Authored by Certain

Serious e-commerce calls for more than just a security blanket

What you should know about Payment Card Industry Data Security Standards

At 8:45 AM, a Los Angeles executive refills her morning coffee when the company's Chief Financial Officer walks into the break room.

"I just got out of a board meeting, and the board wants you to be our company's presence at the London Business Summit next week."

At 8:50 AM, she is back at her office computer googling the summit registration site.

At 8:53 AM after a few quick clicks and some swift keyboarding, she pulls out her credit card to charge the international flight, hotel room and the summit breakout sessions for which she just registered.

At 8:55 AM, she is already on the phone tackling other business, any concern already gone from her mind about the credit card transaction that just transpired in a few short minutes or how securely her personal information just zapped across the internet.

The convenience of e-commerce has evolved the way we all do business. With only a credit card and an internet connection, today's financial transactions can take place between individuals and businesses at the speed of a mouse click. Any size organization from a one-man freelancer to a global Fortune 500 corporation can easily sell products or services to anyone located anywhere in the world. On top of that, they can instantly track that revenue hitting their bottom lines.

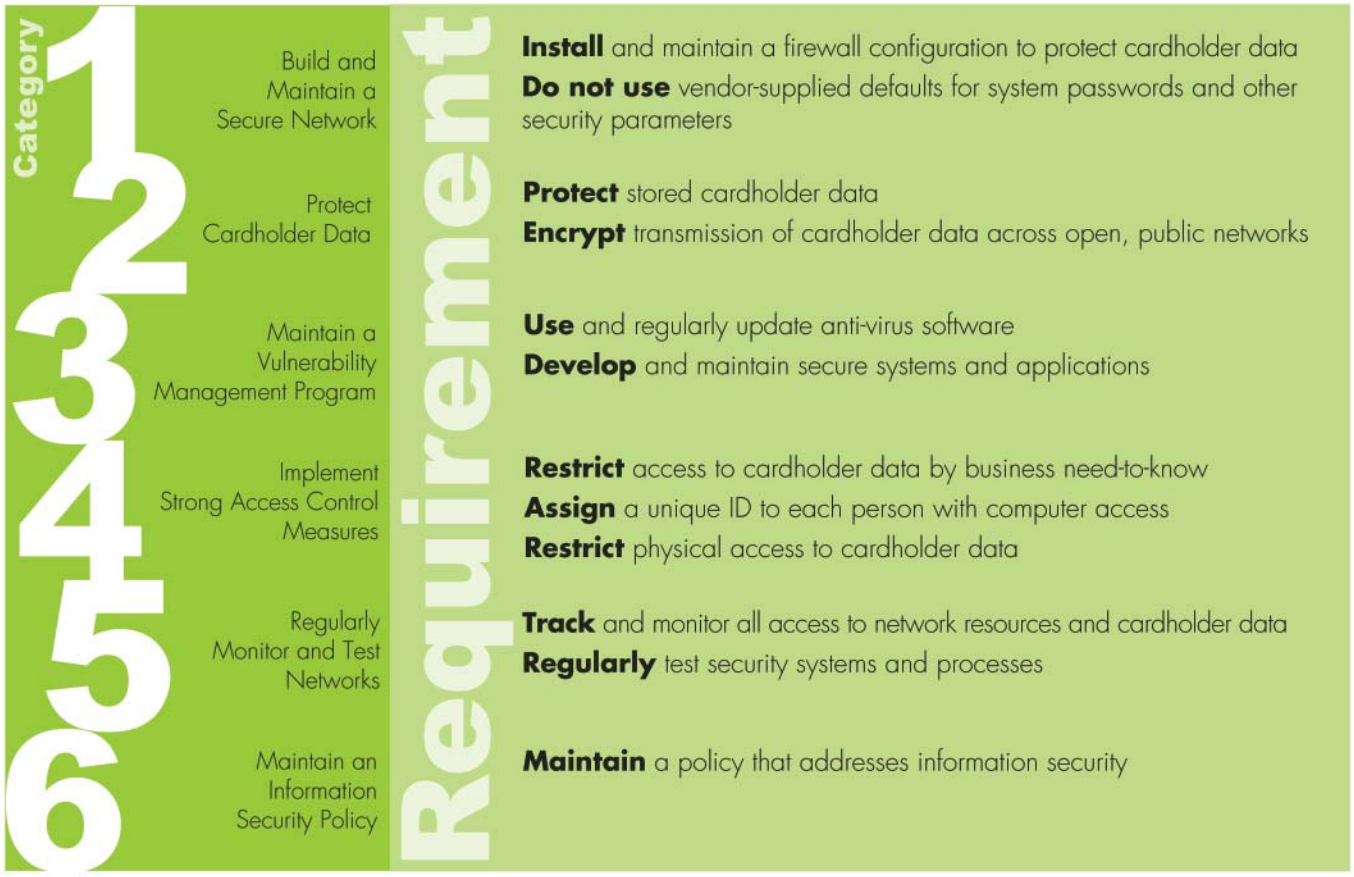
There is, of course, a downside to this convenience. E-commerce has exposed organizations to a new set of vulnerabilities. Organizations processing any volume of highly sensitive personal credit card information put themselves at risk as potentially responsible for data theft by hackers. As the world begins to tighten e-commerce regulations, organizations also face serious financial penalties, restrictions or expulsion from card acceptance programs for non-compliance with newly implemented global standards.

