Global Information Assurance Certification Paper

Information Security Guide for Gramm-Leach-Bliley Compliance

Marcus Moore
November 7, 2003

Summary

If you are an IT Security Professional employed at a financial institution you have undoubtedly heard about the Gramm-Leach-Bliley Act. Enacted in 1999, the Gramm-Leach-Bliley Act is sweeping legislation that modernizes depression-era regulation for financial institutions. In addition to information security provisions, GLBA has seven titles and various sections that address affiliations among financial institutions, insurance, privacy, home loan bank system modernization and other financial industry statutes.

Title V – Privacy, Subtitle A – Disclosure of Nonpublic Personal Information has twenty-seven sections that govern the disclosure of personal information financial institutions gather about their customers. Section 501-Protection of Nonpublic Personal Information is the specific section where the Information Security Department of a financial institution plays an important role in complying with the Gramm-Leach-Bliley Act.

The scope of this document is to outline a basic GLBA compliance framework for financial institutions. Firewalls, intrusion detection, host security, etc. are important technical controls and an exhaustive amount of information is available on how to implement them. Likewise, guidance is available for defining the information security program, risk assessment, and other administrative tasks. Undoubtedly, any financial institution is going to have some amount of these controls in place.

However, the question the Chief Information Officer is going to ask is, “Are we GLBA compliant?”

The following compilation intends to provide a framework for an information security department responsibility in regards to Gramm-Leach-Bliley compliance.

General Guidance and Documentation Resources

Compliance with the Gramm-Leach-Bliley Act is a comprehensive task that includes implementing technical and administrative controls to protect customer information. This is not an easy task and there is not an exact checklist for compliance. However, there is a good amount of information available for guidance.

Start with reading the Gramm-Leach-Bliley Act, Title V, Subtitle A, Sections 501 (a) and (b). It’s actually a relatively small subtitle in the GLBA, but gives an

Information Security Department a feel for what a federal compliance auditor is enforcing. The Interagency Guidelines Establishing Standards for Safeguarding Customer Information are the next thing you want to review. The four federal bodies tasked with enforcing the Gramm-Leach-Bliley Act provided the Interagency Guidelines and contain further details for compliance. The most comprehensive document provided by the enforcement powers is the FFIEC Information Security IT Examination Handbook. This handbook has some great information to assist you with compliance and is the handbook the federal enforcement bodies mentioned earlier use to perform auditing. Last, NIST and ISO are two more organizations that provide standards for information security practices. Although, the standards provided by these organizations have not been formally adopted many of the benchmarks in the examination handbook were created from NIST and ISO documentation.

Gramm-Leach-Bliley Act

The following text is the legislation outlined in the Gramm-Leach-Bliley Act.

Title V – PRIVACY
Subtitle A - Disclosure of Nonpublic Personal Information
Section 501 – Protection of Nonpublic Personal Information
(a) PRIVACY OBLIGATION POLICY
It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
(b) FINANCIAL INSTITUTIONS SAFEGUARDS
In furtherance of the policy in subsection (a), each agency or authority described in section 505(a), shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards-

(1) to insure the security and confidentiality of customer records and information
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) *to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.*[1]

Yes, this is what all the brouhaha is about - two paragraphs of text in a sea of legislation. There are many more titles and sections throughout the Gramm-Leach-Bliley Act but these are essentially the ones a financial institution should be concerned with when protecting customer information. The GLBA is not a set of instructions you can follow to ensure you are compliant, that duty was delegated to federal financial agencies. The two most helpful documents they

[1] Gramm, Phil. Leach, James. Bliley, Tom, GLBA Title V Section 501(b)

have created to enforce the GLBA are the Interagency Guidelines and the IT Examiners Handbook.

The Interagency Guidelines

The Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of Thrift are collectively responsible for publishing guidelines governing GLBA compliance. The following links are available for more information about each of the agencies.

www.occ.treas.gov	The Office of the Comptroller of the Currency
www.federalreserve.gov	Board of Governors of the Federal Reserve System
www.fdic.gov	Federal Deposit Insurance Corporation
www.ots.treas.gov	Office of Thrift Supervision

On June 26, 2000, the Agencies published the proposed Interagency Guidelines Establishing Standards for Safeguarding Customer Information and requested the financial community to provide feedback. The financial community generally supported the adoption of guidelines after having the opportunity to provide input. The input of the financial industry was taken into account and the Interagency Guidelines were approved.

