practice focuses on insurance coverage analysis and business litigation. For questions about this post, please contact Sarah Beth at seb@youngmoorelaw.com or (919) 861-5098.

CONTACT US
Phone: 919-782-6860
Fax: 919-782-6753

OFFICE
Young Moore and Henderson, P.A.
3101 Glenwood Ave. Suite 200
Raleigh, N.C. 27612

MAILING ADDRESS
Young Moore and Henderson, P.A.
P.O. Box 31627
Raleigh, N.C. 27622-1627