VORMETRIC WHITE PAPER

Data Privacy Legislation, Regulations and Standards

Vormetric's CoreGuard Data Security System enables organizations to comply with strict guidelines for protecting non-public, personal information

VORMETRIC

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 privacy legislation, regulations and industry standards affect your business, you should consult a law firm.

Executive Summary

The increasing accessibility of personal data and the rapid escalation in identity theft cases has resulted in a spate of regulatory legislation and industry standards targeted at ensuring confidentiality for personal and confidential information. Compliance with these regulations and standards has resulted in new security challenges for security officers and IT executives.

Vormetric's CoreGuard Data Security System integrates strong data access control, host and application protection and selective encryption of stored data, providing a comprehensive security solution that protects the vulnerabilities in the stored information environment and prevents the unauthorized access and viewing of personal and confidential information. CoreGuard enables organizations to meet the data protection requirements of legislative mandates and industry standards.

Perspective

Perhaps the two most significant changes to the business world that have taken place in recent times have been the transition from paper-based record keeping to electronic media-based data storage, and the increased accessibility of that information via far-reaching private and public networks. A growing awareness of the vulnerability of confidential information to breaches of confidentiality has led to the creation of several legislative measures intended to ensure the security of sensitive, proprietary and/or personal data. For most enterprises' security and IT organizations, this legislation and regulation has resulted in a critical need to secure personal and confidential information, as the exposures and penalties have become more severe for organizations that fail to do so.

Compliance Challenges for Information Protection

Complying with these regulations and standards requires in all cases the ability to both tightly control access to sensitive stored information as well as protect the information from unauthorized viewing. Given the exploitable vulnerabilities that exist in data networks, this requires not only strong authentication of users, applications and processes requesting data, but also the ability to protect against host hijacking and unintended administrative privileges as a means of accessing information. In addition, encryption is often recommended and sometimes required as a means of enforcing data access policies. Tying encryption to context-aware data access control allows management to grant storage administrators access to perform data management duties while still restricting data viewing privileges, ensuring confidentiality for stored data while remaining completely transparent to IT operations. Finally, the capability of auditing all data access attempts, both authorized and unauthorized, can demonstrate compliance to audit committees and shareholders, as well as providing a source of evidence for forensic analysis against any unauthorized access attempts.

Traditional security technologies that focus on securing the network perimeter and points of vulnerability within the organization fall short of providing adequate protection for sensitive stored data. These security methods leave an unknown number of vulnerabilities open to exploit and

require a high level of maintenance. A more effective means of data protection that protects against the unknown, as well as the known, defines the target of permissible accesses and blocks all other data access attempts by default.

CoreGuard Data Security

The architectural and functional capabilities of the CoreGuard Data Security System allow it to complete the requirements necessary for a compliant security environment, preventing theft and viewing of sensitive stored information. CoreGuard secures not only the information itself, but also the points that directly access that data, providing a comprehensive solution that meets the strict requirements of privacy protection legislation.

Architecture

CoreGuard's architecture is designed to separate the Policy Enforcement Point from the Policy Decision Point. The CoreGuard Policy Enforcement Modules (PEMs), installed on protected servers accessing sensitive data, function as the Enforcement Point, ensuring that only data access requests conforming to predefined information protection policies are permitted to access or view protected data. The PEM is also able to provide the CoreGuard Security Server appliance, functioning as the Policy Decision Point, with a high degree of context in deciding whether or not to grant access to the requested information. The Security Server securely stores the information protection policies as well as the encryption keys. The separation of Policy Decision Point from the Policy Enforcement Point greatly reduces the chance of compromising the security of the protected data.

Access Policy

CoreGuard's policy-based enforcement allows easy translation of enterprise security policies designed to protect access to sensitive or confidential information into technical controls, putting control over information distribution in the hands of the trusted security organization. Data protection policies comprise the essential parameters of the request:

- *Who* (data user)
- *What* (authenticated application)
- *Where* (file domain path)
- *When* (access window)
- and *How* (read, write or view data)

By defining policies in terms of known, permissible accesses, CoreGuard is able to prevent all accesses by unauthorized users as well as malware and exploits that attempt to leverage vulnerabilities in the enterprise information environment.

MetaClear™ Encryption

Vormetric's MetaClear encryption technology provides a big step towards compliance with privacy regulations by resolving the conflict between the need to secure data at rest and the need to manage that data. MetaClear operates at the file system-level and encrypts the file content using strong, industry-standard algorithms 3DES and AES. By leaving the metadata in cleartext form, encryption remains transparent to data management applications with no need to expose the file

content in the clear or the subsequent need for re-encryption. MetaClear not only secures data at rest, but also secures data under management, so that data at remote backup or mirror sites is also protected from unauthorized viewing.

