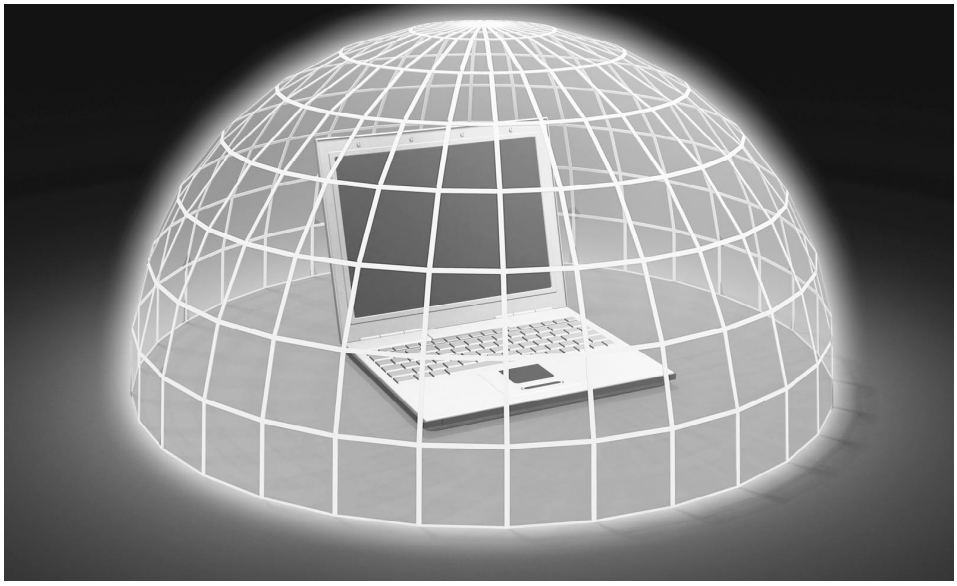
LOS ANGELES
Daily Journal
www.dailyjournal.com
TUESDAY, FEBRUARY 15, 2011

CORPORATE

Cutting Your Technology Budget Can Have Legal Costs

By Alejandro S. Angulo



Times are tough. No matter the source of your financial news, almost every expert agrees that it will take years to fully recover from the "Great Recession." Given these economic realities, it is not surprising that businesses from all sectors are actively looking for ways to save money. While costs related to a business' computer information system may seem like a strategic target for cuts, making such cuts might create problems more costly than the savings.

The decision of what to cut in this area should not be taken lightly, nor should it be made in haste without a second opinion. Companies should involve counsel in their daily information technology cost-cutting decisions. This is particularly true for companies doing business in California, a state replete with a broad range of compliance laws.

Most businesses collect personal information regarding their customers and store this information electronically. The computers used to store this information, however, are typically connected either directly or indirectly to the Internet and are therefore accessible from beyond the walls of the office. Computer hackers, including pranksters and those engaged in corporate espionage, represent a serious risk that consumer information collected by a business may be accessed without authorization. For this reason, all businesses implement some form of electronic security designed to protect against unauthorized access. Thus, the cat and mouse game begins — developers of electronic security technology must actively provide updates because hackers are always developing methods to compromise older versions. According to electronic security experts, this cat and mouse game is played on a daily basis.

While costs related to a business' computer information system may seem like a strategic target for cuts, making such cuts might create problems more costly than the savings.

The Consumer Records Act (California Civil Code Section 1798.80 et. seq.) requires a business that collects and stores personal information about a California resident to "implement and maintain reasonable security procedures and practices...to protect the personal information from unauthorized access..." Importantly, these provisions apply to any business in California — including sole proprietorships and non-profits — that electronically stores consumer information. This article will discuss how to remain in compliance with the Consumer Records Act; the obligations imposed by the Consumer Records Act in the event of a breach of security technology; and some consequences of failing to "maintain reasonable security procedures and practices."

While the California Legislature provides specific definitions for many of the words or phrases used throughout the Consumer Records Act, it did not define what "security procedures and practices" are considered to be "reasonable." To date, California courts have not interpreted what the term "reasonable" means under these code sections. The state Supreme Court, however, recently held that where a statute uses the term "reasonable," the "inquiry into reasonableness is necessarily contextual." *San Leandro Teachers Assn. v. Governing Bd. Of San Leandro Unified School Dist.* (2009) 46 Cal.4th 822, 836.

