

Sacramento small firms told of risk if credit-card data are stolen

Sacramento Bee

When intruders break into an auto repair shop and make off with a laptop, the loss is not just a computer.

Without the proper protection, the computer could yield hundreds of customer credit card numbers, all ripe for the black market at \$25 a pop.

“This is the new wave and it’s starting to hit small businesses,” said Jay Cline, president of Minnesota Privacy Consultants.

Cline, author of a book on credit card security for small businesses, addressed a business summit in Sacramento this week on a growing trend and the consequences of lax security.

It is not the retail giants like Wal-Mart and Amazon.com that are most vulnerable to high-tech thieves but small businesses that have less than 1 million credit card transactions a year, he said.

One breach in security could cost hundreds of thousands of dollars in fines. The impact could be even greater. The Federal Trade Commission could step in and require annual audits for 20 years – at the firm’s expense.

“For a small business, this can be devastating,” Cline said.

Small-business owners could be less aware of security measures, less willing to pay for them or take the time to perform them – and more trusting of employees, he said.

The credit card industry in 2004 created the Payment Card Industry Data Security Standard, rules and regulations that each merchant contracts to follow in setting up a credit card payment system.

Merchants can be a single-person operation selling sunglasses from a kiosk or a household-name retailer with thousands of stores. Fines result if a security breach shows merchants weren't compliant.

"There's no get-out-of-jail-free card for small businesses if there's a data breach," Cline said.

A Verizon Business security report found that protecting stored data, tracking access to cardholder data and developing and maintaining secure systems were the weakest areas of compliance for all businesses that suffered breaches in 2008. Complying with the standards requires encrypting data on Web sites and e-mails, using firewalls, anti-virus and security patches for in-house computer networks, and monitoring and testing, Cline said.

Employee security measures involve changing passwords when employees leave, limiting access to credit card information to necessary personnel and monitoring credit card activity and log-in activity for irregular patterns, he said.

Daytime employees who are logging in at night could signal trouble, he said.

Smaller businesses that believe employees are an extended family should not ignore

their contractual obligations, Cline said.

"You may think you know your employees," he said.

He ranked dishonest employees as the primary cause for security breaches.

Some businesses set themselves up for trouble unnecessarily by stockpiling credit card information they no longer need, either in computers or on paper, Cline said.

The focus on credit card fraud could shift soon toward businesses that maintain health records online, he said. Benefit and claim records hold a wealth of vulnerable information. New federal laws penalize businesses for security breaches.

Sacramento County Sheriff's Detective Sean Smith, who speaks to business groups on how to protect against high-tech crimes, warns that vendors hired to process credit cards should also be secure.

"A lot of hackers siphon off or harvest information and a lot of victims won't even know where they've been compromised," said Smith, who is part of the Sacramento Valley Hi-Tech Crimes Task Force.

He said Web surfing by employees on work computers should be minimized because it invites worms or viruses that could record and transmit sensitive information.

Credit cards that have been “recoded” are increasingly becoming a problem, he said. “The actual face of the card won’t match the magnetic stripe information,” he said. “We’re seeing more and more of that.”

A clerk too busy or inattentive might not always notice the mismatch, he said. Cline said that, for consumers, the risk is somewhat lessened because they are not responsible for illegal charges.