The key element in the Interagency Guidelines is implementing and maintaining a comprehensive information security program that includes administrative, technical and physical safeguards. The information security program of any organization is arguably the most important aspect of maintaining an appropriate security posture. The Interagency Guidelines state a security program must be implemented appropriate to the size and complexity of the financial institution focused on protecting customer information.

The development and implementation of the information security program is the main theme of the Interagency Guidelines. Also included are expectations of involving the board of directors in the process, assessing risk, managing risk, overseeing service providers, and adjusting the program on an ongoing basis.[2]

FFIEC Information Security IT Examination Handbook

The Federal Financial Institutions Examinations Council (FFIEC) is essentially the same group of organizations that created the Interagency Guidelines. The FFIEC IT Examination Handbook is the most detailed set of federal standards you could use to implement your security strategy and complements the Interagency Guidelines in assisting you to reach your compliance goals.

[2] Department of the Treasury – Vol. 66, No. 22 Feb 2001.

The Examination Handbook covers roles and responsibilities, risk assessment, security controls, security testing and monitoring. It also has a great appendix that details the examination procedures. The examination handbooks can be found at www.ffiec.gov and are highly recommended as your main guides to GLBA compliance. [3]

NIST and ISO17799

Currently, the financial industry has not formally adopted a set of security standards; however there are some standards that can provide you some benchmarks for achieving GLBA compliance. NIST and ISO 17799 are two such sets of standards, which financial regulatory agencies use to supplement their documentation.

The National Institute of Standards and Technology is a non-regulatory federal agency that develops measurements, standards, and technology to enhance productivity and trade. Although not a legal requirement, it is prudent to be aware of the NIST IT security standards because they are precursors to federal regulation, and much of the documentation provided by the federal agencies reference NIST documentation. The Computer Security Resource Center is the NIST department in which you will find the IT related security standards and can be found at www.csrc.nist.gov.

ISO 17799 actually started as BS 7799 from the British Standards Institution and was adopted by the International Standards Organization after being approved by a technical committee. As with the NIST standards ISO 17799 is a good reference for implementing a financial institutions security strategy. Also, many of the provisions in ISO 17799 are referenced in the FFIEC Information Security Handbook.[4]

Although not officially accepted as standards various NIST documents and ISO 17799 are great references for your GLBA compliance goals.

Information Security Program

The Information Security Program of a financial institution is the backbone of a solid security posture. Many topics addressed by the information security program - risk assessment, encryption, physical security, business continuity, logical access controls, service provider oversight, malicious code and any other security control or process that mitigates threats to customer information will be included. The FFIEC IT Examination Handbook provides a good index of what processes and controls are expected.

[3] Federal Financial Institutions Examinations Council (Dec. 2002)
[4] International Standards Organization (2001)

Policies, personnel roles, and standard operating procedures should be provided for each security control or process included in the information security program. Again, the FFIEC IT Examination Handbook provides excellent guidance to building an information security program.

Risk Assessment

One of the first bullets in an information security program should outline how risk assessments are performed. Undoubtedly, every financial institution has some amount of security controls in place to protect customer information; therefore, a threat had to have been identified by some form of risk assessment. However, information security is a cyclical process and the risk assessment process is no exception. A risk assessment should be performed on an ongoing basis as new IT systems, lines of business, or acquisitions occur which change the landscape of your infrastructure. A standard risk assessment methodology that is flexible and responsive to change is what is needed.

NIST special publication 800-30 Risk Management Guide for Information Technology Systems is yet another excellent resource for creating your own risk assessment methodology.

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf is the link to the actual document.

Your goal in performing a risk assessment is to determine how much risk customer information is exposed to given any threat. To accomplish this the target of the threat must be characterized, the type of threat identified, the likelihood of the threat occurring and the impact of the threat must be determined. Once all of these variables are identified a risk matrix can be built to produce a value for overall risk to each IT asset or business unit that provides a service or deals with customer information.[5]

Target Characterization

IT systems or business units that utilize customer information can be characterized as targets of threats. For example, a mortgage division of a financial institution could be characterized as a target as well as the IT systems the division utilizes to process customer information. The business unit is a broader target than an individual IT system but either should suffice. Check with the auditor responsible for your evaluation to make sure either is acceptable.

