PHYS ORG

To prevent data theft, businesses race to adopt new technology

April 20 2014

Recent high-profile data breaches at Target and Neiman Marcus have accelerated plans by banks and retailers to implement technologies they say will prevent hackers from stealing consumers' account information.

Malware installed in Neiman Marcus payment terminals exposed 1.1 million debit and credit cards from July to October last year, while the Target incident compromised the personal information of more than 110 million customers in November and December.

The sophistication and scope of the recent breaches has lent increased pressure to the adoption of a new generation of microchipped debit and credit cards and a cutting-edge technique known as "tokenization" to protect online and mobile purchases.

Industry experts say the technologies will limit the volume and value of consumer data stored by retailers, who no longer will have to safeguard sensitive details such as card numbers, PINs and security codes.

"It's not just about protecting consumers from financial loss or the system from financial loss; it's really about maintaining trust," said Ellen Richey, executive vice president, chief legal officer and chief enterprise risk officer for Visa Inc.

In the aftermath of the breaches, Visa and MasterCard announced the formation of a new cross-industry security working group focused on speeding up and coordinating the adoption of the new technologies.

"We were pushing that direction, but this Target event has given it the kind of urgency that it didn't have before," Richey said.

Banks already are starting to issue debit and credit cards embedded with microchips, also known as EMV, which stands for Europay, MasterCard and Visa. The system is widely used in Europe. More than half of all credit cards in the U.S. are expected to shift to EMV by 2016.

To encourage the transition, MasterCard, Discover, American Express and Visa have instituted a policy that a bank or merchant that hasn't adopted chip technology by October 2015 will bear the loss if a transaction turns out to be fraudulent, Richey said.

"It's a fairly powerful incentive," she said.

The United States has been slow to adopt microchipping because of the high costs associated with replacing traditional magnetic-stripe cards and payment terminals, estimated at $15 billion to $30 billion.

"Because of that high cost, there were definitely folks out there who were skeptical of whether they should or shouldn't implement it, and now because of the data breaches, that seems to be moving a whole lot faster," said David Fortney, senior vice president for The Clearing House, the nation's oldest banking association and payments company, which provides payment clearing and settlement services.

Consumers aren't likely to notice changes overnight. Banks will issue the microchipped versions as old cards expire, rather than all at once.

The new chip card will have a little symbol on the front to represent the microprocessor embedded inside.

"It's actually like a little computer, a real little computer with applications and a processor in it," said Visa's Richey. The microprocessor also can be placed in a mobile phone, she said.

Instead of swiping the card to pay, a shopper dips a "contact" chip card into a slot in the pay terminal at checkout.

"Contactless" chip cards will use radio signals, so the shopper has only to tap or hold a card or mobile phone close to the terminal to make a purchase.

The computer in the card produces a cryptographic message that changes with every transaction, so even if thieves steal the account number, they can't make a counterfeit card, Richey said.

"The problem we're having is that criminals can steal information from a merchant environment, and they can get enough information to make copies of the card," she said. "They don't have to have your physical card; they can make copies - and as many copies as they want - because the data is static and doesn't change from transaction to transaction."

Microchipping works only in brick-and-mortar stores. For online and mobile shopping, the proposed security solution is tokenization.

So-called "tokens" are strings of digits that get transmitted automatically when a customer buys something online or with a mobile device.

Essentially, very little changes from the consumer's point of view. You input your payment information as usual on a website, but when you click to finalize the transaction, a "token vault" maintained by your bank will transmit a token to the merchant instead of your card number, expiration date and security code.

The token is a temporary, random number that's tagged to your account number but not mathematically derived from it.

Because tokens consist of dynamically shifting cryptographic codes that change frequently, it's harder for thieves to use them for fraudulent purposes, Fortney of The Clearing House said.

"Effectively, if there were to be a breach - whether it's malware or hacking into the system - those tokens would have extremely limited value, as opposed to those static numbers that we use today," Fortney said.

"It makes it much more difficult to create a fake card, if not impossible," he said.

The Clearing House is working with mobile wallets, networks, retailers and payment processors to test tokens in a four-month pilot project that began late last year, Fortney said. The association plans to expand the trial soon to 10 banks in multiple cities, and hopes to roll it out across the country by 2016.

"The nice thing about tokenization is that it would cost far, far less, because it doesn't have that physical aspect. It's more of a software-based approach," Fortney said.

Retailers welcome the transition to microchipped EMV cards and tokens, but many would prefer to see the chip cards enhanced by the use of PINs instead of easy-to-forge signatures.

Insisting on poorly designed chip-and-signature cards is like installing an alarm on the front door of a home while leaving the back door open, Mallory Duncan, senior vice president and general counsel for the National Retail Federation, said in a statement.

"It doesn't make sense when the technology exists to secure the entire house," he said.

Duncan told the Senate commerce committee last month that protecting all cards with PINs instead of signatures is the most important fraud-prevention step that could be taken quickly.

"It's proven, it's effective and it's relatively easily implementable," he said in his testimony. "PIN debit cards are close to ubiquitous worldwide, and readily producible in the U.S. Chip is a desirable add-on. If speed of implementation is of importance, then substituting PIN for signature is preferable to implementing chip."

Banks and retailers alike have come under increasing pressure from Congress to improve data security since the breaches, but they don't want lawmakers to mandate any specific technological fix.

"These technologies could change quickly, so if they were to get mandated, it would be a bad thing," Fortney said. "It would probably mean the industry didn't roll this thing out on its own and then it would be a law. As technology evolved, it wouldn't be able to adapt to it."

At a congressional hearing on data breaches earlier this month, Sen. Roy Blunt, R-Mo., agreed that lawmakers shouldn't prescribe how to secure a card.

"I'm absolutely confident that the hackers and the criminals will be more nimble than Congress, and if you put the code in the law, you just tell them the code that has to be broken," Blunt said.

Blunt said some changes to data security laws were necessary, however.

He and Sen. Thomas Carper, D-Del., have introduced the Data Security

Act of 2014, a bill that would establish uniform requirements for businesses to protect and secure consumers' electronic data. The bill would replace a patchwork of 49 state and territorial laws that govern data security and notification standards in the event of a breach. The often-conflicting requirements make it difficult for businesses to comply and for law enforcement and consumer agencies to track or prevent crimes, the senators say.

The legislation is among several competing bills lawmakers have floated in the aftermath of the data breaches, including proposals by Sen. Patrick Toomey, R-Pa., and Senate Judiciary Committee Chairman Patrick Leahy, a Democrat from Vermont.

Leahy's bill, which takes a tougher stance than his colleagues' proposals, would make it a crime for anyone to "intentionally or willfully" conceal a security breach of personal data when it causes economic damage to consumers.

©2014 McClatchy Washington Bureau
Distributed by MCT Information Services

Citation: To prevent data theft, businesses race to adopt new technology (2014, April 20) retrieved 2 May 2024 from https://phys.org/news/2014-04-theft-businesses-technology.html