Safe, Sound & Secure: Ensuring GLBA Compliance

Introduction

When Congress drafted the Gramm-Leach-Bliley Act (GLBA) in 1999, Y2K was on the minds of every CIO, not customer data protection. We live in a much different world since GLBA compliance became mandatory as of July 1, 2001. Even as the Federal Reserve, Federal Trade Commission, Federal Deposit Insurance Corporation, Office of the Comptroller and Currency and State Attorneys General have begun holding financial holding companies accountable for ensuring the security and privacy of their customer data, many banks are resisting the change. While excuses range from insufficient funds to poor planning, the Federal Reserve is interested in only one thing: compliance. In order to fully comply with the GLBA, most banks today must go beyond their existing security program, be proactive in assessing the security risks, and put best practices and security policies in place to properly protect their customer information. The good news is that this process is not as expensive or as daunting as many bank executives believe.

Two-Pronged Approach: Privacy and Security

The GLBA addresses two related aspects of customer information: privacy and security. Because technology will continue to alter the way money and information are transacted, the GLBA is necessarily vague when it comes to privacy protection. Section 501(b) of the law states only that "financial holding companies must properly protect privacy information." It is the Federal Reserve, as the enforcer of the GLBA, that has enumerated exactly what "proper" protection entails.

One of the most important parts of the GLBA's privacy management requirements is customer notification. The GLBA requires banks to inform their customers annually on how the customers' private information is being protected. Often, the statement simply assures the customers that their information is safe with the bank, without explaining the details. But the bank must also explain its policy on sharing nonpublic personal information (NPI) and provide "opt-out notice." Consumers have the right to opt-out of NPI sharing, requesting that their NPI not be shared with non-affiliated third parties, such as telemarketers. Banks must give customers reasonable notice—30 to 60 days—to opt out, but the onus is on the customer to make the request. A bank, however, is free to share information with its affiliates for official business purposes, such as check automated clearing houses, without notifying the customer.

The GLBA has clear security management requirements as well. The Federal Reserve requires a financial holding company to create a security program and have a security officer to oversee and maintain that program.

The Role of a Security Officer and Board of Directors

The first step in achieving security compliance is having a security officer. Since the role of a security officer is still fairly new, banks are still struggling to find security gurus that know both the technical side of banking to create a suitable security program as well as the business side to be aware of what a security program must sufficiently protect. Security officers with strictly IT backgrounds might know all about firewalls and encryption, but they might not have the ability to understand the business decisions of executives or successfully communicate with a board of directors. The ability to articulate the security needs to senior management or a board of directors is especially crucial when it comes to obtaining a security budget: a skilled security officer will explain the needs and benefits of a proper security program well enough to obtain the necessary funding.

A common mistake made by a bank is to simply assign the duties of a security officer to its chief information officer. To some extent, the roles of chief information officer and security officer can pose a conflict of interest. Also, with the amount of work that is needed to ensure compliance to GLBA, adding the task of security officer to CIOs usually lead to unsuccessful outcomes.

In addition to creating the role of security officer, the Federal Reserve requires involvement of the bank' board of directors to ensure that the bank takes information security seriously. To show a bank's commitment to security, its board must be briefed on security, at least annually, to oversee development, implementation, and maintenance of the actual security program. By holding the board responsible for knowing that a security program is properly implemented, the Federal Reserve has demonstrated the importance of "protection" as stated in the GLBA.

Building GLBA-Compliant Security Program

Once a bank has a qualified security officer in place, the next step is for that officer to develop a GLBA compliant security program. The easiest way to ensure GLBA compliance is meeting the requirements of the International Standards Organization (ISO), which are approved by the Federal Reserve. Additionally, by simply following the directives listed in ISO-17799, a U.S.-based bank will be compliant with any nation in which the bank operates. ISO-17799 provides 10 basic components that formulate a sound, compliant security program for a bank or financial holding company.

1. **Business continuity planning**. This strategy counteracts interruptions to business activities and to critical business processes from the effects of major failures or disasters. Banks should have a plan for when a hacker or virus strikes the computer systems to ensure that critical information is always accessible.

2. **System access control**. Banks must be aware of all the ways information can be accessed. Can malicious and unauthorized users gain entry into a bank's records? Is a bank's online information accessed regularly by customers? System access control ensures that access to non-public personal privacy information is protected and that non-sanctioned activities are eliminated.

3. **System development and maintenance.** This prevents loss, modification or misuse of a bank's data systems, as well as protects confidentiality. Security must be built into operating systems and around applications, especially if a bank is developing its own online banking software. Involving security right from the start saves time and money later.

4. **Physical and environmental security.** Many people look at this type of security as the responsibility of the IT facilities department, but that shouldn't be the case. This type of security prevents loss and theft of sensitive information from the business premises, anything from a box of checks to a printout of account numbers.

5. **Compliance.** Banks must do everything it can to avoid any breaches of the law and create a security program that follows industry-accepted standards.

