Barry H. Johnson
SANS Security Essentials GSEC Practical Assignment Version 1.4
GLBA: Safety and Soundness Standards. A Financial Institution's Responsibility

ABSTRACT

The financial industry has long made extensive use of computer and network technology. Information technology is used to store customer information, image documents, and process transactions. The financial industry has even embraced the Internet as a way to reach and interface with new and existing customers. However, this same technology has been embraced by individuals' intent upon committing fraud and identity theft. In order to combat this threat, the Gramm-Leach-Bliley Act (G-L-B Act) was created and signed into law in 1999.

The G-L-B Act was established to provide guidance for appropriate measures for protecting customer information. This paper will discuss G-L-B Act section 501. Background information on the G-L-B Act will be discussed as well as the various sections of the G-L-B Act section 501 regarding the creation and implementation of an Information Security Program.

1.0 Background

On November 12, 1999, the President signed the Gramm-Leach-Bliley Act (Pub. L. 106-102) into law. Section 501 of the Act titled "Protection of Nonpublic Personal Information" requires the establishment of appropriate standards for the financial institutions relating to the administrative, technical and physical safeguards for customer records and information. (1)

The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation (FDIC), and Office of Thrift Supervision (OTS) (collectively, the Agencies) along with the National Credit Union Administration (NCUA), the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC) are required under the Act to establish such safeguards. On February 1, 2001, the Agencies published joint guidelines establishing standards for safeguarding customer information effective July 1, 2001, and at the same time rescinded the Year 2000 Standards for Safety and Soundness with an effective date of March 5, 2001. (1)

The guidelines apply to customer information maintained by or on behalf of entities over which the aforementioned agencies have authority. It should also be understood that a subsidiary of a bank holding company is required to be compliant with G-L-B Act as the subsidiary is presumed to be controlled directly or indirectly by the holding company (2). Finally, the G-L-B Act does not provide any exceptions for small financial institutions.

2.0 Standards for Safeguarding Customer Information

Each financial institution, subject to the provisions of the G-L-B Act and therefore the interagency federal guidelines, is to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate for the complexity and size of the bank, and the scope and nature of its activities by July 1, 2001. The information security program is to be designed to meet the following safeguards established in the G-L-B Act (1):

- 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 would result in substantial harm or inconvenience to any customer.

When considering these safeguards, the following terms should be understood. First, a customer is defined as "a consumer who has established a continuing relationship with an institution under which the institution provides one or more financial products or services to the consumer to be used primarily for personal, family, or household purposes (1)." For example, an individual with a checking account would be considered a customer, however, an individual who simply uses a financial institutions ATM machine would not be considered a customer. Interestingly enough, based on the definition of a "customer", a corporation who has an account with a financial institution would not be considered a customer. Second, customer information is defined as "any non-public personal information about a customer, whether in paper, electronic, or any other form, that is maintained by or on behalf of the financial institution (1)." In this case, non-public information would be things such as account numbers and social security numbers, while things such as a person's name and address would be considered public information.

3.0 Development and Implementation of an Information Security Program

The goal of any information security program must be to manage risks to information and information systems. In order for a program to be successful the following three things are required (3):

- A well-defined mission
- Good relationships within the organization
- Intelligent, knowledgeable security professionals

Based on the G-L-B Act, a financial institution's information security program's mission is to:

- Involve the Board of Directors through oversight, approval, and reporting to processes,
- Assess, manage and control risk,
- Oversee service provider arrangements through appropriate due diligence in selection, and
- Adjust the information security program as the financial institution's business changes and develops, and as changes in technology become available.

It is extremely important for an information security program to be understood and welcomed by the entire financial institution and not forced upon them. The G-L-B Act mandates the involvement of the Board of Directors with regards to the information security program; however, it's not the Board of Directors who have to deal with the implications on a day-to-day basis. When creating the program it is essential to involve the various departments of a financial institution. Their inputs and concerns should be noted and addressed during the program's development. If the departments within a financial institution are not included during an information security programs development, then the implementation risks being met with resistance that will doom the information security program to failure.

