Global Information Assurance Certification Paper

The Gramm-Leach-Bliley Act (G-L-B) versus Best Practices in Network Security

Why Privacy does not equal Security

By Thomas G. Hinkel

The G-L-B act, signed into law by President Clinton on November 12, 1999, is a sweeping piece of legislation containing 7 titles and 740 sections, and affecting all financial institutions in areas from fair treatment of women by financial advisors, to the rescission of Glass-Steagall.[1] But the section that is currently getting the most attention is Title V, section 502, entitled "Obligations with respect to disclosures of personal information." Most everyone has by now received a notice from your bank, brokerage firm or insurance company explaining their position on privacy as it relates to your personal information. Most people will probably give the notice only a passing glance, and throw it away. I would advise you to read it carefully, though. The law provides that most larger financial institutions allow for an "opt-out" provision to be made available. Often, in order to opt-out of information sharing you must either sign and return something, or call them. If you do not opt-out using one of the proscribed methods, they can use your private information in any way they see fit. Financial institutions are scrambling to implement the specific provisions of section 502 by July 1, 2001, but in my opinion they are missing the mark.

Although section 502 is certainly a topic worthy of it's own discussion, the focus of this paper is on a less known, but potentially much more problematic section. Title V, section 501 is titled "Protection of nonpublic personal information". This section mandates that financial institutions implement "administrative, technical and physical safeguards" for customer records and information. Specifically, these safeguards are to designed to:

1) Insure the security and confidentiality of customer records and information
2) Protect against any anticipated threats or hazards to the security and integrity of such records, and
3) Protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer.

The guidelines define such things as public vs. non-public customer information, as well as suggest specific measures for safeguarding customer information by developing and implementing an information security program. Essentially section 501 mandates a comprehensive, written "Information security program…appropriate to the size and complexity of the bank and the nature and scope of its activities."[2] But while the

guidelines of section 501 are certainly a step in the right direction, in my opinion it doesn't go far enough, and may even do more harm than good. Aside from the fact that section 502 is getting all the scrutiny, and the means behind the provisions of 502 only a passing glance, there are important differences between the G-L-B guidelines, and what we will refer to here as 'generally accepted best practices' (Appendix 'A'). The first is the key concept of identifying the assets to be protected. G-L-B identifies "non-public customer information" as the asset to be protected. While that may be the focus of the privacy element of the act, it doesn't fully identify all mission critical information and systems. To be fair, the FDIC has addressed information security else ware[3] (and even then identifying only three elements; prevention, detection and response), but according to G-L-B, the stated objective of the Banks' security program is to "ensure the security and confidentiality of customer information" (further defined as only "non-public" customer information).

The second is the concept of accurate assessment. Many small institutions do not have the resources to staff a IS security department. In most cases, one individual may, by necessity, wear many hats. They must rely on outside experts for assistance in highly technical areas if they are to achieve a secure network environment. The FDIC's own Safety and Soundness Examination Procedures state that "the level of sophistication and the rate of change in electronic capabilities may require at least some degree of outsourcing to third parties."[4] In the absence of outside help, these institutions may not be able to fully assess the risks, and may fall short of achieving a truly secure network environment. Even when outside experts are utilized, the institution must have a good understanding of the method of assessment. For example, many institutions outsource their data processing to third party service providers, or in some cases multiple providers. This is especially true in the area of electronic commerce. In these cases, the institutions must rely on independent (third party) audits for confirmation of the adequacy of the providers' internal security controls. The SAS 70 (Statement on Auditing Standards No. 70) developed by the AICPA is one widely recognized standard. But while a SAS 70 audit certainly demonstrates the establishment of "effectively designed control objectives and control activities"[5], it does not (in the case of a Type I report) render an opinion as to the adequacy of the procedures themselves. In fact, a Type I report is simply a "snapshot" of the controls at a specific point in time. If you are an institution relying on the adequacy of the security measures of a data service provider or out-sourcing arraignment, you should insist on a SAS 70 Type II report. It includes detailed testing over a minimum of 6 months, and most importantly, an opinion on whether the methods used were sufficiently effective to provide reasonable assurance that the desired objective would be achieved.

The third, and my biggest concern, is that the Agencies intended for the Privacy provisions of Section 502 to be <u>supported</u> by the Security safeguards of section 501.

> "Several of the comments suggested the proposed effective date be extended for 12 to 18 months. However, the FDIC believes that the effective date for the Guidelines and the Privacy Rule should coincide.

