



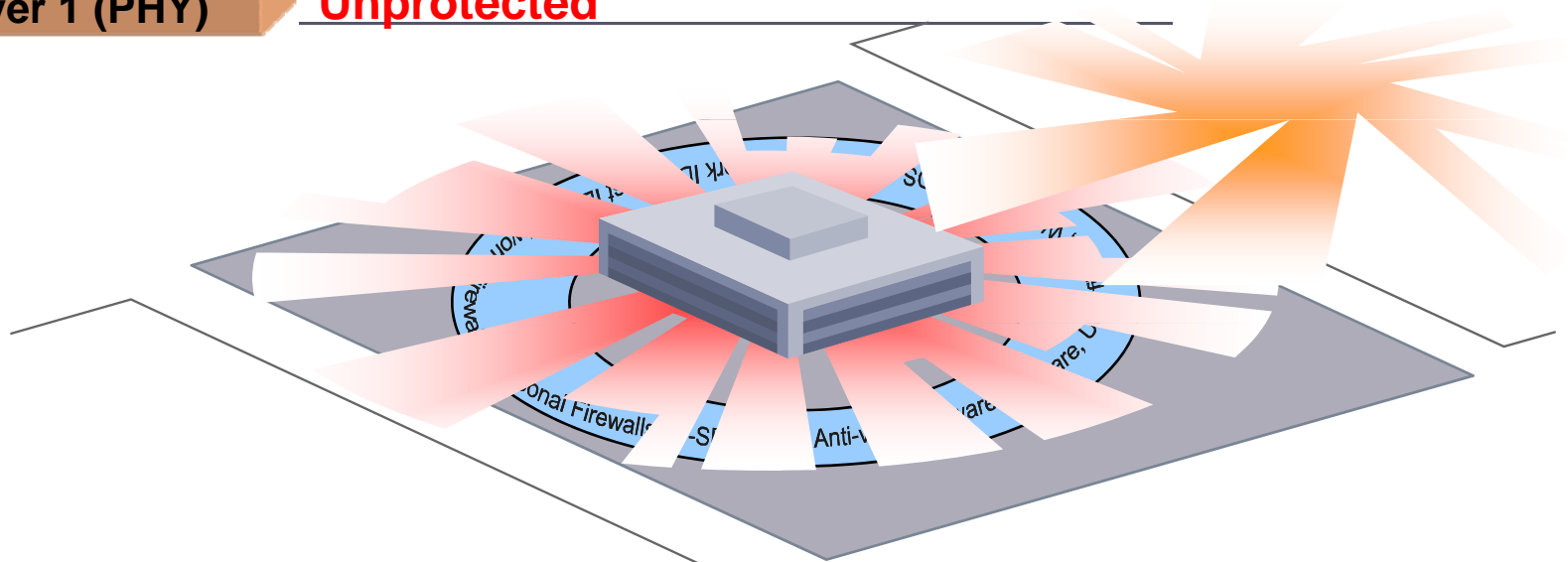
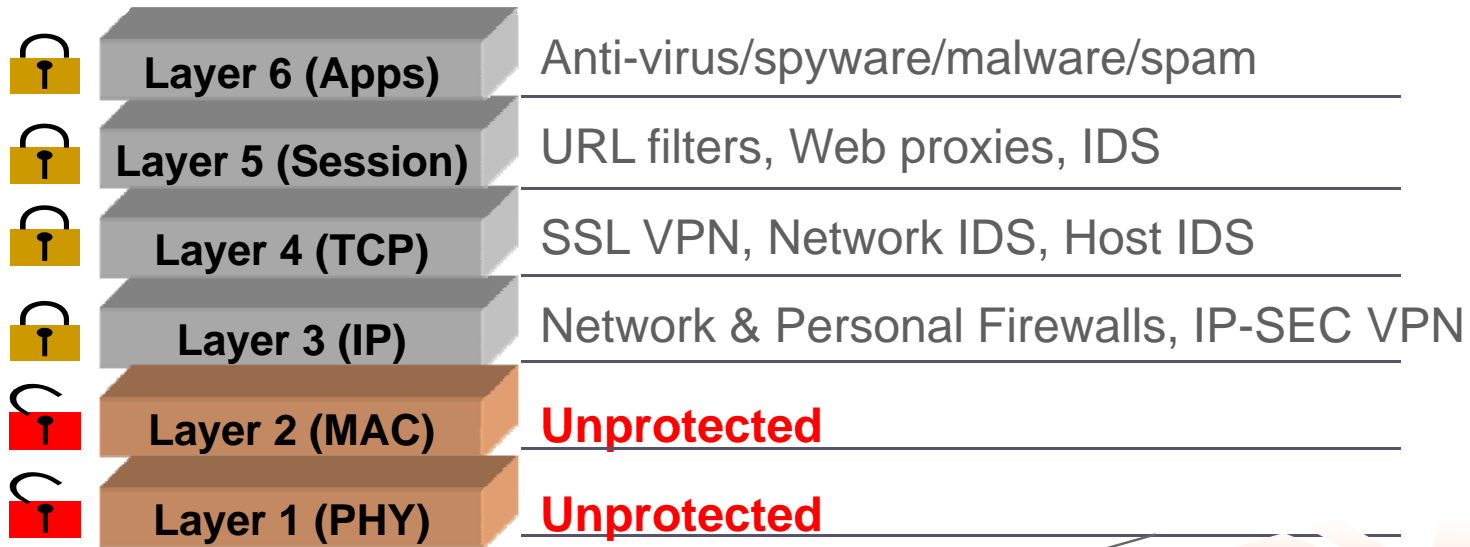
# Wireless Security: Key Trends and Issues

