At Risk: Your Business

Data Security Compliance Can Save Your Firm

Compliance: For Small and Big Companies Alike

When you think of "compliance," we suspect you immediately think of something only large companies have to address. But, data security compliance is no longer just for the Fortune 500 – **all businesses need to safeguard personal information and be prepared to respond to breaches of that information**. It's the law, it helps to minimize risk, and it's good business.

Increasingly, small businesses are faced with a constant flow of federal and state compliance mandates, ranging from the rules that govern a business' products and services to health care reform, employment law (e.g., ADA, FMLA, I-9, background checks), OSHA, etc. Business owners know "compliance" is expensive, but paying fines attributable to non-compliance is even costlier. Few areas of non-compliance can drain a company's bank accounts as fast as inadequate data security compliance. Company financial assets are not the only targets of an attack. Personal information of employees and customers can be used by criminals to commit identity theft, open fraudulent medical insurance policies, file false tax returns, and so forth. It is no wonder that for the past twelve years identity theft-related crimes are the ones most reported to the Federal Trade Commission.

Laws on the Books

Fueled by the explosion of personal smart phones and other devices capable of storing huge amounts of data, the identity theft epidemic has instigated laws at the federal and state levels directed at businesses of all sizes. These laws include:

- Data breach notification mandates in 47 states as well as a number of cities and other jurisdictions.
- Affirmative obligations to adopt reasonable safeguards to protect personal information, including written policies and contracts with vendors. Examples include California, Connecticut, Maryland, Massachusetts, Oregon, and Texas.
- A broad variety of Social Security number protections enacted in all states, such as posting and safeguarding requirements.
- Record destruction mandates in many states to ensure that personal information is properly destroyed or otherwise rendered unreadable before it is discarded.

What Should Businesses Do?

There are five critical components (shown on right) businesses should approach with competent counsel and risk management business partners, ranging from awareness to protection to a response plan. Each component requires careful and thoughtful planning and execution. Since businesses, especially small and midsize, may not be in a position or have the internal expertise to do all that is needed, we suggest seeking outside assistance. Solutions like First Watch's SB 360 product (www.firstwatchcorp.com/sb) address all of these components. But, regardless of how you handle this area, please safeguard your firm's data and prepare for a data breach: it's not a matter of "if" but a matter of "when."

"Why are the bad guys targeting small businesses? Because SMBs often lack adequate security practices. So, what we're seeing is attackers moving down the supply chain and choosing to breach the lesser defenses of a small business that may have business relationships with a larger company."
Byron Acohido, USA Today, April 16, 2013

"According to the National Cyber Security Alliance, one in five small businesses falls victim to cybercrime each year. And of those, 60 percent go out of business within six months after an attack."
Robert Strohmeyer, PC World, Aug. 12, 2013.

There are five critical components for businesses to follow:

- Awareness / Education
- Risk Assessment
- Admin / Physical & Technical Policies
- Insurance / Risk Protection
- Data Breach Response Plan

About the Author

Joe Lazzarotti is a partner with the Jackson Lewis law firm and head of its Privacy, eCommunications and Data Security Practice Group.

jackson lewis
all we do is work