Guard biz data with security strategies

By Bart A. Lazar

MARKETING AND THE LAW

Identity theft is the fastest growing crime in the United States. Consumer advocates are demanding that all companies handling personal information take greater care with data and that the government take action to make this happen. This puts more direct and indirect pressure on how marketers handle their own marketing data.

One result of this pressure has been felt on the Internet, where the Federal Trade Commission has used existing laws to file enforcement actions against Guess?, Eli Lilly and Microsoft for allegedly *not* keeping Internet customer information secure or making inaccurate promises about the level of protection being provided. Another result is new laws (and, sorry to say, there are likely to be more) that require that data be kept secure.

OK—so the lawyer is shouting, "The sky is falling." But is it really? What this situation boils down to is that the laws and government agencies want companies to take a good look at the methods they use to collect, store, access and transfer data, and apply reasonable techniques designed to protect the data. Most regulators understand that a lock-down on data will not help consumers. On the other hand, the key is not to ignore security, but try to understand data security and protect clients, consumers and employees.

Employees? Do we really care about employees? First, recognize that one of the primary ways identity-theft rings get their information is not directly from marketers, but from employers, who collect and manage a large amount of private information about their employees. And the last time I checked, marketers were also employers. According to the results of a survey by Chicago-based Trans Union LLC, the credit reporting agency, theft of employer data is the No. 1 source of identity theft information.

Also, employees are the key to protecting customer data. Even though computer hacking to get data has gotten all the publicity, the more likely scenario is that an employee violates company policy and physically gives or electronically transmits customer or employee data to an unauthorized person. Last year, for example, identity theft rings got personal information from one of the world's largest consumer products companies, a major pharmaceutical company and even a state law enforcement agency. While halting the misuse of data entirely is nearly impossible, the fact that such instances are on the increase suggests that there is not enough being done to protect such information.

> **Employees are the key to protecting customer data.**

Laws such as the Gramm-Leach-Bliley (GLB) financial information privacy statute and the health information privacy provisions of the infamous Health Insurance Portability and Accountability Act (HIPAA) provide security requirements for financial and health data. California recently enacted a law that requires companies to give notice to California residents whose unencrypted personal electronic data has been accessed in an unauthorized manner. The Sarbanes-Oxley Act also has a security component in that any systems that process or provide accounting data need to be secured. Companies that market or employ internationally need to comply with the European Union Data Directive, also called the EU Directive, and local implementing legislation, which imposes security requirements for data collected overseas, whether or not the data is transferred to the United States where our privacy and security laws are deemed to be inadequate.

Baseline "across the board" security requirements likely will be legislated in the near future, so it makes sense to get ahead of the curve. This is particularly true if your company is increasing its IT spending or spending a great deal of time with internal MIS personnel and information technology consultants developing privacy policies and procedures or Sarbanes-Oxley compliance, which is a relatively new law that requires, among other things, accounting systems for public companies to be secure. At this point, focusing solely on privacy while paying lip service to security, or securing accounting information while marketing or employee information is not secured, seems to be an allocation of resources that could be challenged. Security strategies for consumer and employee data should be part of your privacy or compliance plan and your IT people should know about all of this.

One good thing about the existing and expected security laws is that they are, and are likely to remain, technology-neutral. Since technologies keep changing, for any legislation to specify the appropriate technology would be difficult. Also, GLB, HIPAA and the EU Directive all recognize that the goal is to establish a baseline of "reasonable" security, and what is reasonable for one company, may not be the same as for others.

Still, many enterprises would prefer to simply be told what they need to do in order to comply. Clients tend to say, "We just want to do whatever is necessary to comply with the law." The answer to give is not necessarily one clients like to hear, since essentially each company must conduct its own assessment of its systems, policies and procedures and determine if they are handling matters appropriately.

The first question to ask is "Who is in charge?" In many organizations, security issues are part of the responsibilities of many people, or no one. As one example, the Office of Privacy Protection for the State of California commissioned a survey of California businesses and how they planned to comply with the common data security architecture (or CDSA). In response to the question, "Who is in charge of the data security breach communication process within your organization?" the No. 1 answer was "No one." Therefore, first look at your organizational security and determine what your internal information security infrastructure looks like before tackling the technical aspects of your systems infrastructure.

Once someone or a group of people is in charge of analyzing and developing security systems and procedures, he or they should undertake a review of systems and procedures for protecting consumer and employee information as part of an overall assessment. New policies and procedures should be established, and the employees should be trained on the new policies and procedures so they know how to treat information.

Many resources on security best practices exist:

- One good place to start is SANS (SysAdmin, Audit, Network, Security) Institute based in Bethesda, Md.
- For basic information and an outline of nontechnical security best practices, the Office of the Privacy Commissioner published a business privacy handbook in August, and issued a report on dealing with security breaches, available on the Web at www.privacy.ca.gov/recommendations/recomend.htm.
- A comprehensive, 66-page, compliance outline is part of the International Organization for Standardization's international standard for Information Technology-Code of practice for information security management (ISO/IEC 17799) (www.iso.ch; licensing fee approximately $136).

I'll cover more specific best practices recommendations for technological and nontechnological security in my next column. ■

Bart A. Lazar is a partner who specializes in counseling, business transactions and litigation in intellectual property, advertising and promotions, privacy, Internet and related matters for Chicago-based Seyfarth Shaw LLP. He can be reached by e-mail at BLazar@seyfarth.com or news@ama.org.