Global Information Assurance Certification Paper

GLB Risk Assessment: The Good, The Bad & The Ugly
SANS GSEC Practical Assignment Version 1.4 Option 2
Submitted by: Samara Paice

Abstract:

Has the Gramm-Leach-Bliley (GLB) Privacy Act affected your security program? GLB encouraged us to take another look at our security program including risks, threats, impacts, safeguards, and acceptable risk. How did we do this? What were the results of our review? I will get into the steps and detailed results later, but the end result is an accepted risk assessment methodology, greater employee awareness and an enhanced sense of responsibility and ownership.

What is the Gramm-Leach-Bliley Act?

The GLB Privacy Act is federal regulation designed to protect consumer's interests. With the increased use of the Internet and electronic data transfers, consumers' nonpublic personal data is at risk. The act seeks to mitigate the risk to the consumer and mandates information security to the state government level. The act specifically states:

"Sec. 6801. 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) of this section, each agency or authority described in section 6805(a) of this title 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."

How does this apply to us?

Everyone in the financial industry is subject to the GLB Act. I am in the insurance industry and we have a wealth of nonpublic private information at our disposal. Nonpublic personal information can be social security numbers, birth dates, etc. but it can also be insurance information contained on the declaration page of the insurance policy. From personal homeowners policies to commercial workers compensation claims and everything in between, much of our insured's information is nonpublic and private to the consumer. Our policyholder database contains birth dates, driver's license numbers, addresses, property values, policy limits and more. The claims database includes all of the aforementioned information as well as claimant statements and other involved party information.

The glaring problem with GLB and how it relates to information security is that there is no steadfast guidance. Thus our GLB Security Program had to be developed based on interpretation of the act's verbiage and a decision was made as to what and how much we should do as a company to protect our policyholders and claimants interests. In addition, we support the independent agent, which means we need to provide an easy means for the agent to do business with us while protecting the insured's, (their customers') interests.

The Risk Assessment Methodology

Prior to GLB we didn't have a risk assessment methodology. As the team leader and firm believer in the facilitated methods I decided to use Thomas R. Peltier's facilitated risk assessment methodology. Mr. Peltier makes one statement in his book "Information Security Risk Analysis" that hits home "Once resource owners are involved in identifying threats, they generally sit up and look for assistance in implementing cost-effective controls to help limit the exposure. The FRAP allows the business units to take control of their resources. It allows them to determine what safeguards are needed and who will be responsible for implementing those safeguards." This statement sold me on the methodology. After all, who knows better what risks and controls exist in our organization than the employees.

The total facilitated risk assessment process, as described by Peltier was not used as the GLB Security Team made the final decision and they were not accustomed to facilitations, thus reluctant to use an unknown process in such a high priority project. However, we did use much of this process, which is what I will explain.

Understand that this modified methodology worked for us but may not work for all. In addition, those without risk assessment experience, certification, or training may find this a daunting task. Risk Assessment services can be purchased through a variety of vendors and additional risk assessment

methodologies and products can be researched online at www.riskworld.com. The risk assessment methodology can make or break you so research thoroughly and seek input from people that will be involved in the process or will be using the final product. Don't limit yourself to information technology risk assessments. There are numerous methodologies and an industry specific risk assessment may be more advantageous. Input from audit organizations such as www.theiia.org/itaudit can be very helpful. After all, auditors, whether internal or external, will be looking at the final product at some point so doesn't it make sense to prepare the assessment in accordance with what they deem acceptable? In our case, we had Internal Audit representation on the GLB Security Team.

Identification of Nonpublic Personal Information

A typical risk assessment will list all the assets at risk in an organization including people, equipment, information and so on. The risk assessment for the GLB Security Program had to be approached a little differently. Remember, GLB exists for the protection of nonpublic personal information and the interest of the consumer. This means that we had to look at the sources of nonpublic private information within our organization and determine where the information is stored, transferred, communicated, etc.

At the onset of this project many functional areas within the organization assumed they weren't subject to GLB as they didn't physically have possession of nonpublic private information. As we progressed with the project they soon came to realize that no one was exempt. We all have access to nonpublic personal information at some point or simply by virtue of logical access to our enterprise and distributed systems. And so began the identification of nonpublic personal information.

Fortunately we had undergone the Century Conversion project within the past 18 months so we used the information listing as a baseline and updated accordingly. The bulk of our nonpublic personal information resides in the enterprise server database. However, our main concern was not where the information resides but how it is accessed, saved, transmitted and discarded. For example a download of homeowner's policy information can be saved to disk, CD, tape or other media and transmitted via private or public electronic transmission. The download can be printed and sent via US Mail, UPS, or Federal Express or it can be faxed. It can be printed and discarded after a quality review of the output is performed. It can be forgotten and left on someone's desk for an indefinite period of time. In looking at each source of information we had to ask ourselves many questions, including the following:

1. Is the information saved on a diskette, CD, tape, LAN, enterprise server?
2. Will the data be sent via e-mail and if so, to whom?
3. Is the requestor a legitimate recipient of the information?

