C H A P T E R 1

Solution Overview

The Payment Card Industry Data Security Standard (PCI DSS) is generally perceived to be a complicated means to secure sensitive information. As of 2010, according to the PCI Security Standards Council, 100 percent of all breached companies were not compliant at the time of the breach, regardless of whether they were compliant at the time of their audit. How did a company that took such pains to achieve compliance not take equal measures to maintain it? Is the standard really so complex that it is not capable of being sustained? Some pundits have argued that PCI is therefore an unrealistic goal and valueless.

Cisco takes a more balanced stance. PCI is not overly stringent from a security perspective. In fact, Cisco sees the PCI security standard to be the *minimum* security any company should have when taking payments. PCI is a global attempt at setting a minimum bar. Some very large companies and some entire countries have not developed a security awareness that meets the evolved threats of cybersecurity today. From that perspective, PCI is the lowest common denominator that provides the minimum level of protection. Putting in a firewall, changing default passwords, locking the door to the wiring closet, and making sure that you have knowledge of who is configuring a device rather than leaving open a general admin account; these items are not complex.

Although the standard is indeed intricate, the real complexity challenge comes from managing an enterprise network. Enterprise companies do not arise overnight. Most companies that existed in the 1980s did not consider data security to be an ingredient that must be included at all levels. After IP became the de facto network protocol, enterprise companies have been struggling to integrate data with voice systems, video, wireless, digital media, administrative duties, and business processes; as well as holistically integrate protection of payment card information throughout. Each of these technologies was developed independently of each other. With the advent of IP, they have merged, in sometimes inefficient and complex fashion.

Therefore, the real struggle is to develop a simple, sustainable, and operationally efficient enterprise architecture. This foundation needs to have security integrated not only within its technical infrastructure but within its processes and policies as well. This manual is written to provide resources to address these issues and to help simplify compliance.

Executive Summary

The Cisco PCI Solution for Retail 2.0 was developed to help retailers simplify and maintain PCI compliance. The solution consists of strategic guidance as well as tactical implementation. Cisco is in the unique position to apply its enterprise-wide architecture experience to the requirements of PCI. The Architectural Design section discusses what retailers should consider when designing their posture for addressing PCI. It examines enterprise architecture and discusses the related controls within them. Next, this document separates those architectures into their components. The solution is designed to conform to PCI DSS 2.0.

The solution was built and tested using a holistic enterprise perspective including the following:

- Application consideration—Point-of-sale (POS) systems and payment devices, including wireless payment devices
- Administrative concerns within scope of PCI
- Cisco, RSA, EMC, VCE, and HyTrust network infrastructure
- Assessment by a qualified security assessor (Verizon Business)

The result is a set of retail store, data center, and Internet edge architectures and designs that simplify the process of a retailer becoming PCI compliant, maintaining that posture and providing the capability of awareness when under attack. (See Figure 1-1.)

Figure 1-1   Enterprise Architecture
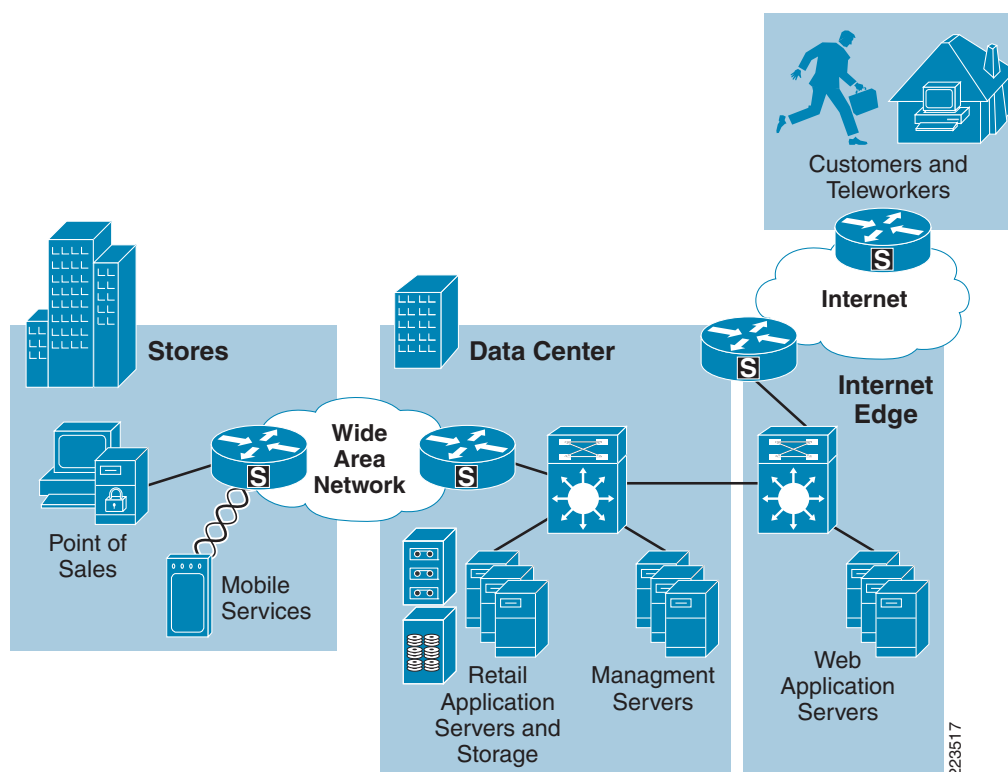
Target Market/Audience

