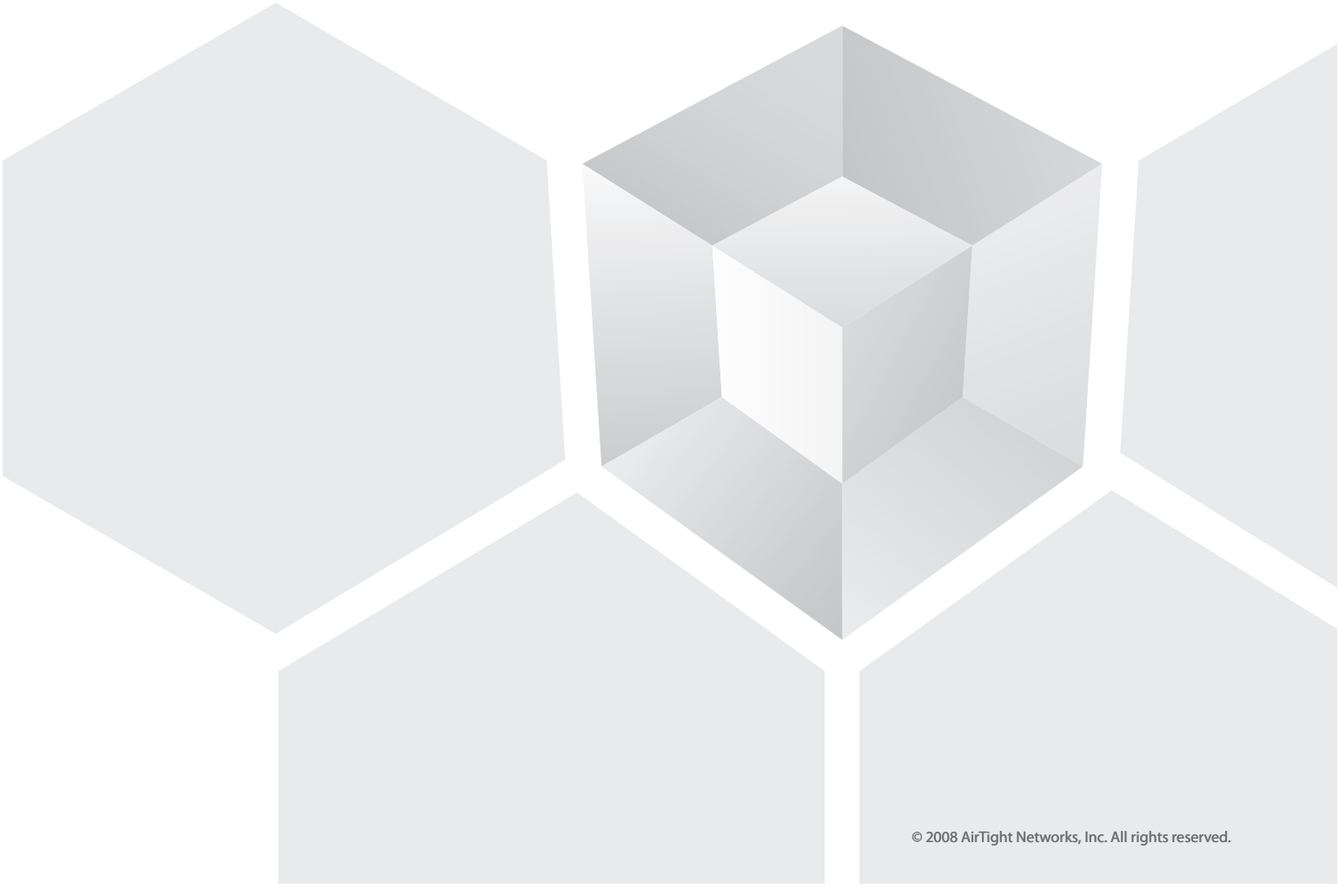
Retail Stores and Wireless Security—Recommendations

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com



On May 4, 2007, The Wall Street Journal reported a Marshall's store in St. Paul, Minnesota—with a wireless vulnerability—was the entry point for hackers who ultimately gained access to at least 45.7 million payment card records from both Marshall's and other stores in the TJX organization.