4. Will the data be sent via a VPN or FTP connection?
5. Will the data be sent mailed? Faxed?
6. If hard copies are made of the download where are they stored? On a desktop? In a locked file cabinet? In a stack on the floor?
7. If the hard copy is discarded is it thrown in the trash? Is it sent to the recycling bin? Is it shredded?
8. Are all employees aware that this data contains nonpublic private information? Has a labeling or classification scheme been adopted to make them aware?

In addition to all of the above questions we also had to assess our physical building security. Did we have it? Did employees understand why we had it and were they complying with policy or general practice? As you can see from this example the security of information is far reaching but with the right discipline and proper planning the result will pay off ten fold.

Threat Identification

A typical compilation of threats consists of three major categories, natural, accidental, and intentional threats.

Our natural threats include tornadoes, hurricanes, snow and ice storms, power outages, floods, etc. Natural threats vary greatly across the United States and since we are located in various cities on the Eastern seaboard I used the State Offices of Emergency Management to ascertain what natural threats all of our offices and therefore information were subject to. It was very eye opening for me and I believe for the rest of the team. Who would have thought that our little New England state ever had a volcanic eruption or there was once a tsunami, albeit not inland where we are located but the state did have one. Each state should have a similar site as each state and many times counties have disaster preparedness plans.

Accidental threats are definitely a concern for our company and should be for everyone. These threats include user or operator error, food or beverage spills, and unintentional disclosure of information. Accidental threats can be compiled based upon experience with the company, office ergonomics, knowledge base, Help Desk logs, and training, etc. You can also obtain lists of accidental threats in various magazines, books, trade publications and the like.

Intentional threats include fire, bombs, sabotage, fraud, cyber terrorism or disclosure. In compiling the list of intentional threats I used state and local statistics found at police department web sites and also by accessing crime reports at the Department of Safety for all of our office locations. Going to the local library may also reveal information about intentional threats in your geographic location that you may have to pay for otherwise.

In addition, there are usually three elements associated with a threat, whether it is natural, accidental, or intentional, as provided in Information Security Risk Analysis by Thomas R. Peltier. These elements are the agent, the motive, and the results.

"1. The *agent* is the catalyst that performs the threat. The agent can be human, machine, or nature.
2. The *motive* is something that causes an agent to act. These actions can be either accidental or intentional. Based on the elements that make up an agent, the only motivating factor that can be both accidental and intentional is human.
3. The *results* are the outcome of the applied threat. For the information security profession, the results normally lead to a loss of access, unauthorized access, modification, disclosure, or destruction of the information asset."

Applying these elements in the threat assessment was important to the results of the program, as you will see in the next section.

The Threat Assessment

We developed a rating scale for the threat measurement. We used a scale of 1 to 5 to have enough categories so as to differentiate the risks. Your scale doesn't have to be 1 to 5 but should be large enough to capture differences without being but so large as to be bothersome. In my opinion, a scale of 1 to 3 or 1 to 5 is usually acceptable with 1 being the event is not likely to occur and 3 or 5, as the case may be, meaning the event is very likely to occur. Fill in the middle of the scale accordingly.

The group assessed the threats to their functional units' identified sources of information. When assessing the threats they asked, "What is the likelihood of this threat occurring? Who or what are the agents? The motives? The results?" For instance, in New England snowstorms are very likely and received a 5 as a rating but tornadoes are not very likely, (or so history dictates), so this received a rating of 1. The agent is nature in both examples, there is no motive and the result would be most likely loss of access due to power outages and possibly destruction of paper files if not physically secured. The key to this assessment is to measure the threat in its purest form and not consider safeguards you may have in place already.

Assessing the Impact

Impact is simply asking the question "If this threat occurs how much will the confidentiality, integrity, or availability of the nonpublic personal information be affected?" The team used the same scale as created in the threat assessment and looked at each information source individually. Staying with the snowstorms

and tornadoes examples and asking ourselves the aforementioned question we would have to give the impact of the snowstorm a low rating whereas the impact of a tornado could be devastating and would receive a high rating. Snowstorms could receive a higher rating if we did not have power outages as a separate threat as every Nor'easter brings power outages.

Assessing the impact was probably the hardest step for the team as this is a very subjective assessment. The impact on a piece of hardware is much easier to assess whereas the impact on information varies greatly depending upon the extent of the content within the information. Once the impact was assessed for each source we moved to the risk factor calculation.

Risk Factor Calculation

The risk factor is the total of the threat and impact assessments by threat by source of information. The risk factors were stratified into categories of risk from high to low. Although most risk assessment methodologies recommend a cut-off point for further analysis we did not use a cut-off. The GLB Security Program and the GLB regulations were new so to be thorough we looked at all threats. The amount of detail we got into for each threat varied based on the total risk factor.

