



What Is PCI Compliance And Should Merchants Be Concerned About It?

December 12, 2007 · by [Brian Getting](#)

The major credit card issuers created PCI (Payment Card Industry) compliance standards to protect personal information and ensure security when transactions are processed using a payment card. All members of the payment card industry (financial institutions, credit card companies and merchants) must comply with these standards if they want to accept credit cards. Failure to meet compliance standards can result in fines from credit card companies and banks and even the loss of the ability to process credit cards.

There are six categories of PCI standards that must be met in order for a retailer to be deemed compliant.

Maintain a secure network

This standard refers to the actual network that cardholder data is exposed to. In the case of an online business, the most obvious vulnerability for this standard is the web server. Luckily, most hosting companies take responsibility for ensuring the security of their networks. However, there is more to this standard than meets the eye. Do you keep cardholder data (even just names) on a laptop that you use on public networks? Does your office network have a firewall installed and reasonable security measures in place?

In short, whenever any personal information about a cardholder is stored on a computer (which is also connected to a network), that computer is behind a firewall and all reasonable measures have been taken to protect that particular network.

Protect Cardholder Data

This category focuses on how cardholder data is stored and transmitted. Business owners that choose to store cardholder information have an obligation to protect that data. Protecting information means that not everyone can access that it. Businesses that store actual credit card numbers will often store them as encrypted data, so that even if someone got access to the database they still could not decipher the information in it.

Ecommerce businesses need to be especially critical of the way that cardholder data is transmitted. When a customer makes a purchase on a website, his/her cardholder information is sent across the Internet. During that transmission, cardholder data must be encrypted with at least a 128 bit SSL certificate in order to meet this standard.

Maintain a Vulnerability Management Program

This one is relatively simple, and translates to keeping up to date with your systems. Vulnerability exposure can be minimized by regularly updating computer hardware, operating systems and software. Keeping up to date anti-virus software, as well as running regular virus scans, is another requirement to meet this standard if your systems are susceptible to such vulnerabilities.

Implement Strong Access Control Measures

The most exploited breach in security is the human element, which is harder to protect. Part of meeting PCI compliance means limiting access to cardholder data to only those persons that need to use it. In addition to restricting physical access to cardholder information, business owners are also responsible for assigning a unique identification to each person that does have access.

Regularly Monitor and Test Networks

Networks that store cardholder data be monitored and tested regularly. Regular scans of security measures and processes, monitoring and tracking of network access to cardholder data are required to satisfy this standard. Consider signing up for a security testing and auditing service, such as ScanAlert's Hacker Safe program, which can help you to identify and fix potential security problems as they arise.

Maintain an Information Security Policy

Considering that humans are generally the easiest part of a system to hack, and also that ignorance does not relieve liability, it's important to draft and implement a company-wide information security policy. Make sure that your employees know and understand their responsibilities with regards to cardholder data before it becomes an issue.

The first step in PCI compliance is to meet the above standards. Credit card companies and financial institutions validate that vendors are abiding by the regulations, giving them ratings based on their volume of transactions. The rating that a company receives determines the process that they must go through in order to be validated. Next month, we'll take a look at the four validation ratings, and what each rating means to a company.

Related articles

- [PCI Compliance Is "Industry Self-Regulation"](#)
- [PCI Report Card: Merchant X \(A Photography Accessory Retailer\)](#)
- [Credit Card Theft: Steps to Protect You and Your Customers](#)

This article is filed under [Hosting, Infrastructure & Software](#) and has the following keyword tags: [pci compliance](#), [data security](#).

Copyright © 2008 Practical eCommerce. All rights reserved.