Finally, any information security program should be developed and implemented by a security professional who is knowledgeable not only of security from a policy and technical perspective, but who is also knowledgeable about the financial industry. It is a basic requirement that a security professional have a sound understanding of the policies required and the technology available to implement a sound information security program. Without this knowledge, the security professional would not know how to assess and properly mitigate risk and to test implemented security measures. Without knowledge of the financial industry, a security professional would not be able to create an information security program that would easily implement into the financial institution for which his employed. This knowledge should include an understanding of financial practices, the flow of information throughout the business process, and an understanding of the financial culture.

3.1 Board Involvement

The G-L-B Act directs the involvement of a financial institution's Board of Directors in the development and implementation of an information security program. Specifically, the Board of Directors or an appropriate committee of the Board shall approve the written information security program and oversee the development, implementation, and maintenance of the program (1). This includes assigning responsibility for implementation and review reports from management.

This aspect of the G-L-B Act is perhaps the most intriguing because responsibility for the safeguarding of customer information has now been made the responsibility of the highest level of management for many financial institutions. By mandating board involvement, the G-L-B Act has forced management to undertake an understanding of the threats related to the information entrusted to their institution, and thereby guarantying management support of the information security program. This is key, because without management support, there is little chance that an institution's employee base will support the implementation of an information security program.

3.2 Assess Risk

Financial institutions are required to establish a procedure for assessing the risk to their customer information and customer information systems. It should be understood that customer information systems are not simply defined as the automated systems that process the customer data. It includes all methods used to access, collect, store, use, transmit, protect, or dispose of customer information (4). The procedure for assessing risk is commonly known as a risk assessment. The risk assessment should identify foreseeable internal and external threats, determine potential damage from threats, and assess policies, procedures, and other arrangements in place to control risk (1).

A qualified individual(s) who cannot only quantify the risks to information and information systems, but has an understanding of the financial institution's business process should perform the risk assessment. The individual(s) should identify the relative sensitivity of customer information and information systems, and use that identification to determine how certain data should be protected (4). The results of the risk assessment should allow the institution to identify and prioritize its risk exposure in order to decide which risks must be mitigated and the order in which the mitigation should occur.

3.3 Manage and Control Risk

An information security program should be designed to manage and control risk. This section will discuss various security measures designed to manage and control risks. It is a financial institution's responsibility to determine which measures to adopt in order to properly address identified risks.

3.3.1 Access Controls

Access controls are measures that have been implemented to restrict access to customer information systems. These controls include mechanisms to authenticate and only permit access to authorized individuals and to prevent employees from providing customer information to unauthorized individuals (1).

Controls should include both technical measures and procedures to guard against non-technical attacks.

One of the first aspects of access controls to be implemented by a financial institution is proper policies and procedures. Access to information should be restricted based upon an individual's role within the financial institution. These restrictions should be described within a financial institution's policies and procedures. In addition, policies and procedures should describe what customer information can be released to third parties and the process for the release of such information. Finally, policies and procedures should describe the authentication methods to be used to properly authenticate individuals prior to granting information access. The actual technology to be used does not have to be described, however, if passwords/PINs are to be used then guidelines for proper password/PIN selection should be provided.

Existing authentication methodologies involve three basic "factors" (5):

- Something the user **knows** (Password, PIN);
- Something the user **possesses** (Smart card, token); and
- Something the user **is** (biometrics).

There are a variety of authentication tools and methodologies that a financial institution can use to authenticate employees. Authentication methods that depend on more than one factor typically are more difficult to compromise than single-factor systems. Single-factor authentication is typically something the user knows such as a combination of userid and password. Two-factor authentication involves something a user knows and something a user has such as a hardware token combined with a password/PIN. For example, RSA Security, Inc. produces a product known as its RSA Ace/Server that operates with their RSA SecurID cards to provide two-factor authentication. With these products an end-user is supplied a SecurID card. When the user wishes to authenticate to a system, he first supplies his userid and then is requested to supply his PIN combined with the information displayed by the SecurID card has his password. If the user supplies the correct information, he is granted access. Another form of authentication is biometrics. According to RSA's security website, biometrics applies to a broad range of electronic techniques that employ the physical characteristics of human beings as a means of authentication. These include (among a wide variety of others) fingerprint readers, iris scanners, face imaging devices, hand geometry readers, and voice readers. Usage of biometric authentication techniques is often recommended in conjunction with other user authentication methods, rather than as a single, exclusive method (6).