Security procedures and practices that are considered reasonable now may not be considered reasonable in the following year because reasonableness must be analyzed in a relevant context; that context being the daily improvements to security technology and a hacker's corresponding success of being able to compromise such improvements. For example, it would probably be unreasonable for a company to refrain from periodically upgrading its security technology where it can be shown that hackers have developed a method to compromise the existing security technology; and replacements (or updates) to that security technology are available and are not cost prohibitive.

Since there are numerous factors that should be analyzed in determining whether particular "security procedures and prac-

tices" are, in fact, "reasonable" in a given context — what does this mean for a business that is looking to lower its overhead by cutting costs associated with the security of its computer information system? It means that any business looking to cut such costs should consult a lawyer and a technology consultant to maximize the probability that the security measures remaining after the proposed cost cutting are considered "reasonable." These issues should also be revisited on at least a yearly basis to ensure that the existing measures do not become obsolete, and therefore, unreasonable.

Regardless of whether a company is in compliance with its affirmative obligation to "maintain reasonable security procedures and practices," one thing is certain: An actual or reasonable belief of a breach of security technology that results in personal information being acquired by an unauthorized person imposes additional obligations. In the event of an actual or reasonably believed breach of security, a company is required to notify its customers of the breach; and restore the integrity of the data system. California Civil Code Section 1798.82.

The notification requirement will certainly impose compliance costs in the form of labor, postage, etc., in addition to legal consequences. Even worse, for certain businesses, the notification requirement will prove to be a public relations nightmare, with ramifications far beyond the legal consequences.

The best way to avoid this notification requirement is to remain vigilant about IT security. Although such vigilance may preclude certain cost cutting, the more up-to-date the security technology, the less likely a security breach. The less likely a security breach, the less likely a company will find itself having to embark on the costly and embarrassing task of notifying its important customers that the security of their personal information has been compromised.

Of course, the consequence of failing to comply with California law may result in additional costs, including litigation costs. Any person injured by a violation of Civil Code Sections 1798.81.5 or 1798.82 may sue for damages. California Civil Code Section 1798.84(b) ("Any customer injured by a violation of this title may institute a civil action to recover damages.")

Currently, there are no published cases that illustrate the scope of available damages — or how such damages may be proven — resulting from a company's failure to "maintain reasonable security procedures and practices." Whether such a case will ever be published remains to be seen since damages suffered by an individual alone may never be sufficient to justify litigation costs through the appellate courts. In at least one pending case, however, a plaintiff is actively prosecuting a class action premised on violations of Civil Code Sections 1798.81.5 and 1798.82 against a large company. *Saenz v. Kaiser Permanente Int'l.*

The Saenz case was filed in state court on Oct. 13, 2009. The complaint alleges that personal information of approximately 29,500 individuals was maintained in an unencrypted fashion; an employee of the defendant removed the personal information without proper authorization; the personal information would not have been possible had the defendant maintained reasonable security procedures and practices; and the defendant waited over two years to provide notification of the rogue employee's unauthorized access to such personal information.

The case was removed to federal court shortly after being filed. In response, the plaintiff sought to move the action back to state court on the grounds that federal law did not preempt her claims. The federal court agreed, granted plaintiff's motion for remand and transferred the case back to state court, where it remains pending and subject to heavy litigation.

Whether the acts giving rise to potential liability in the Saenz case could have been avoided by "reasonable security measures" remains debatable. Nevertheless, the case demonstrates how exorbitant litigation costs can flow from a company's alleged failure to maintain and update reasonable security procedures and practices. If anything, the racking up of litigation expenses in this case illustrates that businesses should carefully consider the whole range of potential long-term costs before deciding to save money in the short term by cutting costs related to the security of computer information systems that store consumer information.

Given the complexities associated with the Consumer Records Act and the potential for time consuming, expensive litigation, California businesses that collect and store personal consumer information should consult counsel before implementing any cost-cutting measures related to the security of their computer information systems.

Alejandro S. Angulo is a partner in the trial section of Rutan & Tucker LLP (www.rutan.com) and a member of the firm's Intellectual Property and Technology Practice Group. He can be reached at (714) 641-3401 or aangulo@rutan.com.