Wireless PCI Compliance

What Is Wireless PCI?

The growth of wireless networking has blurred the traditional boundaries between trusted and untrusted networks and shifted security priorities from the network perimeter to information security. The need to secure sensitive credit card information and avoid unauthorized access to the wireless network must be a priority for ensuring compliance to the Payment Card Industry (PCI) Data Security Standard (DSS).

PCI is applicable to all enterprise, small and medium-sized business (SMB), and retail organizations that handle credit card transactions. From a small hair salon to a large enterprise, businesses of all sizes that store, process, or transmit credit card information are required to comply with PCI. The PCI standard was created by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International.

An evolving standard, PCI DSS Version 1.2, which was released in October 2008, outlines 12 security requirements:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors.

Most of the above requirements have wireless implications. However, the most important changes PCI DSS 1.2 brings as they pertain to wireless are:

- Requirement 4: No new Wired Equivalent Privacy (WEP) implementations are allowed after March 31, 2009, and use of WEP is prohibited after June 30, 2010
- Requirement 11: Verify that a wireless analyzer is used at least quarterly, or that a wireless intrusion detection system/intrusion protection system (IDS/IPS) is implemented and configured to identify all wireless devices.

Why Care About Compliance?

If there is a security breach at a company that has not complied with PCI, significant fines will be issued by the credit card companies, while they may also revoke future credit card transaction rights. As catastrophic as this may sound, according to research published by InformationWeek[1], 69 percent of the average cost per breach in 2008 was in fact attributed to lost business created by the customer's changing perception of the brand.

Securing the wireless network presents an interesting challenge. The business must ensure the wireless transfer of cardholder information is encrypted and secure. Additionally, the business must secure and control the wireless medium itself or risk the threat of unauthorized wireless access creating a "backdoor" to corporate systems. Table 1 lists some possible implications of not complying with the PCI standard for businesses of different sizes.

Table 1. Noncompliance Implications

Size and Type of Business	Example of Noncompliance Implication
Large Wholesaler	• Card issuers sued the chain for US$16 million over compromised credit cards. • Company is suing software point-of-sale vendor over faulty software.
Franchise Restaurant Chain	• Compromised restaurant chain is fined $500,000 plus cost of reissuing cards to customers whose cards were compromised.
Small, Local Grocery Store	• Card associations fined store $50,000.

Cisco Wireless PCI Solution

The increasingly mobile nature of business communications means that a multilayered approach to security is required. To mitigate the risk that the lack of wireless security could compromise cardholder information, Cisco recommends the approach to securing the wireless network outlined in Table 2.

Table 2. Securing the Wireless Network

Security Steps	Mapping Wireless Security to PCI Requirements
Create an Information Security Policy that Includes the Wireless LAN.	The PCI standard incorporates wireless security policy throughout its list of requirements. If a company does not deploy wireless technology, wireless should still be included in the security policy. PCI requirement 11 mandates scans for wireless devices, whether or not wireless technology is deployed.
Secure the Authorized Wireless LAN Against Wireless Threats.	PCI requirements 2 and 4 are directly addressed by implementing Wi-Fi Protected Access (WPA) for the authorized wireless LAN. This standard enables accurate identification of authorized clients and infrastructure through the 802.11i standard and ensures the encryption of cardholder information.

Security Steps	Mapping Wireless Security to PCI Requirements
Defend Cardholder Information from Theft or Tampering.	PCI requirement 5 relates directly to the need for protection against threats that can occur when businesses take advantage of wireless connectivity. Cisco offers wireless Network Admission Control (NAC) and the Cisco® Security Agent to help protect cardholder information from unauthorized access or tampering.
Enlist Employees in Safeguarding the Cardholder Information.	Employee training is often the most effective tool in helping to secure the wireless network and cardholder information. Informational posters and training about security best practices can go a long way toward protecting the network.

According to a VeriSign study[2], the second most frequent reason companies fail PCI assessments is an inability to satisfactorily meet requirement 11, the requirement for regular testing of security systems and processes. The Cisco Unified Wireless Network can assist companies in complying with the PCI Data Security Standard by:

- Offering integrated RF scanning and monitoring capabilities with the use of Adaptive Wireless IPS to protect the wireless media from unauthorized use or attack
- Providing integrated support for industry standards including WPA and WPA2
- Reducing the time required to analyze and report on configurations and settings across the wireless network
- Integrating with the Cisco Self-Defending Network to deliver a comprehensive solution for all PCI compliance needs, including: secure routers, adaptive security appliances, Cisco Security Agent, compliance reporting and management, Wireless NAC, and Cisco WLAN and Security Services

The Cisco Unified Wireless Network is a component of Cisco PCI Solution for Retail, a set of network architectures that has been tested and validated by Cisco security auditing partners to meet the requirements of the PCI standard.

For more information on the complete Cisco Self-Defending Network solution for PCI compliance, see the relevant Self-Defending Network PCI Solution—At-A-Glance.

Should You Think Beyond PCI Compliance?

The Cisco Self-Defending Network can strengthen your company's overall security posture and can help you satisfy PCI requirements in a cost-effective and efficient manner. PCI compliance is a good first step in designing a wired and wireless security architecture that protects not only cardholder data but also sensitive company information. However, the 12 requirements outlined in the standard have their limitations. Just as you would not turn on your firewall periodically, scanning your RF environment on a quarterly basis does not discourage malicious hackers from attempting to break into your network the rest of the time.

Cisco's adaptive wireless IPS solution offers ongoing protection from an expanding list of security threats, with enhanced analysis and reporting functionality that is easy to use. A combination of the Cisco Unified Wireless Network, adaptive security technologies, Cisco WLAN and security services specifically for PCI compliance, and Cisco's WLAN and Security Specialized Partners will ensure a robust security framework that goes beyond the requirements of the PCI standard—to help ensure your peace of mind.

Why Cisco?

Cisco is the industry's only technology provider to offer industry-leading wireless LAN security features integrated with best-in-class security solutions for a comprehensive solution designed to meet PCI compliance requirements. Unlike other providers, Cisco can deliver a tightly integrated solution of infrastructure and application services to allow businesses to benefit from a simple, secure, and scalable platform for the lowest total cost of ownership. By delivering a rich portfolio of security services, Cisco is empowering its customers to maintain the integrity of sensitive information and meet exacting compliance

[1] Source: "Data Breaches Are More Costly Than Ever," WashingtonPost.com, February 3, 2009.

[2] Source: VeriSign; "Lessons Learned: Top Reasons for PCI Audit Failure and How to Avoid Them"