AirDefense™

WHITE PAPER

Best Practices for Wireless Network Security and Sarbanes-Oxley Compliance

Best Practices for Wireless Network Security and Sarbanes-Oxley Compliance

The objective of this white paper is to provide an overall understanding of the impact of wireless network security on Sarbanes-Oxley compliance.

An important component of any effective system of internal controls is maintaining systems that ensure the confidentiality and integrity of corporate, financial and customer data. This white paper will explore what security challenges wireless networks present, suggest best practices to ensure Wireless LAN security, and demonstrate how AirDefense Enterprise, a Wireless Intrusion Detection and Prevention System, can help you define, monitor and enforce your wireless security policy. By adequately protecting the wireless infrastructure, organizations can demonstrate effective internal control over protection of confidential data and ultimately ensure Sarbanes-Oxley compliance.

Sarbanes-Oxley Overview

On July 30, 2002, the Sarbanes-Oxley (SOX) Act of 2002 was signed into federal law, largely in response to accounting scandals, such as Enron, MCI WorldCom, Tyco, etc. The stated purpose of this act is "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws." It applies to all US companies that must report to the Securities Exchange Commission (SEC).

The SOX Act consists of 11 titles, covering new responsibilities and reporting requirements, all designed to renew investors' trust and understanding of financial reporting. The two most relevant sections for this discussion are:

Section 302 – Corporate Responsibility for Financial Reporting

Section 302 is probably the best known section. It requires the CEO and CFO to certify that they have reviewed the financial reports, the information is complete and accurate, and effective disclosure controls and procedures are in place to ensure material information is made known to them.

Section 404 – Management Assessment of Internal Controls

Section 404 is a new section. It has three basic requirements:

1. Management must establish effective internal controls for accurate and complete reporting.

2. Annual assessment by management of the effectiveness of internal controls supported by documented evidence.

3. Validation of management's assessment by a registered public accounting firm.

All public US companies, with a market capitalization of more than $75 million, must comply for fiscal year ending on or after November 15, 2004. All other public US companies will have to comply for fiscal year ending on or after April 15, 2005.

How Sarbanes-Oxley Effects IT

While SOX Section 404 does not specifically discuss IT and security requirements, the reality are that most financial reporting systems are heavily dependent on technology. The burden falls on the CIO and IT department to establish effective internal control over the IT infrastructure that supports the financial reporting process.

At the same time the IT Governance Institute recognizes *that* "There is no need to re-invent the wheel ... and many organizations will be able to tailor their existing IT control processes to comply with the provisions of the Sarbanes-Oxley Act." The intent of section 404 is to build a strong internal control program, which also includes the IT department, and enhance overall IT governance.

Sound practices include corporate-wide information security policies and enforced implementation of those policies for employees at all levels. Information security policies should govern network security, access controls, authentication, encryption, logging, monitoring and alerting, pre-planned coordinated incident response, and forensics. These components ensure information integrity and data retention, while enabling IT audits and business continuity.

Wireless Network Security and Sarbanes-Oxley Compliance

As wireless technology is exploding in popularity, it also presents a new challenge to IT security, especially as it relates to maintaining confidentiality and integrity of data:

First, the air is a shared medium and lacks the physical control of its wired counterpart. Any wireless device can "see" all the traffic of other wireless devices in the network. Sensitive information that is transmitted between wireless devices can be intercepted and disclosed if not protected by strong encryption.

Second, businesses are steadily integrating wireless technology into their wired network, and connecting through the wireless network can often bypass the traditional wired-side security. Rogue or insecure Access Points can compromise network security, making them popular targets for hackers. Even if an organization has no sanctioned Wireless LANs, Wi-Fi enabled laptops and PDAs can open backdoors into the corporate network and render existing security measures useless.

