[Virtual Reality Gets Real After Decades of Hype]

- 

[Rolls-Royce Investigated Over Bribery Claims]

Safari Power Saver
Click to Start Flash Plug-in

Cybercrime

Why So Many Retail Stores Get Hacked for Credit Card Data

By Jordan Robertson March 20, 2014

Photograph by Craig Warga/Bloomberg

(Updated fourth paragraph to clarify how recently PCI assessors took open-book tests.)

When a big retailer gets hacked, it's often quick to note that it has complied with cybersecurity rules set by the credit card industry. MasterCard (MA), Visa (V), and other card companies require retailers to pass an audit sanctioned by the Payment Card Industry (PCI) Security Standards Council, an industry group.

It turns out the accreditation by PCI doesn't always offer much protection against fraud. Neiman Marcus noted it had met PCI standards when it said in January that customer cards may have been compromised from July to October. Target (TGT), which suffered a record-breaking hack in November, had been certified as compliant two months earlier. Grocery chain Hannaford Brothers (DEG) and payment processors WorldPay and Heartland Payment Systems (HPY) were also hacked shortly after receiving passing marks from PCI assessors, who judge a company based on six main groups of security measures, broken into smaller items such as fire walls and antivirus software.

Story: Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

All of which raises the question: Is there something wrong with PCI's standards? Retailers and banks were on the hook for more than $11 billion in global

card fraud in 2012, a 15 percent increase from the previous year, according to the latest data from industry publication the *Nilson Report*. Almost half of all card fraud occurs in the U.S., though the country accounts for just a quarter of global card spending. That's partly because of light enforcement of PCI rules and a lack of accountability for assessors, most of whom are drawn from a pool of hundreds of approved consulting firms, says Avivah Litan, a cybersecurity analyst with Gartner (IT). "They have no responsibility," she says, drawing a comparison to credit-rating agencies in the runup to the 2008 financial meltdown.

Visa, MasterCard, American Express (AXP), Discover (DFS), and JCB International created the PCI security council in 2006 to ward off government oversight of the retail payment systems they control. The systems process much of the retail economy's $5 trillion in transactions a year from 1 million U.S. merchants. There are about 1,800 independent part- or full-time auditors, certified to review PCI compliance. While intensive audits cost tens of thousands of dollars and run for months (Target spokeswoman Molly Snyder says the company's annual reviews take nine months), some assessors charge a couple hundred dollars for simpler audits they finish in an afternoon. Auditors can get certified over a weekend through courses that, until 2010, ended in an open-book test. Small retailers assess themselves.

Large retailers can face fines of $25,000 per month for violating PCI's guidelines. But there's nothing to stop companies from quickly undoing changes they made to their systems to appease inspectors, says Branden Williams, executive vice president for strategy at Sysnet Global Solutions, a consulting firm that works with banks on merchant compliance.

Story: Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data

"People should not think an audit is some kind of insurance policy," says Ellen Richey, Visa's chief legal officer and chief enterprise risk officer. "It requires exertion of effort every day of the year." She says companies deemed PCI-compliant before a major breach have later been found to be out of compliance at the time of the attack. Bob Russo, general manager of the PCI Security Standards Council, says, "We do not hear about all of the attacks that are prevented by the security implemented through adoption of PCI standards."

The U.S. has lagged other countries in adopting stronger security measures, such as authentication chips in cards, point-of-sale data encryption, and secondary ID numbers that substitute for card numbers online. Richey says her industry is working to incorporate these technologies in the next few years. PCI standards have cut the amount of sensitive data stored by retailers, she adds.

The current PCI standard gives every party in the payment system a credible way to redirect blame for a breach, says Jeremiah Grossman, founder of online security company WhiteHat Security. "Basically you have the council blaming the victim, the victim blaming the standard, and the cardholder caught in the middle," he says. "Nothing will change, because the incentives in the system are broken."

Safer Card Tricks

End-to-end encryption
Pros: Encoding at a point-of-sale terminal keeps data safer from the moment it enters a retail system
Cons: No equivalent for online purchases

Chip-and-sign
Pros: Cards with chips in them provide a second layer of verification
Cons: Requires upgrading or replacing conventional U.S. magnetic-stripe systems

Dynamic authentication
Pros: A button on the card that can reset its magnetic-stripe data with each purchase makes storing the data useless
Cons: Can slow transactions

Tokenization
Pros: Temporary codes generated by cards for online purchases reduce how often card numbers are sent to websites
Cons: No common technical standard yet

The bottom line: *Many retailers hacked for customer card information had recently passed industry security audits.*

Robertson is a reporter for Bloomberg News in San Francisco.