6. **Personnel security.** Financial holding companies should use security awareness training to reduce the risk of human errors and abuse of facilities.

7. **Security organization.** A dedicated security organization should manage information security within a company. The ideal security team would be comprised of the CEO, the general counsel, the CIO, the security officer and other security groups that manage information security, the audit group, and the compliance and risk management groups will ensure that all the necessary parties are involved in the security planning.

8. **Computer and operations management.** A typical bank processes more than half of its assets in a day just in transactions. Security must be built into all operational areas where a bank seeks to maintain integrity and availability of all information it is processing.

9. **Asset classification and control.** With so many daily transactions, banks have difficulty tracking the flow of money in the system. Obviously, such information is vital to a security program because those financial assets associated with transactions require appropriate levels of protection.

10. **Security policy**. This policy is formed by the security council and, again, must be approved by the board of directors.

Inside and Out: Where Banks Are Vulnerable

Broadly speaking, most security threats can be categorized into a combination of four types: internal, external, malicious and non-malicious. An external threat is one that attacks the system from outside; an internal threat comes from within the system itself; a malicious threat comes from hackers or other individuals who intentionally damage a system; and a non-malicious threat is typically caused by a user error or a natural disaster. While these quadrants may overlap, a security program must focus on all four quadrants to be compliant.

Although a good security program must be based on sound security policy and processes, technology gaps still pose significant threats to financial institutions today. Not only are banks the most attractive target for malicious hackers, banks also eagerly adopt new technologies to boost efficiency and reduce operational costs, which often introduce new sets of unintended security holes in the process. Even as the banking technology continues to evolve, a number of key technology infrastructure areas have emerged as critical areas of concern for banks for meeting the GLBA security compliance. Fortunately, there is a good selection of off-the-shelf, cost-effective security technology solutions readily available in the market to address them.

One of the key problem areas is the Web application layer, the part of the Internet architecture that enables a user to interact with a site. As more banks began offering so-called "self-service" features on their Web sites—account information access, online payment and credit card application— the Web application layer is increasingly and constantly threatened. In fact, IT consultancy Gartner says that 75 percent of all hacker attacks occur at this layer. Most banks are not aware that a single security hole in hundreds of Web applications that support the site can expose their entire back-end systems to malicious hackers. There are several security software vendors that focus entirely on this area. Their solutions come in two major forms: Web application firewall intrusion prevention solutions and Web application security testing tools. Application firewalls protect the Web site against any and all hacker attacks entering through Port 80, a virtual gateway through which all Web traffic flows, by allowing only legitimate user requests to pass through the system. All illegitimate requests, such as manipulating the system to display account information from back-end databases or extending credit limits, are stopped because they are not recognized as "good user behavior."

On the flip side of the 24X7 protection provided by Web application firewalls, Web application security testing tools automatically assess the level of vulnerability in the actual Web applications and enable financial institutions to be proactive in fixing security vulnerabilities that might expose customer records and other information. Web application security testing tools are typically used by internal application developers, quality assurance (QA) testers and auditors to assess Web application vulnerabilities and fix the security holes during the application design, development and testing process. By providing the security tools at all stages of the application development lifecycle, a bank can not only mitigate risk sooner but can substantially reduce the costs of fixing the application security defects after the application has been deployed to the Web site.

Deploying host-based intrusion detection systems (IDS) is another important area that needs attention. Host-based IDS provides protection against internal threats by looking at the communication traffic in and out of each computer, and checking the integrity of the end-user's system files and watching for suspicious processes. In addition, host-based IDS are able to monitor accesses and changes to critical system files and in user privileges. Networked computer environments are often like an egg: hard on the outside and soft in the middle. Host-based IDS's monitoring capabilities make the insides of a system a little firmer.

Instant messenger (IM) services, available freely on the Web today and extremely popular, are causing significant cracks in the corporate security system. Instant messengers are prime breeding grounds for Trojan horses, programs that allow an unauthorized user to remotely control the network. A hacker can use IM to implant a Trojan horse into a system, gaining the ability to take over that computer from a remote location. Employees don't realize that these programs are a threat to security and upper management is lax about banning IM and other similar programs.

Similarly, wireless access poses a grave threat to financial institutions who are implementing it. A future version of Windows XP will make every system its own wireless access point, or a flung-open door to a company's network. Intel has already started deploying its Centrino wireless access in its new laptop chips. Some security officers may mistakenly believe that the use of Wireless Encryption Protocol, or WEP, equals wireless security, but they don't realize how easy it is to break WEP. Some security officers also incorrectly believe that no one outside the building can access the internal wireless network. A simple antenna made from soda cans (called a "yagi" antenna) can detect an unsecured access point from a mile away. Undoubtedly, too many unprotected access points will guarantee a write-up by the Federal Reserve.

Lastly, the third party application service providers (ASP) often bring in unexpected security threats. Most banks use third parties to process financial transactions and data. If a bank uses a third party to process, store or transmit any privacy data, it is the bank's responsibility to ensure that the information remain safeguarded. If a third party service provider fails to properly protect the privacy information of its bank customers, the banks will ultimately be held responsible for security breaches.

