WiFi and Mobility in Retail Stores

Understanding how WiFi and Mobility affect a retail network

By Bradley K. Cyprus - Chief of Security and Compliance, Netsurion

Introduction

When talking about wireless technology, WiFi and Mobility are often lumped together because many of the solutions using this technology reply upon a shared infrastructure. WiFi describes the local network within a location that is available to facilitate communication. This could include a private wireless network so that a handheld payment terminal can communicate to a point of sale system, or it could relate to a public "hotspot" that allows customers to browse the Internet from within the store. Additionally, many mobility solutions need to eventually communicate to the Internet to work. That connection might be over a cellular network, thus be independent of the merchant locations, or that Internet connection may be provided by the WiFi system that is integrated into the local area network.

PCI and Wireless (WiFi and Mobility)

Regarding wireless technology, the Payment Card Industry Data Security Standards (PCI DSS) requires that strong cryptography is used whenever credit card data is sent wirelessly and that there is a firewall managing the communication between wireless data and the point of sale. Specifically, non-POS (wireless) traffic should not be able to communicate to the part of the network where sensitive cardholder data resides. Other requirements pertain to physical security of the infrastructure and policy and procedures associated with using and tracking the technology.

The following is a summary of the PCI requirements as they relate to Wireless:

1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks.

1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to: the Internet, Wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. (Note: The use of WEP as a security control was prohibited as of 30 June 2010.)

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

10.5.4 Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.

11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. (Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.)

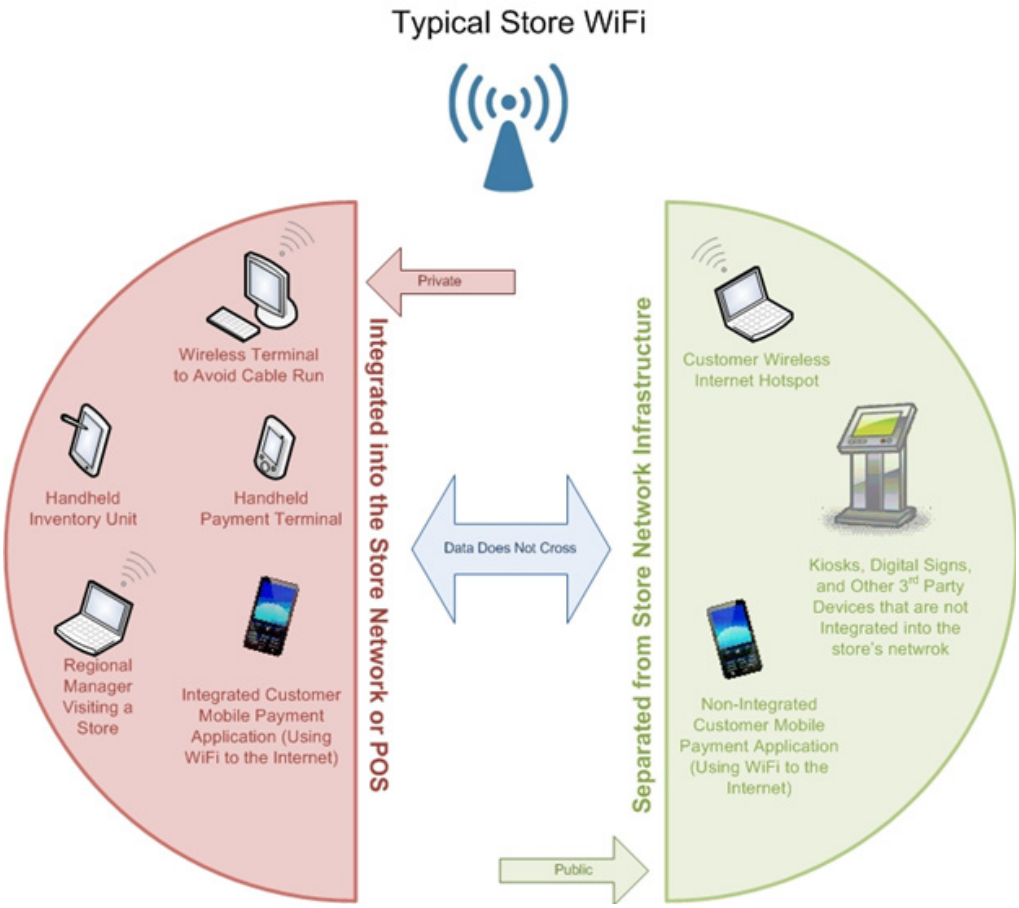
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.