This is the most recently publicized incident involving retailers and wireless attacks. At least three other large-scale attacks have been reported in the press, and undoubtedly there are more that have not made headlines. As reported in the WSL article, the law enforcement community believes that organized crime syndicates from Eastern Europe may be responsible for the TJX attack and several others.

As Wireless Proliferates So Do the Threats

Wireless computer networks are rapidly becoming universal. As a consumer-driven technology, wireless was developed to be simple to install, configure and use. It is that very simplicity, however, that has made it an easy attack vector. More than 95 percent of all laptop computers have wireless built-in; consumers use wireless routers at home to attach to their DSL or cable modems; cell phones and digital cameras are getting Wi-Fi enabled. For a retailer, this means that even if you are not deploying wireless LANs in your establishments, you have a wireless problem and you need a wireless security policy.

Every retailer MUST protect itself and its customer from these attacks. This white paper will give some pointers and suggestions on how retailers can protect the most vulnerable locations—their stores—from wireless attacks.

The Environment/The Challenge

In most retail store environments, there are multiple, separate applications which IT may be supporting. For example:

- **Inventory control**
- **Payroll**
- **Payment/transaction processing**
- **Telephony/phone calls**
- **Web-based applications (e.g., special orders)**
- **Video surveillance**

In a retail store, many of these applications may run over a wireless network—including inventory control, transaction data, voice, and video. The ideal store infrastructure—from a security perspective—is to isolate each of these applications from each other—both from a networking as well as from a server/storage perspective.

However, from a cost perspective, the most efficient infrastructure combines all of the above onto one network and runs it all from a single server per store. Unfortunately, this exposes the retailer to the type of break-in that occurred at TJX.

In most retail environments to date—cost has trumped security and compliance—in terms of priorities and emphasis. Organizations that process, store, or transmit payment card data—virtually all retailers—must be Payment Card Industry Data Security Standard (PCI DSS) -compliant, or risk losing their ability to process credit and debit card payments. But the massive reach and financial consequences of well publicized attacks and PCI DSS are forcing retailers to seriously re-think these trade-offs. So how does a retailer address the wireless security risk?

Three Wireless Security "Openings"

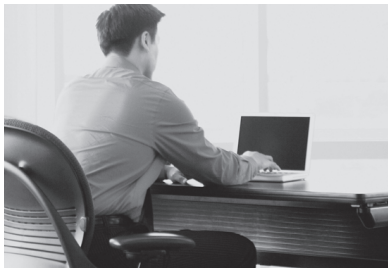
To secure the stores, a retailer must understand that wireless creates three potential security holes or entry points into its network from the retail store environment.

The first is a criminal breaking into the network via some existing wireless equipment in the store. For any store that has deployed wireless in any form—for in-store communications, bar code scanners, inventory readers, etc.—this is a major risk. Much of this

legacy gear cannot support the latest strong encryption methods and, while some companies may claim they can add cloaking or masking to secure these devices, demonstrations using a WEP key cracking application have shown that cloaking may slow down hackers, but cannot stop them from breaking the key.

The second is a 'rogue' wireless access point (AP) that gets installed without the retailers' permission or knowledge. This may be installed by an employee who wants to use wireless in the store, it may be a hacker paying the janitor to install it, or it may be a vendor who visits the site, but it opens the network up to outside access.

The third is an employee who wants to surf the Internet at lunch time—but who can't do it on the store intranet—so he or she logs onto a neighboring wireless network (from another store in the mall, from a wireless hotspot, or from the neighbor across the street). When employees do this—anyone on that neighboring network—can come back through that same connection—into the store network, and see all the data/resources that the employee can see.



The common threat from these three scenarios is that an outsider can gain access to your internal network. What can happen next? The attacker can:

- **Sniff out user IDs and passwords to gain access to other internal resources**
- **Profile the network and servers to figure out where the valuable data resides**
- **Plant software to get at that data**
- **And then go back and cover their tracks**

This is an abbreviated version of what appears to have happened at TJX.

Even if a retailer has not installed wireless in its stores, it is exposed to these threats and potential losses over wireless connections. So, how can a retailer protect itself from these threats?

Recommendations

The first step, as with all security programs, is to define a Wireless Security Policy. This policy should address each of the three threat scenarios above. The wireless security policy should logically complement the wired network security policy. And as with any good security policy, you should define an enforcement and monitoring program for the wireless security policy.