Audit and Reporting

Demonstrating compliance with regulatory standards and legislation requires an audit trail that demonstrates data integrity. CoreGuard provides the organization with information assurance capabilities by auditing and reporting all data access attempts, including those that use the operating system to try and bypass application-level access and audit features. CoreGuard also preserves the evidentiary value of application and database audit logs by locking down access to authorized processes and preventing access by unauthorized users to these logs.

Regulatory Overview

A number of recent legislative and commercial initiatives are requiring increased attention to the privacy and confidentiality of data in corporate information systems. Following is an overview of the most significant regulations, along with a description of the legislation's relevant security issues, its focal points and a description of how CoreGuard can solve the resultant security requirements.

Gramm-Leach-Bliley Act of 1999 (Financial Modernization Act of 1999)	
Overview:	The Financial Modernization Act of 1999 or "Gramm-Leach-Bliley Act" (GLB) was enacted to repeal restrictions prohibiting banks from engaging in previously prohibited practices. GLB also contains provisions to protect consumers' personal financial information held by financial institutions or their service providers. The Safeguards Rule, enforced by the FTC, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information, with the objectives of 1) Ensuring the security and confidentiality of customer information; 2) Protecting against any anticipated threats to the security of information; and 3) Guarding against the unauthorized access to or use of information that could result in harm or inconvenience to any customer.
Legislative Data Security Issues:	• Limit data access and viewing privileges to only those required by their job responsibilities. • Implement appropriate safeguards to prevent viewing of personal data by unauthorized users.
Security Focal Points:	• IT security should provide information assurance by protecting both proprietary financial data and audit logs from vulnerabilities to external and internal attacks. • IT security should ensure that sensitive information can not be viewed by unauthorized persons, e.g., IT administrators, without restricting their ability to perform their jobs. • Database and application audit logs should be locked down to prevent tampering and preserve the evidentiary value of access records. • Outsourced services can be secured by limiting data access and viewability privileges to authorized users only.

CoreGuard Benefits:	• Multi-factor data access control assures that only authorized processes and users are allowed to access protected data, enhancing information assurance. • High-speed MetaClear data encryption prevents users with unintended access privileges from viewing sensitive data, while leaving metadata in cleartext to preserve manageability. • Host and application security locks down servers to their 'gold images,' preventing unauthorized applications, patches and malware from running. • CoreGuard locks down access to audit logs to prevent unauthorized access and tampering, preserving their evidentiary value. • CoreGuard enables outsourced data management services by enabling security administration to control both data access and viewability.

California SB 1386/ Notification of Risk to Personal Data Act	
Overview:	California SB 1386 (and the recently submitted federal version, the Notification of Risk to Personal Data Act) was created in response to the rising rate of identity theft from the compromise of personal information. SB 1386 states that any breach of the security of the data must be expeditiously reported following discovery of the breach to any California resident whose unencrypted personal information was reasonably believed to have been acquired. Personal information is defined as last name and first name or initial, combined with a Social Security Number, Driver's License or California ID Card number; or account, credit or debit card number, with the account access code. Failure to promptly notify the information owner makes the organization liable to civil action, along with the risk of damage to brand and reputation.
Legislative Data Security Issues:	• Implement strong encryption mechanism to protect the organization's interest in the event of media or hardware theft. • Ensure that the encryption mechanism cannot be defeated by circumvention, e.g., host hijacking, unauthorized insiders.
Security Focal Points:	• IT security should implement effective encryption technology that protects data from being accessed or viewed by unauthorized users in cleartext (decrypted) form. The California Office of Privacy Protection provides best practice guidelines in its publication 'Recommended Practices on Notification of Security Breach Involving Personal Information.' • Encryption requires support from strong, multi-factor data access control that prevents breach of the encryption mechanism. • Security should provide data access auditing for forensic analysis that can be used to ensure data was not received in cleartext form. • Any encryption algorithm should be 'strong,' i.e. using minimum 128 bit keys. • Any encryption mechanism must be non-intrusive, i.e., transparent to applications, file systems, data management and storage architecture.