David C. King  
CEO, AirTight Networks

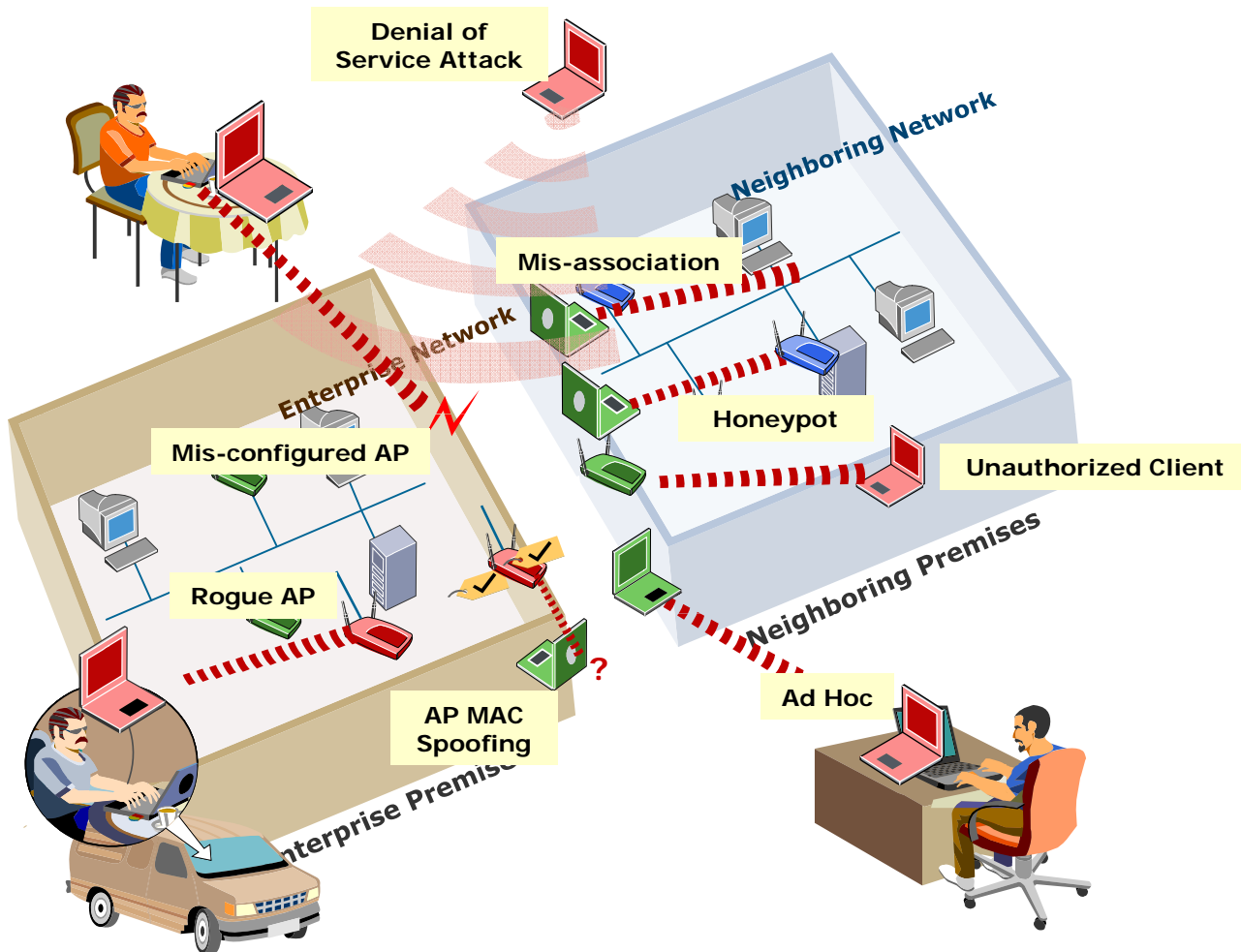
[www.airtightnetworks.net](http://www.airtightnetworks.net)

