

OutSecure, Inc. 'Survival of the Securest'



Contending with California Privacy Legislation

Minimizing Exposure to A.B. 1950, S.B. 1, and S.B. 1386

Executive Summary

Whether an institution is based in California or not, if it does business with or stores the personal data of even one California resident, the implications of several pieces of California privacy law can be profound. This document outlines several rules enacted in California that target data privacy, and describes a solution that helps organizations address today's critical security threats and the increased exposure presented by California legislation.

State Laws with Global Implications

Organizations that store or manage the personal data of California residents are being compelled to rethink the ways they guard this information. While the costs of data theft have already been steep, several pieces of California legislation are serving to up the ante when it comes to the repercussions of security breaches, both from a legal, financial, and brand awareness perspective.

Following is an overview of a few of these mandates:

California's Database Security Breach Notification Act, S.B. 1386

Passed in 2002, this law provides strict requirements for notification of consumers following any breach of unencrypted personal data. This includes any combination of an individual's name and such data as credit cards, social security numbers, driver's license numbers, and other information.

California Financial Information Privacy Act, S.B. 1.

This rule, which took effect in July of 2004, imposes steep fines for the disclosure of personal financial information. This law covers both intentional sharing of private financial information as well as the disclosure of data as a result of negligence or security breaches.

Fines of up to \$500,000 may be assessed in the case of a large-scale breach.

California's General Security Standard for Businesses, A.B. 1950

This rule, which took effect in January 2005, requires organizations that manage personal information to implement security procedures to safeguard that data. This law offers definitions of personal data and states that business managing that information must “implement and maintain reasonable security procedures and practices” in order to protect that data.

While enacted in California, the reach of these pieces of legislation is extremely widespread, potentially affecting any organization that does business with, or in any other way stores or manages the sensitive data of, a California resident.

This document will outline how these legal mandates are placing a premium on ensuring data privacy, and it will detail how OutSecure can help organizations address these mandates.

The Challenge: Ensuring Data Privacy

Just about every sizable enterprise has implemented perimeter security defenses like firewalls and intrusion detection systems. However, the prevalence of data thefts from internal sources, and the fact these perimeter technologies simply aren't fool proof, illustrate that these technologies aren't enough. Today, comprehensive measures need to be taken to ensure data is secured inside the enterprise, which is where the bulk of personal information resides, and where the most devastating thefts occur. To address these threats and minimize the exposure to the impact of California legislation, organizations must ensure data privacy inside the enterprise.

Achieving Data Privacy with OutSecure

Protecting Data Privacy

S.B. 1386 specifies that organizations must “disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” Clearly, encrypting sensitive data is one of the keys to achieving S.B. 1386 compliance, as well as a range of other mandates.

OutSecure works with clients to develop a comprehensive way to encrypt and protect sensitive data at all times, throughout the enterprise. As a result, organizations can better ensure that they are compliant with legislative and policy mandates for security, and eliminate the risks of data thefts.

OutSecure advises flexible implementation options so organizations can deploy in a way that makes sense for their business and security needs—whether at the Web, application, or database level.

Intelligently Protect Sensitive Data

S.B. 1386, S.B. 1, and A.B. 1950 all provide some specific definitions of personal and financial data, which generally constitutes a combination of name and such details as driver's license number, social security number, credit card number, etc.

The reality is that these records are a very small percentage of the volumes of data an enterprise typically manages, but constitute the most critical threat to an organization if that data gets into the wrong hands.

OutSecure helps organizations to protect only the sensitive data that poses a business or liability risk.

Beyond Encryption: Holistic Security Initiatives

Encrypting data alone isn't enough to ensure complete data privacy. For example, if encryption is managed on application servers, data still may not be secure. These servers simply weren't designed for security: they are relatively easy to access, are often misconfigured, and aren't kept up to date with the latest security patches. While encryption can help prevent data theft, ultimately your data is only as safe as the keys that protect it. Whoever has access to the keys has access to your data.

And once an attacker has the key, it's relatively easy to copy, modify, hijack, or destroy sensitive information.

According to SB 1386, a breach is defined as “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.” In other words, organizations need to guard not only against theft, but tampering or disclosure, of personal data.

Address Critical Threats and Privacy Legislation—Cost Effectively

Organizations need to address heightened security risks and exposure, while typically contending with scarce budgets and resources.

OutSecure offers a solution that addresses these security risks, while enabling organizations and fully leverage their existing resources.