White Paper

Achieving GLBA Compliance through Security Information Management

netForensics®

Contents

netForensics®

Executive Summary

Approved by the United States Congress in 1999 to help modernize the financial services industry, the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to develop, implement, and maintain a comprehensive written information security program that protects the privacy and integrity of customer records. The information security program must contain administrative, technical, and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer-information issues. The scope of GLBA covers primarily financial institutions, including banks, securities firms, and insurance companies.

In the Federal Trade Commission's final ruling on the GLBA standards for safeguarding customer information, Secretary Donald S. Clark stated:

> *"As required by section 501(b), the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer."* [1]

Financial institutions must carefully monitor systems and procedures to protect customer information and comply with GLBA regulations or face civil and criminal penalties, including fines, license suspension or revocation, and even imprisonment. Yet GLBA, like other legislation that penalizes companies that fail to secure customer information, presents many challenges for financial institutions. To be compliant, organizations are required to perform in-depth risk assessments and define corrective strategies, develop and train employees on detailed policies and procedures that meet GLBA standards, monitor systems regularly, and maintain an audit trail. An effective approach to GLBA compliance involves establishing a companywide, risk-based, and cost-effective information security program.

Security information management (SIM) can enable financial institutions to meet GLBA regulatory compliance. The netForensics nFX Open Security Platform (nFX OSP) enables a formal process for compliance that is specifically targeted to GLBA control objectives for the confidentiality of customer data. In fact, by installing nFX OSP, M&T Bank Corporation of New York now has a reliable method of monitoring and protecting its technical and financial assets.

Yet safeguarding customer information is more than a legislative matter; it makes good business sense. When customers are confident in the security of their personal information, they feel secure in the company holding that information. Properly implemented, a best-practices SIM solution gives financial institutions real-time visibility into information security-related risk and compliance data, so that customer data is adequately protected.

Introduction: Brief Overview of GLBA

The GLBA was signed into law by the United States Congress in 1999. Also known as the Financial Services Modernization Act of 1999, the act's goal is to modernize the nation's financial services industry, allowing commercial and investment banks to consolidate. GLBA applies to "financial institutions," which includes any company that

offers financial products and services to consumers including banks, insurance companies, mortgage companies, securities brokers, loan brokers, investment advisors, credit card companies, and debt collectors. GLBA also requires vendor agreements and oversight to ensure that any vendor that has access to customer data as a part of the normal course of business has GLBA compliance obligations.

Title V of GLBA focuses on privacy and protection of customer data, mandating that specific privacy and security measures be in place at financial institutions to protect customers' nonpublic personal information. Several rules govern the collection, disclosure, and protection of private customer information, including the following:

- Financial Privacy Rule
- Safeguards Rule
- Pretexting Protection

The Safeguards Rule forces financial institutions to more thoroughly and effectively manage private customer data. Though the act has improved how financial services companies are allowed to do business through the use of electronic formats, the risks associated with networked technologies have the potential to be costly to financial institutions. GLBA places high penalties on companies that do not take the necessary security precautions for compliance. The regulatory bodies enforcing GLBA, including the FDIC, OCC, SEC, and FTC, have proven to be diligent in their auditing and reporting responsibilities.

The GLBA Challenge: Securing Financial Customer Information

GLBA has dramatically impacted how the financial services industry views information technology and information security. The Safeguards Rule requires financial institutions to develop a written information security plan that details how the company is protecting clients' nonpublic personal information. This plan must include the following:

- Assigning at least one employee to manage the safeguards
- Defining and implementing a thorough risk management on each department handling nonpublic information
- Developing, monitoring, and testing the program that secures the financial information
- Modifying safeguards as needed with the changes in how information is collected, stored, and used
- Keeping an audit record of security policies and procedures, including any changes to them over time

To meet the GLBA challenge and develop a written information security program, financial institutions face the following GLBA control objectives:

- Risk Assessment — Financial institutions must identify internal and external threats to customer information, along with the likelihood of potential damages. They must also determine the adequacy of mitigating controls.
- Risk Control and Management — Institutions are tasked with designing an information security program appropriate for the size, complexity, and scope of operations. The Board of Directors is required to approve the information security program and its GLBA strategies, and must oversee and remain accountable for the program. Financial institutions must provide proper information training for employees. They have to perform regular testing to determine the adequacy of

controls and also need to establish change control procedures. Plus, the information security program must include security monitoring, audit logging, incident reporting, and escalation procedures.