**INTEROP**<sup>®</sup>  
THE LEADING BUSINESS TECHNOLOGY EVENT

# Wireless Breaks the Wired Security Model



# Wi-Fi Threat Environment



## Common Vulnerabilities

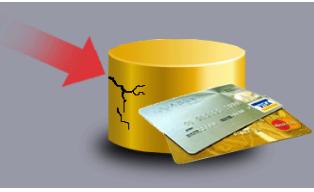



- Rogue Access Points
- Mis-configured APs
- Unauthorized clients
- Client mis-associations
- Ad hoc connections

## Malicious Threats

- Honeypot APs
- Denial of Service
- MAC Spoofing APs

Wired Security and WPA2 Do Not Address These Threats

# Wireless Breaches Pose Serious Business Risks

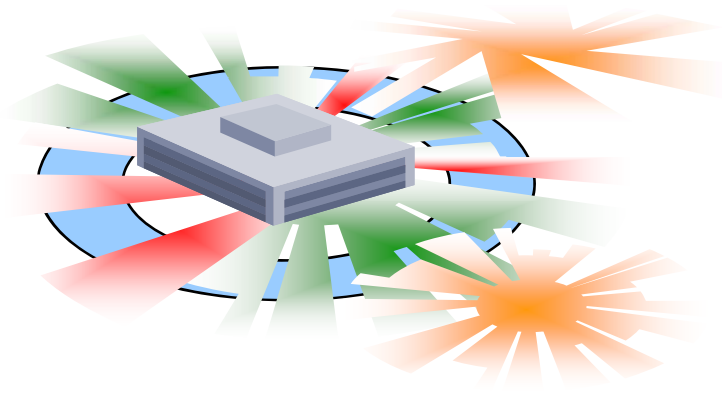
Vulnerabilities compromise	Consequences
 <p data-bbox="716 521 888 570">Privacy</p>	<p data-bbox="1163 526 1440 574">Legal action</p>
 <p data-bbox="716 724 968 773">Operations</p>	<p data-bbox="1163 724 1545 773">Productivity loss</p>
 <p data-bbox="716 927 989 976">Compliance</p>	<p data-bbox="1163 927 1507 976">Fines/penalties</p>
 <p data-bbox="716 1130 852 1179">Brand</p>	<p data-bbox="1163 1130 1692 1179">Customer/revenue loss</p>

# TJX Breach Illustrates the Risk

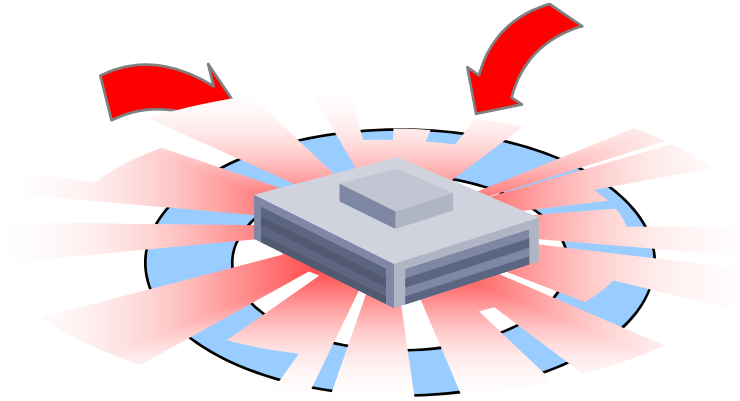


- Marshalls stores hacked wirelessly
- Hackers accessed TJX network & multiple servers for 18+ months
- 94 million payment card accounts compromised
- Estimated liabilities >\$4.5B
  - Over 15 lawsuits already filed
  - Battle over responsibility
- Who will **60 Minutes** profile next?

