THE NATION'S OLDEST WEEKLY BUSINESS JOURNAL

DENVER BUSINESS JOURNAL

VOL. 57, NO. 43 APRIL 28-MAY 4, 2006 72 PAGES $2.00

TECHNOLOGY

Bill mandates notification about security breaches

BY BOB MOOK
DENVER BUSINESS JOURNAL

Businesses operating in Colorado will be required to notify customers when personal data — such as credit cards and drivers license numbers — is susceptible to identity theft.

Gov. Bill Owens signed House Bill 1119, sponsored by Rep. Rosemary Marshall, D-Denver, on April 24. The legislation is intended to raise consumer and business awareness about the issue.

About 8.6 million cases of identity theft were reported in the United States in 2005, according to a national Better Business Bureau report. On average, the theft incidents cost victims $422.

Jessica Wright, executive director of the AeA Mountain States Council — a nonprofit trade organization that represents technology companies in Colorado, Wyoming and Utah — said AeA members supported the legislation from the start, while working with legislators to make the bill friendlier to businesses.

The revised legislation allows businesses to take alternative steps, such as notifying customers through the media rather than sending individual letters or e-mails, if the costs exceed $250,000.

At least 25 jurisdictions have laws or statutes addressing information security, said Phil Gordon, a Denver-based shareholder for the San Francisco-based law firm Littler Mendelson PLC.

Wright said while most businesses have been proactive in preventing security breaches, the new law should encourage companies to put more policies in place to protect customers and themselves from potential ID theft.

Disclosing security breaches could cost companies revenue and customer confidence.

PGP Corp., a privacy consulting firm based in Palo Alto, Calif., estimated that U.S. businesses lost $14 million in 2005 from disclosing security breaches, including $1.5 million in lost productivity (mostly employees trying to resolve their financial concerns during work hours) and $7.5 million in damaged customer relationships.

PGP also reported that 79 percent of the security breaches result from human error — usually from inside an organization.

Another study showed 60 percent of individuals who receive notice of a security breach either cancel or consider canceling their relationship.

"It's not just a technical issue, it's a personnel and management issue," Gordon said.

Gordon, who advises clients on privacy and information-security issues, said it's important to handle breaches properly.

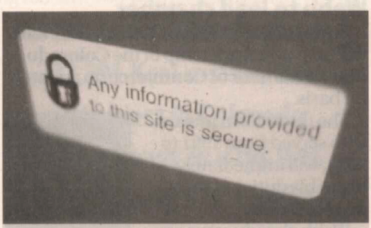
"Keep in mind that when a breach does occur, [notification] is a good way to mitigate damages if there is a lawsuit," he said.

Although security breaches inevitably will damage the customer relationship, Gordon said companies can soften the blow by offering some kind of credit-monitoring services for affected customers to demonstrate responsiveness.

Wright agreed that increasing awareness for consumers who make online transactions could help solve part of the problem. Wright said she personally uses a credit-monitoring service to keep an eye on any irregularities in her charges.

She also said discarded financial statements, not online transaction, are the root of most identity theft.

BOB MOOK | 303-866-9678
bmook@bizjournals.com



DETAILS

Principles of data security, breach notification

Consumers should be notified when:
1) Computerized information has been accessed and acquired by an unauthorized person,
2) And that creates a material risk of identity theft or harm to the consumer.
3) Information that is publicly available is excluded from this definition.

Disclosure should be made:
1) In the most expedient time possible and without unreasonable delay.
2) In a manner consistent with the legitimate needs of law enforcement.
3) It should allow any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

Source: AeA