> The Privacy Rule requires a financial institution to disclose to its customers that the bank maintains physical, electronic, and procedural safeguards to protect customers' nonpublic personal information. Appendix A of the Privacy Rule provides that this disclosure may refer to these federal guidelines. This is only meaningful if the final Guidelines for safeguarding customer information are effective when the disclosure is made."[6]

In other words, all of the specific measures taken to assure privacy and the proper use of customer information presume an adequate security program. **How can an institution assure the privacy of its customer information if it hasn't first addressed the means by which that privacy is assured?** The guidelines clearly state that security is a prerequisite for privacy, yet I've seen considerable attention directed towards drafting and finalizing privacy statements and op-out notices, but little or no effort (or interest) in the process of identifying and controlling the specific threats to customer information. An institution **is** required to conduct an assessment of the risks to customer information and indicate in its security program how it controls the risks, but exactly how will examiners assess the sufficiency of the program? Unless they are comparing against an established standard, the assessment will fall short. On March 18, 2001 FDIC Chairman Donna Tanoue gave a preview of what examiners will likely be interested in. During a presentation to the American Bankers Association Compliance School in Indianapolis she stated;

> "As to be expected, the primary objective of an examination will be to assess the quality of an institution's compliance management program for implementing the privacy regulation. The scope of the examination will depend on the extent the institution shares information with affiliates and nonaffiliates. In order to accommodate the differences in information sharing practices, the examination procedures will be divided into modules. An institution that limits its information sharing activities will generally have a more limited examination than one who shares information more extensively."
>
> She stated the agencies want to minimize the burden and confusion for both the industry and the examiners. The intent is to have examination procedures that that can be used by both examiners and industry compliance officers to measure compliance with the regulation.
>
> "During the examination process you can expect your officers to be interviewed regarding your privacy practices and the use of customer information. The agencies feel a comprehensive understanding of any uses and sharing of information by the institution is essential to enable the examiners to perform an accurate examination.

> The examiners will review all aspects of an institution's privacy program, including internal controls, employee training, monitoring of compliance, consumer complaint resolution and management oversight. You can be sure the examiners will also review your privacy policies and notices, consumer opt-out directions, information sharing agreements, service agreements and joint marketing agreement."

Except for the reference to review of "internal controls", there is no specific mention of security. Is it possible that an institution can offer an assurance of privacy without an adequate security plan? According to Chairman Tanoue, it seems likely that they may be able to demonstrate sufficient compliance with the guidelines of Section 502 to pass an agency exam without a rigorous examination of their security procedures.

The good news is that the Agency guidelines provide most of the basic elements. Institutions only need to incorporate a few changes to the list in Appendix A. First is a more complete identification of the information and systems to be protected. Don't stop at simply the "privacy of non-public customer information", but include all critical information and systems. Items such as e-mail, minutes of meetings, non-public financial information and financial projections, anything the institution considers critical and confidential. If you don't already have a formal security policy, completing this first step provides the framework. A policy defines what you are protecting, and why you are protecting it.

Second is a complete assessment of all of the elements necessary to produce, store and deliver the assets identified previously. Once the policy has been broadened to encompass all critical assets, additional threat elements are identified. These threats are classified in three general categories: Threats to confidentiality, integrity and availability. Oddly, although G-L-B Section 502 focuses on privacy as a function of confidentiality, and section 501[7] mentions specific measures that can be taken to insure that customer information is disclosed to only authorized individuals (integrity), there is no mention of compromise by denial of availability. Denying access to the methods of information access is no less serious, or disruptive, than improper disclosure. In fact, given the rise in popularity of the Internet as an alternate service delivery method (or in the case of Internet Banks, the primary delivery method), the threat to availability should be taken as seriously as the threat to privacy. On final note regarding the assessment process. Make sure your key employees understand how the security process works. Use outside experts when necessary, but insist that they explain how and why a particular tool or technique is used. If your officers and key employees are interviewed regarding your security practices, they should have a general understanding of the methods and techniques used. If Chairman Tanoue expects them to thoroughly understand the privacy issue, shouldn't you expect at least as much from them on security?

Third, regarding prevention, although G-L-B (and other agency publications) mentions several specific preventative tools and techniques, they are silent on the important preventative concept of defense in depth, or layering of defenses. This is particularly

important in the financial arena, where much more than privacy is at stake. Banks have always been keen on layering traditional security. Countermeasures such as vaults, cameras and silent alarms are common. But modern day Willie Suttons'[8] won't try to break in through the front door, they are far more likely to try (and repeatedly re-try) entry through one of the many electronic back doors. The majority of financial institutions today offer transactional access to account information via the Internet, 24 hours a day, 7 days a week. The complexity of the access and delivery methods used to provide these services necessitate a layered approach to security. During one week alone (5/24/01-5/31/01) there were 9 security bulletins advising patches to Microsoft products[9], each one a potential back door. How many other doors remain undiscovered? Incorporate the concept of defense in depth into your specific procedures.

