

Dollars and Sense: Calculating PCI Noncompliance Costs

By Ellen Libenson, E-Commerce Times, 12/12/07 4:00 AM PT

Without question, there is a substantial cost associated with reaching and maintaining PCI DSS compliance requirements. While the initial cost of the technology, staff and other resources necessary to implement satisfactory controls has its price tag, it is vital that all organizations affected by the PCI standard consider both the short- and long-term costs of noncompliance as well as the benefits of meeting the requirements.

You don't have to break the bank to own powerful server technology. The HP Proliant DL380 G5 Server with Systems Insight Manager (SIM) comes equipped with everything your business needs to succeed - including a smaller price tag.

Despite being given a deadline of Sept. 30, 2007, to comply with the Payment Card Industry Data Security Standard (PCI DSS), many Level 1 merchants -- those that process more than 6 million transactions per year -- still do not meet the necessary requirements. In fact, Visa reports that as much as 40 percent of its Level 1 merchants fall into this category.

While monthly fines for noncompliance -- ranging from US\$5,000 to \$25,000 -- may not seem too steep for these large merchants, there are far greater costs associated with noncompliance beyond these monetary fines levied by the PCI.

It is critical for IT administrators and C-level executives to consider all of the costs associated with PCI compliance and noncompliance, especially given the looming Dec. 31, 2007, deadline for Level 2 merchants to demonstrate compliance. Some are palpable, of course, but others may not be as evident, and it is also important to understand the far-reaching benefits of compliance.

The Costs of Compliance and Noncompliance

Calculating the costs of PCI DSS compliance can be difficult. It is not simply a matter of achieving compliance and then maintaining it, because PCI compliance is a moving target. For example, it is moving in response to consumer pressure to make more of the PCI industry standard into law so it becomes a regulatory mandate.

What's more, the technologies and vectors that attackers use to perpetrate their misdoings are becoming more sophisticated; new countermeasures will have to be purchased and implemented to address these emerging threats. This makes the ongoing cost of compliance difficult to measure and can deter organizations from investing the proper resources necessary to meet the standards laid out in PCI DSS. However, the ongoing costs of noncompliance can be far greater.

In addition to the monthly fines, one of the biggest costs on noncompliance is lost business if an acquirer refuses to process card payments for a merchant after a data breach occurs. Many of these attacks involve the theft of magnetic stripe data stored on a merchant's system.

This is often done without the retailer's knowledge, as the information is stored by application software that the retailer cannot decipher. However, storing magnetic stripe data is a violation of the PCI standard. Card companies will likely fine merchants for this noncompliance, and they may also halt processing payments, resulting in potentially huge amounts of lost revenue.

Damaged Reputations

When a data breach occurs, there is also significant damage done to a merchant's stock price, reputation and customer loyalty. Consumer surveys reveal that many people lose respect and/or trust for businesses after customers' personal information was misplaced or stolen from those companies' systems. Logically, most consumers would greatly prefer to conduct business with a company that has never experienced a data breach.

While it is difficult to pinpoint the exact monetary cost of damaged reputations and lost customer loyalty as it relates directly to security, the now-infamous [TJX](#) breach of cardholder data in January of 2007 may have changed the trade-off between the cost of implementing PCI DSS and the potential cost of not doing so -- especially for larger merchants. Now that the extent of the TJX breach is known, research firms estimate that the total cost could exceed \$500 million. Others predict that it could approach \$1 billion over time.

It is clear that the business logic for postponing PCI compliance is quickly evaporating. While the TJX fiasco highlights the potentially astronomical costs of noncompliance, it is important to realize the benefits of compliance beyond avoiding becoming the next merchant to make front-page news.

Benefits of PCI DSS Compliance

PCI DSS compliance delivers benefits felt throughout the organization, some of the more noticeable of which include the following:

- Lower likelihood of a breach and faster recovery if there is a breach;
- Reduced risk of financial loss through fines, lost business, lawsuits and other results of a breach;
- Enhanced industry standing and customer reputation as a leader willing to commit resource to secure cardholder data; and
- Improved operational and financial results.

However, there are a number of less-obvious benefits that executives should consider as well. For example, implementing technologies and initiatives to comply with PCI DSS facilitated a shorter time to be in compliance with other regulations and standards. On average, organizations today must achieve compliance with two or three mandates.

PCI DSS is so granular in securing data, so focused on the workflow of cardholder data as received and processed by industry members, and so general in its best-practices approach to data security that once an organization achieves PCI DSS compliance, most of the work has been done to demonstrate compliance with regulations -- including SOX (the Sarbanes-Oxley Act), HIPAA (Health Insurance Portability and Accountability Act), U.S. federal security standards and others -- designed to protect other data workflows.

Improving Operations

Another benefit to PCI compliance involves risk reduction and risk management. The TJX breach makes it clear that merchants, Internet vendors and service providers must view PCI DSS compliance as a tool for controlling the risk of substantial financial loss. This is true even for small merchants and service providers, since by contract they are liable to acquirers for the costs of a breach. Large merchants and service providers must view PCI DSS compliance as a major component of their corporate risk management planning.

Similarly, complying with PCI DSS can improve operations and security. Viewed as a security model, the control framework necessary for PCI compliance can help companies control compliance costs while developing a more efficient and reliable IT infrastructure designed to deliver better service while incurring less risk. This alignment of business and PCI goals ensures that internal security policies are consistent with PCI requirements.

As discussed previously, a great deal of damage is often done to a merchant's stock price, reputation and customer loyalty when a data breach occurs. Therefore, an added benefit of PCI DSS compliance is developing a stronger competitive profile. Businesses that are already PCI compliant are experiencing all the financial, organizational and risk-management benefits, but they also have a stronger reputation -- and therefore an advantage -- over competitors that are experiencing all the costs of noncompliance and that may be forced to become compliant if they want to stay in business.

A Top Priority

Without question, there is a substantial cost associated with reaching and maintaining PCI DSS compliance requirements. While the initial cost of the technology, staff and other resources necessary to implement satisfactory controls has its price tag, it is vital that all organizations affected by the PCI standard consider both the short- and long-term costs of noncompliance as well as the benefits of meeting the requirements.

This is especially important as PCI DSS evolves and increase in complexity as the standard moves towards becoming a federal regulation. The costs of noncompliance can far exceed the cost of systems to bring a company into compliance as was demonstrated by TJX and others.

By carefully evaluating the costs of compliance versus noncompliance and treating PCI DSS as a top priority, merchants, acquirers and other organizations can enjoy the plentiful benefits while avoiding monthly fines and potentially irreparable damage to brand reputation. Conversely, a laissez-faire approach to PCI DSS compliance efforts is often accompanied by severe costs, not the least of which is the potential for an organization to be permanently adjacent to TJX on the infamous short list of companies that have suffered large-scale data breaches -- breaches from which they may never fully recover.