Companies Must Take Preemptive Measures To Avoid A Data Breach Or Pay Big Bucks To Clean Up The Mess

ADAM SMITH | DATA PRIVACY SOLUTIONS | AUG 19, 2013

Empirical Analysis of Data Breach Litigation, indicated that the average settlement amount in data breach cases was $2,500 per plaintiff. This is staggering for two reasons. First, many companies are employing cloud-based information management systems. While these systems can lead to cost savings through efficiently retaining customer data, they can also leave the company vulnerable to a sweeping breach as these systems generally hold all customer data in one location. Thus, a breach of the system can mean a loss of information for every customer in a company's book of business. Second, data breach plaintiffs will generally file class action lawsuits with the class encompassing the entire group of breach victims for a particular breach. Additionally, notwithstanding a company's potential liability for damage awards or settlement amounts, the average cost of attorney fees associated with defending a data breach lawsuit is approximately $2.1 million. *See Empirical Analysis of Data Breach Litigation, supra.*

Verizon RISK Team, 2013 Data Breach Investigations Report (2013) *identified: 47,000+ reported security incidents; 621 confirmed data disclosers; and at least 44 million compromised records.* Over the past nine years, Verizon has identified over 2,500 data disclosures and 1.1 billion compromised records. Another study from Ponemon Institute, Perceptions About Network Security (2011), indicates that 90 percent of the companies surveyed had at least one data breach.

The potential monetary impact of a data breach strongly encourages preemptive measures. A company's probability of experiencing a data breach demands them. Otherwise companies can expect to pay significant costs once an impending data breach strikes.

ADAM SMITH

Read More