12.9.3 Verify through observation and review of policies that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

12.9.5 Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.

Uses for WiFi in the Typical Store

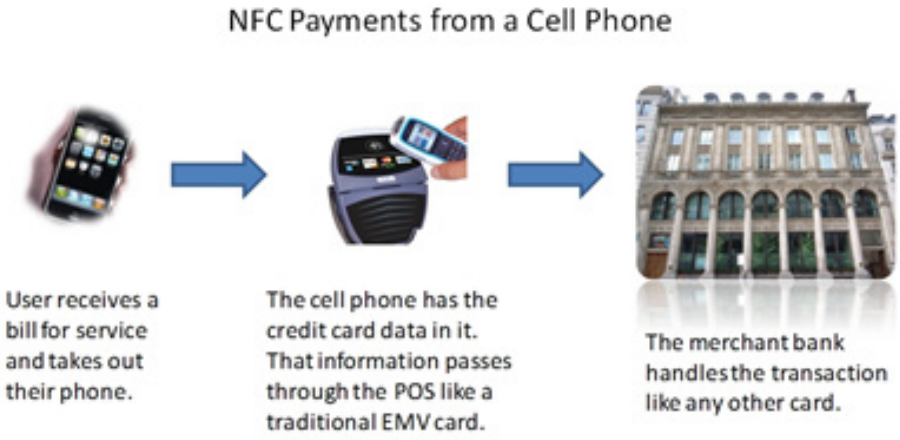
WiFi should be thought of as the technology that either allows wireless devices to locally communicate to the network at the store or to connect to the Internet. It is the backbone for the communication that many systems need in order to function, and Netsurion can assist in proper implementation.



Mobile Applications - Applications that run on smart phones are becoming more popular with merchants today. These applications are specifically written to enhance the shopper's experience while in the store. Many of them have an interface that allows for searching for a particular item, creating a virtual shopping cart, or possibly even allowing for payment. This kind of application is analogous to a website that facilitates shopping. In fact, the first applications that enabled people to shop on their smart phones were simplified versions of corporate websites.

Mobile Wallet – This is a smart phone specific application that allows the owner of the phone to input payment data into the Wallet provider's server (who stores the payment information) so that payments can be made from the phone. The data that passes from the phone through the POS system in this case is NOT credit card data. It is data specific to the mobile wallet and is designed to only be understood by the mobile wallet provider. This means that for a merchant to accept payment from any specific mobile wallet, that merchant must integrate that specific mobile wallet platform into their POS system. This is a fairly new technology, and until there is interoperability between mobile wallet providers, it may be necessary to integrate several different mobile platforms into a POS system if a merchant wishes to take this kind of payment since their customers could have a variety of mobile wallets.

NFC Payments on Mobile Devices – Some smart phones allow for the storage of credit card data within an application on the phone. The phone has an embedded chip on it that will enable the stored credit card data to be transmitted to the payment terminal of the POS system using a technology known as Near Field Communication (NFC). This is the same technology that several credit cards (especially those in Europe) already have that allow them to transmit their information if they are close enough to the card reader. If a merchant wishes to accept this kind of payment, it will be necessary to make sure that the card readers (and /or pin pads) are NFC compatible. If they are not, then they will need to be upgraded before NFC payments can be accepted. It is important to note that NFC technology is inherently more secure than traditional magnetic stripes that most credit cards have today. It is expected to be the chosen technology for all card readers in the future.



About Netsurion

Netsurion is a leading provider of cloud-managed IT security services that protect small- and medium-sized businesses' information, payment systems, and on-premise public and private Wi-Fi networks from data breaches and other risks posed by hackers. Netsurion's patented remote installation technology and PCI compliant cloud-based solutions simplify the implementation process and ongoing support. Any sized branch or remote office, franchise, or sole proprietor operation can use Netsurion without the costs of onsite support. The company serves the retail, hospitality, healthcare, legal, and insurance sectors.

7324 Southwest Freeway
Suite 1700, Arena Tower II
Houston, Texas 77074

P: 713.929.0200
F: 713.541.1065
Netsurion.com