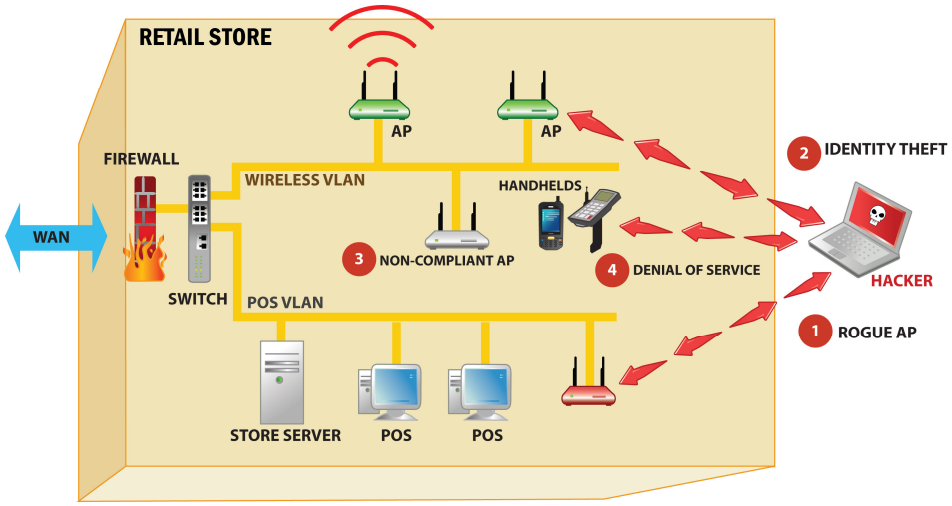
> ***"Wireless devices create backdoors for hackers and can render firewalls, IDS, and VPNs useless."***
> **John Girard, Gartner Research VP**

The wired network can be protected by physical and logical barriers. Physical barriers include limiting corporate network access to employees within the confines of the building. Logical barriers include traditional security, such as firewalls and VPNs. Wireless technology presents a whole new challenge, as the signals bleed through the walls and into the parking lot.

This problem is exacerbated by the simplicity of self-discovery with new wireless devices, which have limited control over other wireless devices with which they connect or "associate." Although "accidental associations" with neighboring networks are relatively benign, "malicious associations" created by intruders are a very serious problem. By exploiting malicious associations, wireless networks can be turned into an easy launch pad for a hacker to attack the corporate network, bypassing existing IT security controls. Clearly, establishing a wireless security policy is a requirement for every organization to

protect the confidentiality and integrity of corporate data. Monitoring its effectiveness is also a must to demonstrate internal control for Sarbanes-Oxley compliance.

Figure 1: Lack of wireless security presents material weakness in IT controls – confidentiality and integrity of data can no longer be assured



Internal Control Frameworks for Sarbanes-Oxley Compliance

Effective internal controls ensure information integrity by mandating the confidentiality, privacy, availability, controlled access, monitoring, and reporting of financial information. The Committee of Sponsoring Organizations of the Tread way Commission (COSO), an independent private sector organization, created a framework that provides a structured and comprehensive set of guidelines for creating and implementing internal controls. Although the COSO framework is not required for Sarbanes-Oxley compliance, the Public Company Accounting Oversight Board (PCAOB) recommended the use of this framework, and COSO enjoys wide acceptance with US companies. COSO is a tool that addresses five components of effective internal control:

1. Control Environment: foundation for all other components of internal control, providing discipline and structure – sets the tone and culture of an organization
2. Risk Assessment: identification and analysis of relevant risks to achievement of the objectives
3. Control Activities: policies and procedures that ensure management directives are carried out
4. Information and Communications: identification, capture, and communication of pertinent information in an appropriate timeframe

5. Monitoring: process that assesses the quality of the internal control system's performance over time.

The COSO framework has a very broad application. It mentions some high-level IT considerations; however, it is not IT-control specific. To address this issue the Control Objectives for Information and related Technology (COBIT) framework was created by the Information Systems Audit and Control Association (ISACA) as a set of guidelines to bridge the gap between IT governance and COSO. COBIT identifies 34 IT control processes that can all be mapped to the more general COSO framework, allowing the user to create a roadmap to SOX compliance. Effective IT governance helps ensure that IT supports the business goals and appropriately manages IT related risks and opportunities.

COBIT Control Process	Control Environment	Risk Assessment	Control Activities	Information & Communication	Monitoring
Ensure Systems Security			●	●	●
Manage the Configuration			●	●	
Manage Problems and Incidents			●	●	●
Manage Data			●	●	

Table I: Selection of the 34 COBIT IT control processes that are most relevant to wireless security and mapping to the COSO framework

The AirDefense Solution for Enhanced Wireless Security Control

By monitoring all 802.11 activities and correlating events from across the wireless network, AirDefense provides a complete enterprise view of everything happening in the airwaves. The AirDefense solution consists of distributed remote sensors and a server appliance. The remote sensors monitor all wireless LAN activities and report back to the server appliance, which analyzes the traffic in real time.

