Avoid the Headlines: Six Initial Steps To Take Now To Improve Your Company's Data Security

Benjamin Jackson
bjackson@mwlaw.com
(501) 688.8887

10/23/2017

Unless you have been living under a rock, you are probably aware that companies are suffering cyber attacks that jeopardize sensitive company or customer data more and more frequently. What you may not know is that even more attacks occur every day that are never reported outside of the victim company. For example, the Online Trust Alliance (OTA) concluded there were about 82,000 reported cyber incidents in 2016, affecting 225 organizations around the world each day. However, the OTA also reported that it believes the actual number of annual cyber incidents could exceed 250,000 because the majority of cyber incidents go unreported.

Like it or not, all businesses, big or small, that utilize or retain any of a large variety of sensitive information – from payment data, to information capable of establishing a person's identity, to personal health information - are constantly at risk of a cyber attack. And if your company does not have the proper policies and protections in place beforehand, or fails to respond appropriately to an identified data breach, that may result in regulatory investigations, attorney general investigations, suspension or loss of license, fines and civil lawsuits.

Below are six initial steps every company should take to ensure they are on the right track to protecting against the fallout of a cyber attack or other data breach.

1. Have a plan, put it in a policy, and train your employees on it.

Every company needs to sit down with the appropriate individuals involved with management, IT, record keeping and employee training and policies, and develop a specific policy and procedure for ensuring data security. This should include the following, but be creative because the more detailed your plan is, the better it looks when the regulators and plaintiff's attorneys ask to see it:

- How data will be maintained and encrypted
- How sensitive data will be maintained uniquely from other data
- Employee and company password and security requirements
- Which employees will have access to what sensitive data and for what limited purposes
- The response team for an identified data breach
- The process for identifying and controlling a data breach as well as how that process should be documented
- The process for notification, a generally accepted timeline for doing so, and the individuals involved

2. Determine if insurance is right for your company.

Cyber breach insurance is available, and companies are willing to work with you to determine what is right for your company. For small businesses, don't just assume that a typical Business Owners Policy (BOP) will be enough. Often, the amounts delegated to a data breach are relatively low. Whether the cost-benefit analysis suggests additional insurance is a question for each company and the answer will invariably differ widely. Nonetheless, at minimum, the conversation needs to occur and that analysis needs to be taken very seriously.

3. Know who your third party response team will be, and contact them in the correct order following a breach.

Will you utilize an in-house IT company to respond? Will you need third party IT assistance in dealing with a breach? If you are dealing with credit card information do you want an expert in PCI compliance? Should you have a public relations firm on call in the event media and social media notification is appropriate? Who will be your legal counsel/breach coach? These are all questions you need to answer before something happens, so that your team can be utilized automatically as a matter of policy. And appreciate the impact of attorney-client or work product privilege: when utilizing third party contractors, these can be contracted through your legal counsel to ensure that appropriate information is protected by privilege. But that requires bringing on counsel first in most scenarios.

4. Know which regulatory bodies govern your company.

Currently, there is still no set standard for responding to a breach among states, or even within them. So what your notification and other responsibilities are will depend on what type of information you maintain, and what regulatory body (or bodies) governs that information. This information can be overwhelming and complex, but periodic assessment from compliance attorneys specializing in these areas can make sure your company knows what its responsibilities are, and what timeline it must operate under. Getting such periodic reviews not only protects your company from post-breach allegations of insufficient security protocols, it also protects you from post-breach investigations and suits for inadequate response, and the associated costs relating to defending them.

5. Think about what data your company is holding unnecessarily, or for too long.

One of the easiest and most cost-effective ways to mitigate risk in this area is to only keep that sensitive data which your company truly needs to maintain. Obviously, this varies from company to company, but every company should take an accounting of this on an annual or bi-annual basis. Are you keeping mailing addresses when e-mail addresses will do? Are you keeping copies of applications that contain individual data subject to protection that your company no longer needs after the application process has completed? How long are you keeping payment data? Regulatory bodies have cited companies who have lost payment data that was being kept 90 or 120 days, when 30 days would have been sufficient to complete the sale and exceed time period for accepted returns.

6. Retrain, retrain, retrain.

Don't just make a policy, train on it regularly. Test on it regularly. Make data security an important part of your company culture. Send your employees fake phishing e-mails to see who clicks on what, so that both your company and your employees can learn from it. Talk about it regularly. Post news reports of data breaches on your breakroom board. And most of all, make sure and mitigate any breach you suffer with documented meetings about what could have been done better, changes in policy, and employee training and education. Because if it happens again because your company did not learn the first time, you can bet the regulatory bodies, individuals affected, and attorneys looking to file a lawsuit will want to know why.

To keep up to date on cybersecurity, privacy and data protection issues, subscribe to our Between the Lines blog here.