

NEWS

PCI Security Standard Gets Played At House Hearing

Payment card industry's data security rules aren't working, critics say; Visa, PCI council continue to defend standard.

By Jaikumar Vijayan

Computerworld |

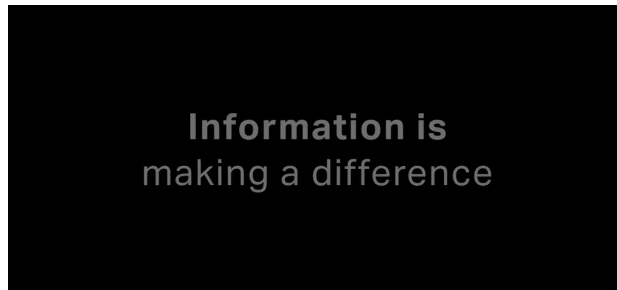
APRIL 01, 2009 08:00 AM PT

The PCI standard, long touted as one of the private sector's best attempts to regulate itself on data security, is increasingly showing signs of coming apart at the seams.

At a hearing in the U.S. House of Representatives Wednesday, federal lawmakers and representatives of the retail industry challenged the effectiveness of the PCI rules, which are formally known as the Payment Card Industry Data Security Standard (PCI DSS). They claimed that the standard, which was created by the major credit card companies for use by all organizations that accept credit and debit card transactions, is overly complex and has done little thus far to stop payment-card data thefts and fraud.

The hearing, held by a subcommittee of the House Committee on Homeland Security, also highlighted the longstanding bitter divide between retailers on one side and banks and credit card companies on the other over the role that the latter organizations should play in protecting card data.

ADVERTISING



[Beware the 9 warning signs of bad IT architecture and see why these 10 old-school IT principles still rule. | Sign up for CIO newsletters.]

In one of the bluntest denouncements of PCI DSS to date, Rep. Yvette Clarke (D-N.Y.), chairwoman of the subcommittee that held the hearing, said the standard by itself is simply not enough to protect cardholder data. The PCI rules aren't "worthless," Clarke said. But, she added, "I do want to dispel the myth once and for all that PCI compliance is enough to keep a company secure. It is not, and the credit card companies acknowledge that."

Much of PCI's limitations have to do with the static nature of the standard's requirements, according to Clarke, who said the rules are ineffective at dealing with the highly dynamic security threats that retailers and other merchants now face.

For instance, she pointed to the data breach disclosed early last year by Hannaford Bros. Co., which said that attackers had stolen card numbers and expiration dates by installing malware on servers at each of the Scarborough, Maine-based grocery chain's stores and capturing the data as cards were swiped at cash registers.

Hannaford was certified as PCI-compliant by a third-party assessor in February 2008, just one day after the company was informed of the system intrusions, which had begun two months earlier. That means the grocer received its PCI certification "while an illegal intrusion into its network was in progress," Clarke said.

[Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!]

Similarly, RBS WorldPay Inc. and Heartland Payment Systems Inc. were both certified as PCI-compliant prior to breaches that the two payment processors disclosed in December and January, respectively. Visa Inc. dropped Heartland and RBS WorldPay from its list of PCI-compliant service providers last month and is requiring them to be recertified, although it has said that merchants can continue to do business with the two companies in the meantime.



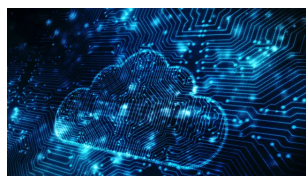
BrandPost Sponsored by eFax Corporate
Will paper records lead to a security breach at your company?

Clarke also blasted the credit card companies and card-issuing banks for continuing to use what she described as "1950s-era" payment systems. She called on them to make the investments that are needed to move away from magnetic stripe and signature transactions to the kind of approaches used in Europe and Asia, such as so-called chip-and-PIN techniques.

"The bottom line," Clarke said, "is that if we care about keeping money out of the hands of terrorists and organized criminals, we have to do more, and we have to do it now."

An independent governing body called PCI Security Standards Council LLC, with representatives from the credit card companies, banks and merchants, was set up to administer PCI DSS in 2006.

But Michael Jones, CIO at arts and crafts retailer Michaels Stores Inc. and one of the people who testified at Tuesday's hearing, said that the PCI rules appear to have been developed more "from the perspective of the card companies, rather than from that of those who are expected to follow them." As a result, he contended, the requirements aren't always about better securing data, but about what's best for the card companies and their financial-institution partners.



SponsoredPost Sponsored by NETSCOUT
Improve performance and service delivery – top priority for migrating to hybrid cloud

And when a breach occurs, it's always the affected merchant that takes the rap and bears the financial costs, Jones noted. "We are the ones in the press, we are the ones who are demonized," he said. But, he added, retailers are required by banks to store card data on their systems, even though many would prefer not to.

