



LOMA

Information That Works[®]

November 2005

RESOURCE

Visit us online at www.loma.org

For Insurance & Financial Services Management



Critical Factors For Success

- Technology
- Transformation
- Regulation

Also Inside:

List of New FLMI's

Reprinted from LOMA Resource

Data Privacy And Security Laws: *Is Your Company at Risk?*

By Ken Sponsler, General Manager, Compliance Services, PossibleNOW

Data Privacy and Security Landscape

More than twenty states have passed comprehensive consumer data privacy and security laws and more are in the process of doing so. Congress is considering several pieces of legislation that will serve to establish a national standard. This legislation will require the Federal Trade Commission (FTC) to promulgate regulations regarding the applicable policies and procedures relative to information security practices for the treatment and protection of personal information.

Should your company be concerned?

In short....yes!

Consumers are increasingly aware of privacy and security issues surrounding their personal data because breaches and other security lapses are highly publicized. If your company is formally investigated and found to be in violation, it could face up to 20 years of more "help" from government regulators with your compliance program than you really want. Your competitors and the media will not let you forget about it.

Although your company MIGHT survive one misstep, companies rarely survive the second. Once you experience a security breach, you may find that you must revert to safer and perhaps far less effective marketing programs. You can mitigate your risk by ensuring up front that your marketing programs include data privacy and security concerns.

What are the major components of the existing state laws and the pending federal law?

Generally, the existing and proposed laws have several commonalities. Most of the proposed national versions now in various stages of development would preempt state laws that regulate information security safeguards, data breach investigations, and notices of data breaches.

In the case of the proposed federal legislation, a violation would constitute an unfair or deceptive act under the FTC Act. The state attorneys general could bring an action under state law, if the state law permits, premised in whole or in part on a violation of this Act. Private civil actions for violations of the bill are expressly prohibited.

Some of the major components of these laws are:

1. Data Security Safeguards

- a. Possess a security policy regarding the collection, use, sale, and other sending or maintenance of personal information
- b. Appoint an individual responsible for managing information security (Information Security or Compliance Officer)
- c. Mitigate against reasonably foreseeable security vulnerabilities (*e.g.*, encryption, changes to practices, and changes to the architecture, installation, or implementation of network and operating software)

2. **Data Security Standards:** The standards account for “appropriateness” of the business activities in order to allow for scaling. The FTC’s regulations on these practices take into account:
 - a. The size, nature, scope, and complexity of the activities engaged by the business
 - b. The current administrative, technical, and physical safeguards for electronic information
 - c. The cost of implementing such safeguards.
3. **Definition Of Non-Public Personal Information:** Non-Public Personal Information (NPPI) is defined as a consumer’s first and last name in combination with any of the following data elements: social security number, drivers’ license number or state ID, or financial account number, credit or debit card number, security code, access code, or password that is necessary to permit access to an individual’s financial account.
4. **Definition Of A Breach:** This definition appears in proposed national bills, but is also similar to many existing state definitions. “Breach of security” is defined as the compromise of electronic personal information where the business has a “reasonable basis to conclude that there is a significant risk of identity theft to the individual to whom the information relates.”

However, if the information was encrypted, a presumption would apply that there is not a reasonable basis to conclude that identity theft would result. This presumption could be rebutted by facts demonstrating that the encryption method has been or is likely to be compromised.

5. **Notice Requirements:** Following the discovery of a systems’ breach, the owner or possessor of such system(s) would be required to provide as promptly as possible and without reasonable delay, notice of the breach as follows:
 - a. Notify each individual whose personal information was acquired by the unauthorized access to the system(s)
 - b. Notify the FTC
 - c. Place a conspicuous notice on the business’s website (if it maintains a website) that includes a toll-free telephone number that an individual may use to find out more information about the breach or the information compromised
 - d. If the breach involved financial account information of a merchant, notify the financial institution that issued the account.

What are the risks of non-compliance?

Companies lose customers when a breach occurs. Victims of personal data security breaches often show their displeasure by terminating relationships with the companies that maintained their data, according to a new national survey sponsored by global law firm White & Case.

The independent survey of nearly 10,000 adults, conducted by the respected privacy research organization, Ponemon Institute, reveals that nearly 20% of respondents say they have terminated a relationship with a company after being notified of a security breach. The survey also reveals that 5% of Americans have hired lawyers upon learning that their personal information may have been compromised.