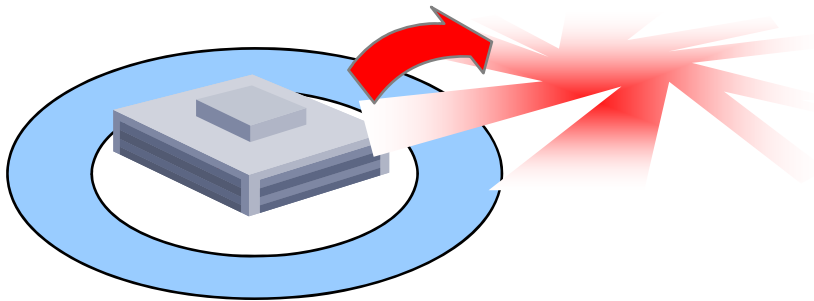
# Four Elements of a Wireless Security Policy



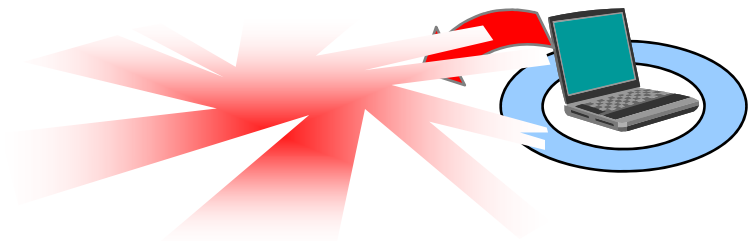
**Control wireless access to wired network**



**Prevent unauthorized wireless “back doors”**



**Keep clients from attaching to other networks**



**Enforce wireless policy outside of the office**

# Market and Technology Forces

## Threat Environment

- New hacking tools
- Evolving attack scenarios
- Organized crime

## Compliance

- PCI
- HIPAA
- GLBA

## Infrastructure

- 802.11a,b,g → **802.11n**
- **VoWiFi**
- FMC

## Client Devices

- Legacy WEP
- Wi-Fi laptops
- **iPhones**

Wireless  
Security  
Requirements

## 802.11n Amplifies Existing Threats



- 802.11n accepted by consumers and SMBs
- Majority of rogue APs are consumer APs
  - Router (NAT) APs
  - Turbo/Super G APs
  - DRAFT 802.11n and Pre-802.11n APs
- Greater range of spillage extends vulnerability
  - **Your APs visible to more unauthorized users**
  - **More external APs visible with neighboring spillage**
- “Outside-in” spillage may create interference or DoS

# Voice over Wi-Fi Threats

- Mission critical applications in key industries
- Latency and interference are biggest issues
- Placement of APs & sensors poses challenges
- DoS prevention is paramount

