PCI
data security compliance

IMPACT *and* EFFECT *on the* RETAILER

AN INDEPENDENT REPORT ON

Payment Data Security

Mitigating Your Risk

- What's the Payment Card Industry Data Security Standard?
- What are the consequences of noncompliance?
- How can I ensure compliance and avoid costly fines and litigation?
- Are my systems providers compliant? How do I know they are?

Sponsored By:

MegaPath™

With Content And Analysis From:

VISA

yankee group

The threat is real, and collectively, retail's defenses are weak. We're talking about payment card holder data security, and according to Visa, only 40% of those it classifies as level-one retailers (those conducting 6 million or more card transactions per year) are compliant. The mid-market fares no better, with Visa counting only 16% of its level-two retailers (those conducting between 1 and 6 million card transactions per year) compliant.

Data Security Breach: Much To Be Feared

Payment data breaches are happening more frequently and becoming more severe. A recent major breach at TJX Companies occurred on computer systems that process and store information on customer transactions for the company's T.J. Maxx and Marshalls banners. This high-profile breach created bad publicity for the retailer, even drawing the ire of Congress. House Financial Services Committee Chairman Barney Frank (D-Mass.) is now pondering payment data security legislation. But retailers that suffer embarrassment and lost sales at the hands of payment data security breaches could also suffer at the hands of the likes of Visa. Fines of $10,000 per month, per merchant are possible, and Visa alone levied $4.65 million in fines last year. Worse yet, the payment giant reserves the right to disallow noncompliant merchants the luxury of accepting Visa cards. That's daunting considering that Visa boasts 1.51 billion cards in circulation, generating more than $4.4 trillion in global sales.

The PCI Data Security Standard*

Build and Maintain a Secure Network

1.) Install and maintain a firewall configuration to protect data

2.) Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3.) Protect stored data

4.) Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5.) Use and regularly update antivirus software

6.) Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7.) Restrict access to data by business need-to-know

8.) Assign a unique ID to each person with computer access

9.) Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10.) Track and monitor all access to network resources and cardholder data

11.) Regularly test security systems and processes

Maintain an Information Security Policy

12.) Maintain a policy that addresses information security

*Standards adopted and enforced by Visa International, American Express, Discover Financial Services, MasterCard Worldwide, and JCB.

Avoid Compromise By Protecting Data

The PCI Security Standards Council outlines the steps to compliance in no uncertain terms, beginning with the Standard Outline on this page (used with permission).

According to Jennifer Fischer, director, payment system risk & compliance at Visa USA, the most common and damaging violation of the PCI Data Security Standard is storage of full track data, or the full range of information contained in a cardholder's mag-stripe. "Track data is only intended to be used during a transaction," Fischer says, "yet many merchants store it knowingly because they aren't aware it's a violation." The danger in storing such information lies in the stored data's connection to the LAN, which, if left unprotected, is a likely source of a breach.

The Difficulty With Regulatory Compliance

Achieving security compliance isn't easy, but it's worth the time and energy, and there are solution providers who can help. Sandra Palumbo is program manager for enterprise IT and communications services at Yankee Group Research, Inc. She recently co-authored a report entitled Security Leaders and Laggards Compliance Survey, which measured enterprise's compliance efforts and attitudes. Her findings might explain the slow adoption of the PCI Data Security Standard. Enterprises are immediately disadvantaged by budget, with 44% reporting compliance budgets totaling less than half a million dollars. But more startling than a lack of funding are the atti-

tudes the study uncovers, illustrated in Figure 1. Of those surveyed, the findings indicate that only 24% fit the "Jail Dodger" profile of having the means and the methods to achieve regulatory compliance.

The study crossed enterprises of several stripes, but it called out retailers in a less-than-flattering way. While most companies (35%) were found to achieve completion of security compliance audits in two to four weeks, most retailers (26%) took 8 to 12 weeks (Figure 2). Palumbo attributes this to the difficulty with industry-specific regulations like PCI Data Security Standard Compliance and the unknown repercussions to noncompliance. Alan Stukalsky, CIO at 1,500+ location Church's Chicken, overcame this difficulty by calling on service providers to help his company get compliant. "To meet the standard on our own, we were faced with significantly expanding our IT staff with tech-savvy data security and networking experts, then sourcing compliant infrastructure and appliances on our own." Instead, Stukalsky called on the retailer's service and systems providers (such as its managed network services provider) to provide compliant solutions.

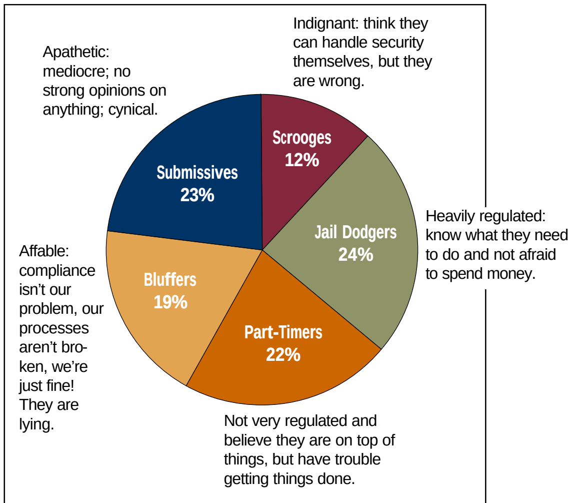


Figure 1: The profiles of C-level executives as they relate to security compliance. Source: Yankee Group Research, Inc.