David Bender, co-head of White & Case's privacy practice says, "Five percent may not seem like much, until you realize that anywhere between 23 million and 50 million Americans have received notification of a data security breach. That means that over one million people out there are likely seeking legal counsel."

This should be particularly troubling to companies, especially in light of several putative class-action lawsuits recently filed in California against companies that experienced security breaches.

How can companies determine where their risks are?

Before you can determine where your risks are, you must first know your data. Surprisingly, many companies do not possess a comprehensive view of the data they have, where it is, how it flows through the organization and who owns it.

A crucial first step to compliance is conducting a "data inventory" to determine exactly what data the company has. The data is categorized such as client-owned, customer NPPI, customer account information, employee data, marketing data, and so on.

Next, companies must determine the level of sensitivity of the data. Data is generally classified according to the damage caused to the company if it were lost or breached. The higher the value or sensitivity, the stronger the security safeguards should be.

A sample classification system is:

- 1. Sensitive:** Loss or breach would violate national or state law or cause irreparable harm to the business
- 2. Proprietary:** Loss or breach would place the business at risk
- 3. Non-Public:** For internal company use only
- 4. Public:** For public viewing or use external to the company

Companies with data security and privacy requirements, including GLB compliance, often turn to experts in these areas. These experts can conduct compliance audits to help your company get an unbiased view of your current processes and their associated risks. These compliance auditors can help your company determine the "appropriateness" of your information security and privacy programs based on industry-wide experiences and benchmarks. Although there is no requirement to use an outside source, an independent expert could show due diligence and ongoing efforts in a convincing fashion.

Will compliance be costly?

Data security and privacy requirements generally should meet an appropriateness test. If your company uncovers areas of risk, you can prioritize resources to the areas that pose the most serious risk. Costly technical solutions may not be required. You may be surprised to find that simple procedural or process changes can make a significant difference in your company's overall compliance posture.

25 risk mitigation steps that your company should consider

Small changes to existing procedures or relatively minor technology investments can greatly reduce risk. It's been shown that roughly 80% of security errors occur from within the organization. Some of this activity may be malicious, but often it's simply due to lack of process, monitoring, negligence or ignorance.

No matter the size of your company, here are some simple rules to follow:

1. Know your data! What data do you have, who owns it and where is it?
2. Classify your data according to its level of sensitivity
3. Apply the appropriate level of safeguards to data based on sensitivity
4. Assign, empower and budget the information security functions
5. Develop a written information security program. If you do not have a written document, you do not have a program.
6. Train your employees on your information security program and document the training
7. Consider an external audit to determine if you have any compliance gaps and the risks associated with these gaps
8. Implement safeguards to control risks based on the gap analysis
9. Oversee your service providers. You cannot contract away your responsibility for reasonable security practices
10. Provide authorization and access to your data based on employee job functions. (Database Administrators don't necessarily need to see the data to administer the database.)
11. Be able to determine who accessed data and what occurred
12. Keep logs of all system and network activity including attempted intrusions
13. Consider restrictions on the use of USB storage devices and RW-CD drives
14. Implement an authentication policy requiring periodic login/password changes
15. Limit paper copies of sensitive information and provide a convenient means for employees to shred unneeded documents
16. Lock storage areas that contain important information
17. Implement policies to limit download and storage of sensitive data to PCs and laptops
18. Store important data and documents on the network instead of on an individual's PC.
19. Backup data routinely and test the process
20. Develop and implement data aging and destruction policies
21. Develop a comprehensive disaster recovery and business continuance plan
22. Acquire and maintain only the data you need. For instance, if you collect customer contact information via your web site for an insurance quote, only collect what is needed to facilitate that contact.
23. Review your privacy policy and make sure you are complying with what it states. If you decide to change your policy about sharing data, you must provide customers notice and an opportunity to opt-out prior to the change taking effect.
24. On your web site, provide a link to your privacy policy at the point of collection and ensure that consumers know if the point of collection is actually on a third party's site
25. Subscribe to a legal information service to remain aware of changes and monitor and enforce all of the above

Ken Sponsler is the General Manager, Compliance Services with PossibleNOW. Ken can be reached at ksponsler@possibleNOW.com or 770-255-1020.