With the growing acceptance of the Internet by financial institution's customer base to perform financial transactions, properly authenticating customers is a growing concern. The Federal Financial Institutions Examination Council (FFIEC) has provided some guidance as it relates to authentication in an electronic banking environment. The FFIEC recommends that institutions implement password length and composition requirements on their customer base (5). Although the FFIEC does not dictate to financial institutions the use of two-factor authentication, it is recommended and at a minimum it suggests institutions should force customers to authenticate using multiple passwords (5). For example, multiple password authentications would be a combination of userid, password, and passphrase.

In addition to measures used to restrict access to customer information systems, financial institutions should implement access control mechanisms designed to restrict access to their networks from outside sources. One such mechanism is a firewall. Firewalls are designed to restrict access between two networks. This is accomplished by establishing a policy on the firewall that states what services will be allowed between the networks. Services are generally defined as items such as email and web traffic. Networks that are connected together without any form of access control mechanisms have no protection from each other and inherit the risks of the connected network in addition to their own risks.

3.3.2 Access Restrictions

Access restrictions at physical locations permitting access by authorized personnel only are a key issue in protecting not only customer information, but personnel also. An open environment where people are allowed to come and go freely is an important aspect in customer relations, but this environment should be limited to areas that are accessible to customers. Areas such as the computer operations center, network drops, and record storage should have access limited to authorized personnel. It should be noted, that just because an individual works for a financial institute, that alone does not make them an authorized individual. For example, Human Resources personnel have little need to access customer's records and therefore should not be allowed to enter areas containing customer information systems or files without an escort. A device such as a locked door that can only be opened by a properly programmed proximity badge is an example of an access restriction device. Physical access restrictions are very important. More damage can be accomplished by an individual simply walking in and removing a server full of customer information, than by the same individual attempting retrieving data on just a handful of customers.

3.3.3 Encryption

The process of disguising information in such away as to hide its substance is encryption (7). G-L-B Act requires the encryption of electronic customer information including while in data is in transit or in storage on networks or systems to which unauthorized individuals may have access (1). The type of encryption and algorithms to be used is not defined by G-L-B Act; therefore the selection of data to encrypt and the encryption techniques should be determined by a risk assessment.

An area that a risk assessment may indicate encryption is required is the storage and transmission of customer data on an Internet accessible website. Many institutions are providing "Internet Banking" access to their customer base allowing customers to access their data from home or work across the Internet by interfacing with an Internet accessible web server. However, this web server is not only accessible by the institution's customers, but by anyone with Internet access. Therefore, the web server and the network it exists on are considered to be accessible by unauthorized individuals. Institutions can address the issue of encrypting the transmission of customer information across the network through the implementation of Secure Socket Layer (SSL). This technology establishes an encrypted session between the end-users web browser and the web server, thereby creating a barrier against network eavesdroppers. However, based on G-L-B Act requirements, if customer information is stored on the web server, the storage of the data should be encrypted also. This precaution is taken to protect the information should the web server be compromised by an unauthorized individual for whom access is obtained to the data contained on the web server due to the compromise. Another area where encryption may be necessary is within an institution's own internal network. Not all employees of a financial institution are considered to be authorized individuals for accessing customer information. In scenarios where networks supporting the transmission of customer information are not segmented properly to prevent unauthorized personnel from eavesdropping on network transmissions of customer data, encryption may be necessary to protect the data, unless procedures are in put place to prevent eavesdropping on network transmissions.