CoreGuard Benefits:	• CoreGuard integrates protection of stored data (encryption) with multi-factor data access control, assuring that only authorized processes and users are allowed to access and view protected data. • CoreGuard's multi-factor data access control checks the Who (process UserID), What (Authenticated Application), Where (Protected Data Path) and When (Authorized access window) before permitting access to encrypted data. • Audit and reporting of all data access attempts provides a means of identifying whether data was received in encrypted or unencrypted form. • MetaClear encryption uses strong (AES or 3DES) encryption algorithms, preventing the use of 'brute force' attacks on stolen data. • File-level implemented is transparent to applications, file systems, and storage architecture. MetaClear encryption leaves metadata in the clear so it is transparent to management applications, e.g. backup.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)	
Overview:	HIPAA was enacted as part of a broad Congressional attempt at incremental healthcare reform, and includes standards designed to: • Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for administrative and financial transactions; and • Protect the security and confidentiality of electronic health information. All healthcare organizations that maintain or transmit electronic health information must comply, including health plans, healthcare clearinghouses, and all healthcare providers. After the final standards are adopted (2/20/03 for security standards) healthcare organizations have 24 months to comply (small health plans have 36 months). The law provides for significant financial penalties for violations, including wrongful disclosure of personal health information. In general, healthcare providers, health plans, and clearinghouses are prohibited from using or disclosing all personally identifiable health information except as authorized by the patient or permitted by the regulation. Healthcare providers and health plans are required to create privacy-conscious business practices, including the requirement that only the minimum amount of health information necessary is disclosed. In addition, business practices should ensure the internal protection of medical records, creation of mechanisms for addressing patient privacy complaints, and designation of a privacy officer. Covered entities are encouraged to use de-identifiable information wherever possible, which is not subject to the privacy regulation restrictions.
Legislative Data Security Issues:	• Insure that only properly authorized individuals can view confidential patient/customer health information • Provide long-term information assurance for confidential archived data

Security Focal Points:	• IT security should provide information assurance by protecting both personal healthcare data and audit logs from vulnerabilities to external and internal attacks. • IT security should insure that sensitive information can not be viewed by unauthorized persons, e.g., IT administrators, without restricting their ability to perform their jobs. • Outsourced services can be secured by limiting data access and viewability privileges to authorized users only.
CoreGuard Benefits:	• Multi-factor data access control assures that only authorized process users are allowed to access protected data, enhancing information assurance. • High-speed MetaClear data encryption prevents users with unintended access privileges from viewing sensitive data, while leaving metadata in cleartext to preserve manageability. • Enables outsourced services by enabling security administration to control both data access and viewability.

Food and Drug Administration 21 CFR Part 11 (1997)	
Overview:	21 CFR Part 11, the **Final Rule on Electronic Records and Electronic Signatures,** applies to all electronic records that are created, modified, maintained, archived, retrieved, or transmitted in companies or departments that work under any kind of FDA regulation or records submitted to the agency under the requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act. All GxP-regulated industries (pharmaceutical companies, medical devices manufacturers, laboratories, etc.) must comply. Section 11.10 describes controls for closed systems, systems to which access is controlled by persons responsible for the content of electronic records on that system. These controls include measures designed to ensure the integrity of a system's operations and stored information, including validation; the ability to generate accurate and complete copies of records; archival protection of records; and use of computer-generated, time-stamped audit trails that must be maintained for as least as long as the corresponding electronic records. Section 11.30 describes controls for open systems, those in which system access is not controlled by persons who are responsible for the content of electronic records on the system. They include those described in Sec. 11.10 plus document encryption and use of appropriate digital signature standards, as needed, to ensure record authenticity, integrity, and confidentiality.
Legislative Data Security Issues:	• Ensure that Enterprise Content Management (ECM) systems have not been breached or bypassed by unauthorized administrative users with unintended privileges • Provide long-term information assurance for confidential archived data

Security Focal Points:	• IT security should provide information assurance by protecting both confidential electronic records and audit logs from vulnerabilities to external and internal attacks. • IT security should insure that sensitive information can not be viewed by unauthorized persons, e.g., IT administrators, without restricting their ability to perform their jobs. • Information assurance requires auditing of all data accesses as a means of demonstrating compliance with FDA regulations. • Ensure secure long-term archiving at remote storage locations and third-party storage facilities by limiting data access and viewability to authorized parties.
CoreGuard Benefits	• Multi-factor data access control assures that only authorized process users are allowed to access protected data, enhancing information assurance. • High-speed MetaClear data encryption prevents users with unintended access privileges from viewing sensitive data, while leaving metadata in cleartext to preserve manageability. • Audit and reporting of all data access attempts provides a means of demonstrating compliance to FDA regulations. • Ensures security at remote locations or third-party storage facilities by enabling security administration to control both data access and viewability.

