Cisco PCI Solution for Government: Securing Citizen Payment Data
Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 has been released, providing clarification and reinforcing the need for government agencies, merchants, and other organizations to identify all system components, people, and processes to be included in a PCI DSS assessment. Simply achieving device and system compliance is not enough to protect agencies and citizen data. Cisco® PCI Solution for Government helps you:

- Address current PCI compliance requirements.
- Protect citizen data in your data center, kiosks, services centers, at the Internet edge, and in contact centers and between partners, such as payment processors.
- Simplify compliance.
- Offer guidance on security best practices.

Introduction

Achieving PCI compliance is mandatory for government agency organizations that accept payment cards and other forms of electronic payment.

The Verizon 2010 Payment Card Industry Compliance Report is based on a sample of approximately 200 PCI DSS assessments performed by Verizon Qualified Security Assessors. Of the organizations assessed in the study, only 22 percent were validated as compliant at the time of the Initial Report on Compliance (IROC). Interestingly, many of these organizations had been successfully validated as compliant during a previous assessment.

In addition to avoiding noncompliance fines, a credit card breach can cost your agency exponential amounts in possible litigation from cardholders, legal fees, and damaged reputation for the agency and elected officials. Fines can range from US$5000 to $500,000. Fines can also be accompanied by ongoing monthly penalties, additional fines per breached record, and possible cancellation of an agency and or government retailer’s credit card service privileges for continued noncompliance.

Attempts at identity theft, malware, hacking, Structured Query Language (SQL) injection attacks, and exploitation of default credentials—all are increasingly common and vicious. With so much at stake, why is compliance still lagging? The answer: Achieving PCI compliance is not easy. For example, the Verizon report notes that organizations must pass approximately 250 testing procedures, many of which may not exist in a typical security program used by merchants or government agencies or organizations.

Version 2.0 of the PCI Data Security Standard, effective January 1, 2011, included clarifications designed to make adoption easier for agencies and government organizations.

The most significant revisions in PCI Version 2.0 include:

- Clarifications reinforcing the need for agencies and other organizations to thoroughly scope their data storage and network infrastructure environments and to have a method for knowing where cardholder data resides.
The Challenge of Securing Citizen Payment Card Data

The primary goal of the PCI DSS standard is to secure citizen payment card data. Although technology advances deliver productive new capabilities, they also increase the difficulty of keeping pace with compliance changes. It is not surprising that most organizations struggle with protecting stored credit and debit card data, monitoring access to network resources and citizen data, and regularly testing security systems and processes. In order to accurately assess their own risks, agencies and government organizations must understand the increasingly complex path of data as it travels through the networks of card issuers, acquirers, and banks.

Unfortunately, there is no single “silver bullet” technology that can address a growing list of detailed standards and requirements. Technologies such as encryption, tokenization, and Europay, MasterCard, and Visa (EMV) smartcards address portions of your infrastructure, but none provide a single compliance solution. For these reasons, your security strategy should employ best practices and an architecture that will support PCI compliance and other benefits. For example, it should help you secure the facilities, online and purchasing environments, prevent identity theft, reliably protect agency and elected official reputations and assets, mitigate financial risk, and provide a secure foundation for adding new services.

Breaches More Numerous, Sophisticated, and Costly

Threats are growing rapidly, and efforts to steal data are also becoming more sophisticated, using programmed techniques and hidden code to exploit vulnerabilities. According to the Ponemon Institute’s 2009 study¹, the percentage of data breaches from malicious attacks and botnets doubled—from 12 percent to 24 percent—from 2008 to 2009, and cost substantially more than those caused by human negligence or IT system glitches. The average cost per compromised record across all causes has continued to increase each year, from $202 in 2008 to $204 in 2009. The Identity Theft Resource Center recorded 662 breaches on its 2010 ITRC Breach List, a slight increase over 2009².

Agency Facilities and Online Environments Increasingly Complex

Data can be at risk in many places throughout your infrastructure, as well as outside of your organization. Consolidation and collaboration often result in inheriting different systems and policies. Sensitive data is used, transmitted, or stored across a wide range of locations, including kiosks, e-commerce sites, stores, cafeterias, and distribution centers with service and processing centers. Data streams into your organizations in high volumes and through channels that may include kiosks, call centers, email, and websites. And new agency, database, or communications applications can create new vulnerabilities.