3.3.4 Procedures

Financial institutions should implement procedures to ensure that modifications to customer information systems adhere to the information security program (1). An institution should develop a configuration management policy stating systems should be baselined by function, software packages, and operating system. In addition, a set of technical procedures for servers, applications, desktops, and other equipment deployed within the institution's network that is capable of processing customer data. These procedures provide the specifics on system setup while the configuration management policy provides an overview of general requirements. The technical procedure should include a security checklist. Many such checklists can be obtained from product vendors. For example, Microsoft provides several checklists and guidelines available on their website. For end-user workstations, the checklist should not only include items such as hardware and software, but also network setup, use of password-protected screen savers, and timely updates of vendor supplied patches and upgrades. A properly instituted set of procedures can remove vulnerabilities and reduce the likelihood of a successful intrusion. Prior to installation of any system, a vulnerability test should be executed against the system to ensure that all vulnerabilities have been addressed. In cases where a vulnerability cannot be addressed, the vulnerability and the risk associated should be documented and approved by management.

3.3.5 Dual Control Procedures

Dual control procedures are internal control procedures designed to minimize fraud and other risks. These procedures are put into place to ensure that employees only have access to information required to perform their job function. These procedures generally call for a segmentation of duties. For example, it is not uncommon for financial institutions to place the information security department or information security responsibilities within the control of the IT or internal audit departments. This usually occurs out of IT's need for security policy and incident response or from the idea that the audit department is responsible for compliance and therefore they should develop policy. Although the information security department should have a good working relationship with the respective departments, they should not be part of the departments as this generates a conflict of interest. In regards to the IT department, the IT department is generally tasked with the technical implementation of security such as the installation of a firewall. It is not appropriate for the IT department to be tasked with the responsibility of developing policy and then implementing it. The same can be said for the placement of information security within the internal audit department. The purpose of the internal audit department is to validate compliance and generate policy. Once again, it is not appropriate for the internal audit department to generate policy and then determine its compliance. On another note, the placement of the information security department within an institution should be in area where policies and the management of policies can span across the entire institution.

In addition to segmentation of duties, it is recommended that financial institutions perform background checks on employees (1). At a minimum, background checks should be performed on any employee with access to customer information or customer information systems. In addition, references for new hires and past job history should be reviewed. These additional reviews may discover unsettling information that is not included in a criminal background check.

3.3.6 Monitoring

G-L-B Act requires the implementation of monitoring systems and procedures to detect actual and attempted attacks on or intrusion into customer information systems (1). Because financial institutions vary in size, institutions may select monitoring systems and procedures that are appropriate for them. Monitoring systems and procedures include some or all of the following:

- Network and Host Intrusion Detection Systems (IDS)
- Network traffic monitoring
- Manual review of logs

Network and Host IDS are a combination of systems that work in conjunction with each other. Network IDS is generally installed on critical network segments and monitors network traffic for intrusion attempts. Host IDS is generally installed on critical servers and monitors the server for intrusion attempts. Both types of IDS are signature based, meaning that like virus scanner, they require an attack signature to compare logged data against in order to determine if an intrusion is occurring. In addition, current Host IDS is heavily dependent on the underlying operating system's audit logs. Host IDS monitors a system's audit logs and issues alerts based on the data being logged. However, Host IDS is capable of monitoring file integrity and detecting if unauthorized attempts are being made to modify a file.

The monitoring of network traffic can allow information security personnel to identify attack traffic as well as inappropriate system configurations. Monitoring of network traffic is usually reactive in nature, meaning, the network activity is logged and then reviewed at a later date. For smaller networks, manual reviews of network traffic may suffice, but for larger networks an automated tool is required as humans generally have a difficult time reviewing large log files. Skilled individuals who understand what they are reviewing can discover network traffic that is either a precursor to an attack or an actual attack. In addition, network monitoring can uncover misconfigured nodes on a network, because these nodes may broadcast unnecessary network communications.

Regardless of whether an institution implements one of the prior types of monitoring systems, critical servers should be configured to maintain audit logs. These audit logs should be reviewed on a regular basis. For a small institution with a small user base and a limited number of servers, a manual review of audit log files may be sufficient. However, even this can be cumbersome for an individual. For institutions with a large number or servers or a large user base, the use of automated log analysis tools is recommended. These tools can perform a comprehensive analysis on supplied logs and generated easy to read, meaningful reports. These reports can be used to detect innocuous abnormalities in an end-users use of the system, or detect obvious activity such as failed login attempts.