The PCI Security Standards Council and the PCI Data Security Standard

Most organizations have implemented ad hoc security policies, but in recent years there has been a push for universal standards to keep businesses on the forefront of e-commerce security. This is being led by major influential bodies including the Payment Card Industry (PCI) Security Standards Council and the US Federal Government.

In 2006 credit card brands Visa, MasterCard, Discover, American Express and JCB converged to form the PCI Security Standards Council. The council is an open global forum for the development and enhancement of payment account data security.

PCI Data Security Standard



PCI Data Security Standard (PCI DSS) Version 1.1 is the latest standard which addresses evolving security threats and recommends actions by which merchants and vendors can fortify application and network level security. PCI DSS is the basis by which organizations can be evaluated for their level of PCI Compliance.

The six categories within PCI DSS spell out what security measures must be taken to protect the private information during any credit card transaction.

Why think about being PCI compliant or using PCI compliant vendors?

Any company that accepts, processes, or stores credit card information needs to comply with the standards set by the Payment Card Industry Security Standards Council.

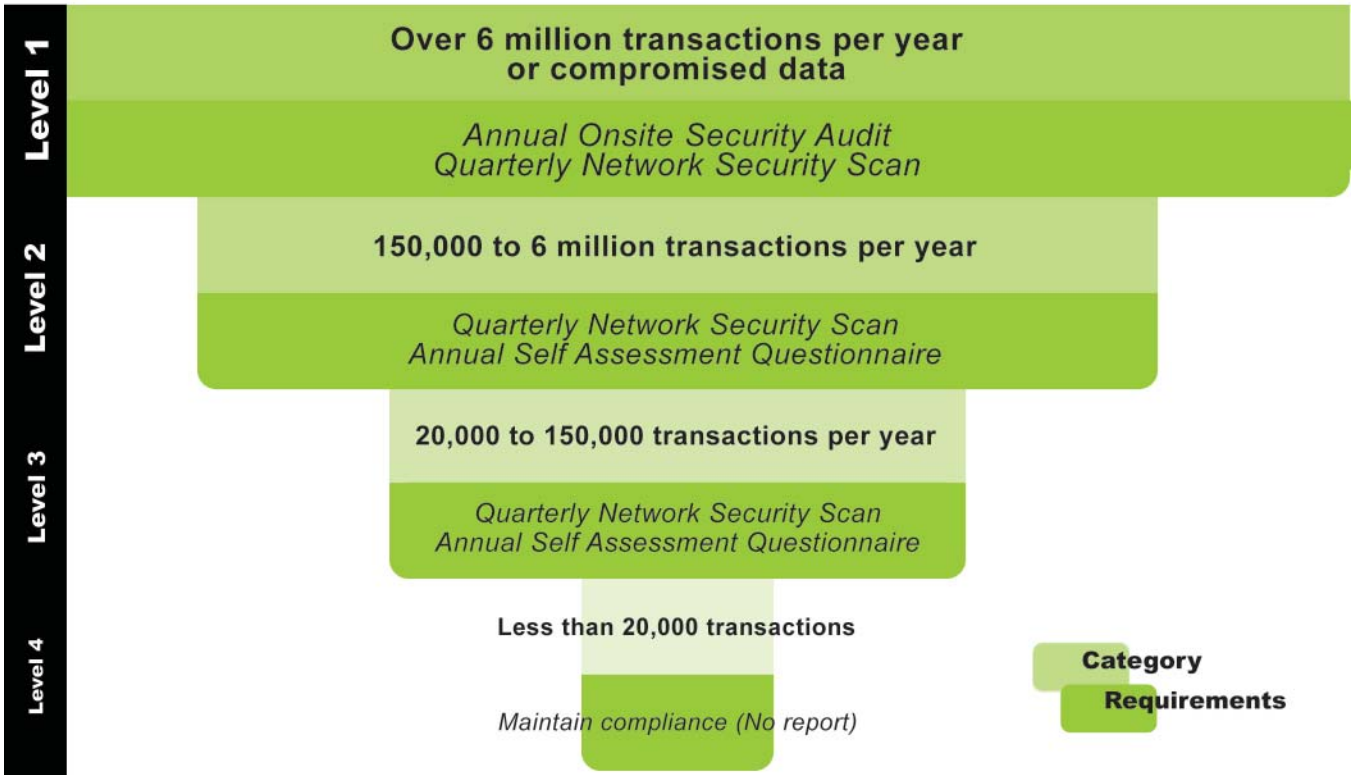
How do organizations become PCI compliant?

Organizations are divided into four different levels based on the number of transactions they process throughout a year. The requirements for becoming PCI Compliant are dependent upon the merchant levels that a company falls under.

