Global Information Assurance Certification Paper

Option 2 – Case Study in Information Security: Securing the Network & Business Processes of a Small Financial Services Company Within the Guidelines of the Gramm-Leach-Bliley Act of 1999

Timothy Pendergrass
December 6, 2002

Track 1- GIAC Security Essentials (GSEC)
GSEC Practical Requirements (v.1.4b) (August 2002) – Option 2 Case Study in Information Security

Summary

I was contracted by a small personal financial services company to perform a business security assessment under the guidelines of the Gramm-Leach-Bliley Act of 1999 (GLBA). Since the basis of this project was security, the confidentiality of the Client is required. The Client wanted to develop an understanding of their security posture in context of the requirements of the GLBA. They wanted recommendations and guidelines on establishing a compliant security policy, with a definition of the necessary infrastructure, procedures, and protection technologies for securing their business processes and information system under the subject regulations.

While the Client Organization was initially determined not be in compliance with Federal regulations set forth in the GLBA, some stopgap measures were quickly put in place to reduce their security risk until a more secure and scalable solution could be developed. This paper provides a description of the short-term measures that were put into place, as well as a longer term, more scalable solution consistent with the Client's business processes and strategic plans.

Introduction

I was contracted by a small personal financial services company to perform a business security assessment under the guidelines of the GLBA. Since the basis of this project was security, the confidentiality of the Client is required. The Client will be called ABC Financial Services. The release of any ABC information could be very damaging to the reputation of ABC and could have a critical effect on future business so this paper is sanitized to protect the confidentiality of my Client. Prior to my publishing this paper, the ABC reviewed the paper for sensitive information and approved its public release.

ABC Financial Services wanted to develop an understanding of their security posture in context of the requirements of the GLB Act of 1999. They wanted recommendations and guidelines on establishing a compliant security policy, with a definition of the necessary infrastructure, procedures and technologies for securing their business practices and information system under the subject regulations. ABC Financial Services has annual revenues of approximately $3M in personal loans with an average loan amount of $2,500. The average size of loan payment transactions is approximately $150. ABC's typical customers

request loans for the purchase of automobiles, small consumer items, and in some cases real estate financing.

ABC's management provided their strategic plan that indicated their plans to open at least 4 other offices in other cities within the state, so all the security policy, network design, etc needed to be scalable and transferable. Management disclosed a longer-term objective of the organization was to develop a regional personal financial services organization that would be attractive for acquisition by a larger financial services organization.

ABC is classified as a "licensed industrial loan and thrift corporation". Unlike banks and other federally regulated and audited financial institutions, ABC's class of organization is audited for compliance by a state financial regulatory organization. The State, under whose jurisdiction this financial firm resides, had no information system compliance examiners at the time this work was performed. State legislation is underway to develop stricter, better-defined guidelines for regulation and auditing of the industrial loan and thrift corporations. Given the evolving regulations within the state and ABC's strategic plans, they wanted to be proactive in developing a security posture for complying with any and all regulations governing the protection of customer privacy.

Background and Legal Framework

The Gramm Leach Bliley Act of 1999 (referred to as GLBA or the Act), also known as the Financial Services Modernization Act of 1999, requires financial institutions to develop privacy notices and give their customers the option to prohibit these institutions from sharing their customer information with non-affiliated third parties. More importantly for this project, the GLBA also requires financial institutions to have a comprehensive written information security program for safeguarding nonpublic customer information[1],[2].

In execution of their duties regarding the Act, the Office of the Comptroller of the Currency (OCC), the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) published a joint final rule entitled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information". By attaching these guidelines as an appendix to each of their safety and soundness regulations, these agencies mandated the same requirement for all financial institutions to comply with the Act.

[1] **Customer information** is defined as "any records containing nonpublic personal information, as defined by the Privacy Rule, about a customer." Since the GLBA refers to the protection of customer records and information, the guidelines uses customer information to refer to both information and records.

[2] **Nonpublic personally identifiable information** is defined as personally identifiable financial information that is not available publicly and is either created or contains nonpublic personal information. Examples of nonpublic personally identifiable information would be lists containing information such as loan balances or overdraft information.

The GLBA requires the information security plan be designed to protect customer information by:

- Insuring the security and confidentiality of customer records and information;
- Protecting against any anticipated threats or hazards to the security and integrity of such records; and
- Protecting against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer.

The GLBA specifically requires a comprehensive information security policy be provided to ABC's Board of Directors for review and approval with continuing reviews to be conducted at least annually. The security policy is to outline a proactive and ongoing program consisting of administrative, technical, and physical safeguards to effectively:

- Prevent
- Detect, and
- Respond to information system intrusions or compromises.

Simplistically, GLBA requires organizations manage their data (i.e., handling, protection, and monitoring) to insure they maintain the confidentiality, integrity, and availability of that data. ABC is required by law to conduct an assessment of the risks to customer information and indicate in its security program how it manages the risks.

In collaboration with ABC the following set of guidelines were used for conducting the security assessment and for establishing a comprehensive information security policy for ABC.

- Section 501(b) of the GLB Act
- Federal Deposit Insurance Corporation's (FDIC) "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" – *(See Annex 1 for specific information security measures required by the guidelines)*
- Office of the Comptroller of Currency's Privacy Rule: Small Bank Compliance Guide dated December 2001
- Office of the Comptroller of Currency's "Uniform Rating System for Information Technology", OCC 2001-35 Attachment B.

