More than an IT guy

By Kathy Finn
Published Jul 7, 2014 at 6:00 pm (Updated Jul 7, 2014)

Though data security breaches have been the stuff of news headlines for years, the dangers may not have hit home for many people until a major U.S. retailer fell victim to electronic hackers.

Last year's security breach at Target Corp., the third-largest retailer in America, compromised the credit card accounts of as many as 40 million people who had shopped at Target stores, forcing many to cope with credit disruptions.

Investigators concluded the criminals captured data that was stored on the magnetic stripes of cards that customers had swiped at cash registers. The breach put into the hands of the attackers everything they would need to create counterfeit cards.

The rising incidence of companies failing to protect data they collect from customers and vendors sends concerns rippling through businesses of all kinds.

Many whose data worries previously centered on storing information in ways that ensure access to it in the event of emergency now are focused on how to bolster protections against assaults by high-tech thieves.

"It has become important for all businesses to protect this information, not only because of legal requirements but also because the threat to these information assets' has become so much more serious," says Jack Pringle, a partner with Adams and Reese.

Pringle, a lawyer in the Columbia, S.C., office of Adams and Reese, says the law firm is bolstering its expertise in data protection and privacy issues across its offices in order to help clients navigate and comply with relevant laws and guide them toward making better use of the data they collect.

"The question is, not if, but when you're going to have a data breach," Pringle says. "It's just good business to be thinking about these things."

Federal laws have been in place for a number of years requiring certain types of businesses, primarily financial institutions and health care providers, to protect information that could cause damage to individuals if it is disclosed without their authorization.

The existence of these laws is well-known to financial services customers and health care patients, who often must sign authorization forms showing that a banker or doctor has their permission to share information about them with appropriate other parties.

Such forms have become commonplace since enactment of the federal Health Insurance Portability and Accountability Act of 1996, whose privacy provisions recently were tightened, and the Gramm-Leach-Bliley Act of 1999, which applies to a wide range of financial institutions and providers, including some retailers that extend credit to consumers.

KNOWING THE RULES
In the wake of highly publicized data breaches of the past decade, privacy laws have cast a wider net. Along with a host of federal statutes and standards related to information use, most states, including

Louisiana, enacted information protection laws that apply to businesses of all kinds. Many of the statutes focus on when and how a business must notify its clients or associates of a data security failing.

Matthew Almon, an attorney with the law firm Stone Pigman Walther Wittman, says an important statute for Louisiana businesses to know is the state's Database Security Breach Notification Law, which went into effect in 2006. The law requires any entity that holds personal information of individuals—whether employees, customers, vendors or other associates—to notify those individuals if they believe their "unencrypted" information has been acquired by an unauthorized person due to a security breach.

The law defines "personal information" as an individual's first name or initial and last name, with one or more of the following elements: Social Security number; driver's license number; or an account, credit card or debit card number in combination with a security code or password that would permit access to the individual's financial account.

Noting that identity thieves can obtain crucial information from sources ranging from credit card transactions to magazine subscriptions, the law says that because victims of identity theft must act quickly to minimize damage, speedy notification is essential.

Notification can occur via written or electronic communication, including email. Publicizing the breach through major statewide media or by "conspicuous posting" on the website of the agency or person responsible also is allowed.

While businesses that operate at multiple locations and have widespread information-sharing networks probably are more likely to have a serious data breach than a single store or a company that serves a narrow customer base, advisers say every enterprise should be on guard.

"It's not just big businesses that are subject to these laws," Almon says. "If your business is dealing with personal identifying information of individuals, then the law applies and you need to be in compliance."

Failing to disclose a potentially serious data loss can result in civil lawsuits or fines, he says. But the law does provide an exemption if the responsible party can show that no one is likely to be harmed by the breach. Notification also may not be required if the data that was stolen was encrypted or coded in such a way that unauthorized parties wouldn't be able to read it.

Because data protection is a highly technical field with many legal implications, some law firms are beginning to team up with data center providers in order to collaborate on customized data protection services for clients.

Given how fast electronic technology evolves and how difficult it is to stay ahead of the curve, such service combinations could eventually become commonplace.

Says Almon: "As quickly as people figure ways to protect the information there are other people figuring ways to steal it."