Top Ten Recommendations for Improving Your Company's Data Security Compliance

Aug 04, 2009 Top Ten

Salvatore Colletti, Chief Privacy Officer, Pfizer Inc, **Divonne Smoyer & Bernard Nash**, Partners, Dickstein Shapiro LLP

The combination of increasingly complex laws and a dramatic increase in data losses makes data security compliance an urgent matter for corporate counsel. In recent years, the body of federal and state laws governing data security and data privacy has expanded. In the last seven years alone, 45 states – plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands – have passed laws imposing notice obligations on entities experiencing a data breach. States also have enacted a slew of data protection laws intended to safeguard information. In the same time span, the frequency of hackings, phishing scams, stolen laptops, and other data losses has increased. Since 2005, breaches have resulted in the exposure of more than 250 million records and have caused businesses to incur substantial expense: by some estimates, the average breach costs more than $6.5 million. Aside from cost, breaches can also lead to negative press and high profile investigations and lawsuits by federal and state enforcement officials and the plaintiffs' bar, and can irreversibly tarnish a company's image. Therefore, companies should take proactive, affirmative steps to ensure the protection of confidential data. Below are ten recommendations for improving data security:

1. Account for Existing Laws and Regulations

No one law or regulation governs the whole realm of data privacy and information security. The federal government has taken a sectoral approach to the protection of personal information; laws such as the Health Insurance Portability and Accountability Act (HIPAA), and the Graham-Leach-Bliley and Fair Credit Reporting Acts regulate how certain industries protect information. At the state level, more and more states are enacting breach notification laws as well as establishing minimum safeguards for the protection of personal information, including Social Security number protection laws and data disposal statutes. Companies must be aware of this patchwork of laws and regulations and understand how it applies to their business operations.

2. Prepare for New Federal and State Laws and Regulations

As the data security legal landscape changes rapidly, companies must stay on top of new and proposed laws that may affect their businesses. Many new laws have wide ranging impact and require significant advance preparation in order for a company to be in compliance with them when they become effective. Recent noteworthy items include:

- The HITECH Act: Part of the stimulus bill signed into law by President Obama on February 17, 2009, the law imposes notice obligations on entities covered by HIPAA when they suffer a breach affecting protected health information. It requires notice of any breach to affected individuals and to the U.S. Department of Health and Human Services. If more than 500 consumers in a state or jurisdiction are affected, notice to the media is also required. A breach of some specific electronic health records requires notice to the Federal Trade Commission (FTC) in addition to affected individuals.

- Massachusetts data security regulations are set to take effect on January 1, 2010, and they will apply to any company that collects or maintains information on a Massachusetts

resident. Among other things, these regulations mandate that companies adopt a comprehensive written security program, encrypt personal information stored on laptops and portable electronic devices, and document actions taken in response to breaches.

- Federal data breach notification legislation (H.R. 2221, the Data Accountability and Trust Act) is moving through the U.S. House of Representatives. The bill requires entities possessing personal information to establish and implement certain data security measures, and mandates notice to the FTC in the event of a breach. The legislation, as currently drafted, would preempt state breach notice laws, be enforceable by the FTC and state Attorneys General (AGs), and permit civil penalties of up to $5 million for violations.

3. Consider International Laws and the Impact of Transferring Data Between Countries

Companies must consider international data protection and security laws. A growing number of countries have substantive data protection requirements, and in some cases, breach notification requirements. American businesses need to be aware of the contours of these laws and how they are triggered. Further, companies transferring data between countries must understand and comply with the growing number of laws regulating data transfers. For example, the European Commission (EC) Directive on Data Protection prohibits the transfer of personal data from the European Union (EU) to other nations unless certain privacy protection standards are met. Many U.S. companies dealing with data transfers from EU countries have adopted the "Safe Harbor" principles, which were created by the U.S. Department of Commerce, in consultation with the EC, to provide a streamlined means for U.S. businesses to comply with the EC Directive.

