

## CorreLog for GLBA Compliance

GLBA, the Gramm-Leach-Bliley Act of 1999, establishes strict compliance standards for protecting customer data and customer privacy at financial institutions. This US Federal law mandates that financial institutions place IT controls upon computer systems and applications that contain customer data. If you are a bank, brokerage, insurance company, or other financial institution, and you have no verifiable IT controls over your customer data, you are NOT compliant with GLBA. *Penalties for violating GLBA are quite severe; a financial institution can be fined up to \$100,000 for each violation!*

As defined in GLBA (Section 6081), financial institutions have an affirmative and continuing obligation to respect the privacy of their customers and to protect the security and confidentiality of nonpublic personal information. To comply with GLBA, financial institutions must establish appropriate standards related to administrative, technical, and physical security.

GLBA mandates the following:

- Safeguards must exist to insure the security and confidentiality of customer records and information against disclosure to non-authorized persons.
- Safeguards must exist to protect against any anticipated threats or hazards to the security or integrity of such records.
- Safeguards must exist to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

If you are a financial institution, GLBA compliance is mandatory, whether you disclose nonpublic information or not. A policy must be in place and be enforced to protect your customer information from security threats, and ensure privacy and data integrity.

*The CorreLog Security Correlation Server meets and helps satisfy the requirements of GLBA. It provides compliance with various privacy and security standards. It safeguards your enterprise against attacks, and provides a verifiable audit trail of data access. Additionally, CorreLog provides real-time notifications of security breaches. You can easily demonstrate your compliance to auditors, and company directors, and defend your enterprise against insider and external threats.*

## About GLBA Regulations

### Question: What Does GLBA Require of Financial IT Departments?

Answer: GLBA, among its various provisions, requires companies to safeguard the privacy of their customer data, and prevent unwarranted access to customer information. This includes the safeguarding of networks, establishment of firewalls, and protection of the computing infrastructure, as well as tracking access to customer data by employees.

GLBA contains three major provisions that affect the operation of IT departments:

#### **Privacy Rule.**

GLBA affirms that customers have the right to keep their data private, including information such as e-mail addresses, occupations, and other public information. Customers may opt out of any disclosures. If you are unable to demonstrate an audit trail of employee access to customer files, you may be creating severe potential liabilities for your corporation. *Customers need only to demonstrate "inconvenience", and not specific "harm" due to your violation of the GLBA privacy rules.*

#### **Safeguard Rule.**

According to GLBA, customer data needs to be specifically safeguarded against cyber threats. This includes deployment of industry standard safeguards such as firewalls, virus protection programs, and security information management software. For example, failure to protect a computer that contains encryption keys ultimately fails to protect customer privacy. Likewise, failure to manage configuration changes to firewalls and user permissions renders the organization highly vulnerable to attack. *You need to safeguard your security, continuously monitor your security perimeter, and be immediately notified of security breaches.*

#### **Pretexting Protection.**

GLBA has specific rules to prevent and inhibit "pretexting", where a malicious third party uses your private information to defraud your customers. (For example, if a malicious ex-employee contacts one of your customers, and convinces them they still work for your bank, they are guilty of "pretexting".) To prevent pretexting, organizations must safeguard more than just customer data, but must also safeguard things such as e-mail of corporate officers, personal identity of all employees, and other information that might be misused to steal your corporate identity. *All data in your enterprise should be kept secure!*



## CorreLog Support for GLBA Compliance

### **Question: How Does CorreLog Support GLBA Compliance?**

Answer: CorreLog establishes security and audit controls for your enterprise by logging pertinent system activity, and correlating the results to create actionable notifications and tickets. This protects the network against real-time attacks, and establishes a database for post-attack forensics. In addition to making your organization more secure, CorreLog provides demonstrable evidence that your organization is GLBA compliant.

### **Verification of Firewalls and Security Infrastructure.**

CorreLog provides an open, extensible, and standards based IT framework that leverages the existing framework elements of an enterprise. Using CorreLog, you can continuously monitor firewalls, virus protection programs, intrusion detection systems, and other security systems. You can show these items are operating, and you can monitor changes to security policies. *CorreLog provides a highly interoperable framework that ensures long life cycle, flexibility, scalability, and functionality.*

### **Establishment of Business Audit Trails.**

CorreLog creates an audit trail of IT business activities in an enterprise. It records user logins, access to user data files, database metrics, and many other critical items to provide a real-time recording of what objects have been accessed and changed, and by whom. Audit trails provide a method of independent verification that customer data is being protected, in compliance with GBLA objectives. *This also provides a useful and comprehensive audit trail of management and worker activity, with application apart from security monitoring.*

### **Establishment of Security and Risk Management.**

CorreLog employs sophisticated security correlation rules that detect security violations. CorreLog detects attacks on the network and on business systems. It furnishes real-time notifications of potential security threats and breaches, helping to proactively protect all the data within the enterprise. CorreLog relies on the passive monitoring of log data within the enterprise, tapping into existing data stores to record and analyze the behavior of the network. *The CorreLog system provides a fast return on investment for entities by reducing installation effort and learning times.*

### CorreLog GLBA Highlights:

- ❖ Demonstrate compliance to the GLBA regulations, and reinforce your security policies.
- ❖ Track user access; provide a history suitable for investigation and auditing.
- ❖ Monitor system security, including servers, routers, and firewalls.
- ❖ Easy to deploy, scale and adapt. CorreLog reduces GLBA compliancy costs.



## CorreLog: Security Correlation Server

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution.

CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting requirements set forth by GLBA, Sarbanes-Oxley, PCI DSS, and other regulations.

*You can begin demonstrating immediate compliance to GLBA regulations through one simple download and installation. Visit our website for more information!*

## CorreLog, Inc.

<http://www.correlog.com>

Copyright © 2010