Current and Potential Safeguard Identification

What safeguards did we have in place to mitigate the risk identified in the aforementioned steps? What are safeguards? Safeguards, also referred to as controls, are used to prevent, detect, or react to a risk. The best places to look for safeguard/control information on the Internet, in my opinion, are audit sites. Of course this is only my opinion, but as an ex-auditor I know the amount of control concentration that profession has and I constantly use their resources as my own. The CoBIT Model (Control Objectives for Information and Related Technology) may be of value and can be downloaded for free at www.isaca.org. Keep in mind that safeguards are often time policies and procedures and that your business users will be a wealth of information if provided the opportunity to provide input.

Also remember that the objective of the GLB Security Program was to protect nonpublic private information from a compromise of confidentiality, integrity, and availability. Each functional area of our team was responsible for revisiting the policies and procedures surrounding each source of nonpublic private information. If a policy did not exist but the procedures were standard practice we put pen to paper and created these policies.

In the meantime I considered an overall control to get the broadest coverage possible for the protection of this information. The first thing that came to mind at the time was employee awareness. As you probably know this is no easy task

and takes time. A couple of months would not be sufficient. An employee awareness program will still be developed but was not a deliverable for this project.

The next thing that came to mind was a legal document to attempt to make employees aware. Working with the Legal Department and the Human Resources Department we were able to create a Confidentiality and Nondisclosure Agreement (NDA) to be signed by all employees. This NDA provided definitions of nonpublic private information specific to GLB privacy and security concerns, company proprietary data, confidential information, etc.

The key to the NDA was to get it right, be as thorough but brief as possible and as stated by Mary Hanson in her article, "Nondisclosure Agreements, Protect Your Business Information", "There is no substitute for taking protective action early on. One cannot reverse the harm of disclosure." This article had a significant impact on the creation of our NDA and is a highly recommended reading. It can be found at www.bizadvisor.com/nondisc.htm.

I could write a whole article on the preparation, approval, and communication of the NDA but suffice to say that there are two elements you must concentrate on. The first is to obtain management buy-in and support. The second is communication, communication to senior management throughout the process and the communication to the employee's of the company. To our organization the NDA was new and was received with some skepticism. With the support of the Legal and Human Resource Departments we were able to address concerns and obtain the acknowledgements needed.

Summation of Safeguards

It's one thing to have policies and procedures. It's quite another thing to document why and how they will be enforced. Fortunately we began this project with a rather detailed risk assessment. This enabled us to link the safeguards to the risk we were controlling with the safeguard. Any open items could easily be addressed as we had the cross-referencing at our fingertips. This also allowed us to revamp current procedures, forms, approvals, etc. to comply with the protection of information. The main ingredient, taking from the NDA discussion, was the communication of why the safeguards exist and how the safeguards will be monitored and enforced.

What was the end result?

The Good

Our GLB Security Program is ready to roll. Our risk assessment is complete and safeguards have been identified. The policies and procedures manual is in place and accessible by all.

The GLB security project had so many arms it's impossible to summarize all the results but I can honestly say that my two biggest accomplishments were the acceptance of the risk assessment methodology which can and has been used on other projects since the wrap-up of GLB, and the enhanced awareness of our employees. The enhanced awareness is our greatest achievement. Employees feel a sense of ownership. They are not just dealing with information. This information has a consumer attached to it and we take them personally. Nowadays when requested to send policyholder or claimant information via e-mail our employees are thinking twice about it.

The Bad

Not really bad as problematic. As with any project of this size the amount of people and the coordination of the information, whether it be the risk assessment or the safeguard information, was difficult. I highly recommend using regular communications to all team members throughout the process. A little communication goes a long way.

The Ugly

The paper, reams of paper. Although our product is also electronically available we had to make hard copies available for review throughout this process. I've personally planted a few trees this year to apologize for all the waste.

Author's Final Comments

Do not be discouraged by the risk assessment process. It is long. It is tedious and it is trying on the patience but the results are worthwhile and it will make your life much easier in the long run. Good luck.

List of References:

Federal Trade Commission. “Gramm-Leach-Bliley Act. 15 USC, Subchapter I, Sec. 6801-6810 Disclosure of Nonpublic Personal Information.” URL:http://www.ftc.gov/privacy/glbact/glbsub1.htm#6801 (28 June 2002).

Peltier, Thomas R. Information Security Risk Analysis. Boca Raton: CRC Press LLC, 2001. 8.

Peltier, Thomas R. Information Security Risk Analysis. Boca Raton: CRC Press LLC, 2001. 71.

Information Systems Audit and Control Association. “Control Objectives for Information and Related Technology Third Edition.” July 2000. URL:http://www.isaca.org/ (17 July 2002).

Hanson, Mary. “Nondisclosure Agreement, Protect Your Business Information.” 2000. URL:http://www.bizadvisor.com/nondisc.htm (23 July 2002).

New Hampshire Office of Emergency Management. “State of New Hampshire Natural Hazards Mitigation Plan.” 23 May 2002. URL:http://www.nhoem.state.nh.us/mitigation/state_of_new_hampshire.asp (17 July 2002).

New Hampshire State Government Online. “Checklist of New Hampshire State Department Checklists.” URL:http://www.state.nh.us/nhsl/checklist94/safe.html (17 July 2002).