10 PCI Compliance Best Practices to Protect Your Business and Customers

In 2014, Home Depot suffered a data breach of historic proportions. Hackers gained access to the retailer's payment systems, compromising credit card information for 56 million customers. That breach cost Home Depot $179 million. While no organization can claim immunity from cyber-attacks, following PCI compliance best practices can mitigate the extent of the damage.

All organizations that process credit cards must adhere to the Payment Card Industry Data Security Standard (PCI DSS) or face stiff fines. More importantly, PCI compliance represents a starting point for effective cyber security. Following best practices not only keeps you compliant but protects both your business and your customers.

1. Use Firewalls

Firewalls form the first line of defense for your network and all devices connected to the network. Make sure to maintain those firewalls, applying software updates as soon as they become available.

2. Change Default Passwords

Many devices critical to your system, including routers and point of sale (POS) systems, come installed with default passwords. Always replace the defaults with strong passwords. Hackers know the defaults and have used them successfully over and over again to gain access.

3. Encrypt All Transmitted Data

Credit card and customer information must be encrypted at every stage of the process. Make sure that you properly configure and enable encryption features on your wireless router and payment gateways.

4. Keep Software Up to Date

Make it a point to apply security patches in a timely fashion. This applies to your operating system, anti-virus and anti-malware, and all other software you use. Pay special attention to updating software on all devices that interact with credit card data.

5. Restrict Access to Cardholder Data

No one should have access to cardholder data unless their work duties require that access. Deny access for anyone else. Ideally, you should avoid storing sensitive cardholder data on your server or hard drive at all. Most modern payment gateways will provide a vault feature for you to store cardholder information away from your website.

6. Monitor and Log All Activity

In the event of an issue, you need to be able to trace the problem to its source. First, make sure that every user has a unique identifier. That is, you should never have multiple employees sharing generic credentials for a device.

Second, create access logs to document all activity relating to cardholder data. Finally, review system security and audit logs regularly to search for compliance issues and anomalies.

7. Run Regular Security Tests

PCI DSS requires an annual network vulnerability scan and Self-Assessment Questionnaire. But demonstrating PCI compliance once a year will hardly ensure cyber security. Run mini audits regularly to test systems and procedures and highlight vulnerabilities.

8. Choose Your Payment Processor Wisely

Payment processors offer a variety of features. Every provider will provide a measure of PCI compliance service, and will charge you accordingly. But some vendors provide more comprehensive services than others. Do your homework and thoroughly review your contract before signing on.

A good payment processor will provide regular security scans and give you access to the logs. They will ensure that processing systems are PCI compliant. Many will also include encryption.

9. Monitor for Card Skimmers

Train employees to monitor POS systems for credit card skimmers. Thieves can install them in seconds, so while self-service lanes pose the greatest risk, any POS can be compromised. EMV technology reduces the risk, although criminals have even begun to target chip cards, as well.

10. Train Employees

No matter how effective your network security and anti-virus, the human factor remains the weakest link in the security chain. Communicate policies clearly and provide regular, industry-specific training for employees. Approach cyber-security training on multiple levels, from in-person seminars to posters and workflow reminders.

Expert PCI Compliance Management Services

eMazzanti provides proven retail IT services, with staff trained at the highest levels in retail data security. As an active member of the PCI Security Standards Council, we are working to advance world-wide PCI security standards. Our QIR certified PCI experts work hard to implement and monitor your POS system, build robust network security and ensure PCI compliance.