Understanding and addressing PCI compliance across agencies and facilities operations is a complex task. Data in use, at rest, and in motion must be secured at the data center, in all physical locations, across wired and wireless networks, and in transit between the Internet edge and payment processors.

Wireless Networks Considered to Be Public

The wireless environment is growing and staying in government agencies. However, many government organizations are unsure how to apply the PCI DSS to

¹: Ponemon 2009 Annual Study: Cost of a Data Breach
Fifth annual survey shows a significant spike in legal defense spending while breaches involving third-party organizations remained the most costly: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf

²: 2011 ITRC Breach Report
their wireless environments, especially when there may not be wireless technology deployed in their cardholder environments. Savvy cybercriminals can configure a server, laptop, printer, or other device to exploit weaknesses in kiosk, point-of-sale (POS) terminals or other facility systems, even if there is not a wireless network deployed. As a result, almost any environment is susceptible to attack. The PCI standard recognizes wireless LANs as public networks, automatically assuming that they are exposed to public vulnerabilities and threats. Therefore, the best wireless security is based on a strategy that looks across the entire wireless spectrum for intrusion.

PCI DSS 2.0 guidelines address PCI compliance requirements specifically for wireless networks and prescribe two fundamental practices:

- Government agencies must have firewall segmentation between wireless networks and point-of-purchase networks, or in front of any network that comes in contact with credit card information.
- Government organizations must implement a system to detect unauthorized wireless devices and attacks.

Cisco PCI Solution for Government

Maintaining compliance is an ongoing commitment because new threats emerge, service needs change, and the PCI specification evolves. The Cisco PCI Solution for Government helps you secure citizen payment data, citizen privacy, and your agency assets at every point: from the data center, to service centers, websites, and contact centers, and to the Internet edge and payment processors. The Cisco PCI Solution for Government is built on network security best practices, and proven Cisco products, services, and partner technologies that are validated for compatibility with Cisco PCI solution architectures and meet PCI DSS requirements.

Network Architecture Built on Validated Design

A critical element of the PCI solution is Cisco’s network architecture and validated network designs. More than just printed diagrams, the underlying products were deployed and tested in Cisco labs. Verizon Business, a Cisco partner, reviewed the products and network designs and issued an assessment report. With Verizon Business, Cisco developed designs that include end-to-end PCI security best practices and recommendations. You can use these design guidelines for your own network as you achieve and maintain PCI compliance.

Cisco network architectures have been designed for agencies and government facilities, stores, enterprise data centers, contact centers, and the Internet edge to support e-commerce operations, store employees, citizens, and teleworkers. Cisco PCI Solution for Government also supports wireless 3rd Generation (3G) technology deployments and multiple agency formats, including kiosks, service centers, e-commerce sites, in addition to typical small, medium, and large organizations. Cisco network architectures include products for both wired and wireless deployments, helping you effectively address PCI requirements across all users and environments.

Cisco and Partner Products with PCI Intelligence

Many Cisco products already include features and the specific intelligence needed to help meet PCI requirements:

- **Routing**: Cisco ISR Integrated Services Routers and ISR G2, Cisco ASR Aggregation Services Routers
- **Switching**: Cisco Catalyst® compact switches, Cisco Catalyst access switches, and Cisco Catalyst data center switches, Cisco Nexus® 1000V Series Switches, Cisco Nexus 5000 and 7000 Series Switches, Cisco Application Control Engine (ACE), Cisco MDS Multilayer Director Switches with Storage Media Encryption module
- **Network security**: Cisco ASA Adaptive Security Appliances, Cisco IronPort® Email Security Appliances, Cisco Network Admission Control (NAC) appliances, Cisco AnyConnect™ VPN Client, Cisco Firewall Services Modules (FWSM), Cisco Intrusion Detection System Services Modules (IDSM), Cisco Intrusion Prevention System (IPS) Network Modules, Cisco Nexus Virtual Security Gateway for Nexus 1000V Series Switch, Cisco IOS® Firewall, Cisco IOS IPS, Cisco Secure Access Control Server (ACS)
- **Wireless**: Cisco Aironet® Access Points, Cisco Wireless LAN Controllers, Cisco Mobility Services Engine with Enhanced Local Mode (ELM), Cisco Adaptive Wireless IPS
- **Physical security**: Cisco Video Surveillance Operations Manager (VSM), Cisco Video Surveillance IP Cameras, Cisco Physical Security Multiservices Platform (MSP), Cisco Physical Access Manager, Cisco Physical Access Gateways
- **Compute systems and storage**: Cisco Unified Computing System™ (UCS), Cisco UCS Express
Management: Cisco Security Manager, Cisco Wireless Control System (WCS), CiscoWorks LAN Management Solution (LMS)