Threats

Malicious code, natural disasters, untrained employees, third party service providers, etc. are all threats to customer information. In assessing your risk it is

[5] Stoneburner, Gary. Goguen, Alice. Feringa, Alexis. (Oct. 2001)

required that you identify reasonably foreseeable internal and external threats that could result in customer information being compromised. Assign threats to each target that was characterized earlier. For example, individual branches have been identified as a target. Would a natural disaster, virus or inappropriate access control threaten customer information or service at the branch?

Likelihood

Once the targets have been characterized and the threats have been identified it is time to derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exploited. One approach may be to assign a value of high, medium or low to the likelihood a threat will attempt to compromise the security controls of a financial institution. The risk assessment process is cyclical so make sure the current controls such as a firewall or email policy are taken into account. Natural disasters, for example, may have had a high likelihood of occurrence due to the location of a service center. If the service center was relocated the likelihood of a natural disaster could be reduced to low. Also, changes in threats such as viruses can circumvent controls thus changing the likelihood to high.

Impact

The next step is to analyze the adverse impact resulting from a successful exploitation of vulnerabilities. The organizations or systems defined earlier as targets are the elements that would be impacted. The impact can be measured against the security objectives of the institution, which are the integrity, availability, and confidentiality of data. As with likelihood, high, medium or low can be the values used to measure the impact of a successful exploitation by a threat. For example, the impact of a virus to human resources department may be low, however the impact to a mortgage department may be high.

Risk

The targets have been characterized, the threats identified, and values have been assigned to likelihood and impact. The overall risk is measured in a way to reflect the security posture of an organization by using the following formula.

Likelihood * Impact = Risk

This formula helps determine whether or not current controls are sufficient and how much risk the organization is willing to accept for each threat associated with each target. If you have determined the likelihood of a threat is low, but the impact is high, the average would be a medium. It may be helpful to substitute numerical values instead of high/medium/low for a more precise value.

The Risk Matrix

The last piece of the risk assessment puzzle is to have a method of organizing all the information gathered in a way that expresses risk exposure in a uniform manner. A risk matrix is very helpful in accomplishing this, simply put in the variables as they are determined and a uniform risk methodology will begin to materialize.

Target	Threat	Likelihood	Impact	Overall Risk
Dept A	Viruses	High = 3	Med = 50	150
	Disaster	Low = 1	High = 100	100
	Hacker	Med = 2	High = 100	200
Dept. B	Viruses	High = 3	Med = 50	150
	Disaster	Low = 1	High = 100	100
	Hacker	Med = 2	High = 100	200

The above example is a very simple risk matrix that can show all the necessary information needed to complete a risk assessment. The risk assessment should be meticulous in determining the values for likelihood and impact. In addition, be thorough when listing the targets and threats. Once a risk matrix is created on ongoing cyclical risk assessment methodology will be a much easier task and assist greatly in complying with the Gramm-Leach-Bliley Act.

Roles and Responsibilities

Defining the roles and responsibilities in regards to maintaining a sufficient security posture is another section that should be addressed in an Information Security Program. Employees, management, senior management, information security, third party service providers and the board of directors all have a stake in information security. Throughout much of the documentation provided by the regulatory agencies the board of directors are mentioned as being responsible for approving and overseeing the information security program. Therefore, it is important to include the expectations of each person in the information security program. For example, employees would be expected to adhere to written policies, management would be expected to review reports related to security, the information security department would be responsible for providing reports to management, etc.

Most importantly, it is the board of directors who are ultimately responsible for overseeing the information security program per the Interagency Guidelines for Establishing Standards For Safeguarding Customer Information. The most pointed examples of federal guidelines state that each bank shall report to the board at least annually about risk assessment, risk management, security breaches, etc.

Policies

The policies in the information security program extend beyond the typical access and email policies every employee is expected to adhere to. The FFIEC Information Security Handbook has a table of contents with all the security controls that should be included in a financial institutions security posture. Access controls, physical security, encryption, malicious code, personnel security, media handling, service provider oversight, etc. should all have policies that state an effort is made to mitigate risks based on all the controls listed.

