



# Wireless Security: Key Trends and Issues

David King  
Chairman & CEO  
AirTight Networks

[david.c.king@airtightnetworks.net](mailto:david.c.king@airtightnetworks.net)

# INTEROP<sup>®</sup>

BUSINESS. TECHNOLOGY.  
ONE WEEK. ONE PLACE.

# Market and Technology Forces

## Threat Environment

- New hacking tools
- Evolving attack scenarios
- Organized crime

## Compliance

- PCI
- HIPAA
- GLBA

## Infrastructure

- 802.11a,b,g → n
- Muni Wi-Fi
- FMC

## Client Devices

- Legacy WEP
- Wi-Fi laptops
- Smartphones

Enhanced  
Wireless  
Security

# Key Wireless Security Issues

## *Current Challenges*

**WIPS**

- Pre/Draft 11n rogue APs
- New threat scenarios (DoS, MultitPot)

**Basic WIDS**

- NAT/encrypted rogue APs
- Misbehaving clients

**Encryption/Authentication**

- WEP handheld still prevalent
- Legacy fat AP networks

# Key Elements of Wi-Fi Security

**Secure**

**1<sup>st</sup> Generation  
Security Gateways**

**Encryption**

**Authentication**

**2<sup>nd</sup> Generation  
WIDS**

**3<sup>rd</sup> Generation  
WIPS/WNAC**

**Monitor**

**Detect**

**Visualize**

**Auto-  
Classify**

**Prevent**

**Locate**

- 2.4 and 5 GHz
- All channels
- Continuous
- Association
- Activity

- APs and clients
- Alerts/alarms

- Live RF maps
- Site specific
- Access points
- Security sensors

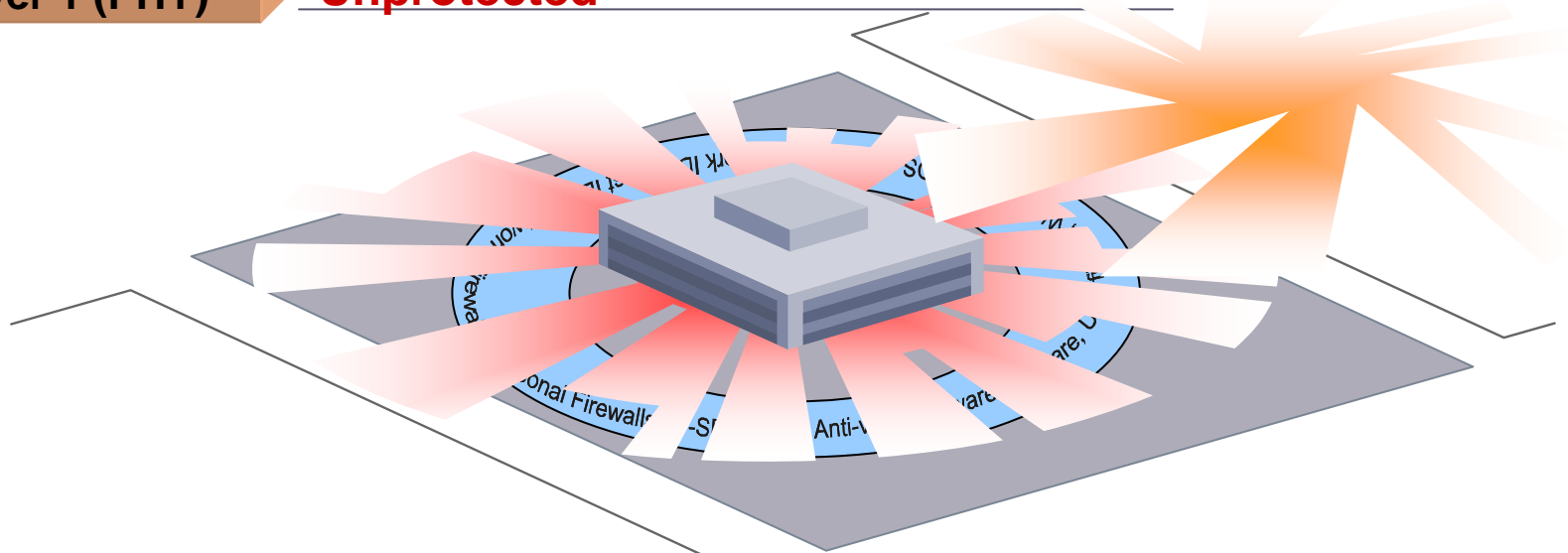
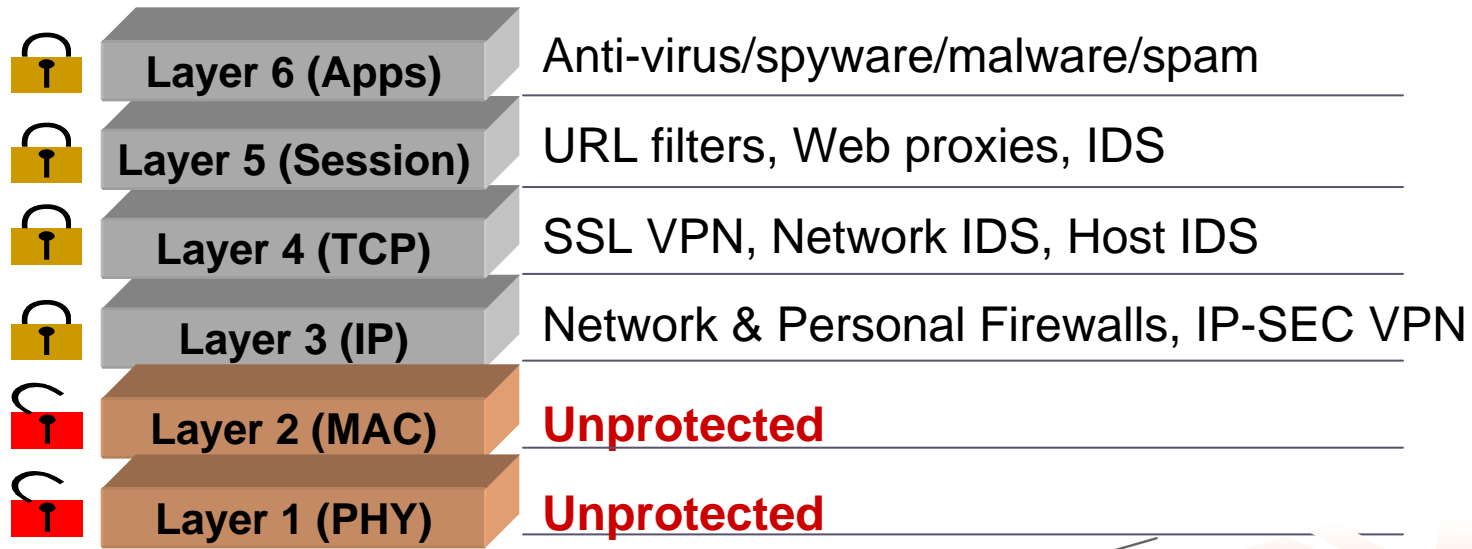
- Accurate filtering
- All devices
- All threats

