

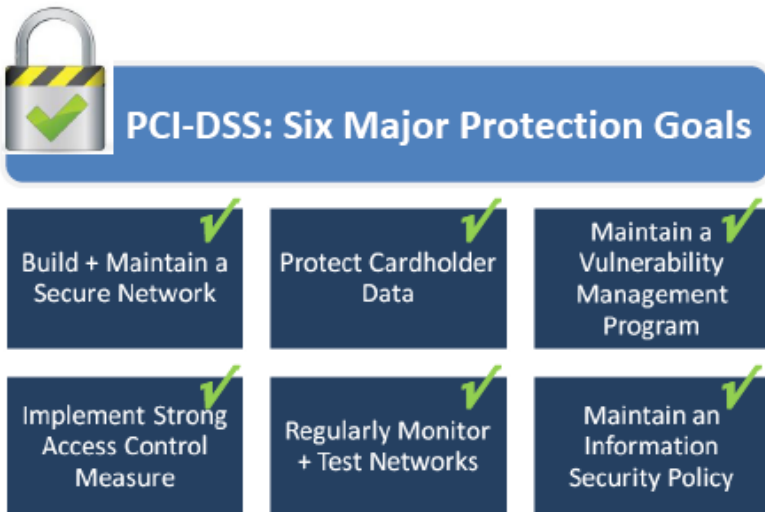
Protect Your Clients, Protect Your Business

A Payment Card Industry (PCI) Overview

By Brad Rossiter, CISA, CISM, CISSP
Security Practice Manager
Clear North Technologies

The Payment Card Industry (PCI), for all practical purposes, revolves around their published standards for protecting consumer credit card information. The PCI Security Standards Console is made up of members of Visa, Master Card, American Express, Discover and JCB whose focus is to manage and publish these security standards. The primary standard is the *Data Security Standard (DSS)*, which is designed to

protect consumers from fraud and identify theft, but in effect transfers the burden of keeping card data safe from the card companies to the merchant. DSS is a global data security standard adopted by the major card brands where **six major protection goals** are outlined and further broken down into as many as 240 control objectives. However, the validation of requirements demanded of a particular merchant is dependent on its annual transactional volume (not dollar amount).



The PCI-DSS standard, as it is commonly referred to, is a *mandate* that applies to all entities that store, process and/or transmit cardholder data. *The standard itself is neither law nor government regulation, but a best-practice method by private industry to minimize the risks associated with credit*

card commerce. However, many states (in response to widespread fraud) are appropriating resources to protect their citizens and ultimately creating acts of legislation (such as Minnesota's *Plastic Card Security Act*) to enforce some of the very same things that the PCI-DSS standard considers. One example is prohibiting the retention of security information stored on the card's magnetic strip after the transaction is completed.

For many organizations that are effected by PCI-DSS it may be the first time that information security has made it on the executive's to-do list. In the past, firewalls and password management were the extents of implementing security for these organizations, staying well below the radar of most decision makers. As with Sarbanes Oxley, PCI-DDS should be seriously considered a major business initiative. Penalties for non-compliance can be substantial and include increased processing fees, fines of more than half a million dollars, and suspension of the ability to process transactions. Furthermore, consumers will be armed to receive compensation from those businesses that were responsible for protecting their information in the first place.

Those of us in the information security industry are quick to point out that regulatory control is not a substitute for proper risk management. In other words, regulation and security are not synonymous, nor are they mutually exclusive. Their main objectives are not the same, and in fact focusing on regulation could weaken the overall security governance of the business by applying too much control to one specific area of concern (card privacy) while not holistically considering other information assets that should be protected at or above the levels described in the PCI-DSS standard.

How can we get secure while properly adhering to regulatory requirements? How can we return maximum value from minimum effort? Where did the previous effort leave us for future regulation? To answer these questions, ask yourself: *"Is our business protection strategy aligned with today's threats and tomorrow's regulation?"* In the end, each organization should be able to manage technology risks by operating and maintaining an information security program that will be flexible enough for future regulation to fit within the context of the program, and allow for *appropriate* levels of control over information. In doing so, an organization will, by default, be PCI-DSS compliant.