The Encryption "Magic Bullet"

How to Make Sure Your Encryption Solution Hits the Target

09.23.2010

William R. Shenton
Pamela A. Scott

Every organization in business today is holding personal information about individuals. Whether they are consumers, customers, clients, patients, employees, or business partners, you collect a mass of personal information about them, such as Social Security numbers (SSNs) and other government-issued identifiers, consumer reports, background checks, test results, medical files, financial or health information, and perhaps even biometric data.

Forty-six states, the District of Columbia, the Virgin Islands, Puerto Rico, the Federal Trade Commission, Federal Financial Regulators, and the Department of Health and Human Services all have adopted some form of notification requirement that will obligate you to notify individuals if their information is affected by a security breach. You also may have to notify regulators, consumer reporting agencies, and the media, depending on which laws are implicated. But these laws, despite their diversity on other topics, all have one thing in common: if the data affected was encrypted and the encryption key was not compromised, the breach does not have to be reported. With the average security breach estimated to cost $6.75 million (according to the Ponemon Institute's 2009 study on the topic), is it any surprise that organizations are rushing out to purchase encryption solutions for their laptops, thumb drives, PDAs, and even internal systems? In fact, encryption is required in certain circumstances by HIPAA, Nevada state law, Massachusetts regulations, and numerous state laws governing use of SSNs.

But before you hurry out to snap up the first encryption package a vendor dangles in front of you, please make sure the solution will actually provide the "magic bullet" you are seeking. Be aware that the laws at issue vary in what they are willing to consider "encryption."

At least one state specifically sets a floor on acceptable encryption technology, requiring at least 128-bit encryption. Others will require you to meet a security standard that may change over time, such as specifications issued by the National Institute of Standards and Technology. Others may not define encryption or will use the following (or similar) language: "Encryption means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key." You should also keep in mind that several of these laws may apply to your business, meaning that you will have to reconcile the requirements before choosing a solution. While some apply only in certain specific circumstances (e.g., transmission of SSNs over the Internet, information handled by your health plan), others apply based on where you do business. Still others apply based on the residency of the individuals whose information you hold. That means that if you have employees or

customers in multiple states, several different definitions of encryption could be relevant to your identification of an appropriate encryption solution.

Our Privacy and Information Security Practice can help your company identify the legal requirements that apply to the sensitive personal information you hold, and map a strategy to implement encryption as part of a comprehensive data management and security plan.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075