

VORMETRIC WHITE PAPER

California SB 1386 & AB 1950: Implementing Effective Encryption Protection for Personal Information Privacy

A comprehensive information protection strategy enables organizations to avoid exposure to personal data privacy legislation



VORMETRIC

Copyright © 2005 Vormetric, Inc. All rights reserved.

Vormetric, CoreGuard, MetaClear are trademarks or registered trademarks of Vormetric, Inc. in the U.S.A. and certain other countries. Other names and products are trademarks or registered trademarks of their respective holders.

This document contains Proprietary and Confidential Information of Vormetric, Inc.

The information in this document is subject to change without notice and must not be construed as a commitment on the part of Vormetric, Inc. Vormetric, Inc. assumes no responsibility for any errors that may appear in this document. No part of this documentation may be reproduced without the express prior written permission of the copyright owner.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.

Vormetric is not a law firm, this document was not prepared by lawyers, and Vormetric is not offering legal advice. Should you require legal advice on how CA SB 1386/AB 1950 affects your business, you should consult a law firm.

Perspective

California's SB 1386, operative since July 1, 2003, was created in response to the rising rate of identity theft as a result of compromised personal information. SB 1386 affects any state agency, business, or person that conducts business in California and maintains computerized data that includes personal information. Security analysts believe that most large companies, whether actually domiciled in California, will thus be affected. SB 1386 states that any breach of the security of the data must be reported in the most expedient time possible following the discovery of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.¹ Personal information is defined as an individual's last name and first name or initial, in combination with a social security number; driver's license or California ID Card number; or account, credit or debit card number, in combination with any security code, access code or password that would permit access to the account. Failure to promptly notify the information owner or licensee of the data makes the organization liable to civil action to recover damages.

AB 1950 takes personal data privacy a step further, requiring that businesses owning or licensing such personal information about a California resident, when held in unencrypted form, to implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification, or disclosure.²

SB 1386 and AB 1950 are having a significant impact on the way an enterprise protects its electronic data due to the potentially severe penalties that can be inflicted by class-action lawsuits and other potential penalties that may be levied against the organization for negligence in exercising an adequate standard of care. Additional costs that can be attributed to SB 1386 and AB 1950 include the damage to image, reputation and brand resulting from public awareness of security breaches, the cost of notifying data owners, and the cost of defending lawsuits brought against the agency or enterprise. Data privacy legislation modeled after California bills has been introduced at the federal level as well, which should have the effect of making the identity theft issues raised by the California legislation of even greater concern nationally.

The Role of Encryption as a Security Mechanism

Differing interpretations in the media of the intent and effects of SB 1386 indicate that significant confusion exists regarding the role of encryption in excusing liability for safeguarding personal information. The bill states that any breach of the security of the data in the system shall be disclosed following discovery or notification to any resident of California whose "*unencrypted*

¹ California State Senate, "BILL NUMBER: SB 1386 CHAPTERED BILL TEXT," September 26, 2002, <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>, (5/28/03).

² California State Senate, "BILL NUMBER: AB 1950 CHAPTERED BILL TEXT," September 29, 2004, <http://info.sen.ca.gov/pub/03-04/bill/asm/ab_1901-1950/ab_1950_bill_20040929_chaptered.html>, (12/23/04).

personal information was, or is reasonably believed to have been, *acquired by an unauthorized person*.”³ While some have chosen to interpret the use of data encryption by the organization as an automatic exemption to the law, a more accurate interpretation of the law's intent points to the function of encryption as a security mechanism. If the encryption method used to safeguard personal information is defeated by an unauthorized person, as is known to frequently happen with other traditional security measures, such as firewalls, then the data should be assumed to be acquired in unencrypted format and the agency or enterprise is responsible for notifying data owners under SB 1386. Defeating the data encryption may be accomplished by acquiring authorized user status on a host upstream from an inline data encryption device, for example, allowing the attacker to access information in cleartext form. Only in the case where the data is acquired while unmistakably still in ciphertext form, such as via theft of backup media, is the enterprise not required to notify data owners.

Similarly, AB 1950's definition of 'personal information' as a name or a defined data element that is not encrypted or redacted is vaguely worded. While encrypted data is clearly exempt from the rule, a defeated encryption mechanism that allows the information to be received by the unauthorized user in cleartext form would not be interpreted as a loophole to the legislation.