As high-profile breaches continue to occur, it's very likely that organizations like Visa will crack down more often and more publicly. Palumbo urges retailers to partner with their solution providers in an effort to expedite compliance. Potential fines and litigation aside, she stresses the collateral damage done when a brand is connected with the compromise of consumer data. "In retail more than most industries, noncompliance and a subsequent breach can cause your company to end up on the front page of The Wall Street Journal. This makes security compliance much more than an IT and security issue, it makes it a board-level issue," she says.

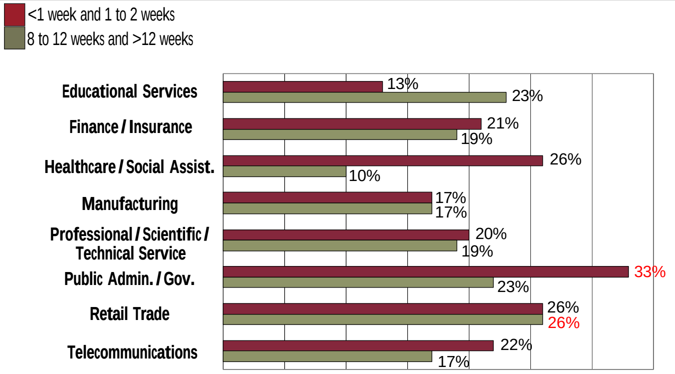


Figure 2: Retailers take longer to complete audits. Source: Yankee Group Research, Inc.

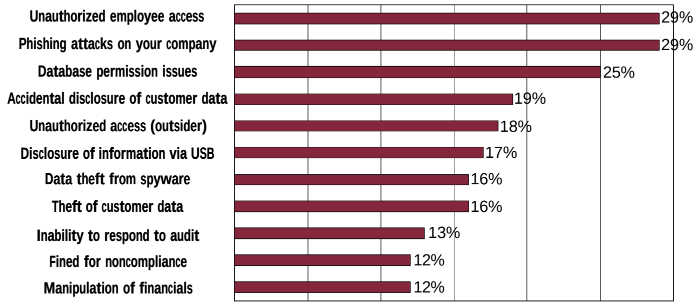


Figure 3: Which of these incidents did your organization experience in the last 12 months? Source: Yankee Group Research, Inc.

Get Compliant Now

Partnering with the solution providers you outsource to can help you hit all 12 overarching bullets on the PCI Data Security Standard and avoid data compromises like those measured in Figure 3. Choose a managed network service provider that is itself PCI compliant; has experience in the retail market; offers built-in firewalls, encryption, intrusion prevention and detection, and antivirus software; and segregates POS and credit card terminals from other devices on the LAN.

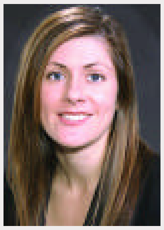
Meanwhile, Eduardo Perez, vice president of payment system risk & compliance at Visa USA, says that meeting the requirements set forth in the PCI Data Security Standard takes a holistic approach. He advises retailers to choose vendor partners that have demonstrated their commitment to data security. "Entitities handling the processing, storage, or transmission of payment data must be validated, compliant agents," says Perez. Keep this tip in mind as you build and upgrade systems. Visa maintains a list of compliant agents for your reference at www.visa.com/CISP.

Content & Analysis Partners:

About Visa:

Visa is a private, membership association jointly owned by more than 20,000 member financial institutions around the world. The organization is dedicated to serving those members, their cardholders, and their merchant clients by facilitating payment anywhere, anytime, and any way.

www.visa.com



Jennifer Fischer
Director,
Payment System
Risk & Compliance,
Visa USA

Eduardo Perez
Vice President,
Payment System
Risk & Compliance,
Visa USA

About Yankee Group:

As the first independent technology research and consulting firm, Yankee Group is a respected source of deep insight and counsel on the impact of the global connectivity revolution on enterprises and consumers. Its expertise spans the technologies creating communications change, and the regions and industries affected by that transformation.

www.yankeegroup.com

MegaPath is the leading provider of managed IP (Internet Protocol) communications services in North America. MegaPath specializes in designing and deploying network security solutions for the retail industry. The company was the first network service provider to become CISP/PCI compliant. Megapath's service addresses several of the standards for retailers:

- *It provides a managed 24x7 firewall service*
- *It protects stored data via the segregation of POS and credit card terminals from other devices on the LAN*
- *It encrypts transmission of credit card data across public networks (3DES encryption) ensuring that cardholder data is kept private*
- *Its antivirus service is continually updated with the latest AV signatures*
- *It secures systems and apps via its IPS (Intrusion Prevention Service), which identifies and blocks suspicious network activity*
- *Its strict internal policies and procedures ensure that only appropriate individuals have access to its customers' network infrastructures.*
- *By using an SSL (secured socket layer) remote access VPN (virtual private network) service, granul ar application-level restriction is possible*
- *24x7 network monitoring ensures security systems are in place and working*
- *Detailed reports help retailers identify threats and maintain security policies.*

MegaPath boasts industry-leading retail customers such as Papa Johns, Check Into Cash, Church's Chicken, El Pollo Loco, Jenny Craig, Kiddie Kandids, RadioShack, Shell Oil, and Subway. Find out why these leading retail companies rely on MegaPath to secure their networks.

For more information call
(877) 634-2728

or visit the Web site at
www.megapath.com