This solution is targeted toward the following audiences:

- Technical or compliance-focused individuals seeking guidance on how to holistically design and configure for PCI compliance
- Retailers that require a qualified security assessor to provide a Report of Compliance
- Retailers interested in preparing for growth that will someday require a Report of Compliance.

Although all retailers that take credit cards are required to be PCI compliant, this solution is designed to help the larger companies simplify the complexity of compliance. Smaller companies can benefit from the design and guidance as well, but should consult their acquiring banks for specifics if they do not currently require an onsite audit. Specific card programs are available at the following locations to determine their specific categorization process;

- American Express—http://www.americanexpress.com/datasecurity
- Discover Financial Services—http://www.discovernetwork.com/fraudsecurity/disc.html
- JCB International—http://www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide—http://www.mastercard.com/sdp
- Visa, Inc.—http://www.visa.com/Cisp

Solution Benefits

This solution demonstrates how to design end-to-end enterprise systems that conform to PCI DSS 2.0 guidelines. Companies can simplify the process of becoming PCI compliant by building a similar network with the recommended configurations and best practices. In addition, this solution provides the following benefits:

- Insight into the Cisco Connected Retail enterprise architecture and the controls used to address PCI
- A detailed analysis and mapping of Cisco and Partner components and their relationship with PCI DSS sub-requirements
- A scalable set of architectural designs that can be used as a reference during the PCI compliance process
- Insight into compensating controls and best practices to harden retail network and data systems
- A centralized management tool kit, which provides operational efficiency compared to managing the distributed endpoints individually
- Insight into the PCI audit process by providing a lab model and associated reference architecture report from Verizon Business

PCI Solution Results

Table 1-1 provides a summary of the PCI assessment results.

Table 1-1   PCI Assessment Results Summary

Component	Primary PCI Function		Component	Primary PCI Function
Endpoints and Applications			**Infrastructure**	
Cisco Unified CM and IP Phones	9.1.2		Cisco store routers	1.3, 11.4
Cisco Video Surveillance	9.1.1		Cisco data center routers	1.2, 1.3
Cisco Physical Access Control	9.1		Cisco store switches	9.1.2, 11.1b, 11.1d Segmentation
Cisco IronPort Email Security Solutions	DLP		Cisco data center switches	1.2, 1.3, 11.4
Cisco UCS	Servers		Cisco Nexus 1000V Series Switch	Segmentation
Cisco UCS Express on Cisco SRE	Servers		Cisco Nexus data center switches	Segmentation
Scope Administration			Cisco Wireless	4.1, 11.1
Cisco ACS	7.1		Cisco MDS Switch	3.4
RSA Authentication Manager	8.3		Cisco ASA-store	1.3, 11.4
HyTrust Appliance	10.5		Cisco ASA-data center	1.3, 11.4
Cisco Security Manager	1.2		Cisco FWSM-data center	1.3
EMC Ionix NCM	1.2.2		Cisco Nexus VSG	Virtual firewall
RSA Data Protection Manager	3.5		Cisco IDSM-data center	11.4
EMC CLARiioN	Storage		Cisco TrustSec	7.1, 11.1b, 11.1d
RSA enVision	10.5			