PCI Compliance Level 1 is the highest level of compliance, intended for companies with capacity to handle the most massive credit card transaction volume. Each year, Level 1 companies must undergo an extensive, on-site Annual Security Audit performed by an PCI Approved Quality Security Assesor. Each quarter, Level 1 merchants must have compliance verified through Quarterly Vulnerability Assessment Scans performed by a PCI Approved Scanning Vendor.

PCI Compliance Level 2 and 3 companies typically process a moderate credit card transaction volume. Both Level 2 and 3 merchants are required to undergo the Quarterly Vulnerability Assessment Scans performed by a PCI Approved Scanning Vendor. In addition, each year both levels complete an Annual Self Assessment Questionnaire.

Levels of PCI Compliance



PCI Compliance Level 4 companies handle a low credit card transaction volume. There is currently no requirement for Level 4 companies to report their compliance, but to avoid penalties they must be prepared have their compliance with PCI DSS evaluated at any time.

The PCI compliance evaluation process can take anywhere from one day to two weeks. The amount of time it takes for a company to be considered PCI Compliant is dependent on the threats the PCI scan discovers and the amount of time it takes to complete the self assessment questionnaire.

With the looming risk of potential hacking or penalties, it is now essential for organizations doing any amount of credit card business to evaluate solutions providers on their ability to meet the latest developments in e-commerce security.

What about FACTA?

In addition to what credit card brands are doing to solving the problem of data security for the business world, US Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which is an amendment to the Fair Credit Reporting Act (FCRA), in 2003.

FACTA Section 113, in full effect since December 2006, ensures that only the last five digits of a credit card number or the expiration date are printed on the transaction receipt.