Before

In performing the security assessment I worked closely with ABC's staff conducting a series of interviews to develop an understanding of their business policies and processes, as well as the functions and transactions that must be executed to conduct day-to-day business operations. I observed employees

interacting with the computer network and specific applications to execute business transactions and developed a list of the processes. Then I developed an inventory list of all ABC's hardware, software applications and operating systems on each computer including specific service packs and upgrades that may have been applied. I also conducted limited testing (port scanning, virus scanning, access control permissions, the GRC "leakage" test) on the hosts and the network to quickly develop a basic assessment of ABC's security posture. The following section describes my findings.

ABC's Business Processes

The key processes that are routinely conducted during each day of ABC's business operations are summarized below. I looked at the individual transactions to develop an understanding of the specific events that put customer private data at risk (*See Annex 2- ABC Financial Processes and Detailed Transactions.)*.

1. Processing customer information necessary to make a decision on whether or not to make a loan to a customer
2. Establish a customer account on an automated software system
3. Execute loan papers (including an acknowledgement that ABC does not sell or share customer information)
4. Process customer payments against the customer account
5. Process, print and mail delinquent notice in the event the customer does not pay in a timely manner
6. Report customer delinquency (after the delinquency period meets a predetermined criteria).
7. Repossess assets used a loan collateral as authorized by the law.

Key Applications Running in ABC's Environment

The list below summarizes the application software installed on each of the PCs within the network. These applications are used to conduct day-to-day business operations.

- *Microsoft 98 OS Second Edition* – This OS was installed on each of the three (3) PCs on the network. None of the Microsoft Service Packs or system upgrades, or critical security patches had been downloaded and applied.
- *Microsoft Office 97 Application Suite* – was installed on each PC.
- *Outlook* – the Internet Service Provider maintains Company email accounts.
- *Loanmaster* – This software represents the core functionality of ABC's business process. ABC uses this software as a loan calculator, loan accounting, loan tracking, and loan servicing systems. It stores all private and sensitive customer private data. This application resides on the standalone PC designated as the office server. The software vendor provides upgrades and systems improvements via floppy disks or CD-ROM, depending on the size of the upgrade.

- *Symantec PCAnywhere* – was installed on the supervisor's PC, which is designated as the Internet gateway access computer. This software was installed to allow the Loanmaster Vendor remote access for the purpose of time critical troubleshooting of Loanmaster related problems.
- *Norton Anti-Virus* – an old copy was loaded on the supervisor's Internet gateway computer only. The subscription service had expired and the virus definitions had not been updated in approximately 1 year.

Network Description

ABC's initial network configuration is a peer-to-peer configuration consisting of a standalone PC designated as an application/database server networked to 2 standalone PCs using USB cables and Internet Connection Sharing software by Sygate. The operating system was Windows 98 Second Edition. The supervisor's PC had a modem installed for Symantec PCAnywhere remote dial-in access and an outdated anti-virus program installed. Internet access was provided via a dial-up modem in the supervisor's PC. The initial network is described in Figure 1 on the following page.

Problem Definition

After observing ABC's business operations in action and preparing the inventory lists, I reviewed the test results to make an assessment the state of ABC's security posture. The following section describes my findings.

A. Physical Security Deficiencies

- ABC Financial Services did not have a written security policy.
- Hardcopies of applications and loan papers were stored in unsecured containers in an open work area.
- Trash cans were being used to dispose of papers that could have contained customer private data. There was no segregation of trash from draft or trash loan papers that were being disposed.
- The computer designated as the "server" which contains all of ABC customer private information was located under the receptionist's desk – an unsecured location.
- Surge protectors were not used to minimize the risk of electrical surges to the information network.

B. Information System Security Deficiencies

- ABC Financial Services did not have an information security policy.
- No firewalls (hardware appliances or software) were present on any of the computers or the network perimeter.
- The server where the Loanmaster and all private customer data reside was fully accessible by anyone on the network. There were no access privileges on the server, or the customer database.
- The supervisor's computer (the Internet gateway computer) was the only one of the three computers had anti-virus software installed and the service subscription had expired and virus definitions were outdated for

over one year. A virus scan of this machine discovered 1 file infected with the W32.HLLW.Bymer virus.

