

PCI Data Security Standards Compliance: It's All or Nothing

By Bob Cedergren, Partner

June 2010

Cyber thieves work long and hard to steal credit card and other personal information. Since 2005, nearly 356 million records containing sensitive, personal information, including credit card numbers, have been compromised due to security breaches (www.privacyrights.org).

In 2006 as a result of growing threats, a consortium consisting of the major credit card companies combined their efforts to create a single standard of security requirements in order to better protect cardholder data.

Known as the Payment Card Industry Data Security Standard (PCI DSS), it today specifies 12 requirements that merchants accepting credit and debit cards must meet and maintain. And nothing less than 100% compliance with all the standards is acceptable . . . period!

PCI DSS isn't just intended for retail merchants. It applies to any organization that accepts, transmits, or stores any cardholder data, regardless of the company's size or the number of transactions.

That means it applies to auto dealerships that accept credit/debit cards for service work performed. To health care clinics that see patients who use credit/debit cards for copayments. And to manufacturers that sell to credit-card-paying customers via an e-commerce website or during annual overstock warehouse sales.

PCI DSS applies across all industries. And it applies even if an organization has just one customer who prefers payment by credit card.

The High Price of Noncompliance

Organizations that fail to comply with PCI DSS face serious consequences. Not only does noncompliance put companies at great risk by leaving their data vulnerable and their customers exposed to theft, but it also comes with costly fines of \$5,000 to \$100,000 per month!

Companies can face additional card-replacement costs of \$50-\$90 per card and may even lose their ability to accept payment cards, which could prevent them from conducting business altogether. Worse still is the risk to an organization's reputation that the wrong kind of publicity brings, as well as potential class-action lawsuits that could follow.

In all, the average cost per compromised record is estimated to be between \$90 and \$300 per customer!

The Top 3 Compliance Mistakes

Companies that store, process, or transmit customer credit card data must take the initiative to implement a robust PCI DSS compliance program and employ best practices for securing sensitive

information. Depending on an organization's size, merchant level, and resources, this can be a daunting task.

In many cases software programs must be installed, and ongoing monitoring must be put into place. Compliance reporting is also required.

Along the way, organizations often experience complications, confusion, and even chaos. Here are the top pitfalls to avoid when pursuing and sustaining PCI DSS compliance:

- **Pinning total compliance efforts on a single product.** One piece of software is not the magic ticket to making an organization compliant. As with any risk management program, technology is but one element of the overall effort. Real security depends on a holistic approach that also entails processes, policies, control measures, testing, and training.
- **Assuming that completion of the self-assessment questionnaire (SAQ) equals compliance.** For organizations that are not required to perform onsite assessments, this is technically true—but only for that one particular moment in time. Any changes made in the environment or system can instantly create a noncompliance situation. Once an SAQ is completed, only a post-breach analysis can again prove PCI DSS compliance.
- **Believing that being compliant means being secure.** As stated above, successfully completing a security scan or assessment will provide only a snapshot in time. In the meantime, cyber and security threats are relentless and ongoing. In 2008, 2 out of 10 companies that experienced a security breach were considered PCI DSS compliant. Therefore, compliance efforts must be a continuous process of assessments and risk mitigation to ensure the sound protection of cardholder data.

About the Author

Bob Cedergren leads Wipfli's Risk Management Practice. He assists clients with PCI DSS compliance and developing other risk management programs. For more information, contact Bob at 651.766.2889 or bcedergren@wipfli.com.

About Wipfli LLP

With almost 800 associates and 15 offices across the Midwest, Wipfli ranks among the largest accounting and business consulting firms in the nation. Serving businesses and individuals since the firm's start in 1930, Wipfli has one of the region's strongest risk management practices, with an extensive list of clients across the Midwest. For more information, visit www.wipfli.com.