Voice: Cisco Unified Communications Manager, Cisco Unified Contact Center Enterprise, Cisco Unified Intelligent Contact Management, Cisco Unified Customer Voice Portal, Cisco Unified IP Phones

WAN optimization: Cisco Wide Area Application Engine (WAE), Cisco Wide Area Application Services (WAAS)

Validated Technology Partners

Products from Cisco technology partners have been validated for compatibility with Cisco PCI Solution for Government network designs and products. Technology partners include RSA, VCE, HyTrust, EMC, and Verizon Business.

RSA

RSA provides authentication, security, and compliance technology for data centers and stores.

Products include:
- RSA Archer eGRC Platform: An integrated governance, risk, and compliance platform that help agencies assess security, identify areas of concern, prepare for a PCI audit and manage the reporting process.
- RSA enVision®: Tightly integrated with RSA Archer, RSA enVision offers an effective security and information event management (SIEM) and log management system, capable of collecting and analyzing large amounts of log and event data in real-time.
- RSA SecurID®: Two-factor authentication based on something you know (a password or PIN) and something you have (an authenticator); provides a much more reliable level of user authentication to cardholder data than reusable passwords.
- RSA Data Loss Prevention (DLP) Suite: Enables organizations to discover and classify cardholder data, educate end users and ensure citizen payment data is handled appropriately, and report on risk reduction and progress towards policy objectives.
- RSA Data Protection Manager: Enterprise tokenization and encryption controls further strengthen PCI compliance by protecting citizen data at rest and in transit across public networks.

VCE

VCE provides next-generation virtualized converged infrastructure and private cloud technology. Products include Vblock™ Infrastructure Platforms, which are preintegrated, best-in-class data center infrastructure and rapid deployment private cloud platforms. Built with industry-leading VMware virtualization; Cisco networking and computing; and EMC storage, security, and management technologies.

HyTrust

HyTrust provides virtualization infrastructure security and logging products. The HyTrust Appliance provides policy management, access control, logging, and logical infrastructure segmentation for virtual infrastructures.

EMC

EMC provides storage and storage management technology. Products include:
- EMC CLARiiON® CX4 Series: Scalable networked storage optimized for virtualized environments
- EMC Ionix™ Unified Infrastructure Manager (UIM): Simplified, integrated provisioning, configuration, change, and compliance management across network, storage, and compute resources for Vblock Infrastructure Platforms
- EMC Ionix™ Network Configuration Manager (NCM): Model-based and automated compliance, change, and configuration management for networks

Verizon Business Consulting Services

Verizon Business Qualified Security Assessors provide PCI audits, PCI readiness assessments, the PCI Compliance Management Program, penetration testing, vulnerability scanning, and PCI consulting and remediation services

Cisco Advanced and Advisory Services

Cisco Advanced Services and Cisco Advisory Services help make networks, applications, and the people who use them work better together. Using a Lifecycle Services approach, Cisco Services provides planning, design, and optimization services to help increase business value and return on investment. Several of our services help you address PCI compliance concerns:
- Cisco IT GRC Security Assessment Service: The Cisco IT Governance, Risk Management, and Compliance (GRC) Security Assessment Service works with customers to
assess effectiveness of their security programs and processes, establish benchmark metrics, and map security technical controls to PCI requirements and other standards.

- Cisco IT GRC Strategy Planning Service: This service helps organizations benchmark their security programs against industry standards and best practices. They also identify organizational inefficiencies, misalignments, and redundancies that may be undermining success.

- Cisco Security Posture Assessment Service: To directly address PCI Requirement 11 for penetration testing, the Cisco Security Posture Assessment Service performs vulnerability and penetration tests on the customer’s perimeter and internal networks. The service discovers security weaknesses in the existing network by successfully gaining unauthorized access to the cardholder data environment and credit card information.