Employee training/education is another required element—to ensure that all the store employees understand the dangers of wireless and their responsibilities in maintaining the security of the store infrastructure.

From a network perspective, establish separate virtual local area networks (VLANs) for the different applications running in the store—and firewall them off from each other. The most critical, and this cannot be emphasized enough, is to keep the transaction data separate from all the other data, but it also makes sense to isolate the wireless traffic onto its own separate network(s). PCI DSS specifically calls for the use of firewalls to provide segmentation between wireless networks and networks used for point-of-sale transactions.

Then, from a wireless network infrastructure perspective, it is strongly recommended that you upgrade any wireless devices (scanners, laptops, PoS terminals, etc.) and APs in the store to use the strongest encryption standard. The industry has defined and implemented WPA2 as the strongest standard encryption for wireless. The two earlier standards, WEP and WPA, have been shown to be not very secure. Because migrating your equipment to this new standard may take time, you should rotate your encryption keys on a monthly basis at a minimum if you are still running the older standards. Although this is not a requirement of PCI DSS, and most retailers don't do it, they should.

The final step for wireless security is to periodically conduct a wireless vulnerability assessment of your network. Effective wireless vulnerability assessment should:

- **Automatically scan for all known vulnerabilities enabling zero-day attack protection**
- **Accurately detect and locate existing and potential vulnerabilities without false positives**
- **Create an inventory of critical assets and unauthorized devices in the airspace**
- **Present the scan results in a concise, but informative report that classifies vulnerabilities, prioritizes them according to well-defined severity levels, summarizes the main findings, and recommends remedial actions**
- **Compare reports generated at different times**
- **Present a view of your global wireless security posture**
- **Map wireless vulnerabilities in the context of the relevant regulatory compliance**

A recommended best practice is to conduct a wireless vulnerability assessment of your network every 15 days.

You can use wireless handhelds or freeware tools on a laptop to periodically conduct such wireless vulnerabilities assessments. However, this approach has many limitations:

- **It is manual and takes a lot of coordination**
- **Consolidation of data and reporting is very difficult**
- **It consumes valuable IT resources**
- **It is hard to repeat very frequently**
- **It is very expensive. You pay for handhelds, IT resource time and travel.**
- **It is not scalable for large retailers with thousands of locations across the globe**

An alternative approach is to use an automated system for wireless vulnerability assessment. Such a system provides 24x7 scanning, automatic vulnerability classification and consolidated reporting on a global scale at a fraction of the cost of manual assessment with wireless handhelds.

AirTight is the only wireless vulnerability management company to offer a flexible, end-to-end solution that gives retailers visibility into their wireless security posture—and choice in how they manage it.

SpectraGuard Online offers retailers a cost-effective, unbundled Wireless Vulnerability Management solution, delivered through an on-demand Software-as-a-Service (SaaS) model. There is no capital investment and no product obsolescence—just a small monthly service fee. Organizations can grow organically and pay only for what they need. This modular solution includes:

- ***Vulnerability Assessment* service providing 24x7 wireless scanning to detect wireless activities, identify threats, identify and prioritize all wireless devices, and allow wireless security posture assessment.**
- ***Regulatory Compliance* service providing wireless compliance assessment capabilities for regulatory compliance standards such as PCI DSS.**
- ***Vulnerability Remediation* service providing instant notification of wireless vulnerabilities via email, automated or manual remediation capabilities for common threats, ability to track the location of wireless threats on a floor map, and the ability to visualize wireless signal spillage from corporate APs.**

SpectraGuard Enterprise provides retailers with a complete wireless intrusion prevention system that automatically identifies and blocks WLAN security threats.

Retail Stores and Wireless Security—Recommendations

About AirTight Networks

AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry's leading wireless intrusion prevention system (WIPS) and the world's first wireless vulnerability management (WMV) security-as-a-service (SaaS). AirTight's award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, healthcare, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 11 U.S. patents and two international patents granted (UK and Australia), and more than 25 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit www.airtightnetworks.com

Wireless Vulnerability Management

AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 www.airtightnetworks.com info@airtightnetworks.com

AirTight® NETWORKS