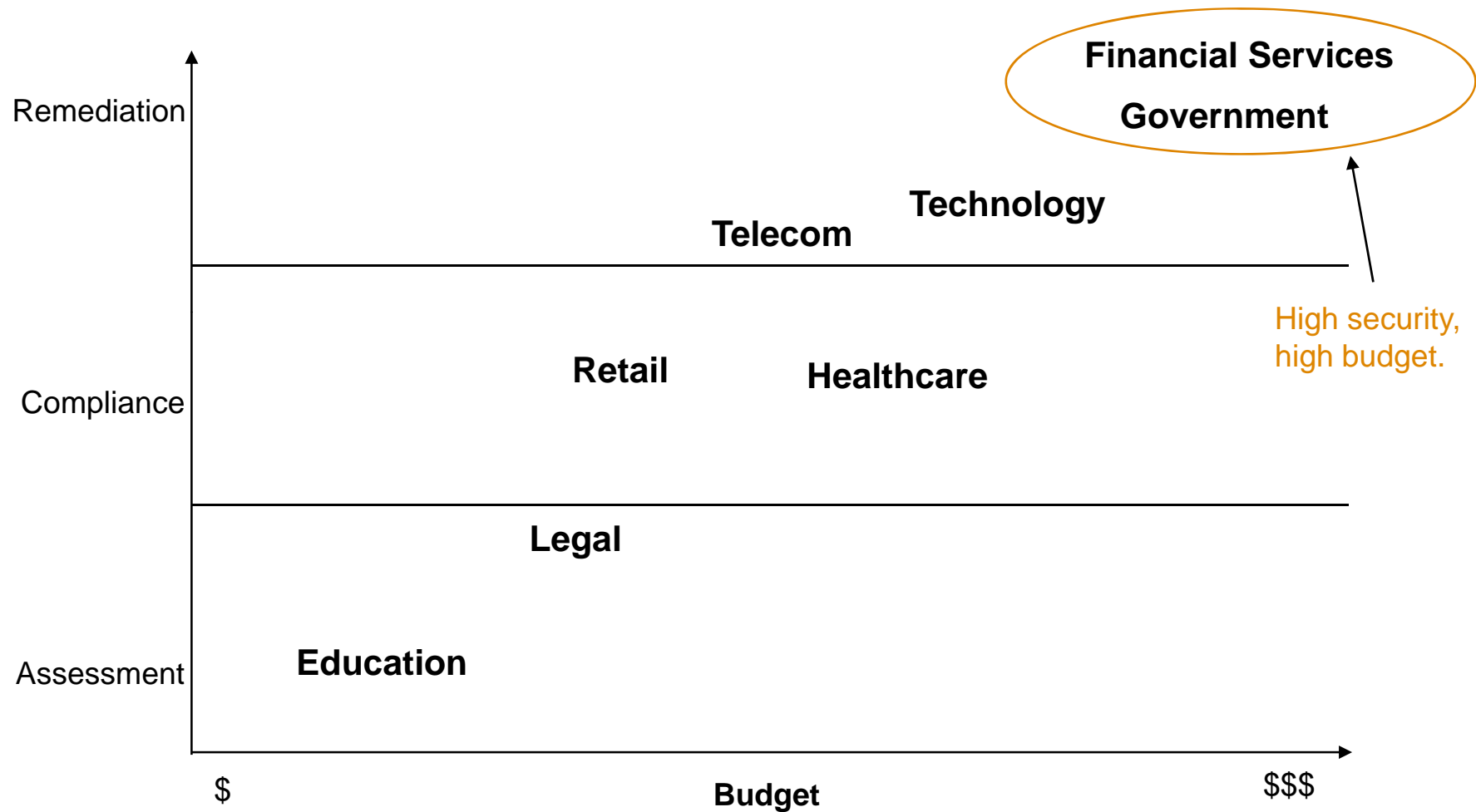


# iPhone: Wireless Security Paradigm Shift

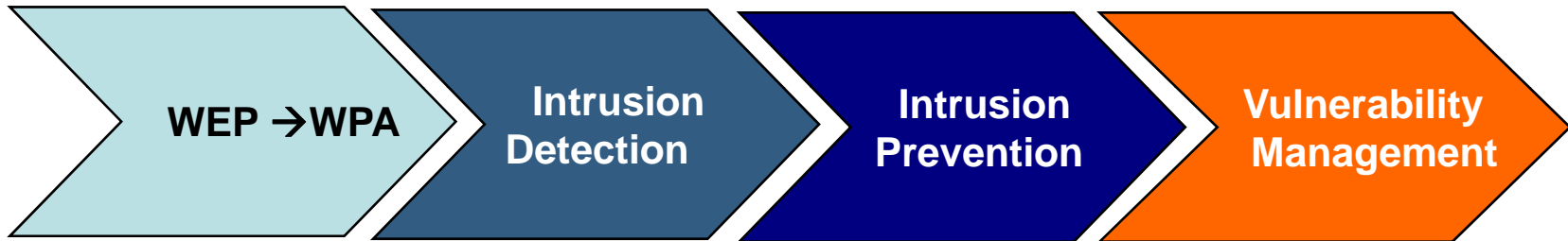
- Device is showing up everywhere
- Users seek free Wi-Fi wherever its available
- New wave of wireless security events
- Network boundaries completely blurred



