Get Ready for Retail Season by Ensuring You Are PCI DSS Compliant

Retail season is almost here, but before you get too excited about what this means for your business, it's vital you understand the following about PCI DSS.

What Is PCI DSS?

When someone makes a purchase from your company with a credit card, you may think that this transaction is just between the two of you. You couldn't be more wrong, though, and this mistake could cost you more than just in money.

That's because credit card transactions that involve major companies like American Express, MasterCard, Visa, Discover, China UnionPay and JCB have to follow a certain set of rules. While this isn't law, these companies insist on a proprietary form of security standard called the Payment Card Industry Data Security Standard (PCI DSS). Accepting their cards as payment means you agree to follow these rules. If you don't, then yes, expect law enforcement to get involved, especially if your noncompliance means a customer had their information compromised.

Aside from the fact that all major credit card companies insist on this standard, it was actually started by a few of them too. Discover Financial Services, American Express, MasterCard Worldwide, JCB and Visa International actually all came together to create these standards.

However, it's also important to appreciate that these security standards are far from set in stone. The PCI DSS has its own website where you can learn all about its ongoing development, dissemination and implementation.

The PCI DSS really has three main goals, though they're extremely broad (and are growing by the day, as we just mentioned). These goals are to prevent:

- Credit card fraud
- Credit card hacking
- Other types of security compromises

Essentially, it's about ensuring the integrity of credit card use, specifically by preventing malicious third-parties from having their way with a user's private information.

Although its aims may seem relatively simple, PCI DSS takes a number of measures to secure their attainment. Amongst other things, this multifaceted security standard includes rules for security:

- Management
- Procedures

- Policies
- Software Design
- Network Architecture

There are a number of other protective measures in place as well, but these categories cover the main versions.

The 12 Requirements of PCI DSS

For a better understanding of just how comprehensive PCI DSS is in its approach to credit card security, it will be helpful to go through all 12 of the distinct requirements it insists on. The compliance objectives of this standard can be broken down into six categories like this:

Category 1: Built and Maintain a Secure Network

- Install a firewall and maintain its configuration to protect cardholder information
- Replace vendor defaults for passwords and any other security measures

Category 2: Protect Credit Card Data at All Times

- Protect stored cardholder data
- Encrypt any transmissions of cardholder information, whether it’s across public or open networks

Category 3: Maintain a Program for Managing Vulnerability

- Use anti-virus software or programs and regularly update it
- Develop security systems and applications and maintain them

Category 4: Implement Strong Access Control Measures

- Restrict access to cardholder data to essential personnel only
- Assign unique sign-in credentials to each employee with computer access
- Restrict physical access to credit card data

Category 5: Regularly Monitor and Test Your IT Infrastructure

- Track and monitor access to cardholder data and the rest of your network
- Regularly test every component of your security system

Category 6: Maintain an Information Security Policy

- Maintain a policy for addressing information security for both employees and contractors

Furthermore, complying with these 12 categories can summarized by three main stages:

- Event Collection: Securely collecting and storing all event data so that it can later be reviewed and analyzed
- Reporting: Providing evidence that safeguards have been put in place in order to protect information and confirm compliance during an audit
- Monitoring: Having systems in place for monitoring access and usage of any sensitive data and immediately alerting administrators if any failures take place

Merchant Levels

Finally, before we take a look at implementation, let's talk about merchant levels, as you'll need to know where your business falls.

- Level 1: Those with over six million credit card transactions and any with credit cardholder data that has been compromised before
- Level 2: Any with transactions that amount to more than a million, but fewer than six million
- Level 3: Merchants with fewer than a million transactions, but more than 20,000
- Level 4: Everyone else

The level you're at will also determine what validation processes you have to undertake to achieve and maintain compliance.

How to Implement It

Hopefully by now, you can tell that PCI DSS isn't some simple set of rules you can treat like a checklist. Abiding by this security standard can be a lot of hard work, despite the fact that you probably need to take dozens, if not hundreds or thousands, of credit card payments every day to keep your business going.

This is why an entire industry has grown around the need companies have for help with accepting credit card payments while abiding by PCI DSS requirements.

Today, you can find software that will handle virtually every component of proper credit card management short of actually swiping the thing for you.

Each of your employees will receive a unique ID that can only be used once they go through multifactor authentication, even if they're trying to access a system remotely. Of course, no matter where it happens from, encryption will be used to keep all passwords safe during transmission and while it's in storage.

With IDs assigned, the movements of all users within the digital environment can be tracked and recorded. Automated audit procedures can also be implemented across systems making it easy to recreate key events. This makes it impossible to later go back and modify what occurred as well. The record is then kept in storage for at least a year and available online for at least three months.

With retail season right around the corner, you're probably looking forward to seeing as much credit card use as possible. However, if you don't understand PCI DSS and take the necessary steps for implementing it, all those credit cards will actually come back to hurt you in a big way.

Source:

http://cdn2.hubspot.net/hub/215468/file-447595487-pdf/PDF/PCI/AuthAnvil_for_Retail_IT.pdf