The exemptions in SB 1386 and AB 1950 for encrypted data theft also highlight another ambiguity—the lack of definition of qualifying encryption. Instead, the bill puts the onus on the organization to support the current standard for adequate data protection. Diligent security practices for protecting data at rest now call for a minimum 128-bit key length for symmetrical encryption keys (i.e., 'strong' encryption). The use of weaker encryption, or the practice of encrypting only short fields (which is inherently weak), may allow ciphertext data to be cracked in hours or even minutes using a fast computer. As a result, data acquired by unauthorized persons in encrypted format—ostensibly releasing the enterprise from its responsibility—might be subsequently decoded in a short period of time, leaving data owners vulnerable to the exploitation of their personal information by identity thieves. Only if an enterprise uses strong encryption (e.g., AES, 3DES), and the encryption key was stored in such a way that it could not have been obtained by the attacker, can it be reasonably assumed, post-attack, that unencrypted personal information was not acquired by an unauthorized person.

In order to help clarify these ambiguities, the California Office of Privacy Protection has published their “Recommended Practices on Notification of Security Breaches Involving Personal Information.” Recommended safeguards include the implementation of host protection and access control functionality to support data encryption wherever feasible, and specifies the use of AES encryption technology.⁴ As this is not a legally binding set of practices, however, court cases will be required to formally clarify this issue over time.

³ California State Senate, “BILL NUMBER: SB 1386 CHAPTERED BILL TEXT,” emphasis added.

⁴ California Office of Privacy Protection, “Recommended Practices on Notification of Security Breaches Involving Personal Information,” Oct. 10, 2003, < <http://www.privacy.ca.gov/recommendations/secbreach.pdf>>, (11/4/03).

Protecting Vulnerabilities to Data Theft

The intent of California data privacy legislation is to protect data owners from the exposure of usable personal information to identity thieves. There are, however, many opportunities for attack originating both inside and outside the perimeter that unauthorized users might exploit to obtain or corrupt information. These include the following attacks, based on the vulnerability being exploited:

Root Attack	The ability to illegally obtain 'trusted' root access privileges.
Worms and Trojans	The alternation or insertion of executable code for the purpose of running an unauthorized application.
Buffer Overflow	Overflow of stored data into adjacent buffers, executing code that triggers malicious or unauthorized activity.
Unintended Admin Privilege	The use of privileges to access, copy, or tamper with data outside the requirements of a user's authorized role.
Unauthorized Data Viewing	The use of privileges to view information outside the requirements of a user's authorized role.
Audit Log Tampering	Prevents tampering with audit log files data by restricting access to allow only authorized users and applications.
Physical Theft	The theft of information through extraction from stolen hardware or storage media.

While providing an effective barrier against the unauthorized viewing of information off of stolen media, the ability of encryption alone to protect against unauthorized access to stored data is very limited. Architectural approaches to encryption that provide no linkage into the context of the request at access point, such is the case with inline bulk encryption devices installed into the SAN fabric, are unable to determine the context of I/O requests and generally assume a 'trusted fabric' above the storage layer. Similarly, backdoor access to a server or workstation left open by an unpatched vulnerability or Trojan horse attack provides an opportunity for attackers or root users to obtain access to cleartext information if their identity has not been confirmed by the network authentication service. Storing encryption keys on a host platform where they can be accessed by IT administrators provides another example where a poorly designed architecture provides an opportunity for protected information to be compromised, and defeats the separation of duties principle. Encrypting stored data encryption alone, without integrating host protection and context-aware access control or using an architecture that protects access to encryption keys leaves the organization vulnerable to legal action, since it is unlikely that the courts will accept the solution as meeting the intent of the law. A comprehensive information protection solution with an effective architecture is needed that provides active enforcement for policies defining the appropriate use of personal data.

CoreGuard Protects Sensitive Data from Attack

As discussed, the use of stored-data encryption alone to protect personal data does not provide adequate protection from attack. Vormetric's CoreGuard Information Protection System takes a comprehensive approach to protecting stored data as well as protecting the integrity of the

systems that access stored data. The technologies employed by CoreGuard to prevent identity theft can be segregated into four main functional areas:

- **Transparent, High-Speed Encryption**—The ability to protect stored data in files or databases with strong, policy-based encryption with no significant performance impact.
- **Context-Aware Access Control**—The ability to tightly scrutinize and control each and every attempt to access data through an application or a file system call.
- **Host and Application Integrity Protection**—The ability to prevent unauthorized applications, including malware, from running on protected hosts and enforce change management procedures.
- **Audit and Reporting**—The ability to provide a secure, detailed audit log of all data access events for reporting or forensic analysis.