- Oversight of Service Provider Arrangements — Financial institutions must have monitoring capabilities to ensure that all third-party contracts and agreements are being met in terms of security controls that protect customer data.
- Information Security Program Adjustments — Institutions are required to adjust the information security program as needed to facilitate continuous improvements of customer data security. They need visibility into security information to make such adjustments, and need insight into the validity of any adjustments made.
- Reporting to the Board — Information technology organizations must report at least annually to the Board on the status of the information security program, including: risk assessment; risk management and control decisions; service provider arrangements; testing results; response to security breaches and violations; and recommended changes to the information security program.

Security Information Management: The Foundation that Enables GLBA Compliance

Meeting GLBA compliance can be a complex and overwhelming task, given the breadth and depth of control objectives financial institutions face. Not only must financial agencies monitor security from the network level; they must now monitor and secure compliance-related data throughout the enterprise at both the application level and network activity level, and they must do so on an ongoing basis. Most importantly, financial institutions must adopt a policy-driven security program.

In December 2001, the Federal Financial Institutions Examination Council (FFIEC) published a comprehensive information security booklet to help financial institutions comply with GLBA regulations. The booklet assists both financial institutions and examiners in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices. The FFIEC says the following about information security best practices as they relate to GLBA:

"Organizations often inaccurately perceive information security as the state or condition of controls at a point in time. Security is an ongoing process, whereby the condition of a financial institution's controls is just one indicator of its overall security posture. Other indicators include the ability of the institution to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions. A financial institution establishes and maintains truly effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk tolerance levels. Financial institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks." [2]

- Define a policy-driven security management program that can be incorporated early on into business processes — Identify the people and technology controls

needed to satisfy the organization's security mission and ensure compliance. Also, ensure that security initiatives are integrated into business processes at their onset, rather than after the fact.

- Validate security controls — Provide for the monitoring and reporting of controls on human actions and decisions, process controls, and information technology controls.
- Implement a risk management approach to information security — Comprise active monitoring of risk as defined and measured by key control indicators (KCIs) and key risk indicators (KRIs), correlating the relative value of information assets, the threats to the confidentiality, integrity, and availability of the assets, and the vulnerability of the systems and architecture that store and carry the assets.
- Demonstrate due diligence in the application of internal controls — Create a link between the security infrastructure and policy by capturing all security events from all network hosts, devices, and assets in an auditable database.
- Develop and implement an effective security-incident management process — Demonstrate that the proper steps were taken to correct systems and adjust policy if a non-compliant situation is identified.
- Enable reporting that can help demonstrate compliance — Demonstrate the ongoing security of compliance-related assets over a period of time, recreating the financial institution's security posture in the event of an audit, and enabling security performance management against metrics that can be leveraged for corporate governance initiatives.
- Establish capabilities for archiving and data preservation — Preserve near-term and long-term data in its purest form for forensics and evidentiary presentation.

By implementing effective, comprehensive policies and procedures for establishing accountability and consistent reporting practices, financial institutions can successfully meet GLBA regulatory compliance demands and secure customer information.

The Case for Security Information Management

With the challenges of security threats and regulatory compliance, companies are increasingly turning to SIM solutions. SIM can provide ongoing visibility into an organization's risk and security posture, as well as its compliance status.

For M&T Bank Corporation, a New York-based bank with assets of $52.9 billion in 2006, improving security and complying with GLBA were key business challenges, especially since the bank typically experiences 4 million security events per day that require monitoring. The bank searched for a scalable solution that would enable them to bring third-party security monitoring back in house to reduce costs. They additionally needed a solution that would provide highly available and measurable data to support strict accountability controls, a stringent GLBA requirement. M&T Bank needed to improve financial controls monitoring and streamline notification of changes in security threats through an effective security reporting structure.

The bank employed a security management platform to meet its security and GLBA objectives. nFX OSP provides M&T Bank customizable asset reporting groups, quick implementation on any device or operating system, and stability. Since installing the nFX OSP solution in five days in early 2005, without the need for additional hardware, M&T Bank can identify and rank the security vulnerabilities of its financial systems and controls in detail, and has a reliable method of monitoring its technical and financial assets. With SIM embedded in its IT infrastructure, the bank has improved threat identification, reduced risk, and been able to meet GLBA compliance requirements.

