BROOKS PIERCE

"New Year's Resolution? Think Data Security."

01.05.2016

Article as published in the 1/1/16 edition of the Triangle Business Journal, copied here with permission. Business Journal subscribers may view the article here.

The start of a new year offers a fresh opportunity to set goals for your business.

With data breaches on the rise, privacy and data security issues are worth addressing as you plan for the coming year.

Here are six privacy related tasks we recommend for your 2016 corporate agenda.

Learn what data you collect from your customers, users and employees. Between marketing, human resources and benefits, and IT departments, companies frequently house large amounts of data. To meaningfully evaluate privacy and data security risk you must first know the scope of the data you have. We suggest you take stock and assess what data you collect and store – you may be surprised at the amount of personal information you have on hand.

Know what data is protected or regulated. Data you might not expect to be regulated sometimes is, and regulation of that data may depend on where the person who provided it lives, or what technology was used to collect the data. For example, some businesses are unaware that marketing to mobile phone numbers is regulated by the FCC pursuant to the Telephone Consumer Protection Act, or that the combination of email and password are protected by law in California and Florida. Once you know what regulated data your business has, you can establish appropriate security and safeguards.

Consider collecting and storing less regulated data. If your company is keeping regulated data that is unnecessary for any business purpose, you should seriously consider changing its practices so that unnecessary data is no longer collected or stored. Of course, if you do decide to delete or discard the data, it should be disposed of safely, securely, and in keeping with legal requirements.

Look at your related data-security policies. Make sure your policies appropriately reflect what information you are currently collecting, using, storing and sharing. Many times, policies are drafted and set aside while data practices change over time. Conduct an internal privacy audit by reviewing your company's website privacy policy, internal information security policy, records retention and disposal policy, contracts with vendors outlining responsibility for data, and policies that govern financial (credit card or wire) transactions.

Form a data breach response plan. Data breaches happen, not only due to hackers, but also to everyday human error. In fact, a recent study of in-house attorneys conducted by the Association of Corporate Counsel Foundation found that employee error was the most common reason for a breach. Having a data breach response plan will give your company the tools to react appropriately to minimize the disruption to your company and its reputation with your customers.

Consider Data Breach or Cybersecurity Insurance. These products are quickly evolving to keep up with the market, and some will suit your circumstances better than others. After you complete your internal privacy audit (see above), you'll have a better understanding of your risks and which insurance product may work best for you.

We tell our clients that it's not a question of if you will suffer a data breach, but when, and to prepare accordingly so you are in the best position to respond. Start 2016 off on solid footing by proactively assessing your data privacy and security practices.

Charles Marshall and Elizabeth Spainhour are attorneys with the Brooks Pierce law firm in Raleigh.

PEOPLE

Elizabeth Spainhour

SERVICES

Privacy