# Differing Security Requirements



# Evolution of Wireless Security



- Encryption
- Authentication

- Monitor
- Detect

- Prevent
- Locate

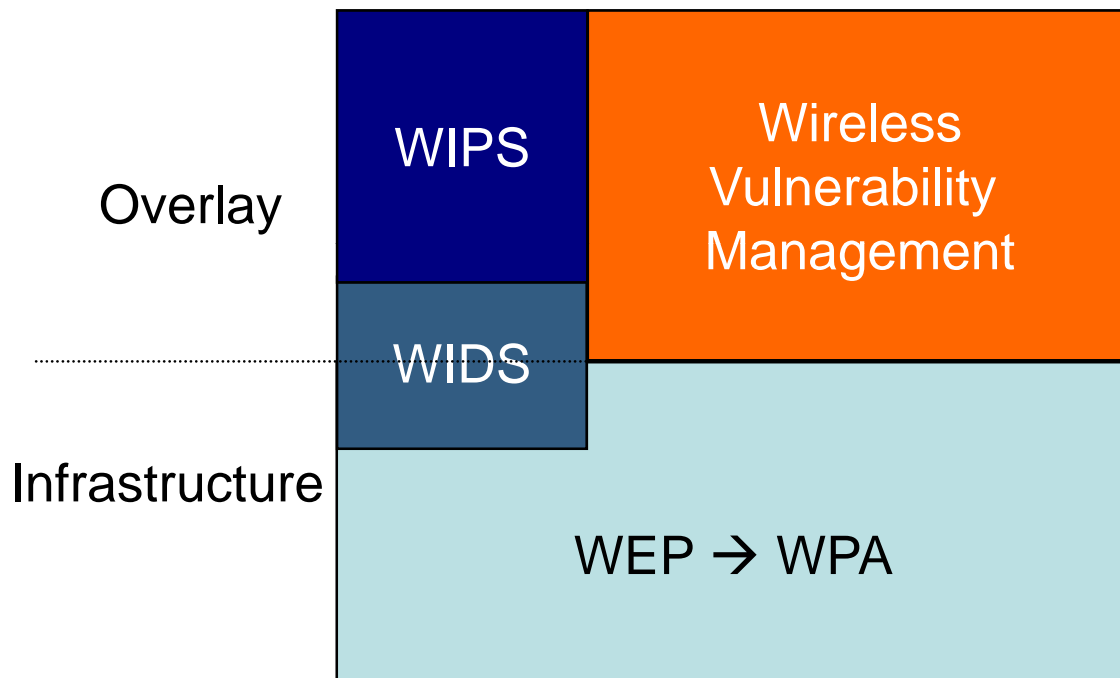
- Assessment
- Compliance
- Remediation

# Trend Towards 24X7 Visibility

## Wireless Vulnerability Management

	<b>Assessment</b> Visibility into Wireless Security Posture	<b>Compliance</b> Regulatory Compliance Reporting	<b>Remediation</b> Wireless Breach Protection
<b>Handheld Scanner</b>	Point in time view Lack of central visibility Remote ops not possible	No consolidated reporting No historical reporting	Not possible
<b>Real Business Needs</b>	<ul style="list-style-type: none"> <li>✓ 24x7 wireless scanning</li> <li>✓ Identify &amp; prioritize all wireless devices</li> <li>✓ Scan and classify wireless vulnerabilities</li> <li>✓ On demand &amp; scheduled reporting</li> </ul>	<ul style="list-style-type: none"> <li>✓ Wireless compliance assessment</li> <li>✓ Pre-defined regulatory reports including PCI, SOX, HIPAA, GLBA</li> <li>✓ On demand &amp; scheduled reporting</li> </ul>	<ul style="list-style-type: none"> <li>✓ Instant notification of wireless vulnerabilities</li> <li>✓ Automated or manual threat remediation</li> <li>✓ Threat location tracking</li> <li>✓ Visibility into wireless signal spillage</li> </ul>

# Wireless Security Landscape



- Scales seamlessly for all size organizations
- Solves different problems for different organizations
- Addresses specific needs at specific times



## Wireless Security: Key Trends and Issues

David C. King  
CEO, AirTight Networks

[www.airtightnetworks.net](http://www.airtightnetworks.net)

**INTEROP**<sup>®</sup>  
THE LEADING BUSINESS TECHNOLOGY EVENT