4. Monitor Computer Systems to Detect Any Weaknesses and Intrusions

Intrusions caused by hackings and malware (software designed to infiltrate or damage a computer system without the owner's consent) can result in unauthorized access to private information. A 2009 study conducted by the Verizon Business RISK team analyzed approximately 600 breaches, involving more than a half-billion compromised records, from 2004 to 2008, and found that hacking and malware are the leading causes of breaches. Firewalls, virus protection software, and anti-spyware programs have been effective in thwarting many of these intrusions. Because cybercriminals constantly employ new techniques to circumvent protections and steal information, companies must stay vigilant by monitoring computer systems, updating anti-virus and anti-spyware software programs, and diagnosing and addressing potential vulnerabilities.

5. Assess (and Reassess) the Sufficiency of Company Data Security Policies and Train Employees on Such Policies

Because technology is rapidly evolving, laws are changing, and business practices are frequently modified, it is important for companies to periodically assess and update their data security policies. Companies should review the adequacy of data security measures at least once a year, or whenever there is a material change in business practices that could implicate the security of personal information. Yet policies themselves are not sufficient if they are not enforced. Therefore, a company should conduct compulsory employee trainings on company policies and procedures, and should measure employees' meaningful compliance with them.

6. Limit the Amount of Personal Information Collected and Stored and Establish Mechanisms for Disposal of Personal Information

Businesses should collect only information that is necessary for business purposes so as to mitigate risk and minimize the scope of any data loss. However, dealing with sensitive information is a necessary part of business for many companies. Therefore, appropriate disposal mechanisms should be in place so that private information leaving the company is not at risk of exposure; a system for shredding, erasing, or otherwise modifying records so that they are unreadable or indecipherable is essential.

7. Ensure Data Security Practices of Third-Party Contractors Are Adequate

Many companies incorrectly believe that if a third-party contractor loses sensitive data belonging to the company, there are few or no implications for the company. In actuality, most of the burden of handling the breach will fall on the company. Under the state breach notification laws, for instance, a third party contractor maintaining data on another company's behalf merely has an obligation to notify the data owner, who, in turn, must notify the affected individuals. When dealing with contractors, therefore, there are a number of steps a company should take to ensure the protection of data. Security audits and contractual provisions requiring third parties to protect sensitive information are essential. Companies should also limit the personal information collected by contractors and limit the time contractors are permitted to retain such information. Further, businesses operating as third-party contractors should themselves assess their security procedures and make sure they are aware of their legal and contractual obligations.

8. Develop an Incident Response Plan for Losses of Personal Information

Despite a company's best efforts to enact state-of-the-art privacy policies and procedures, data losses can and do occur. These incidents are often complicated and require time to investigate the circumstances of the breach, assess the nature of the risk, and determine what was exposed and whether notifications may be required. To avoid loss of valuable time, having a dedicated internal team in place and strong relationships with forensics firms and outside counsel are important measures. A well-conceived incident response plan can make the difference between a company making timely notifications, versus opening itself up to investigation or potential lawsuit.

9. Encrypt Private Information

By encoding information so that it is rendered unusable, encryption technology ensures that sensitive information cannot be misused. Encryption is a powerful data protection tool that is useful particularly for portable electronic devices (e.g., laptops, Blackberries) and sensitive data that is transferred electronically. Almost all of the state data breach notification statutes exempt companies from having to report a data loss when the exposed personal information is encrypted. With the costs of notification, the average breach is estimated to cost millions of dollars, so investing in encryption technology can be a cost-effective prophylactic measure.

10. Do Not Forget Paper Records

When assessing data security compliance, many companies tend to focus predominantly on electronic records. However, paper records often contain sensitive personal information that is susceptible to unauthorized access or disclosure, and companies that have improperly disposed of such records have been the subject of significant investigation and litigation, including by state AGs. Company policies and procedures must therefore account for both electronic and paper records containing sensitive information.

The authors would like to thank Ryan Mehm of Dickstein Shapiro LLP for his contributions to this piece.

http://www.acc.com/legalresources/publications/topten/top-ten-recommendations-for-improving-your-company.cfm