



Conforming to the Myriad of State Data Privacy Laws: A Daunting but Manageable Task Mark Seward, senior product manager, Qualys, Inc.

In 2004, over 10 million people were victims of identity theft caused by data security breaches. Over 20 states have enacted data privacy laws outlining penalties that can result in fines and jail time. Vulnerability management with QualysGuard can help stop customer data leaks and protect your company and your customers.

Congress estimates that nearly 10 million people were victims of identity theft in 2004 alone¹. In some cases the corporate custodian of the customer data deemed the breach not significant. However, in other cases, the breach was of such staggering proportions that customers were notified by the company or governmental agency. Even when customers were notified, this notification was generally made after the fact by days, weeks, or even months.

In the past several years, a number of high profile network security breaches have resulted in the loss of enormous amounts of private personal and financial data opening the door to identity theft for millions of individuals. Indeed only a year ago a massive breach at the CardSystems network focused attention on the Payment Card Industry Data Security Standard (PCI) introduced by MasterCard International, Inc. and Visa U.S.A., Inc. This was a courageous move on their part which established a standard. When such standards are established, companies have a measured, understandable way to make progress toward data security.

Breaches of the kind mentioned above have a variety of causes. Everything from social engineering schemes to simple mis-configuration of servers and hosts to spyware and adware to malicious attempts to take advantage of known software vulnerabilities have been causes of security breaches and identity theft.

Legislators React

With individual corporations responsible for deciding under what circumstances customer notification would take place and deciding when notification would occur, the possibility for abuse of the public trust was substantial.

This situation coupled with some high profile security breaches raised awareness with politicians and their constituencies. The first legislative body to react was the State of California in 2003.

¹ Source: section 2 (3), Personal Data Privacy & Security Act of 2005

The Security Breach Information Act, California Civil Code § 1798.82 et seq., was the first law passed in the United States that requires notification to customers of companies that do business in California for security breaches of personal information and notification required by the law must occur "in the most expedient time possible and without unreasonable delay.". Customers injured by violations of the statute can bring private lawsuits for damages. With the size of the California economy, the law effectively impacted almost any company engaged in electronic commerce and certainly gave added weight to the need for more careful handling of personal data.

Personal Information, in the California law, is defined as “the first name or initial and last name of an individual, with one or more of the following: Social Security Number, driver’s license number, credit card or debit card number, or a financial account number with information such as PIN numbers, passwords or authorization codes that could gain access to the account.”² Although meant to cover the data relationship between company and customer, it has been determined that the law covers the company and employee relationship as well.

The California law goes on to address financial penalties, types of notification of customers, notifications to the media and possible prison time. Although there are a few exemptions included in the California law, the most important is encryption. Maintaining personal data in an encrypted format brings the likelihood of a serious breach causing harm to nearly zero. This was considered to be a piece of ground breaking legislation, a bellwether law and a blueprint for other states.

Since 2003 over 20 states have enacted very similar laws regarding security breaches and notifications (see Table 1). All of these laws address the breach/notification scenario in a way similar to the California law. Many of these new laws also identify encryption is a safe-harbor for customer data. A few examples of key differences include: an expanded definition of personal information in the North Dakota law to include electronic or digital signatures and marriage certificates; very specific information about notifications in the North Carolina law; and, an expanded definition of the types of businesses subject to the law (corporations, partnerships, sole proprietorships, joint stock companies, or any other legal entity), in Louisiana.

Federal legislation that would preempt state law is being considered. Most companies that do business in many states would rather operate under a single Federal standard. However, in the absence of national legislation, state law compliance remains a priority for companies holding personal data in those affected states and industry pressure and standards such as the Payment Card Industry (PCI) standard puts the onus on compliance for most business which swipe magnetic card transactions.

Nearly every organization maintains some records that contain some level of personal data and the more personal data that is stored by companies, the greater the risk of identity theft and the

² PROSKAUER ROSE LLP, Updated January 2006: States Continue To Pass Security Breach Notification Laws: Businesses Must Comply With Various And Sometimes Conflicting Regulations:
http://www.proskauer.com/news_publications/client_alerts/content/2005_12_13/res/id=PDF/11105-121305-Security%20Breach%20Notification%20Laws-ca-v4.pdf

misuse of personally identifiable information. As data is not always maintained in an encrypted state, there are many points at which networks are vulnerable to intrusion and data is vulnerable to Identity Theft. Vulnerable hosts is subject to malicious attack. Key loggers, Trojans, worms, viruses and simple misconfigurations can result in a trickle or a flood of customer data leaving the organization.

The QualysGuard Solution for Vulnerability Assessment and Management

QualysGuard® vulnerability management gives companies an easy way to assess, prioritize and remediate network vulnerabilities which helps avoid the triggering of security breach laws and lowers the level of risk faced by companies that handle customer or employee private data. Regular scheduled network maps and scans using QualysGuard allows customers to address threats from ad-ware, spyware, software based key loggers and mis-configurations that can result in the loss of personal data.³

QualysGuard helps with automating the detective portion of these controls by allowing the user to create a report template that specifically includes Qualys checks (QIDs) from the malware and patches categories. Using this report the status of particular asset groups or the enterprise can be assessed on a regular basis. Add to this template password and patch related checks as a way to complete a strategy for Data Privacy Compliance and network security audits.

The process of remediation of hosts that are found to contain malicious software is built into QualysGuard. Remediation tasks can be assigned to specific users with pre-defined deadlines for these tasks.⁴

QualysGuard is an important part of an overall malware strategy that is part of a data privacy strategy for the enterprise that is then part of a top-down risk mitigation strategy for the enterprise that can provide assistance in compliance with state data privacy laws.

³ This addresses the “Malicious Software Prevention, Detection and Correction” control in CobIT 5.9, and, sections 8.3 and 8.3.1 of ISO 17799 – “Protect Against Malicious Software,” and, “Detect and Prevent Malicious Software” respectively.

⁴ This addresses the “Remedial Actions” control in CobIT ME1.6 and, section 6.3 of ISO 17799 – Respond to Information Security Incidents.

State	Law	Safe harbor for encrypted data?
Arkansas	SB 1167 (Act 1526)	Yes
California	SB 1386	Yes
Connecticut	SB 650 (Public Act 05-148)	Yes
Delaware	HB 116 (amendment to Title 6, Chapter 12b of the Delaware Code)	Yes
Florida	Bill 481 (Chapter No. 2005-229)	Yes
Georgia	SB 230 (Title 10, Chapter 1, Article 34 of Official Code of Georgia)	Yes
Illinois	HB 1633 (Public Act 94-0036)	No
Indiana	SB 503 (Act 503)	No
Louisiana	SB 205 (Act 499)	Yes
Maine	LD 1671/HP 1180 (Sec. 1. 10 MRSA c. 210-B)	Yes
Minnesota	HF 2121	Yes
Montana	HB 732	Yes
Nevada	SB 347	Yes
New Jersey	A-4001/S-1914	Yes
New York	A-4254, A-3492	Yes
North Carolina	SB 1048	Yes
North Dakota	FRBS-0500	Yes
Rhode Island	H 6191	Yes
Tennessee	SB 2220/PC-0473	Yes
Texas	SB 122	Yes
Washington	SB 6043	Yes

Table 1 -- Current Applicable State Laws for Data Privacy and Notifications⁵

⁵ Identity Theft and U.S. Data Protection Legislation: An Overview, GuardianEdge Technologies, December 2005, www.guardianedge.com