PGP® Compliance Brief

May 2008

California Senate Bill 1386

Overview

The landmark California Database Security Breach Notification Act (also called Senate Bill 1386, or SB 1386) took effect in July 2003. It immediately impacted all organizations that do business with California residents, even if the organization is not located in California. Many other states have since enacted similar laws and rules.

"This bill requires a business or a State agency that maintains computerized data that includes specified personal information to disclose any breach of the security of that data to any California resident whose ***unencrypted*** personal information was, or is reasonably believed to have been, acquired by an unauthorized person. By giving consumers such notice, the bill gives them the opportunity to take proactive steps to ensure that they do not become victims of identity theft."[1] In other words, encrypted data is not subject to the bill's notification requirement.

Highlights

- Under SB 1386, "a security breach" is defined by the California Office of Privacy Prevention as, "Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information." "Specified personal information" is defined as *unencrypted* computerized data that includes name and any of the following: Social Security number, driver's license or California Identification Card number, financial account number, credit card number, or debit card number accompanied by its PIN or access code required for account access.[2]
- SB 1386 requires organizations to "disclose any breach of the security of the system … to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[3] Missing data is assumed breached unless proven otherwise.
- SB 1386 applies to all organizations holding personal information of a California resident, regardless of where the organization is based or conducts business.
- Penalties for violations of SB 1386 include civil lawsuits from affected residents or from the California Attorney General.
- SB 1386 does not require organizations to encrypt personal information. It does state that the law does not apply to data that has been encrypted.

Why Enterprise Data Protection?

The spirit of the law calls for organizations to practice due diligence to prevent identity thieves from misusing personal information. Due diligence requires adequate encryption. If an encryption solution fails to adequately protect personal information in all forms (for example, in storage and in transit, in server databases, or on personal computers and laptops) throughout the information lifecycle, the organization can be found negligent and therefore liable.

In part because of laws such as SB 1386, the cost of a data breach now approaches $200 per record.[4] An organization can avoid millions of dollars in expenses and protect its reputation and brand simply by encrypting sensitive or confidential data in storage and in transit.

Encryption is the Protective layer of enterprise data protection, which comprises the strategy, technologies, and processes that work together to ensure data security. Effective enterprise data protection includes these four components:

- **Protection** of data with encryption
- Controlled **Access** to data with strong authentication and authorization systems
- **Detection** of data at risk, to prevent data leakage
- Comprehensive **Management** of data throughout its lifecycle, from creation through archive

The California Office of Privacy Protection specifically recommends, “Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information. Data encryption should meet the National Institute of Standards and Technology’s [NIST] Advanced Encryption Standard [AES].”[5]

Best Practices

Best practices for enterprise data protection that are recommended by the California Office of Privacy Protection include:

- Conduct an information asset inventory to determine which assets contain personal information.
- Protect higher-risk personal data using data encryption in conjunction with access control, host protection, and centralized management.
- Use standard AES encryption solutions with centralized key and policy management. (Some states also specify rules for protecting encryption keys.)
- Track data security breaches through central logging and auditing of all cryptographic functions and access. Lost or missing data that was encrypted is not considered breached.

Why PGP Encryption?

PGP Corporation is the leading provider of data and email encryption solutions. Its award-winning solutions free organizations from the penalties associated with SB 1386 security breaches. PGP® encryption technology is one of two data security standards recommended by NIST.[6] Further, NIST qualifies AES algorithms as providing the highest level of security[7], and AES algorithms are the core of PGP encryption technology.

All PGP encryption applications are managed through the central PGP® Encryption Platform. This flexible platform enables phased deployment of encryption applications. For example, an organization may begin by encrypting its email in transit, and later use the same platform to extend encryption to laptop computers and USB drives. Major features of the award-winning PGP Encryption Platform include:

- Centralized policy and key management
- Centralized logging and auditing of encrypted devices
- AES encryption of data in transit and at rest, even beyond the enterprise network
- Patented PGP Additional Decryption Key (ADK) technology that ensures access to data protected by lost or forgotten keys

PGP encryption applications that can protect organizations from violating SB 1396 include the following:

- PGP® Whole Disk Encryption: Enables encryption of files on desktop and laptop computers and removable media
- PGP® Endpoint: Prevents data loss resulting from the use of unauthorized devices and connections
- PGP® Mobile: Provides proven, easy-to-use data encryption for smartphones
- PGP Universal™ Gateway Email: Automatically encrypts email messages, without requiring client software
- PGP® Desktop Email: Provides automatic end-to-end encryption of email messages
- PGP® Support Package for BlackBerry®: Extends PGP Desktop Email functionality to BlackBerry devices
- PGP® Command Line: Encrypts and signs information for bulk data storage, FTP transfer, and backup
- PGP® NetShare: Encrypts network-based files and folders for collaborating teams

Learn more about enterprise data protection and PGP data encryption solutions at www.pgp.com, or contact your PGP account representative.

PGP invites peer review of its source code, which is available online for download at http://www.pgp.com/downloads/sourcecode/index.html.

References

[1] http://www.oispp.ca.gov/consumer_privacy/privacy_leg/leg2002.asp

[2] *Recommended Practices on Notice of Security Breach Involving Personal Information*, California Department of Consumer Affairs, Office of Privacy Protection, http://www.oispp.ca.gov/consumer_privacy/pdf/secbreach.pdf- 2007-08-03, p. 7

[3] SB 1386 Bill (full text): http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[4] *2007 Annual Study: U.S. Cost of a Data Breach*, The Ponemon Institute, November 2007, http://www.pgp.com/downloads/research_reports/index.html

[5] *Recommended Practices on Notice of Security Breach Involving Personal Information*, California Department of Consumer Affairs, Office of Privacy Protection, http://www.oispp.ca.gov/consumer_privacy/pdf/secbreach.pdf- 2007-08-03, p. 10

[6] NIST, *Guidelines on Electronic Mail Security*, p. 3-2 http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf, February 2007

[7] NIST, *Guidelines on Electronic Mail Security*, p. 3-2 http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf, February 2007