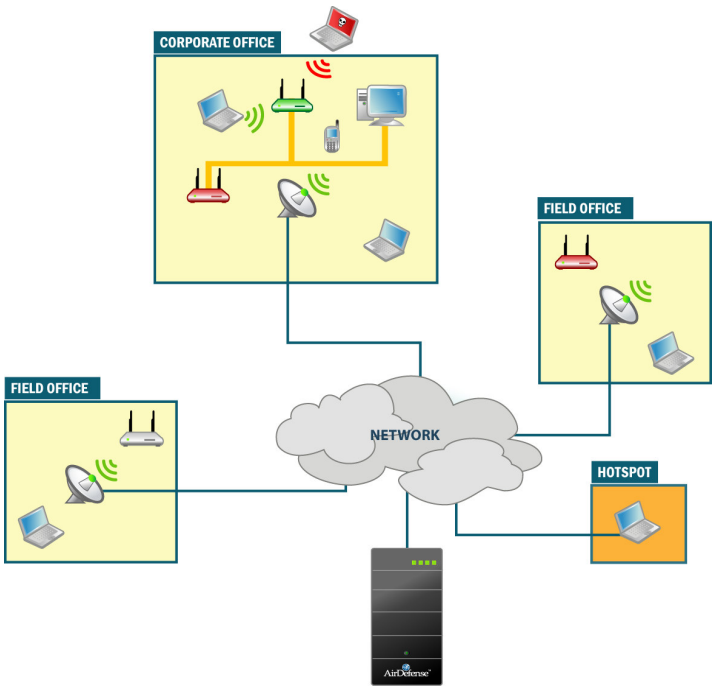


Figure 2: Overview of the AirDefense Wireless Intrusion Detection and Prevention System for wireless security policy enforcement.

Powered by advanced intrusion detection engines, policy manager and correlation engines, AirDefense accurately detects and protects the network against all wireless threats and unauthorized associations with wireless devices. This enables organizations to detect wireless intrusions, rogue WLANs, policy violations, and other adverse factors affecting the security and performance of the wireless LAN, and mitigate the risks either automatically via predefined policies or actively through intervention. AirDefense provides a layer of security that only can be provided with 24x7 monitoring of the network.

The AirDefense system provides a complete suite of wireless security and operational support solutions to enable risk-free wireless LANs. Moreover, the system provides the capability to test the effectiveness of the wireless security policy and report on incidents, serving as a valuable tool for security audits as part of SOX compliance.

Table II on the next page shows a detailed overview of some of the features of the AirDefense Enterprise Wireless Intrusion Detection and Prevention System mapped to the applicable IT control requirements as specified by COBIT. Some of the key features are:

- Ability to define wireless policies in the Policy Manager, detect policy violations (such as mis-configured devices), and enforce compliance through on-command or policy-based termination
- Advanced rogue management, pinpointing those with the highest threat (i.e., rogues on the network)
- Multi-dimensional detection engine assures accurate detection of intrusions, attacks, and suspicious activity on the Wireless LAN – recognizes both known and unknown threats (day-zero attacks)

- Flexible alarm and notification management, enabling prioritization and segregation of incident response functions
- Vulnerability assessment capability to assess effectiveness of wireless security policy
- Stateful monitoring of all wireless LAN activity allows the system to maintain historical data that powers forensics, historic trending, and incident analysis; critical events can be investigated with a single click
- Automatic generation of summary compliance reports for management and IT security administrators

Significance of Reporting

Often, demonstrating compliance to executives, customers, and auditors is equally as important to business as being compliant. The best way to show compliance is to present a series of reports and data that quantify and illustrate enforceable policies.

The AirDefense system has been designed to generate compliance reports for SOX (and other regulations affecting wireless security). Examples of these include, but are not limited to:

- Wireless asset management report
- Policy violations report, i.e., mis-configurations, unauthorized associations
- Vulnerability assessment report, i.e., intrusions, threats, suspicious activity

Table 2: COBIT Process Requirements and Solutions

COBIT Process Requirements	AirDefense Solution
Ensure Systems Security	
An information security policy exists and has been approved	• Knowledge of end-to-end WLAN assets (including Access Points, laptops, PDAs, bar-code scanners, etc.) • Can enforce compliance through active or policy-based termination
A framework of security standards has developed that supports the objectives the security policy (asset classification control, workstation security, etc.)	• Monitors compliance to WLAN policy; can generate reports on policy violations
Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms	• Dashboard provides visibility into Wireless LAN security policy compliance • Detects over 200+ threats, attacks, and intrusions • Can automatically terminate unauthorized associations • Provides vulnerability assessment reports to review policy effectiveness