Finally, regarding the element of response, G-L-B requires all intrusions be reported on the interagency Suspicious Activity Report (SAR)[10]. The SAR is the same form used to report counterfeit currency, credit card fraud, money laundering, etc. A single additional check box has been added to Part III item 35 f ("summary characterization of suspicious activity") called "Computer Intrusion", which is defined as:

> "…gaining access to a computer system of a financial institution to a) remove, steal, procure or otherwise affect funds of the institution's customers; b) remove, steal, procure or otherwise affect critical information of the institution including customer account information; or c) damage, disable or otherwise affect critical systems of the institution."

Attempted intrusions are apparently not reportable events via the SAR. In fact, it goes on to state that,

> "For the purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information."

No distinction is drawn between an informational website, and a transactional one. Even in the most recent revision of the SAR (June 2000), websites are categorized along with "other non-critical information systems". In today's interconnected network environment, this response procedure is dangerously inadequate. All intrusion attempts, whether or not they are successful, and wherever they occur, must be detected and reported. Furthermore, they should be reported to a centralized security organization, such as CERT or GIAC so the information can be shared among all institutions.

In conclusion, G-L-B requires privacy, and privacy requires security. Only when the public demands closer scrutiny of security by the regulators, will regulators require higher security standards from institutions. In the meantime, companies should take this opportunity to use the mandate of privacy to take a closer look at their own security policies and procedures, and compare them not just to regulatory requirements, but to generally accepted best practices. Only in this way will they be able to comply with both the letter and the spirit of G-L-B.

Appendix A

For our purposes, "generally accepted best practices" (or GABP) in network security shall consist of elements from each of the following:

1. Identification – What assets are critical to your company, and where do they reside.
2. Assessment – A comprehensive review of the hardware and software environment providing access to, or storage of, the assets identified in step 1 for the purposes of identifying the threats to each element.
3. Prevention – Specific measures taken to manage and control the threats identified in step 2.
4. Detection – Collection, review, and analysis of audits and logs designed to capture the forensic evidence of a compromise.
5. Response/Reaction – Procedures designed to specify a response to a compromise or the evidence of an attempted compromise.
6. Recovery – The ability to restore critical information and systems functionality to their original condition in a timely manner.
7. Training – Informing the staff on their role in security program, specifically the procedures in steps 5 and 6.
8. Testing – Regular tests of the key controls, systems and procedure

Note: Credit is acknowledged to the following sources for confirmation, and re-confirmation of the basic elements in this list: SANS Institute, Security Essentials course (various instructors), Secret & Lies, Bruce Schneier; Cybershock, Winn Schwartau,; Maximum Security, Anonymous; FDIC FIL 68-99

References:

[1] Marion Lang gave an excellent summary of the privacy and security elements of the G-L-B Act at www.sans.org/infosecFAQ/legal/gramm.htm
[2] FDIC 12 CFR Chapter III Part 364.101 Appendix B Item III G 1
[3] FIL 68-99, Risk Assessment Tools and Practices for Information System Security
[4] http://www.fdic.gov/regulations/safety/manual/00EBANK_main.htm
[5] www.sas70.com/about.htm
[6] Department of the Treasury, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, Page 62
[7] Appendix B, Item III C 1
[8] http://www.fbi.gov/fbinbrief/historic/famcases/sutton/sutton.htm
[9] MS00-035 v. 2.0 – Patch Available for "SQL Server 7.0 Service Pack Password" Vulnerability
MS00-079 v. 2.0 – HyperTerminal Buffer Overflow Vulnerability
MS01-023 – Unchecked Buffer in ISAPI Extension Could Enable Compromise of IIS 5.0 Server
MS01-024 – Malformed Request to Domain Controller can Cause Memory Exhaustion
MS01-025 – Index Server Search Function Contains Unchecked Buffer
MS01-026 – Superfluous Decoding Operation Could Allow Command Execution via IIS
MS01-027 – Flaws in Web Server Certificate Validation Could Enable Spoofing
MS01-028 – RTF document linked to template can run macros without warning
MS01-029 – Windows Media Player .ASX Processor Contains Unchecked buffer
[10] http://www.treas.gov/fincen/f9022-47r.pdf

© SANS Institute 2000 - 2005 Author retains full rights.