3.3.7 Response Programs

There is no such thing as being completely secure; sooner or later a financial institution will be forced to respond to a security incident. A properly defined response program is an essential piece of any information security program. In fact G-L-B Act requires institutions to develop response programs that specify actions to be taken in the event an institution suspects or detects that an unauthorized individual has gained access to customer information (1). A poor response policy could result in financial and public relations trouble.

The policy should have a background section in order to explain the motivation and purpose driving the policy (8). The policy should define what is considered an incident, detail what evidence will be collected and directs the creation of an intrusion response team. In addition, the policy should define a detailed response procedure for the handling of information security violations. When creating the detailed response procedures, institutions should ensure that it identifies the participants, their function and responsibility, the process for data collection in order to maintain the integrity of evidence, and assigns decision making authority to a member of the staff in order to allow for the inclusion of third-party assistance for the collection of evidence and aid in identifying the perpetrator and methods used for the intrusion. A crucial element to consider in a useful incident response policy is that of business continuity (8). For example, if critical systems become compromised, a decision to halt the systems may need to be made, and methods for continuing business need to be addressed. Financial institutions should review the policy on a regular basis to ensure that all team members understand their responsibilities. In addition, similar to the testing performed for a disaster recovery plan, personnel assigned to the Incident Response team should perform incident response testing. This can be accomplished in a conference room question and answer session. The questions should propose possible incident scenarios and the appropriate team members should answer regarding actions to the incident. Finally, the policy should define which incidents simply require the reporting to management, and which incidents require reporting to regulatory and law enforcement agencies.

3.3.8 Environmental Protections

G-L-B Act requires financial institutions to implement measures to prevent against the loss or destruction of customer information due to potential environmental hazards such as fire or technological failures (1). Key aspects to protecting against environmental hazards are a sound backup policy, a disaster recover plan, a business continuity plan, and the implementation of technology to protect against environmental hazards.

One of the first aspects in protecting information from environmental hazards is the installation of technology to protect against the hazards themselves. This technology generally consists of Uninterrupted Power Supplies (UPS) for critical servers and proper air conditioning and fire suppression for Network Operation Centers (NOC) housing critical servers. These precautions not only protect customer information, but the systems that house and process the information. This technology should be followed up with a sound backup policy. A backup policy helps to ensure against the loss of customer information due to hardware and software failures or environmental causes such a fires or water damage, but also protects against the loss of information due to accidental deletion or overwriting by end-users. A backup policy should consist of a combination of daily and weekly backup coordinated with a monthly archive. Weekly backups and monthly archives should be stored within an offsite facility to further ensure their protection. Finally, the backup policy should require periodic testing of the backup tapes to ensure the back up process is operating properly. A disaster recovery plan is aimed at the definition of business processes, their infrastructure supports and tolerances to interruptions, and the formulations of strategies for reducing the likelihood of interruptions or its consequences (3). A disaster recovery plan will define disasters, identify recovery strategies, state recovery objectives, and identify disaster recovery management teams and support personnel. A business continuity plan is an overall process consisting of disaster recovery, business recovery, business resumption, and contingency planning (3). In addition to securing against the loss of customer information due to a disaster, the focus of both plans is to ensure the smooth transition and recovery of business resulting from an unforeseen event that disrupts the flow of business.

3.4 User Awareness Programs

Security awareness training is essential to the success of any information security program. G-L-B Act recognizes this, as it is a requirement that staff be properly trained to implement an institution's information security program (1). There are several types of security training that must take place in any organization:

- User awareness training to make sure users and managers are aware of risks and are aware of policies and procedures designed to reduce the risk.
- Security solution technical training to make individuals within the organization who are responsible for security aware of products and solutions available to reduce risk.

There are numerous benefits to security training. First, users and management become knowledgeable about vulnerabilities within the systems they use, the threats to information they handle, the policies they must follow, and the tools at their disposal to help comply with policies (3). Another benefit is the deterrent factor. If a user is told of policies and procedures and is made aware of an institution's capability and desire to monitor compliance, the user is less likely to conduct mischief (3).