Table 2: COBIT Process Requirements and Solutions *(continued)*

COBIT Process Requirements	AirDefense Solution
Where network connectivity is used, appropriate controls, including intrusion detection and vulnerability assessments exist and are used to prevent unauthorized access IT security monitors and logs security activity, and reports identified security violations to senior management	• Automatically generates periodic summary reports for management, security and network administrators • Notification Manager provides SNMP, email, and/or pager alerts for various system activities; also provides capability to prioritize and manage the number of alerts
Manage the Configuration	
System infrastructure, including firewalls, routers, switches and other devices, is properly configured to prevent unauthorized access	• Policy Manager to create and define configuration policies • Integrated and automated security management with plug & play configuration • Policy-based automatic termination of unauthorized associations • Automatic downloads of software and policy updates, to protect against newly discovered security threats
Manage Problems and Incidents	
Operational events that are not part of standard operation, incidents, problems and errors, are recorded, analyzed and resolved in a timely manner	With multiple IDS & Correlation Engines, identifies attacks and intrusion attempts by monitoring WLAN activity 24x7 • Provides forensics capabilities to analyze events and patterns • Qualifies the threat level and generates alerts; correlation across multiple sources minimizes false positives • Remote troubleshooting and fault diagnostics capability
Provide adequate audit trail facilities that allow tracing from incident to underlying cause	• One-click analysis (time of attack, entry point, length of exposure, transfer of data, systems compromised) • Forensics & incident analysis tools available for audit trails
Manage Data	
Management protects sensitive information in storage and during transmission	• User can define encryption and authentication policies, monitor network compliance, and identify devices that deviate from policies • Identify primary users of Access Points and monitors all associations (who is connected to whom) • Detects wireless activity and can automatically disconnect unauthorized (ad-hoc, accidental) associations

It is through such reports that executives can determine their level of effort for compliance and quantify their progress. These reports further assist auditors in understanding the controls put in place by the company for wireless security and their effectiveness. Achieving compliance is important and it must be demonstrated and supported by documented evidence.

Practical Steps for Implementation of a WLAN Security Policy

While the COBIT control objectives encompass all IT processes, they still give limited insight into best practices or implementation of standards to ensure compliance. Other sources that can serve as a benchmark for the creation of policies, specifically as they relate to wireless security, are:

- ISO 17799 – A comprehensive set of controls comprising best practices in information security
- SANS Institute – SANS (SysAdmin, Audit, Network, Security) Security Project
- ITL (Information Technology Library) – Guidance on Security for Wireless Networks
- NIST (National Institute for Standards and Technology) – Special Publication 800-48 Wireless Network Security

The following is a summary of baseline best practices for wireless security, using the sources above, industry analyst reports, and internal research.

1. Define, monitor and enforce a wireless security policy (even if there are no sanctioned, corporate Wireless LANs)
   - Policy should cover all 802.11 and Bluetooth wireless devices
   - Define wireless policies for mobile workers
   - Ensure wireless devices are not used until they comply with the wireless security policy

2. Take a complete inventory of all Access Points and 802.11 devices in the airwaves
   - Eliminate rogue Access Points and unauthorized user Stations.

3. Define secure configurations for Access Points and user Stations
   - Change default setting
   - Disable SSID broadcast
   - Turn-off “ad-hoc” mode operation

4. Define acceptable encryption and authentication protocols
   - Turn-off “open” authentication
   - Use strong authentication (WPA, PEAP, 802.11x recommended)
   - Use strong encryption with at least 128-bit keys (WPA, AES recommended)
   - Deploy a layer-3 Virtual Private Network (VPN) for wireless communication

5. Monitor the airwaves to identify suspicious activity
   - Deploy a Wireless Intrusion Detection System (IDS) to identify threats and attacks
   - Detect and terminate unauthorized associations in a timely manner
   - Monitor wireless assets for policy violations
   - Log, analyze, and resolve incidents in a timely manner
   - Gather and store wireless activity information for forensic analysis

Conclusion

Sarbanes-Oxley compliance is a requirement for all publicly traded US companies. The CIO and IT management have critical responsibility for the effectiveness of internal IT control of the financial reporting process. In the short term this will increase the workload on the IT department, however, at the same time it may provide the justification for an increase in resources to address security issues.

An important component of effective internal control is wireless security to ensure confidentiality and integrity of corporate, financial, and customer data. The AirDefense Intrusion Detection & Prevention System, along with wireless security policies and procedures that are properly managed, can assist with maintenance of internal controls and ensure an ongoing, effective compliance program.

The AirDefense solution provides an organization with:

- 24x7 monitoring of their wireless security activity, with the industry's most accurate intrusion detection
- A proven, enterprise-class platform to help define, monitor, and enforce the organization's wireless security policy
- Comprehensive reporting, forensics, and incident analysis tools to facilitate audits and demonstrate compliance with internal control processes.

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring*'s Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. ***All trademarks are the property of their respective owners.***

