Security Compliance Requirements in the Retail Industry

Whether you're a multibillion dollar corporation or a small mom and pop Internet merchant, if you accept credit card payments, it is critically important you are in compliance with the PCI Data Security Standard (PCI DSS) to ensure customer data is kept secure.

The Payment Card Industry Data Security Standard was developed to encourage the adoption of consistent data security measures and provide standard requirements designed to protect cardholder data. PCI DSS applies to all entities along the payment card processing supply chain, not just merchants, but processors, issuers and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

What Does PCI DSS Compliance Mean, Exactly?

PCI DSS compliance can be looked at in a couple of different ways. In terms of security, it means that businesses must adhere to the PCI DSS requirements for vital security measures such as policies, security management, procedures, network architecture, and software design.

In operational terms, it means that merchants do their part to ensure customer payment card data is kept safe throughout every transaction and protected against a data breach.

Who is Required to be PCI DSS Compliant?

PCI DSS applies to every entity that processes credit or debit card information. This can include merchants and third-party service providers that store, process or transmit credit card/debit card data. In 2007, PCI compliance became a requirement instead of a request. Those businesses that still question whether they are responsible or not for complying with PCI DSS should follow this simple rule of thumb: If you house or store credit card information in your server, in whatever form, you are required to be compliant.

Best Practices for Maintaining PCI DSS Compliance

As new technologies emerge and new ways of hacking personal data are discovered, compliance to the PCI DSS rules will continue to evolve. Just because a business is currently compliant doesn't mean that it will be in the future.

Businesses should take the following steps to maintain PCI DSS compliance:

Establish an Effective Long-term Process

It's important to not lose sight of the driving objective – which is simply to secure cardholder information. Very often, businesses focus on the compliance process itself but fail to establish effective long-term processes for maintaining security. To reduce vulnerability, all stakeholders must take part in the effort, commit to the long-term process, and consider why they collect certain data and if it's absolutely necessary in order to conduct business.

Appoint a Compliance Manager

Maintaining PCI DSS compliance requires coordination of numerous people and resources as well as the integration of a well-managed security program. For this reason, a compliance manager should be appointed and made responsible for security activities and collecting, preparing, indexing and storing data evidence for assessments and internal reviews.

Detect and Respond to Security Control Failures

Not only do organizations need to be able to detect failures in security controls, they must also have processes in place for responding to those failures and in a timely fashion.

Define Your Metrics

Maintenance will require a set of metrics to be defined and developed that will measure the performance of the security controls and program.

With credit card data being stored virtually, in accessible areas, PCI standards are important to help businesses implement better security practices. Being PIC compliant is a requirement in today's digital marketplace, yes, but all businesses should be happy to comply because ensuring the safety of customers' payment information just makes good business sense.