It should be understood that people within a financial institution view policies and procedures differently. End-users view policies and procedures as something they must comply with. Managers and system administrators view policies and procedures as something they must enforce (3).

End-user training awareness should be focused on why policies and procedures are important in helping to secure an institution's information and information system, because ultimately, end-user acceptance of an information security program is what will make or break it. End-users should be shown that if they comply with established policies and procedures that they help to reduce the likelihood of something bad happening to the financial institution, which in turn could result in something bad happening to them, such as layoffs. Training for managers should be similar to general user training, but managers need to be aware of additional issues. Managers should be aware of the threats to the information for which they are responsible. In addition, management should be made aware of laws and regulations that affect their information protection requirements (3). Individuals who are responsible for the implementation of security within an institution, such as system administrators, should be receive end-user training and product specific training. They should be reminded of their roles and responsibilities and they should be trained on the technology and other solutions that they administer.

Employee awareness training should occur multiple times a year and be in many forms. For example, new hires should review all policies and procedures before being allowed to start work. Annual seminars can be held to remind users of their roles and to review policies and procedures to ensure they are understood. Web sites can be setup for the posting of all existing policies and procedures and to provide tips and reminders. Employee awareness training should be an ongoing event as it is perhaps the best and most cost-effective measure to reducing security risks (3).

3.5 Testing of Control Systems

Financial institutions are required to regularly test key controls, systems, and procedures of their information security program (1). In order to perform these tests, the institution must identify the controls and understand they can be both technical and procedural in nature and the tests must address key risk areas. For example, the testing of an Internet firewall configuration would be technical in nature and the area of risk would be in verifying the firewall is sufficiently protecting an institution's internal network from the Internet. However, test designed to determine how easy it would be for an unauthorized person to gain access to a restricted are within an institutions facilities would be procedural in nature and the are risk would be to determine if implemented procedures are sufficient in protecting not only customer information but personnel as well.

The test should be conducted or reviewed by persons independent of those who operate the systems, including the management of those systems (4). The persons who conduct the test should be qualified to conduct and understand the results of such tests; therefore a security professional is generally required. However, the term independent should not be confused to mean that a third-party from outside the financial institution is required to perform the testing. This is not the case. The term independent simply means that the individuals who maintain and control the systems cannot perform the tests, even if they are qualified to do so. The individuals performing the test can be individuals from departments not responsible for the systems to be tested, as long as the individuals are qualified and properly trained.

4.0 Third-Party Oversight

Financial institutions have an obligation to oversee their third-party service providers. Institutions should exercise appropriate due diligence in selecting service providers, including conducting a review of measures taken by the service provider to protect customer information. Some factors to consider when performing due diligence include ability of provider to provide services, expertise to mitigate risks associated with customer data, use of third-parties or partners, adequacy of services provider's standards, policies and procedures, privacy protection, and the state of a service providers financial condition (9). When entering into a contract with a third-party service provider, a financial institution should ensure the scope of service is defined, include required performance standards, and be allowed to receive audit reports such as SAS 70 Type I and II reviews (9). Once a contract has been entered into, the financial institution should continue to perform oversight of the third-party. The institution should monitor financial condition and operations, assess quality of service and support, and monitor contract compliance (9). In some cases, a financial institution may wish to make use of a foreign-based third-party service provider. In addition, to the consideration for domestic-based service providers, a financial institution should consider the following items when performing their due diligence (10):

- Country Risk – Will the service provider's country's economic, social, and political conditions adversely affect the financial institution.
- Compliance Risk – The use of a foreign-based service provider must no inhibit a financial institution's ability to comply with all applicable U.S. laws and regulations.
- Choice of Law – Institutions should consider which country's law they wish to control the relationship.
- Confidentiality of Information – Institutions should ensure that any contract with a foreign-based service provider prohibits the service provider from disclosing or using bank data or information for any purpose other than to carry out the contracted services.

