KRASNOW SAUNDERS
KAPLAN & BENINATI LLP

500 North Dearborn Street, Second Floor
Chicago, IL 60654
312.755.5700 p 312.755.5720 f
krasnowsaunders.com

# 5 STEPS TO PROTECT YOUR BUSINESS FROM PRIVACY RISKS

**1. Recognize that your company is in the data business.**

Every company collects information about its employees, suppliers, and customers regardless of whether it manufactures products or provides services, and regardless of its industry. Many companies, however, do not have a thorough understanding of what information they collect or how they use and store it. This can create problems because a company cannot determine whether or not it lost data if it doesn't know what information it collects and stores in the first place.

**2. Give serious thought to what data is collected and how it is used.**

Business data takes many forms. It frequently includes personnel records, logistical data, sales records, account reconciliations, payment information, names and contact information, market research, and customer-specific requirements. This is a lot of information. Each company should conduct an inventory of its data that: (1) identifies the types of records it collects and maintains, (2) profiles how and where that data is stored, and (3) documents how information is shared with third parties. The inventory should also categorize records by their sensitivity.

**3. Develop policies and train employees.**

A data inventory is only the first step. Once a company understands its data, it needs policies to regulate who can access each type of information and under what circumstances it can be disseminated. Additionally, employees need to be trained to follow the policies and understand the sensitive nature of the data they deal with everyday. Employee training is critical: a 2014 study conducted by the Ponemon Institute found that 31% of data breaches with a result of employee (*i.e.*, authorized user) negligence. In other words, a company can reduce its data breach risks by training and supervising employees' compliance with sound policies.

**4. Start monitoring systems for data breaches.**

Every company needs an information technology professional to implement security safeguards and monitor for unusual and anomalous system usage. Last year, the Ponemon Institute's "2014 Cost of Data Breach Study: United States" found that approximately 25% of reported data breaches were caused by system glitches and 44% of breaches were caused by malicious criminal attacks.

**5. Develop and regularly update the data breach response plan.**

Data breaches are costly. In addition to incurring direct costs of responding to a breach, companies may suffer indirect loses. For instance, customers may terminate their relationships with a company that suffers a data breach and fails to respond timely in a way that protects the customers from harm. Although the costs of data breaches is increasing, companies with strong security and incident response plans in place prior to the breach sustain fewer expenses.

Every company needs an incident response plan that, at a minimum, sets forth what should be done after a data breach has been detected: (i) to prevent negative public opinion and media reports; (ii) to prevent the loss of customers' and business partners' trust and confidence; (iii) if the breach involves proprietary information or intellectual property; and (iv) to notify victims and regulators of the breach. Response plans should be updated regularly and companies should run "fire drills" to test the effectiveness of their plans.