American Express Data Security Standards	
Overview:	American Express provides their Data Security Standards for merchants accepting the American Express Card to help them establish appropriate security programs. Section 1, entitled General Standards, includes their “Do’s and Don’ts for Data Storage.” Do’s include: Encrypt all stored payment data using triple DES encryption; Assign employee access to payment data on a need-to-know basis; and Be prepared to provide audit reports to American Express or allow American Express audits.
Data Security Issues:	• Implement 3DES encryption mechanism to protect the data in the event of media or hardware theft. • Ensure that the encryption mechanism can not be defeated by circumvention, e.g., host hijacking. • Limit data access and viewing privileges to only those required by their job responsibilities. • Provide long-term information assurance for confidential archived data. • Provide an audit trail of all data access attempts via authorized and unauthorized channels for forensic analysis if required.
Security Focal Points:	• IT security should provide protection to sensitive data and audit logs from vulnerabilities to external and internal attacks. • IT security should insure that sensitive information can not be viewed by unauthorized persons, e.g., IT administrators, without restricting their ability to perform their jobs. • Information assurance requires auditing of all data accesses as a means of demonstrating compliance with AMEX standards. • Ensure secure long-term archiving at remote storage locations and third-party storage facilities by limiting data access and viewability to authorized

	parties.
CoreGuard Benefits	• Multi-factor data access control assures that only authorized process users are allowed to access protected data, enhancing information integrity assurance. • High-speed MetaClear data encryption prevents users with unintended access privileges from viewing sensitive data, while leaving metadata in cleartext to preserve manageability. • Audit and reporting of all data access attempts provides a means of demonstrating compliance to AMEX standards. • Ensures security at remote locations or third-party storage facilities by enabling security administration to control both data access and viewability.

VISA Cardholder Information Security Program (CISP)	
Overview:	VISA's CISP (Account Information Security (AIS) outside of the US) was launched in April, 2000 for merchants and services providers who process, store or transmit cardholder data, with the objective of protecting information assets and meeting the obligations to the VISA payment structure. CISP provides a standard of care and enforcement for protecting sensitive information, and includes 12 basic security requirements with which VISA payment system users must comply. CISP requirements include #3, "Protect stored data" and #6 "Restrict access by 'need to know'", and #9 "Track all access to data by unique ID." For (#3) protecting stored data, VISA recommends encryption[1]. If encryption can not be used, more stringent data isolation architectures and protection practices must be implemented. For (#9) tracking all data access, VISA emphasizes tracking those with root or administrative access.[2] Failure to participate may result in considerable fines starting at $50,000 imposed by VISA or exclusion from the VISA program.
Data Security Issues:	• Implement strong encryption mechanism to protect the data in the event of media or hardware theft. • Ensure that the encryption mechanism can not be defeated by circumvention, e.g., host hijacking. • Limit data access and viewing privileges to only those required by their job responsibilities, protecting against unintended privilege by root or admin users. • Provide long-term information assurance for confidential archived data. • Provide an audit trail of all data access attempts via authorized and unauthorized channels for forensic analysis if required.
Security Focal Points:	• IT security should provide protection to sensitive data and audit logs from vulnerabilities to external and internal attacks.

[1] VISA U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting, 12/9/2002, page 9.

[2] VISA U.S.A. Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting, 12/9/2002, page 17.

	• IT security should insure that sensitive information can not be viewed by unauthorized persons, e.g., IT administrators, without restricting their ability to perform their jobs. • Information assurance requires auditing of all data accesses as a means of demonstrating compliance with VISA standards. • Ensure secure long-term archiving at remote storage locations and third-party storage facilities by limiting data access and viewability to authorized parties.
CoreGuard Benefits	• Multi-factor data access control assures that only authorized process users are allowed to access protected data, enhancing information assurance. • High-speed MetaClear data encryption prevents users with unintended access privileges from viewing sensitive data, while leaving metadata in cleartext to preserve manageability. • Audit and reporting of all data access attempts provides a means of demonstrating compliance to VISA standards. • Ensures security at remote locations or third-party storage facilities by enabling security administration to control both data access and viewability.

Summary

The recent introduction of legislation and regulations aimed at preventing unauthorized access to electronic stored data is just the start. In the future, organizations will increasingly be required to attest to audit committees, shareholders, customers and information owners that the data in their custody is safeguarded from unauthorized access and viewing, or suffer a stiff penalty in terms of fines, lawsuits, and loss of brand image. CoreGuard provides organizations with a comprehensive, integrated solution that enables them to comply with privacy and information protection requirements and provide information assurance to their stakeholders.

* * *

For more detailed information on information protection and how Vormetric's CoreGuard Data Security System ensures compliance with data privacy legislation, regulations and standards, please refer to the following Vormetric documents available at www.vormetric.com:

Vormetric White Paper— "Protecting Enterprise Information"

Vormetric White Paper—"GLBA-Compliant Data Security for Financial Services"

Vormetric Technical Brief—"Defending OS Vulnerabilities in an Oracle Environment"

Vormetric Technical Brief—"Defending Against Malware Attacks"

Vormetric Solution Brief—"Sarbanes-Oxley: Enforcing Control Objectives for Enterprise Data Environments"

CoreGuard Data Security System Datasheet

CoreGuard Frequently Asked Questions

Vormetric, Inc.
888.267.3732
www.vormetric.com
sales@vormetric.com

VORMETRIC