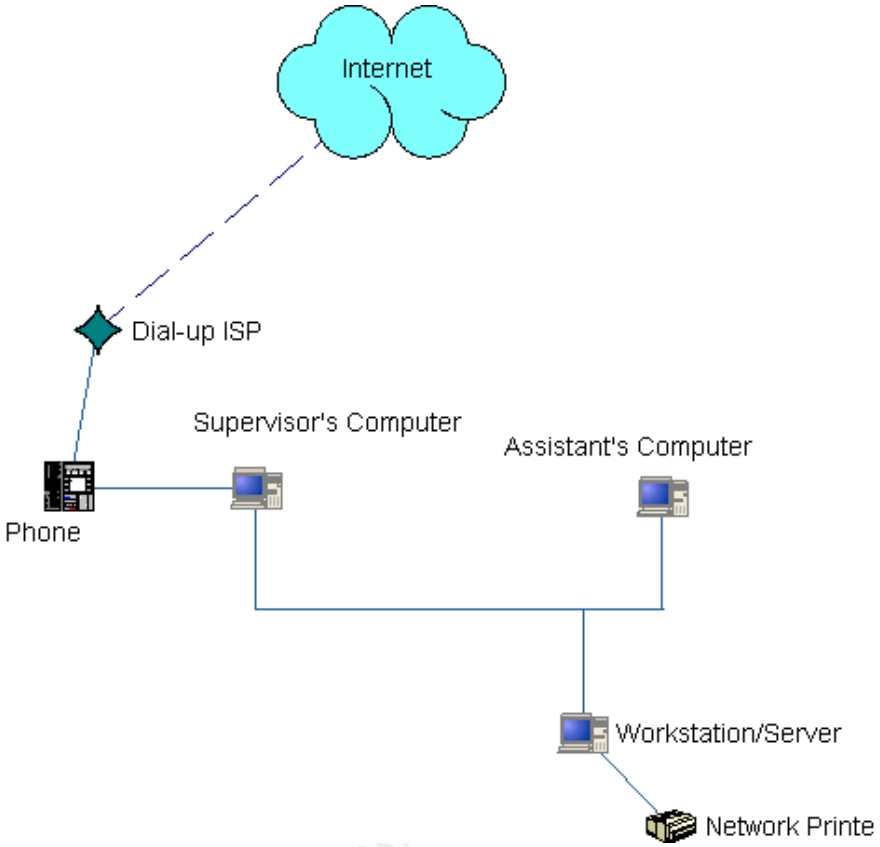

Figure 1. ABC's Initial Network Configuration

- The supervisor's Internet gateway computer made an automated dial-up connection – failed GRC's leak-test.
- Sygate contained passwords for ABC's dialup access account for Internet connection sharing. The computer automatically dials out to the Internet without any action required from a user. Sygate also contained other user ID's and passwords for some other type of unidentified account.
- PCAnywhere was configured such that it allows dial-up remote access with no password or authentication of any type.
- Microsoft Windows 98 Second Edition Operating System (OS) offers inadequate security features for providing access controls to private customer data.
- The OS had not been updated with Microsoft's Service Packs or critical service packs.
- Plans call for Internet access via a DSL service provider.
- Strategic planning indicated a requirement for VPN connection between future offices.

What became obvious very quickly was that, as with many small, local financial services firms that are not rigorously audited by bank examiners, they did not have a security policy, and unfortunately they had no information system security measures (procedures or technologies) in place. It became immediately apparent ABC would not be able to pass an audit under the GLB Act based on their lack of a security policy and security measures. Upon delivering the bad news to the ABC's management, they immediately responding saying that this situation must be repaired as soon as possible and that GLB compliance was a firm requirement for their organization.

As an interim solution and stopgap measure, I installed a combination firewall, intrusion detection system, and anti-virus software package to reduce the networks exposure to risk. Each workstations and the server was scanned for viruses. Additionally, a basic 56K dial-up router with NAT firewall protection was installed. This provided an increased level of security such that other infrastructure and security alternatives could be identified.

During

The fundamental approach I used in addressing ABC's security risks and risk mitigation mechanisms was the application of systems engineering process to balance security, cost, and business need. This included developing an understanding of the following:

- Who and what are the threats?
- What are the most important attacks to defend against?
- What are the implications if assets were damaged or lost?
- What can be done to minimize exposure to the loss or damage?

The following sections address each one of these questions.

Who and what are the threats? – Threats are described as anything that would contribute to the tampering, destruction or interruption of a service or item of value. A threat is applied against vulnerability and that results in a compromise, denial of service, or damage. A threat vector is the method a threat manifests itself against a target. Threat analysis should consider every element of risk that could conceivably happen including human threats and those that are non-human.

The human threat matrix is divided into threat categories, actors, and motivations. Each motivation category is then assigned a business environment judgment based ranking factor. A value of "1" indicates a low likelihood, "2" is moderate, and "3" is the greatest or most likely motivation. The specifics business objectives and environment of ABC Financial Services influence the likelihood factor.

Table 2 below represents the "Human Threat" matrix with my judgment rankings as to the likelihood of a threatening event occurring based on the profile of ABC Financial Services. It is my judgment the primary threats include the shared and local threat listed below:

- Shared threats
  - Industrial espionage,
  - Organized crime, and
- Local threats
  - Institutional hackers,
  - Recreational hacker,
  - Employee/Insider.

Reasons/motivations for these threats manifesting in compromise or damage appears to be the following:

- Financial gain,
- Identify theft,
- Unintentionally accident caused by internal person,
- Competitive advantage, or
- Hacker performing untargeted damage or compromise for the thrill or challenge.

Currently the hostile or intentional insider threat is low, however it will increase as ABC expands and opens new offices.

The Non-human threat vectors include events such as:

- Computer viruses,
- Natural disasters (floods, lightning strikes, earthquakes, tornados)
- And facility problems or failures (plumbing failures, fire, electrical problems, air quality (dust), heat control).

A computer virus is probably the most likely non-human threat vector. Based on the location of ABC's facility, floods and earthquakes are very unlikely occurrences. While quite common, the threat from electrical problems and lightning can be minimized by the use of surge protectors and back-up power supplies.

What are the most important attacks to defend against? – In the Problem Definition section I described the security posture of ABC and outlined both physical and information system vulnerabilities. In developing a security policy and secure network it is important to understand how some of the systems vulnerabilities could be attacked.

