Security Breaches Costly and Inevitable?

Insights
3.06.17

Yahoo recent announcement that CEO Marissa Mayer would forego a 2017 stock award (after giving up a 2016 cash bonus) following security breaches in 2014, 2015 and 2016 underscores the importance of having a security team in place to prevent or at least mitigate, security breaches. The Yahoo Board found that the company's response to the initial security breach should have been more vigorous. In addition to the penalty paid by Ms. Mayer, Yahoo allegedly suffered a $350 million discount on its sales price because of the breach, and its head of legal lost his job for the legal team's alleged failure to fully investigate the 2014 breach. These costs don't include the costs to defend numerous legal actions alleging that Yahoo did not do enough to understand or investigate the earlier breaches and therefore take action to prevent future such actions.

While data breaches may begin to feel inevitable, with the bad guys seemingly always one step ahead, it is clear that companies need to take cybersecurity seriously, including devoting personnel and money to the issue. Security breaches are not inevitable, but companies need to take the threat of such breaches seriously and implement commonsense protections prior to discovering a breach. It is no longer enough to wait until something happens to take data security seriously. A recent IBM/Ponemon Institute annual report estimates the cost of a data breach to be around $4 million, but that is only a small piece of the total picture. In addition to the immediate data breach response cost, there is the inevitable wave of legal action following the breach, and the long-term damage to company goodwill, reputation and customers.

What can your company do to protect itself now? Start with a data security assessment. If your company does not have the internal resources to perform the assessment, or doesn't know where to start or what to assess, there are a number of outside firms that can provide a thorough assessment for a reasonable fee. The assessment should look at insider and outsider threats, and examine both systemic threats as well as threats to software/applications, among other items. Consider putting appropriate security personnel in place. Many mid-size to larger firms are considering the advantages of having an in-house chief information security officer (CISO) to deal with the continually and rapidly evolving world of cyber security, freeing up the already overburdened IT and legal departments from trying to keep up with the evolving cybersecurity landscape. If your company doesn't have the resources to employ a full-time CISO, there are data security firms who will sell you the services of a part-time CISO.

Prior to discovering a breach, companies should consider cybersecurity insurance coverage. It isn't enough just to call up your broker and buy a policy – make sure your policy covers what you think it

enough just to call up your broker and buy a policy - make sure your policy covers what you think it covers. When a breach occurs, you won't want to discover for the first time that coverage for fines or third-party litigation aren't covered, for example. If you don't feel you have the expertise to fully evaluate a cybersecurity policy, consider working with a third-party cybersecurity firm to help you analyze the proposed policy and determine whether it will fully meet your company's needs. A third-party expert can also help you negotiate the coverage you need.

In subsequent posts, we'll discuss in more detail how companies can protect themselves from data breaches and mitigate when a breach occurs.

Related People

Danielle S. Urban, CIPP/E
Partner
303.218.3650
Email