

SECURING YOUR NETWORK-THE INTERNET EVOLVES FROM INNOVATION TO REGULATION

Surfing the web and internet use has been principally a leisure activity. While we “see” the possibilities, few of us have become fully dependent on the use of the internet for basic activities. As consumers we will need to develop confidence in the ways and means in which our information is protected. Building confidence in the system is done partially through (and some will argue, solely through) regulation. Just as the phone and highway systems were initially innovative, then regulated to protect and build confidence, so will be the information highway.

Regulations currently in place provide the initial “roadmap” on information security requirements.

The awareness of the need for security has increased significantly. With the

- Distributing of the Love and Melissa viruses and other similar attacks,
- Hacking into networks and resulting publication of the names and respective credit card numbers of thousands of bank customers,
- Establishing of the Computer Security Institute by the FBI,
- Implementing of Gramm-Leach-Bliley Act and HIPAA, and
- Announcing of the government’s cybersecurity plan,

the awareness of the need for security is well established. New workers coming into the marketplace are expecting to use technology in their daily jobs and to see technology grow in importance as they progress in their careers. This will mean that the information you keep on your network will be subject to more and more exposure as the use of your network grows.

Regulations and Standards for the creation, transmission and storing of information in electronic format are becoming part of the laws in two sensitive areas: financial information (GLB) and health information (HIPAA).

If paper documents are stolen from your office you would investigate how access was gained to steal the documents. Was a lock broken? Was a door left open? Can we trust everyone that has access to our office? In any case, you know 1st, you have potential exposure for the theft of the information and 2nd, you have a claim against the thief and anyone who wrongfully uses the information, if you find them.

How would you respond to your employees if it was confidential employee information that was stolen? To your customers if the information was customer purchasing patterns and proprietary products or services you provide?

Strictly from an employee relations and morale standpoint you have a keen interest in maintaining the confidentiality of each employee’s information. Adding on basic state and federal employment laws, you accept the fact that as part of operating your business you will keep employee information confidential. This same attitude applies to the information you keep in electronic format.

In addition to employee information, what about customer information? Even if you had no rules or laws about keeping customer information confidential, would you allow unfettered disclosure of such information? Of course not.

Maintaining the confidentiality of information about employees and customers has always been good business. And while it will continue to be good business, the securing of information in electronic format has lagged behind the technological expansion in electronic storage, transmission and maintenance of information. As a result, the federal government has stepped in and passed laws that address the two areas that we are most sensitive about: our money and our health. These laws help give us insight into the expectations of all network owners and operators in the future.

Gramm-Leach-Bliley

While the Gramm-Leach-Bliley Act (GLB) accomplishes many things, including allowing banks, brokers and insurance companies to be commonly owned, it requires financial institutions to adopt and communicate privacy policies and to regularly assess and monitor the security of their businesses in order to demonstrate a reasonable relationship

between the sensitivity of the information and the protection afforded the more sensitive information. GLB is principally administered by the four federal banking agencies (Federal Reserve Board, OTS, OCC and FDIC) and the Federal Trade Commission (FTC) (and the SEC with respect to brokers and the NCUA with respect to credit unions).

Under GLB any business that is "significantly engaged" in "financial activities" is governed by the Act. Governed business activities include:

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders.
- Providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors.
- Brokering or servicing loans.
- Debt collecting.
- Providing real estate settlement services.
- Career counseling (of individuals seeking employment in the financial services industry).

Businesses that engage in "financial activities" (i.e., more than bank and savings & loan businesses) are required to develop a written information security plan that describes their program to protect customer information.

The FTC is integrally involved since many of the "financial institution" businesses come under its rules. Examples of businesses that the FTC deems are engaging in "financial activities" include:

- Mortgage lender or broker
- Check casher
- Pay-day lender
- Credit counseling services
- Retailer that issues its own credit card
- Collection agency services
- Financial or investment advisory services including tax planning, tax preparation and instruction on individual financial management
- Auto dealers that lease and/or finance
- Sale of money orders, savings bonds, or traveler's checks

Most of the publicity around GLB has been regarding the privacy notices and the "opt-in, opt-out" requirements. Behind the scenes, though, all of these businesses that engage in "financial activities" are required to *develop a written information security plan* that describes their program to *protect customer information*.

While there are variations between the requirements of the banking agencies and the requirements of the FTC, the formality of implementing information security is the common theme. The security plan must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must:

1. designate one or more employees to coordinate the safeguards;
2. identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
3. design and implement a safeguards program, and regularly monitor and test it;
4. select appropriate service providers and contract with them to implement safeguards; and

5. evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

These requirements are designed to be flexible. Each financial institution should implement safeguards appropriate to its own circumstances. For example, some financial institutions may choose to describe their safeguard programs in a single document, while others may memorialize their plans in several different documents, such as one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may spread this responsibility among several employees who will work together.

HIPAA

In addition to financial information, we value our health related information. While we value our privacy and the security of this information we also know that to receive the best health care advice and services, doctors and other professionals must have access to our information, especially in times of emergencies.

In adopting HIPAA, the government recognizes that more and more health care providers, plans and others are utilizing electronic means of storing and transmitting health information. As stated in the publication of the final rules and regulations, "(t)he electronic information revolution is transforming the recording of health information so that the disclosure of information may require only a push of a button. This ease of information collection, organization, retention, and exchange made possible by the advances in computer and other electronic technology affords many benefits to individuals and to the health care industry." The publication further states that ". . . the accompanying greater flows of sensitive health information, . . . strengthens the arguments for giving legal protection to the right to privacy in health information."

HIPAA adopts national standards for the transactions and privacy (for which final rules have been issued) and for security (final rules in development). If you are in the health care business or provide services to a business in the health care industry, you will be required to comply with HIPAA.

The standards under GLB and HIPAA will probably become "de facto" standards. Several agencies have decided to "follow form" by adopting regulations that are the same or substantially the same as the regulations under GLB.

Regulations and Standards

Why understand the pertinent provisions of GLB and HIPAA? Because as the first broad initiatives establishing confidentiality and security obligations and standards, they will be followed by other industries, probably become "de facto" standards for many other industries and even be the standards that courts begin to look to for guidance on proper security efforts. Since both GLB and HIPAA indicate that they will rely on industry standards regarding security of electronic information, you need to understand and apply those standards-eventually those will be the legal standards for which owners and operators of networks will be held accountable.

With regards to securing information on your network, expect the standards to evolve so that operation of all networks will require:

- conducting a risk assessment of vulnerabilities
- implementing a written information security program
- performing ongoing testing and monitoring