Table 2. Human Threats, Actors, & Motivations[3] Against ABC Financial Services

Threat Category	Actors	Motivations	Likelihood*
National Security Threats	Info Warrior	Reduce US Decision Space, Chaos, Target Damage	N/A
	National/State Intelligence	Information for Political, Military, Economic Advantage	N/A
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change	N/A
	Industrial Espionage	Competitive Advantage	2
		Intimidation	1
	Organized Crime	Revenge	1
		Retribution	1
		Financial Gain – ID Theft	3
		Institutional Change	1
Local Threats	Institutional Hacker	Monetary Gain	3
		Thrill	1
		Challenge	1
		Prestige	1
	Recreational Hacker	Thrill	2
		Challenge	2
	Insider/Employee	Accident	3
		Financial Gain	1
		Revenge	1
Likelihood Ranking: N/A – Not applicable, 1- Low, 2 – Moderate, 3 - Highest			

There are many variations in attack methods, but they are generally grouped in four categories:

- Information gathering,
- Unauthorized access,
- Disclosure of information, and
- Denial of service.

Information gathering is not specifically an attack; it is a set of actions an attacker may perform in preparation for an attack. This activity is conducted to gather information about the computers, services running on the computers or network, and the users - ABC's employees. Information gathering activities include the following:

[3] Methodology by Eugene H. Spafford, "A Small Dose of Infosec". November 2000, Purdue University, Center for Education and Research in Information Assurance and Security

- Social engineering attack - An attack of this nature might be human-based and it could involve a person trying to obtain critical customer information (password, key, file or record) from an ABC employee. Typical techniques involve using the excuse of urgency, impersonation and third-person authorization.
- Computer based social engineering attack - An example might be a pop-up window saying your Internet connection has timed out, please re-enter your username and password to log back on. Another more recent approach would be for someone to email something with a funny or sexy subject title to attempt to get an ABC employee to open an email attachment out of curiosity. Opening the attachment could allow the use of a "worm" to obtain your user name and password.
- Dumpster diving – Dumpster diving could be used to search through ABC's trash to find customer records or data. Dumpster divers would also be looking for notes with passwords and user IDs scribbled on them. Additionally, organizational information and ABC employee information could be useful in trying to impersonate a staff member in a social engineering attack.
- Sniffing – "Sniffing" is the process of reading network traffic via a protocol analyzer. This is a viable information gathering technique since many protocols do not encrypt information. Passwords and usernames can be harvested using protocol analyzers. Currently, ABC and their Credit Agencies use secure socket layer (SSL) encryption to minimize the possibility of someone "sniffing" the communications link between the two and avoid them harvesting customer data in transit.
- Basic services - Another means for information gathering is the use of "Basic Services", such as FINGER, NETSTAT, and the SMTP primitives VRFY and EXPN. These types of services are still widely enabled and can be used by an attacker to find out information about ABC users or see if particular accounts exist.
- Scanning - "Scanning" refers to the process of attempting to connect to a range of port numbers or IP addresses to identify what services or computers exist at ABC and if they are turned on. It is one the most widely used method by attackers to find out if what they are scanning is going to be their next potential victim. Scanning tools are automated, and they are numerous variations of these tools widely available to aid an attacker. During scanning an attacker will look for your operating system version hoping your system is "unpatched" and has vulnerability.
- War dialing – "War dialing" is the scanning of phone numbers in an attempt to find ones with modems on them in the hopes that the attacker can break into the computer via the attached modem. These back doors to an organization's infrastructure are usually poorly secured (if secured at all) which makes the attacker's job easier to gather information or break into a system.

Unauthorized access could be used to break into ABC computer network and download information, manipulate data, delete files, and open other routes for access to ABC's information systems. Some of the types of unauthorized access include the following:

- Misadministration - Hackers will also try to exploit systems that have trust relationships that may have been misadministered. Trust relationships can range from basic user accounts allowing people to access computer resources; to services of other networked computers which users or computers are allowed to have access to. "Individual User Accounts" are the most basic trust relationship. Accounts come with passwords: users tend to use passwords that are easy to remember (pet's name, birthday, etc.). Alternatively, if users are forced to use account passwords that are difficult to remember, they will write them down or record them somewhere, which is considered to be more insecure. Passwords are also susceptible to being sniffed by an attacker.
- Exploiting non-authenticated services - There are a number of network services that do not use any authentication. These services could be easily spoofed, or could be used to access or modify information on ABC's computers. TFTP (Trivial File Transfer Protocol) does not use logins or passwords, and relies only on file system access permissions. SMTP (Simple Mail Transfer Protocol) has no mechanisms for positively identifying the sender of e-mail, making it very easy for an attacker to spoof e-mail. DNS (Domain Name Service) uses a hierarchy of name servers to look up IP addresses for domain names. RIP and IGRP are routing protocols used by routers and hosts, which broadcast information of how to route to other networks. They have no authentication, so any host or router listening for RIP or IGRP packets could be misdirected to an attacker's network.
- Exploiting centralized services - There are network services that aid in assisting network administrators in managing networked hosts and these services can also be susceptible to vulnerabilities if not properly administered or accessed outside your trusted network. SNMP (Simple Network Management Protocol), which is used to manage network devices and read traffic information, uses a community name as its password. This password is transmitted as clear-text and is usually set to the word public, which makes it very easy for an attacker to guess.
- Malicious data - These data could be injected into ABC's computer environment by visiting and downloading software from websites or from email attachments. Malicious data is information input to programs that can cause the program to take action that the program would not normally do or cause damage to the host system. Also, new features within programming allow much more action to be taken based on input data. These features can come in the form of macros, auto play features, Java and ActiveX, and postscripts. They add power to applications, such as inputting data automatically into an application or downloading executable data to be run on a client's computer.

- Spoofing – "Spoofing" is pretending to be someone or something you are not. User account spoofing is using another person's account name and password without their permission or authority. Sniffing the network or breaking password files aids an attacker in user spoofing.