The netForensics Solution: Aligning with GLBA Objectives

netForensics provides the SIM infrastructure to drive GLBA compliance initiatives. nFX OSP provides financial institutions greater visibility, better intelligence, and more effective response. nFX OSP features a variety of tools and technologies to help institutions conquer complex GLBA compliance and risk management challenges. The enterprise-class SIM technology from netForensics includes the following:

- Actionable Security Intelligence — With broad security intelligence, financial institutions have a foundation from which to maintain GLBA compliant operations. Institutions can establish a continuous process of threat collection, identification, and remediation, and ensure business continuity.
- Enterprise-Class Security Decision Support — Financial institutions can meet compliance requirements through automated threat identification, by reporting against controls, and via incident resolution management. Additionally, they can resolve incidents as they occur. Metrics enable performance measurement, with baselines for security and performance gauges at the analytical and executive dashboard levels.
- Scalable, Robust SIM Architecture — A scalable SIM architecture cost-effectively supports growth and reduces total cost of ownership in mid-size to large environments. The SIM architecture incorporates data from security and network devices, applications, scanners, and databases to deliver global visibility into all security-related activities, regardless of numbers.
- Correlation Technology and Processing Power — A comprehensive correlation technology goes beyond simply logging security information, and instead speeds threat identification and provides an accurate picture of risk. The nFX OSP technologies are architected to handle the massive volume of security information from network-related sources as well as server logs, applications, databases, and identity management systems, and pinpoint attacks from the inside and beyond based on a thorough understanding of network and user activity. The correlation technologies process large volumes of data from the perimeter down to the core to identify real-time threats and historical patterns.
- Visualization, Reporting, and Analytics — Financial institutions can visualize threats as well as the security information underlying the threats. Through the in-depth reporting functionality, key stakeholders and especially auditors have ready access to comprehensive GLBA compliance data. The deep level of analytics enables institutions to measure compliance, risk, and operational performance so that security analysts, operators, and executives can determine the security posture and take any necessary steps to improve it.
- Incident Resolution Management Workflow and Embedded Security Knowledge — nFX OSP offers guidance through a repeatable incident response workflow, allowing financial institutions to effectively eradicate threats and prevent reoccurrences. Through actionable security intelligence, the incident remediation process is documented for security policy management and improvement purposes, as well as for regulatory audits. The embedded knowledge base integrates third-party security information that includes a pre-populated database of incidents and guidance on how to resolve them.
- Application Security Monitoring — nFX OSP provides comprehensive security

monitoring at the application layer. Flexible deployment options allow nFX OSP to be configured optimally to handle application events, while failover and redundancy guarantee the availability of events from identity management systems, server logs, and traditional network security devices. Dashboards and reports allow everyone involved in the process of enterprise security to understand the impact of an application-level incident on business continuity.

Conclusion

The security of financial institution customer records is not a discrete event, but rather a dynamic, ongoing process that must be maintained and adjusted. GLBA calls for leveraging information security best practices of risk and vulnerability management to ensure the integrity and confidentiality of private customer data within financial institutions. nFX OSP enables actionable security intelligence for advanced incident detection, real-time monitoring, logging, and a complete incident investigation and response framework, along with the necessary compliance reporting for managers, board members, and auditors. Aligning processes, people, and technology with a fully implemented SIM solution like nFX OSP allows financial institutions to successfully meet GLBA objectives.

References

1. Standards for Safeguarding Customer Information; Final Rule, Federal Trade Commission, http://www.ftc.gov/os/2002/05/67fr36585.pdf
2. FFIEC Information Security IT Examination Handbook, Federal Financial Institutions Examination Council,

http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

About netForensics

netForensics transforms all security related information into actionable intelligence, enabling more than 450 enterprises and government agencies to better respond to security threats, maintain compliant operations, and ensure the continuity of key business processes.

By harnessing the power of our award-winning Security Information Management platform that manages more security events at more organizations than any other product in the marketplace, we help customers deliver security management solutions that rely on the availability of timely and relevant information security information.

We facilitate these actionable security intelligence (ASI) solutions by rationalizing security information from strategic applications and critical compliance-related assets, as well as the perimeter devices that protect them. ASI solutions make this information available to technology domains and users within the security organization and beyond — by unifying network and security organizations, while supporting IT governance, enterprise compliance, and risk management initiatives.

200 Metroplex Drive • Edison, NJ 08817 • p 732.393.6000 • f 732.393.6090
www.netforensics.com • info@netforensics.com