- Cisco Design and Implementation Service: This service develops or refines the security architecture so that it adheres to compliance regulations and industry-leading practices and can provide implementation engineering consulting and support.

---

Cisco Technical Services

Cisco Technical Services can cost-effectively maintain secure payment systems for customer-sensitive information while also improving operational efficiency. Based on best practices, Cisco Technical Services are designed to help accelerate your transition to an advanced payment architecture that optimizes performance, reliability, and security, and scales easily with growth in financial transactions.

- Cisco SMARTnet® Service: Your IT staff gains direct, anytime access to Cisco engineers and extensive Cisco.com resources to accelerate problem resolution, facilitate 24-hour business continuity, and improve operational efficiency.

- Cisco Services for IPS: This service protects your intrusion prevention system with the most up-to-date information to defend against attacks from local and global threats. Cisco Services for IPS not only helps reduce risk exposure, but also helps support the productivity of internal staff that is charged with maintaining security systems.

- Cisco Remote Management Services for Security: Cisco Remote Management Services (RMS) for Security provides 24/7/365 remote management, surveillance, monitoring, and remediation for networks to help protect against sophisticated attacks and new vulnerabilities.

---

Business Benefits

Securing Private Clouds, Virtualized Infrastructure and Applications

VCE Vblock Infrastructure Platforms and HyTrust Appliance technologies allow agencies to take advantage of the economic benefits of virtualization within their PCI infrastructures. Vblock Infrastructure Platforms deliver a completely integrated offering that combines best-in-class VMware virtualization, Cisco networking and computing, and EMC storage, security, and management technologies. This platform is designed for the high scalability, reliability, flexibility, and security needs in PCI environments.

Protecting Mobile Applications and Data

Cisco Unified Wireless Network products can be deployed on your premises network to protect the wired network from wireless threats and to help secure private communications over authorized wireless LANS. Built-in security capabilities support:

- Confidential communications.
- User segmentation for access to appropriate resources.
- Security strategies for client devices: Cisco Unified Wireless Network products support industry standards, such as Wi-Fi Protected Access (WPA) and WPA2, as well as integrated radio frequency (RF) scanning and monitoring capabilities. Support for industry standards enables you to secure sensitive cardholder information in both wired and wireless network environments and protect wireless networks and mobile applications from unauthorized use or attack. Cisco Unified Wireless Network products can also identify and prevent rogue access points and unmonitored networks from gaining access to your network. For government and agency sites that do not have wireless LAN coverage, innovative air monitoring capabilities enable retailers to protect these sites from unauthorized wireless access.

Building a Foundation for Ongoing Compliance

Cisco architecture, validated network designs, and proven products from Cisco, RSA, EMC, VCE, and HyTrust encompass the entire range of your operational needs to help you address PCI requirements across all users and environments.
Enhancing Agency Security and Risk Management
While adaptive security technologies help address PCI requirements, the Cisco PCI Solution for Government can also strengthen your agency’s overall security posture by:
• Supporting and helping enforce security best practices.
• Helping protect brand image and assets.
• Mitigating the risk of noncompliance fines, penalties, and lost revenue.

Enabling New Opportunities and Initiatives
Investing in a flexible, PCI-ready network enables you to take advantage of new opportunities. You can add capabilities, such as wireless or voice services, without redesigning the network. The same security capabilities that facilitate PCI compliance can also support new initiatives such as interactive kiosks, unified communications, and wireless applications. In addition, an advanced network facilitates highly secure access for partners and helps keep sensitive citizen data from leaking outside of enterprise and agency boundaries.

Strengthen Citizen Services and Transaction Security
Investing in security best practices is also an investment in your agency business. The same Cisco PCI Solution for Government and proven products that protect e-commerce sites, services, employee, and citizen data can be confidently used for programs that enhance and improve citizen services and maintain the reputations of agencies and elected officials.

Why Cisco?
Whether you have a single location or thousands of locations around the world, Cisco and our technology partners have the technology, experience, and expertise to help improve your effectiveness and operational capacity. The Cisco PCI Solution for Government helps you pull everything together to effectively address the PCI Data Security Standard.