Denial of service (DoS) attacks cause the loss of access to a resource rather than allow the attacker to gain unauthorized access to the resource. They usually involve overloading a resource such as disk space, network bandwidth, internal tables of memory or input buffers (buffer overflow). The overload causes the host or particular service to become unavailable for legitimate use.

What are the implications if assets were damaged or lost? – Assets that were considered included the loss of communications, loss of access or functioning of computer system services, and the loss of data.

- Loss of computer communications - ABC does not conduct website transactions. The only transaction that uses the Internet is the transmission of customer data to the Credit Reporting Agencies and receipt of credit reports from those agencies. The service can be executed via fax machine if necessary, so the primary impact of the loss of Internet data communications would a delay and disruption in loan processing.
- Loss of computer access or functions –Loss of automation or computer services can be devastating in any business in today computer society. While the loss of computer would certainly delay and disrupt business operations, ABC staff members have used hand-ledgers, calculators, typewriter and other manual methods to conduct business in the personal financial service market.
- Loss of data – ABC conducts weekly backups of all activity and stores that data in a secure, fireproof container, so business operations could be reconstituted. However, in a worst-case scenario loss of customer private could destroy ABC's business through GLBA induced fines and customer lawsuits *(See Annex 1 for fines for lack of* compliance).

What can be done to minimize exposure to the loss or damage? - After interviewing staff members and watching them perform their daily job functions, I developed a series of security policy guidelines considering the GLBA regulations and the inventory of ABC's assets (operating system and application software, and a topology of the computer network including all hardware).

Minimizing Customer Data Exposure Using the Interagency GLB Guidelines

The GLBA requires ABC Financial Services to have a comprehensive written information security program for safeguarding nonpublic customer information. After developing an understanding of the specific requirements imposed by the Act and follow-on guidance I began preparing a list of security guidelines and provided security policy templates (from the SANS website) such that the ABC Financial Services management can develop a GLB Act compliant security policy

for the Board of Directors to approve and review on a continual (at least annually) basis.

Referring back to the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" requires financial institutions to adopt the following measures to the extent that they are likely to protect customer information:

1. Access controls on customer information systems;
2. Access restrictions at physical locations containing customer information;
3. Encryption of electronic customer information;
4. Procedures to ensure that system modifications do not affect security;
5. Dual control procedures, segregation of duties, and employee background checks;
6. Monitoring systems to detect actual attacks on or intrusions into customer information systems;
7. Response programs that specify actions to be taken when unauthorized access has occurred; and
8. Protection from physical destruction or damage to customer information.

Some of the considerations that went into developing my specific recommendations were things such as the specific business processes, functions, and transactions that were detailed earlier in the report. Great consideration was given to specific transactions that could potentially expose or disclose customer information. As an example, the handling and storage of hard copy credit applications, transmitting customer sensitive data across the Internet to the Credit Bureaus. The emphasis is to provide guidelines that are not too complex or restrictive such that the employees circumvent them. Ideally, the security becomes a natural part of ABC business process.

The specific policy guidelines I prepared recommended the following considerations that are consistent with Interagency Guidelines listed above. These recommendations included:

- Access controls - user IDs and passwords should be implemented at a network and host level, depending on employee responsibilities and access.
- Separation of duties – the small number of staff members reduced the importance of this measure at this time. However, as ABC continues to

grow and more offices open, this security measure should receive a higher priority.

- User authentication, through user ID's and password. Password should be 7 or 8 characters long and should contain 3 of following (4- upper and lowercase, numbers, special characters)
- Workstation lock screens – this should be implemented. Deployment of Windows 2000 Professional will provide this capability.
- Encryption – SSL encryption is utilized to transmit customer private information and data to and from Credit Bureaus. Encryption of customer data on the database server should be considered in the future.
- Proper directory and file permissions – Windows 2000 Professional will allow the Manager/Supervisor to easily restrict access to certain files on the server (e.g., no one other than the Supervisor has global access to the Loanmaster customer database).
- Properly defined user rights – Limit read/write access should be implemented to avoid accidental damage to files, systems, and the network.
- Change control policy – System or network changes should only be limited to authorized users only. Document any and all changes made to the system/network configuration.
- Social engineering prevention – Establish a policy that no customer information will be passed over the telephone, and all persons requesting information on customer accounts must be positively identified with photo identification.
- Applying patches/updates – Microsoft website should be checked for new patches and upgrades on a weekly schedule. Deployment of Windows 2000 Professional eases management and installation of operating system patches and upgrades. Each system should be upgraded when new patches or upgrades become available. The Loanmaster software should continue to be upgraded via floppy disk or CD-ROM, but only after the media is virus scanned.
- Server-based data integrity assurance solution – A commercially available server software will be used to assure the security and integrity of customer private data on ABC's servers by notifying users if, when, and how files have changed.
- Firewalls - A network perimeter router/firewall appliance should be installed behind the DSL modem. Each host should have a personal firewall and intrusion detection system installed.
- VPN tunneling – The router/firewall appliances deployed at the network perimeter could have a VPN option.
- Anti-virus software – Keep your virus definitions up to date. Virus software should be used on the network perimeter router/firewall. Also use individual virus software on each individual computer.
- Background investigations – Conduct a background investigation on each new employee. Consider routine investigations on a periodic basis.