- Block threats
- Automatic
- Non-disruptive

- Plot on floor plan
- Permanent removal


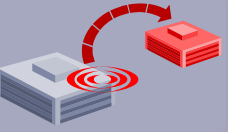
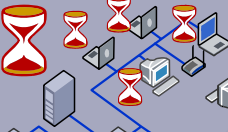
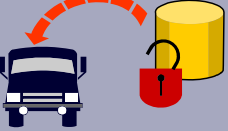

**INTEROP**

# Wireless Breaks the Wired Security Model





# Wireless Poses Major Risks to Your Business

Wireless breaches compromise	Consequences	
 A newspaper icon with the headline "The News" and a red box containing the text "DATA LOST!!".	Brand	Loss of customers/revenue
 An icon showing a server rack on the left and a red box on the right, with a red curved arrow pointing from the server to the box.	Intellectual property	Loss of leadership/differentiation
 An icon showing a network diagram with several hourglass symbols, representing operational downtime.	Operational downtime	Loss of productivity
 An icon showing a blue car on the left, a red padlock in the center, and a yellow cylinder on the right, representing privacy concerns.	Privacy	Legal action
 An icon showing a document with a checklist and a signal wave, representing compliance.	Compliance	Fines, penalties

# TJX Breach Illustrates the Risk

**WSJ**  
.com

**THE WALL STREET JOURNAL.**  
ONLINE

As of Friday, May 4, 2007

**PAGE ONE**

***BREAKING THE CODE***  
**How Credit-Card Data**  
**Went Out Wireless Door**

**Biggest Known Theft**  
**Came from Retailer**  
**With Old, Weak Security**

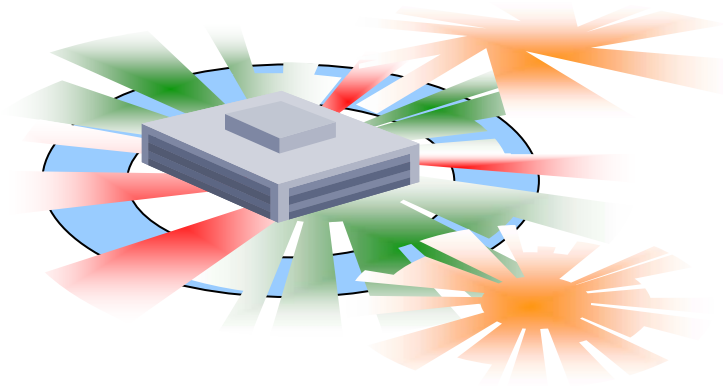
By **JOSEPH PEREIRA**  
*May 4, 2007; Page A1*

The biggest known theft of credit-card numbers in history began two summers ago outside a Marshalls discount clothing store near St. Paul, Minn.

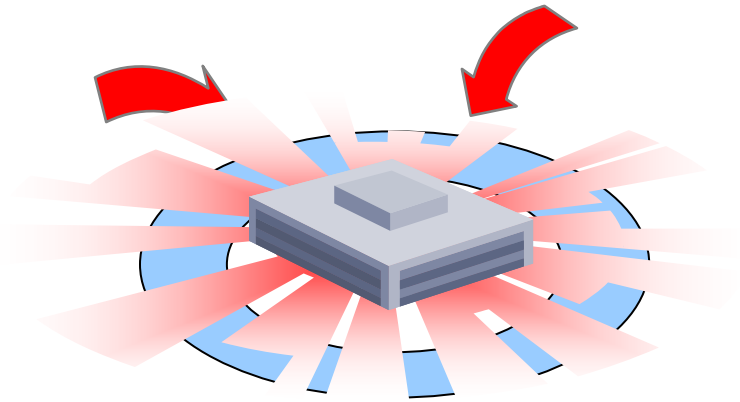


- Marshalls stores (Miami) hacked via wireless
- Hackers accessed TJX network & multiple servers for 18+ months
- 45.7 million payment card accounts compromised
- Estimated liabilities >\$4.5B
- 18 lawsuits listed in the TJX 10K and counting

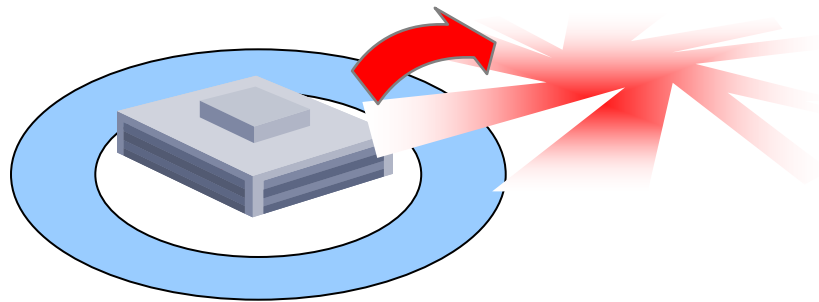
# Four Elements of a Wireless Security Policy



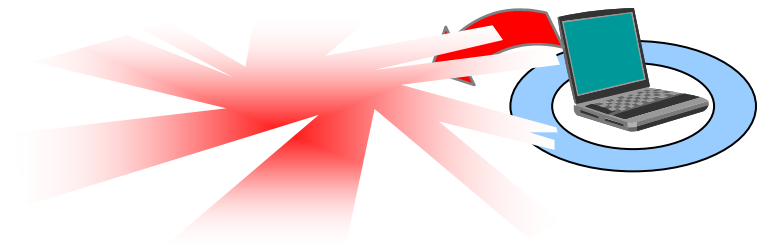
**Control wireless access to wired network**



**Prevent unauthorized wireless “back doors”**

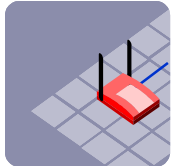


**Keep clients from attaching to other networks**



**Enforce wireless policy outside of the office**

# Wireless Security Policy Enforcement Steps



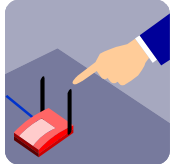
Detect wireless threats real-time



Determine/classify what is a real threat



Automatically disable unauthorized wireless activity



Physically locate and remove threats



Secure wireless assets outside the office

Organizations are Unprepared



# Wireless Security: Key Trends and Issues

David King  
Chairman & CEO  
AirTight Networks

[david.c.king@airtightnetworks.net](mailto:david.c.king@airtightnetworks.net)

**INTEROP**