Consequences of Non-compliance

Failure to comply with GLBA security demands results in an internal downgrade by the Federal Reserve. The Federal Reserve rates compliance on a one to five scale, one being "outstanding" and five being "gross negligence." Two is passing and three is not acceptable. Essentially, if a bank's security program is rated a three, it will have an internal, or non-public, downgrade. If a bank fails to address the security issues raised by the Federal Reserve within six months following the audit, the Federal Reserve will issue a public downgrade. Often, this will be in the form of a public announcement notifying that the bank has failed to properly protect its customers' information. In extreme cases, the OCC and FDIC will further investigate the bank's non-compliance and take punitive action, such as fines, officer removal or forced sale of the bank to another financial holding company that will comply with the GLBA requirements.

The Federal FDIC can also pull a bank's FDIC insurance. Fortunately, these types of extreme punitive actions have not taken place to date, but some banks have certainly been fined and downgraded internally as the Federal Reserve is trying to get its point across without harming the bank.

Besides the Federal Reserve, a bank's security program also falls under the scrutiny of the Federal Trade Commission and state attorneys general via public notice of information sharing policies. If a bank promises to its customers that their information is secure and this turns out to be false, the FTC will begin investigating. It is against the law to mislead customers, and doing so encourages litigation filed by state attorneys general. For example, the Minnesota Attorney General sued U.S. Bancorp in June 1999 for sharing customer information with third-party telemarketers in violations with its own policies and without customer knowledge or consent. U.S. Bancorp, eventually sued by 39 other state attorneys general, settled the case.

Current State of GLBA Compliance

Even when banks know what comprises a compliant security program, many are still lagging in the implementation. The most frequent excuse a bank makes is a lack of funds or resources. When the GLBA was signed in 1999, the economy was robust. Banks could afford to hire security officers and integrate the latest technology solutions necessary for compliance. As the economy softened, so did banks' enthusiasm for compliance. As with most sectors, security has suffered in the recession. Banks have laid off security officers and engineers and failed to update security software, all in the name of reducing cost. Even worse, some banks chose to address security by covering up security breaches before they become known to the board, shareholders or regulators.

This is a substantial risk for banks to take. If a bank tells the Federal Reserve that it did not comply with the GLBA because it could not afford a proper security program, but later shows a profit for the year, the Federal Reserve will penalize the bank. In doing so, the bank is essentially admitting that it had lied to the Federal Reserve. Another gambit, often attempted by mid-sized banks, is to keep a few security employees in the IT department and try to pass this off to the Federal Reserve as being compliant with the GLBA. Banks should realize that this tactic does little to impress the Federal Reserve.

Some banks try to pin their security failings on the security officers, but that excuse simply isn't acceptable to the Federal Reserve. If a security officer is reporting directly to a senior executive and withholds information from that executive, the security officer is at fault. But if the senior executive goes against the guidance of the security officer, the executive is at fault. A savvy security officer will keep a written record of every time a senior executive does not follow what the officer suggests as the best course of action.

Besides the lack of money from slack economy, other issues are more political in nature. Some bank executives simply do not welcome the Federal Reserve's mandates on how to run a proper security program. This attitude leads to a common error of waiting to create a compliant program until the Federal Reserve comes knocking with a complaint.

As a result, the bank not only creates distrust with the Federal Reserve, but more importantly, leaves its customer data susceptible to unauthorized and malicious use. A hacker or a virus does far greater damage in the court of public opinion than an internal downgrade by the Federal Reserve. A bank that gets hacked could lose millions, far more than the fraction it would cost to establish a proper security program.

Conclusion

A financial institution can best please the Federal Reserve simply by being proactive. A bank should not wait for the next audit to show the Fed what it has or lacks in a security program. Create a program, begin to implement it, and then give the Fed a status report to determine if the correct steps are being taken. Remember that the Fed examiners can be there to help, not just to fine.

If internal resources and expertise to meet the GLBA compliance requirements are not available or limited, consider outside assistance. Banks without a compliant security program could benefit from a GLBA gap analysis. In such an analysis, a security consultant examines a bank's security program from both business and technical angles to map the road towards compliance.

Technology changes should not affect a solid security program because a proper security program is stable over time. A GLBA-compliant security program requires sufficient risk assessment and management, a qualified security officer with authority to implement strategic changes, and the support of a well-informed board of directors and a senior management. Without such a program, a bank unwittingly opens its vault for victimization by anyone with a computer and a knack for hacking. It only takes a few keystrokes through a security hole to cost a bank millions in assets and possibly irreparable damage to its reputation. An average customer may not know about the intricate details of the GLBA compliance, but he/she knows to take their banking business elsewhere if their personal information is deemed to be at risk.

For more information:
Sanctum Inc.
www.SanctumInc.com
sanctumsales@sanctuminc.com
phone: 877-888-3970 (US/Canada)
408-352-2000 (International)
+44 7710949512 (European HQ)