These four functions work in concert to ensure host and data integrity, and to create a trusted system that is, itself, relatively impervious to attack. The combination of these technologies creates a solution that can effectively thwart threats to personal data, and stop identity theft.

Innovative Architecture

The key to CoreGuard's solution lies in its innovative architecture. The combination of the software PEM that enforces information protection policies at the data access point and the Security Server appliance that provides a secure repository for policies and encryption keys provides benefits in manageability, scalability and security. The insertion of the PEM at the file-system level enables granular inspection of all data access attempts and a high degree of transparency for easy installation and manageability.

Benefits of the CoreGuard architecture include:

- Separation of policy enforcement from policy decision making
- Visibility into the complete context of data access requests
- Separation of duties between IT administration and security administration
- Transparency to applications, DBMSs, network file systems and data storage
- Extensibility across heterogeneous environments and applications
- Scalable and manageable across widespread enterprise networks
- Limited load on host CPU, negligible performance impact on applications
- Policy updates in Security Server eliminates need for host updates

How CoreGuard prevents attacks:

Root Attack	Enables the blocking of all local root user accesses and privileges based on user defined policies. Verifies the use of strong authentication services.
Worms and Trojans	Verifies the authenticity of application code prior to allowing execution, preventing worms, Trojans, malicious code, unauthorized patches and altered code from running and propagating.

Buffer Overflow	Prevents running unauthorized code that triggers malicious activity. Prevents unauthenticated escalation of privileges and unauthorized acquisition of root user status.
Unintended Admin Privilege	Prevents root users and system administrators from accessing or viewing data by blocking execution of unauthorized applications and file system operations.
Unauthorized Data Viewing	Prevents backup administrators and storage outsourcing partners from viewing data under management.
Audit Log Tampering	Prevents DBAs from tampering with audit log files by restricting access to authorized users and applications.
Physical Theft	Encryption of data renders theft of hardware or storage media useless for the purpose of data extraction.

The following table summarizes the effectiveness of various architectural approaches to encryption, and underscores the need for a comprehensive approach to effectively protect the data layer from unauthorized access:

	Privilege Theft	Unintended Privilege	Application Tampering	Hardware Theft	Tape Theft
CoreGuard Information Protection System	●	●	●	●	●
In-line, network file-level proxy encryptor				●	●
Field-level database encryptor (rows or columns—weak encryption)	◐			◐	◐
In-line, block-level encryptor				●	●

So, while several security approaches offer data encryption as a means of securing data, only CoreGuard meets the intent of California privacy protection laws by effectively preventing access and viewing by unauthorized persons either through the access point (server) or via a direct attack on the data at the storage layer.

Solution Benefits

- Transparent encryption installs easily with no application coding changes required
- Policy-based security provides active enforcement of an organization’s appropriate use of information policy
- Comprehensive, integrated solution protects data at rest more effectively than multiple, disparate point products and greatly reduces system management requirements
- Access audit, logging and real-time alert provides forensic data for identifying unauthorized access attempts, as well as a record of all past data access attempts

- Application, database and storage infrastructure transparency supports heterogeneous networks with a single security appliance
- Strong, high-speed data encryption enables storage security without introducing a perceptible performance impact
- Extensible architecture provides local enforcement of information protection policies throughout a widespread IT environment

* * *

For more detailed information on Vormetric's CoreGuard Information Protection System please refer to the following documents available at www.vormetric.com:

Vormetric White Paper: "[Protecting Enterprise Information](#)"

Vormetric Success Story: "[Financial Services Institution Success Story for GLBA Compliance](#)"

Vormetric Success Story: "[University Health Services Center Success Story for HIPAA Compliance](#)"

[CoreGuard Information Protection System Datasheet](#)

[CoreGuard FAQ](#)

Vormetric, Inc.
800.440.2043
www.vormetric.com
sales@vormetric.com