- Prompt removal of terminated/transferred employee accounts –Insure default passwords and unnecessary services are not running on the system,
- Review and management signoffs of user authorizations – This should be implemented as the organization grows and new offices are opened.
- Use of checksums with attendant software to report file modifications – in the case of Loanmaster, if upgrades are downloaded from the Internet, require the use of a checksum to insure the software you downloaded is the software you think it is. Also, checksums could be used to insure the integrity of the Loanmaster customer database.
- Enable audit logging and perform log reviews – Firewall, anti-virus, and intrusion detection software maintains historical log files. Learn to understand them, and review them routinely for indications of an intrusion or system compromise.
- Conduct vulnerability assessments – Use port scanners and vulnerability scanners to review open ports and services to insure the network configuration and systems are consistent with your security policy. Your security policy and banner ads should state that you monitor your network routinely and user access is acknowledgement that their actions may be under subject to monitoring.
- Routine backups – regularly scheduled back-ups with cold boot installations from back-up to insure integrity of back-ups.
- Secure your trash – Do not allow employees to put anything but trash (soft drink cans and bottles, food wrappers, debris, etc.) in the regular trash containers. Purchase a locked security trash container for disposing of customer private data, financial forms of any type, and other proprietary data. Purchase a shredder to destroy this information. Don't allow "dumpster divers" to gain access to your sensitive data.
- Use lockable filing cabinets - Store all customer applications, data, forms, and customer lists in locked filing cabinets located outside of the normal flow of business traffic.

In developing these guidelines, previous reviews with management indicated that they wanted to consider building a new network infrastructure. This provided an opportunity to build in the proper security into the system design and provide mechanisms to upgrade as their network and business expands (e.g., VPN tunneling from the Corporate Office to other Regional Offices).

After

ABC's management's desire to be compliant with the GLBA, and have a work environment that was scalable as new offices were opened dictated a new information system infrastructure. I considered a full range of operating systems and security technologies consistent with the GLBA customer data protection regulations and ABC's business environment. This placed restrictions on the specific operating systems, intrusions detection systems, and overall network architecture in that ABC Financial Services has a small staff with extremely

limited information technology and security skills. This fact placed a significant responsibility to implement simple security measures in the new network security architecture and procedures. Employees will need some training on security procedures per the ABC Security Policy once the new architecture is established. Consideration of the IT skills of the staff members limited some of the alternatives, while other alternatives were too costly. Consideration should be given to use of a properly vetted third-party to monitor the network and assist management in maintaining a proper security posture.

An Improved Network Design with Built in Security

The proposed system architecture is based on the concept of defense-in-depth security. The architecture provides security at four layers:

- **Layer-1:** Perimeter Defense – router with stateful firewall appliance and anti-virus software, and intrusion detection system.
- **Layer-2:** Operating Systems and Servers Protection – Protections and authorizations that limit who can change configuration setting and add new software or upgrades.
- **Layer-3:** Host Protection – individual, host based firewall and IDS
- **Layer-4:** Information Protection - IDS on Server, data and application integrity assurance protection.

In reviewing ABC's application software I noted that Loanmaster worked with a limited number of Windows operating systems: Windows 95, 98 SE, NT, and 2000. Windows 2000 was selected as the network operating system. Windows 2000 Server will be installed on the File Server where Loanmaster resides. Windows 2000 Professional will be installed on the workstations.

ABC will use Microsoft's Knowledge Base Article – 303323: "How to Maintain a Secure Small Business Server Installation" (http://support.microsoft.com/default.aspx?scid=kb;en-us;q303323) to assist in the installation of the Windows 2000 Server on the file server. ABC will install any critical security service packs.

ABC will use Microsoft's "Make Your Desktops Secure" to install Windows 2000 Professional on each of the workstations. (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/ChkList/dsktpSec.asp)

Appropriate host-based firewalls, intrusion detection systems and anti-virus software will be installed on each of the workstations, as well as the server.

Based on the ABC's policy guideline recommendations the network architecture described in the following section was proposed. ABC is planning to allow a qualified third-party to deploy this system, and I will be conducting vulnerability

assessment and security auditing to insure the configuration is consistent with the planned deployment configuration.

Figure 2 below describes the general network architecture. The general specifications of products selected are described below.