Third party oversight is critical to not only ensuring the protection of customer information and information systems, but to ensuring the reputation of the financial institution itself. If a third party service provider has an incident that affects a financial institution's customers, it is the financial institution that looks bad in the eyes of the customers, not the third party provider. Customers have entrusted the financial institution to protect and secure their information, and it is the financial institution's reputation that suffers when an incident occurs.

5.0 Program Adjustments

The type of threats to information changes over time. In addition, a financial institutions information systems and information sensitivity may change. Mergers and acquisitions, joint ventures, outsourcing arrangements, and upgrades or replacements to existing customer information systems may cause these changes. Therefore, financial institutions should monitor, evaluate, and adjust, as appropriate, their information security program. Institutions should make proactive changes to their information security program prior to making change to customer information systems as this allows an institution to take a proactive stance in mitigating risks before changes to the customer information systems are made.

6.0 Report to Board

At a minimum on an annual basis, financial institutions must provide a report to their Board of Directors describing the overall status of the information security program and the institution's compliance with the program. The report should address issues such as: risk assessment; risk management and control decisions; service provide arrangements; results of testing; security breaches or violations and responses; and recommendations for changes in the information security program (1).

The Board of Directors is the highest level of management within many financial institutions and their involvement is mandated by G-L-B Act. Therefore, they should be kept abreast of current status of information security within the institution. The minimum time frame suggested by G-L-B Act is just that, a suggestion. The Board of Directors should be informed immediately of any security breaches and violation and how the institution responded to the incident. Not doing so could result in unnecessary delays in making required changes to the existing information security program. In addition, it should be understood that risk assessments and testing of implemented security measures should not be limited to annual testing. In many cases, an annual test is sufficient as long as proper configuration management procedures are in place to ensure the mitigation of discovered vulnerabilities within products. However, if an institution performs an infrastructure migration from one system to another, then a risk assessment should be performed and the results reported to the Board of Directors. The Board of Directors should receive an annual summary report of all activities that occurred during the year; however, they should receive additional reports through out the year to keep them abreast of the current state of the information security program.

7.0 Summary

The G-L-B Act directs financial institutions to create a complete and comprehensive information security program. The ultimate responsibility for this program is placed within the hands of an institution's Board of Directors. The purpose of the program is to insure 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 would result in substantial harm or inconvenience to any customer. Financial institutions were required to be in compliance with the G-L-B Act by July 1, 2001 with a grandfather clause for bringing third-party service provider contracts existing prior to March 5, 2001 into compliance by July 1, 2003.

Although the safeguards and measures described by the G-L-B Act are uniform. It is written in a way to be scalable to the institution in question. It is recognized that that a smaller institution may not have the same risks as its larger cousins. However, small institutions must take steps to understand and implement a comprehensive information security program that will address their risk. In addition, it must be understood that cost for implementing a comprehensive information security program may not be cheap, and the importance of the program must not be devalued simply due to the size of the institution implementing the program. Fortunately for all institutions involved, there exist technology to aid in the enforcement and deployment of an information security program, and for those institutions that get lost along the way or do not know where to start, there are is flood of consultants waiting to guide the way.

References:

1. Federal Register 2001, URL: www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf

2. The Bank Holding Act of 1956, URL: www.fdic.gov/regulations/laws/rules/6000-100.html

3. Sieglein, William, et al Security Planning & Disaster Recovery McGraw-Hill/Osborne. 2002

4. Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information. 2001, URL: www.occ.treas.gov/ftp/bulletin/2001-35a.pdf

5. Authentication in an Electronic Banking Environment. 2001, URL: http://www.ffiec.gov/PDF/pr080801.pdf

6. URL: http://www.rsasecurity.com/rsalabs/faq/7-20.html

7. Schneier, Bruce. Applied Cryptography 2nd edition. John Wiley & Sons, Inc. 1996

8. Wright, Timothy. “How to Design a Useful Incident Response Policy” 2001. URL: http://online.securityfocus.com/infocus/1467

9. Guidance on the Risk Management of Outsourced Technology Services. URL: http://www.ffiec.gov/PDF/pr112800_guidance.pdf

10. Bank Use of Foreign-Based Third-Party Service Providers. URL: http://www.occ.treas.gov/ftp/bulletin/2002-16.doc