As an example, an encryption policy would state,

"The bank mandates encryption will be utilized to mitigate the risk of unauthorized disclosure of sensitive information. The strength of the encryption shall be sufficient to protect sensitive information for stored data and communication channels. If encryption keys are required for the encryption mechanism to operate then the key will have an effective key management process. The encryption techniques of the bank must be reliable and appropriate safeguards will be put in place for any encryption endpoint."

The policies in the information security program should be written to reflect requirements for a control to be implemented rather than the details of how to it is implemented. Standards, guidelines and procedures will provide the details of how a control is implemented to fulfill a policy requirement.[6]

Security Standards, Guidelines and Procedures

Standards, guidelines and procedures are more detailed methodologies and procedures for securing an infrastructure. Compiling the detailed processes for how an institution implements every authentication mechanism, firewall, encryption scheme, virus protection implementation, and every other control that mitigates risk can be a daunting task. Malicious code, for example, will have control for every desktop, every server, remote access users, email gateway and the Internet perimeter. Documenting the procedures for each of these could possibility involve numerous functional groups, technologies and managers, and coordinating this effort will be a challenge.

There are numerous categories of controls that require documentation. Documentation for intrusion detection, firewalls, host security, and every other control have examples readily available with the help of a search engine. It's quite possibly the most tedious task in creating a solid information security program but necessary nonetheless.

[6] Krutz, Ronald. Vines, Russel. P. 1-26

Conclusion

A robust information security program is a primary task when complying with the Gramm-Leach-Bliley Act. A good ongoing risk assessment using the methodology documented in the information security program is also very important and will help determine what controls need to be put in place. In most cases, every financial institution has the necessary controls and documentation for the information security program. It's usually a matter of using the information security program as hub for all the policies, risk assessment and controls documentation. The result of the Gramm-Leach-Bliley Act germane to information security has been to ensure the board of directors is aware of the security posture and that information about the security posture be centralized.

The goal of the legislation is to protect customer information. There are real threats of organized hackers attempting to steal customer information for their own benefit.

Tips for Compliance

If you are responsible for Gramm-Leach-Bliley compliance here are a few helpful tips to keep in mind.

- Use the intranet if available, and if not create a website. Web based technologies are very helpful in consolidating and organizing information in one central location. A web page is easily accessible everyone, but keep it simple. The content is what counts. As the content matures a database with a web front end is very helpful but don't let a technical nicety hold up your progress.

- Don't try to take it all on at once and write every policy and procedure yourself. The scope of personnel involved is very diverse and much of the documentation you'll need exists already. It simply needs to be consolidated.

- Try to keep it simple. The risk assessment alone can seem overwhelming at first. Start small and complete an information security program framework first. The details will come it time and it will get easier as the information security program begins to fill out.

- Compliance is not a piece of software. There is no amount of software that is going to make your institution compliant. Compliance is achieved through a combination of controls, procedures, policies compiled in a comprehensive information security program. Cooperation and diligence are the ingredients for success.

- A vulnerability assessment is not a risk assessment. A third party vendor scanning the network for vulnerabilities does not constitute a risk assessment. A risk assessment can include a vulnerability assessment but not vice versa.

References

Internet

[1] Gramm, Phil. Leach, James. Bliley, Tom "Gramm-Leach-Bliley Act" http://www.senate.gov/~banking/conf/ (1999)

[2] Department of the Treasury. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" http://www.federalreserve.gov//boarddocs/SRLETTERS/2001/sr0115a2.pdf (February 2001).

[3] Federal Financial Institutions Examinations Council. "Information Security IT Examination Handbook" http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/information_security.pdf (December 2002)

[4] International Standard 17799 Information technology – Code of practice for information security management. Switzerland: International Standards Organization, 2001.

[5] Stoneburner, Gary. Goguen, Alice. Feringa, Alexis. "NIST Special Publication 800-30 - Risk Management Guide for Information Technology Systems." http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (October 2001).

[6] Krutz, Ronald. Vines, Russel. The CISSP Prep Guide. New York: Wiley Computer Publishing, 2001, 1-26.