CARLTON FIELDS

Start a Five-Step Privacy Program for Your Business

March 05, 2013

A business cannot get away with a mere privacy policy anymore—it needs a privacy program. But what does that mean? Must you hire an entire staff and invest huge sums of money to guard against a potential or hypothetical risk? No. Instead, take the following five steps to put your business on the right privacy protection track. **STEP 1 – Assign an Owner** Someone must be in charge and accountable for privacy within your organization. This "privacy officer" should be in a senior leadership position and must be at the table when risk and business decisions are made. By choosing a senior leader for this role, you will signal to your employees and customers that your business takes privacy matters seriously, and is committed to protecting information and providing adequate security. **STEP 2 – Know What Data You Collect and Store** Every organization must know what data it collects, why it is collected, where it is stored, and for how long. The senior privacy officer in your organization should collaborate with leaders from operations teams throughout your organization and determine what personal information is collected; why and how it is collected; how it is secured; how long the information is kept; who it is shared with and, if shared, how it is transmitted to third parties. Understanding how your organization collects and uses data will allow you to more easily comply with regulations and best business practices. Additionally, it will allow you to deliver more transparent privacy policies to employees and customers. **STEP 3 – Know the Rules** External rules governing how your organization manages data include laws, regulations, industry best practices, and contractual obligations. Laws vary from jurisdiction to jurisdiction and in many cases may overlap. Depending on your industry, your organization may also be subject to regulation by state, federal, and international agencies and regulatory bodies. For example, the health care industry and its "business associates" must comply with HIPAA regulations and the U.S. financial industry is regulated by the FTC, the FFIEC, the NCUA, FDIC, and the Federal Reserve Board. **STEP 4 – Create a Uniform Privacy Policy and Make All Data Practices "Process Based"** Document your internal privacy standards and rules. Every organization needs written privacy guidelines, standards, and processes. These inform and direct employees regarding their behavior and safe data management. Staff must also be trained regularly to ensure they understand the rules, which constantly change, and that they are complying with your privacy program. **STEP 5 –Evaluate, Reassess, and Improve** Privacy policy, threats, vulnerabilities, regulations, and processes are constantly evolving. Once an organization has completed steps one through four, it must evaluate its

process by creating analytics that measure performance; reassess and identify new needs, threats, obligations, and vulnerabilities; and improve the privacy program as needed. A privacy program must be agile and dynamic. As technologies change, and more and more data is collected and stored, new threats will arise. A nimble privacy protection program will allow your organization to rapidly respond to new regulations, threats, and customer concerns.

Related Practices

Business Transactions
Cybersecurity and Privacy