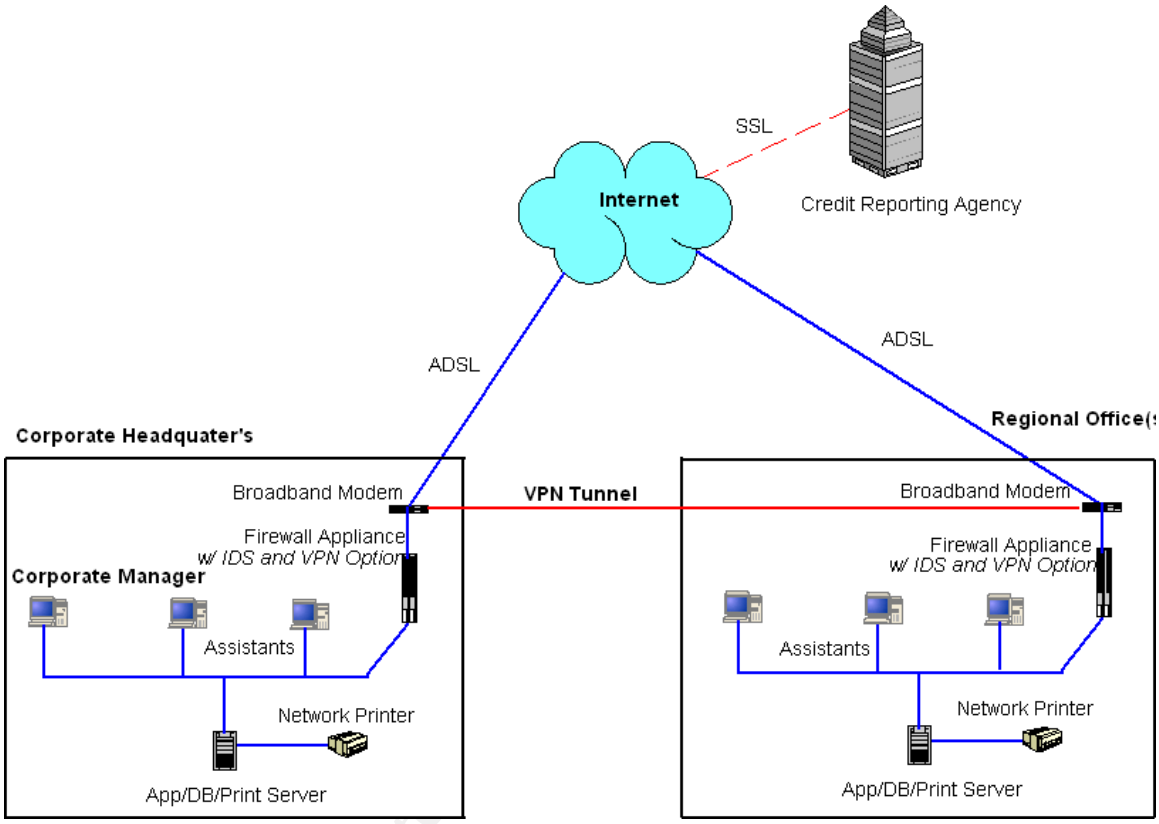

Figure 2. New GLB Compliant Network Architecture

General Equipment Specifications – (While specific hardware was specified in collaboration with ABC management, general technical specifications are only described in this paper)

- Internet access – ADSL access with provide ABC with Internet access.
- Perimeter-based firewall appliance – A combination router/firewall appliance with stateful packet inspection (SPI) and intrusion detection denial of service (DoS) attack protection and VPN pass-through and Network Address Translation (NAT) Routing. The VPN pass-through will allow secure access to other ABC office networks.
- Server with Windows 2000 Server – A host-based firewall, intrusion detection system, and anti-virus software will reside on the server. The server will have an Ethernet adapter installed for access to the router.

Additionally, the Loanmaster database and software will be protected by a data integrity assurance application that notifies the users, or monitoring center if, when, and how files are modified.

- Workstation with Windows 2000 Professional. - A host-based firewall, intrusion detection system, and anti-virus software will reside on the server. Each computer will have an Ethernet adapter installed for access to the router.

ANNEX 1: What Information Security Measures Do the Guidelines Require?
Section III.C.1. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" requires financial institutions to adopt the following measures to the extent that they are likely to protect customer information:

1. Access controls on customer information systems;
2. Access restrictions at physical locations containing customer information;
3. Encryption of electronic customer information;
4. Procedures to ensure that system modifications do not affect security;
5. Dual control procedures, segregation of duties, and employee background checks;
6. Monitoring systems to detect actual attacks on or intrusions into customer information systems;
7. Response programs that specify actions to be taken when unauthorized access has occurred; and
8. Protection from physical destruction or damage to customer information.

Although the Guidelines by and large do not require institutions to use specific products, the agency Examination Procedures specifically advise examiners to look for intrusion detection systems in connection with item 6 above:

> "Review monitoring systems and procedures, *including network and host intrusion detection systems (IDS)*, network traffic monitoring, manual reviews of logs and other information available to assess management's monitoring process."[4] (Emphasis added)

[4] Federal Register 12 CFR Part 30 et al. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year

These Examination Procedures were created by the agencies as a checklist for examiners to use when determining whether institutions meet GLB requirements under the Guidelines. Although the Guidelines have been in effect since July 1, 2001, many institutions may only now be preparing for their regular agency examinations. Given that an intrusion detection system is one of only two specific technologies that the Examination Procedures identify (the other is encryption), the relative weight that examiners assign to an intrusion detection system may become very important during a review of the institution's GLB compliance.

Damages, Fines and Penalties Under GLB

Under GLB Section 505, the agencies may enforce GLB with the same sanctions that they currently use to regulate financial institutions. For example, the FDIC may enforce violations under Section 8 of the Federal Deposit Insurance Act, which gives the FDIC the authority to impose penalties ranging from $5,000 per day up to $1,000,000. GLB Sections 521 and 523 also provide enhanced criminal penalties for persons who gain fraudulent access to protected financial information. Clearly failure to comply with current and emerging regulatory guidelines could be a very expensive and detrimental business decision.

Additionally, Congress is considering regulations like the Financial Institution Privacy Protection Act, which would amend the GLBA to make officers and directors liable for up to $10,000 for each privacy violation. In contrast to this, cases where state institutions have regulatory authority over financial institutions, the degree to which the state examines companies for their compliance with the security policy and procedures requirements varies greatly from state to state. So anyone performing a security or risk assessment with a state regulated company should check the state regulatory agency for that state's requirements. In the state where my ABC is located, the state compliance examiner only monitors to insure that annual privacy notices are mailed to all customers.