"As a retail CIO, I would like nothing better than to not store a single credit card number anywhere in our network of systems," Jones said. But that data has to be kept in case of disputed transactions in which a bank might ask a retailer to prove that a purchase actually took place. Retailers that can't provide such proof have to bear the costs of the disputed transactions, according to Jones, who said the issue could be addressed relatively easily if the industry switched to a model in which unique identifiers were assigned to each transaction.

Joining in the PCI bashing was David Hogan, CIO at the National Retail Federation, who claimed that PCI is little more than a tool to shift financial risks off of the balance sheets of banks and card companies and onto those of retailers. Hogan slammed the card companies for forcing retailers to scrap existing security programs and spend billions of dollars overall to implement a standard that he argued has done little to improve data security.

Echoing Jones' comments, Hogan said that what's ironic about the current situation is that retailers are being compelled to store card data - making them an attractive target for attackers. "If the goal is to make credit card data less vulnerable, the ultimate solution is to stop requiring merchants to store card data in the first place," he said.

Bob Russo, general manager of the PCI council, downplayed the concerns and insisted that the security rules are based on an industrywide consensus and input from all stakeholders. Russo defended the effectiveness of PCI DSS and said that when implemented correctly, the standard is useful in protecting against data breaches. He also repeated previous contentions that in every instance in which an organization has been breached, it was found to not be compliant with PCI DSS at the time of the breach.

Validation of compliance by an assessor represents only "a snapshot in time" of a company's security status, Russo added. "Effective compliance is a full-length feature film where the organization is compliant in each and every frame of that film," he said.

Voicing similar sentiments was Joseph Majka, head of fraud control and investigations at Visa. Majka refuted Clarke's claim that the PCI requirements are static and said periodic reviews and updates of the standard are meant to ensure that the rules stay aligned with current threats. He also argued that while the tendency has been to focus on the data compromises, the standard has helped to reduce breaches and fraud at companies that comply with it.

In addition, Majka insisted that Visa doesn't require retailers to store card data on their systems and said that it was up to them to work with card-issuing banks on unique transaction identifiers if they want to adopt that approach. And he pointed to efforts to get retailers to purge magnetic stripe and PIN data from their systems as an example of the work that is being done to reduce the amount of cardholder data that is being retained.

Yesterday's hearing is sure to add to the growing chorus of doubt about the effectiveness of the PCI rules. Initially, PCI DSS was seen as a shining example of how the private sector could responsibly regulate itself on security matters. But a seemingly never-ending stream of data breaches has taken some of the luster off of the standard.

The key takeaway from the hearing is that the time may have come "for some real oversight in the credit card industry" on how card data is secured, said Tom Kellerman, vice president of security awareness at Core Security Technologies, a security software vendor in Boston. "We saw PCI being challenged in a way it never has been," he said.

Kellerman, who was a member of a think-tank commission that issued a set of cybersecurity recommendations for the federal government in December, added that security standards should be based on actual threats, not on a consensus approach aimed at appeasing all stakeholders. And, he said, the credit card companies need to realize that merely transferring to merchants the risks and responsibilities associated with securing data won't cut it any longer.

This story, "PCI Security Standard Gets Played At House Hearing" was originally published by Computerworld.


Next read this:

- [15 IT resolutions for 2019](#)
- [The 9 new rules of IT leadership](#)
- [20 ways to kill your IT career \(without knowing it\)](#)
- [IT manager's survival guide: 11 ways to thrive in the years ahead](#)
- [7 key IT investments for 2019 \(and 3 going cold\)](#)
- [10 signs top talent may soon leave](#)
- [11 red flags to watch for when hiring](#)
- [7 things IT should be automating](#)
- [8 digital transformation mistakes \(and how to fix them\)](#)
- [8 IT cost cutting mistakes you need to avoid](#)
- [Why IT-business alignment still fails](#)
- [CIO resumes: 6 best practices and 4 strong examples](#)
- [4 KPIs IT should ditch \(and what to measure instead\)](#)
- [6 practices of influential IT leaders](#)

Jaikumar Vijayan is a freelance technology writer specializing in computer security and privacy topics.

Follow      

Copyright © 2009 IDG Communications, Inc.

 **FREE Download: Get the Spring 2019 digital issue of CIO magazine!**

SPONSORED STORIES ::



Born Billions: The 25 Richest Heirs and Heiresses in America

Investing.com



Switch to Progressive and you could save \$699 on car insurance

Progressive



The Unusual Link Between Eggs And Diabetes (Watch)

healthbenefits.vip



An Apple Engineer Designed a Sweatshirt That's Disrupting American Manufacturing

American Giant on Business Insider



[Pics] These Yearbooks Were Printed And Handed Out To The Whole Student Body Before The...

Livestly



What Legal Cannabis Means For NY In Next Few Months

FTI Journal



Data governance is key to a data-driven business

CIO



Top 10 blockchain startups in Southeast Asia

CIO



The future of system architecture

CIO



The Link Between Vitamin D and RA

HealthCentral



[Pics] Priscilla Has Revealed What Elvis Used To Ask Of Her, And It's Astonishing

Direct Expose