Annex 2: ABC Financial Services Processes and Detailed Transactions

Process 1 - Processing customer information

- A customer physically visits ABC's office to request a personal loan. The potential customer is required to present photo identification before a loan can be processed.
- ABC collects customer private data (name, date-of-birth, social security number, addresses, employment history, next-of-kin (name, address, phone numbers)) and financial information (salary, credit card numbers, loan numbers, and assets (property

---

2000 Standards for Safety and Soundness; Final Rule" February 1, 2002, URL: http://www.ots.treas.gov/docs/73112.pdf

addresses, vehicle identification numbers, etc.) in hardcopy format via a credit application.

- ABC transmits specific customer information (name, address, social security number, and date-of-birth) to one or more of the major credit agencies (Experian, TRW, or Equifax) via the Internet using secure sockets layer (SSL) data security.
- The credit agency sends a detailed customer credit history report to ABC via the Internet using SSL data security. The detailed information provided to ABC by the customer along with the credit reports from the Credit Agency are utilized to make a final determination regarding whether to make a loan to the customer.

Once the decision to make a loan to a customer is made, a different series of transactions occur.

Process 2 – Establishing a Customer Loan Account

- All of the information collected in the loan application process is entered into Loanmaster software to prepare a Customer Loan Account. This software provides a hardcopy of a standard loan package for the Customer to sign. This software provides "auditing functionality" such that if a loan is created and check is issued, the software notes any and all transactions including clerical errors that cannot be erased or deleted. Information cannot be deleted once it is entered.

Process 3 – Execution of the Loan Agreement

- This loan documentation is executed in duplicate (1 copy of Customer, 1 for ABC's records). ABC does not share customer information with any unaffiliated 3rd parties, it was further noted that no written documentation is provided allowing the customer to "Opt-Out" from private information sharing per the Act.

Process 4 - Process customer payments against the customer account

- ABC receives loan payments in the form of cash or check via two methods. Most check payments are received via mail; cash payments are typically made in person at ABC's office. Each customer transaction is executed using the Loanmaster Software and copies of the transaction are provided to each customer. This software provides "auditing functionality" such that if a loan is created and check is issued, the software notes any and all transactions including clerical errors, which cannot be erased or deleted.

Process 5 - Process, print and mail delinquent notice in the event the customer does not pay in a timely manner

- In the event the Customer does not pay each payment in the contracted time period, ABC mails a "late payment notice" to the customer.

Process 6 - Report customer delinquency to credit agency (after the delinquency period meets a predetermined criteria).

References

1. Lang, Marion. "Gramm Leach Bliley Act of 1999: What Information Security Professionals Need to Know", April 4, 2001. SANS Reading Room. URL: http://rr.sans.org/legal/gramm.php
2. Public Law 106-102, 106th Congress, 1st Session. Gramm-Leach-Bliley Act of 1999. November 12, 1999. URL: http://www.finmod.state.tx.us/content/theact/glba.pdf.
3. Federal Register 12 CFR Part 30 et al. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule" February 1, 2002, URL: http://www.ots.treas.gov/docs/73112.pdf
4. Federal Register: May 23, 2002 (Volume 67, Number 100, Page 36483-36494) Federal Trade Commission, 16 CFR Part 314, "Standards for Safeguarding Customer Information; Final Rule". URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-12952-filed
5. FDIC: Privacy Choices, "Privacy Choices for Your Personal Financial Information". URL: http://www.fdic.gov/consumers/privacy/privacychoices/index.html#appendix
6. FDIC: Financial Institution Letters, "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information", August 24, 2001. URL: http://www.fdic.gov/news/news/financial/2001/fil0168a.html
7. Office of Currency Comptroller. Pamphlet OCC 2001-35, Attachment A: Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information.
8. Piepers, Eric. "Cost-effective Information Security (Information Security from a business perspective)", June 6, 2001. SANS Reading Room. URL: http://rr.sans.org/audit/cost-effective.php
9. Litzau, David. " Risk Management: A Foundation for Information Security", June 7, 2001. SANS Reading Room. URL: http://rr.sans.org/audit/risk_manage.php

10. Eugene H. Spafford, “A Small Dose of Infosec”. November 2000, Purdue University, Center for Education and Research in Information Assurance and Security
11. Nichols, Arthur. “A Perspective on Threats in the Risk Analysis Process”, August 31, 2001. SANS Reading Room. URL: http://rr.sans.org/audit/risk_analysis.php
12. Bayne, James. “An Overview of Threat and Risk Assessment”, January 22, 2002. SANS Reading Room. URL: http://rr.sans.org/audit/overview.php
13. Vono, Vincent. “A General Overview of Attack Methods Vincent”, June 25, 2001. SANS Reading Room. URL: http://rr.sans.org/threats/attack_methods.php
14. Garbars, Kurt. “Implementing an Effective IT Security Program”, August 28, 2002. SANS Reading Room. URL: http://rr.sans.org/audit/IT_sec.php
15. Mathew, Dennis. “Choosing an Intrusion Detection System that Best Suits your Organization”, September 16, 2002. SANS Reading Room. URL: http://rr.sans.org/audit/best_suits.php
16. Fyfe, Bruce. “Building a Secure Windows® 2000 Professional Network Installation - A Best Practices Approach to Securing a Windows® 2000 Networked Workstation”, April 24, 2002. SANS Reading Room. URL: http://rr.sans.org/win2000/net_install.php
17. Microsoft Knowledge Base Article – 303323: How to Maintain a Secure Small Business Server Installation, http://support.microsoft.com/default.aspx?scid=kb;en-us;q303323
18. Microsoft “Make Your Desktops Secure” (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/ChkList/dsktpSec.asp