AirTight NETWORKS™

Sarbanes-Oxley Compliance and Wireless LAN Security

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

AIR COVER FOR NETWORK SECURITY

Sarbanes-Oxley Compliance and Wireless LAN Security

While at first glance, Sarbanes-Oxley would seem to have very little to do with IT departments and network security, closer study reveals that it actually has major impact on IT departments and IT security in particular. Passed in 2002 by the United States Congress in the wake of a series of corporate financial scandals, the Sarbanes Oxley Act is designed to protect investors by improving the accuracy and reliability of corporate disclosures by all public companies. Chief information officers are responsible for the accuracy, reliability and security of the systems that manage and report the financial data. Section 404 specifically calls out that each annual report 'shall contain an internal control report, which shall--

1. state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

2. contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting,

As financial recording and reporting is computer-based, IT systems underpin all controls. Since IT underlies the very business of recording and reporting all financial activity, it follows that a lack of control over IT security would imply a lack of control over the organization's financial reports, in direct violation of Sarbanes-Oxley section 404. Control of IT systems integrity is therefore required in order to maintain financial reporting integrity. Security is therefore a core component of a Sarbanes-Oxley compliance evaluation. When a wireless LAN is part of the network infrastructure, it too must be subject to the strictest controls to ensure the credentials of those using it. Beyond this, all laptops which use embedded Wi-Fi must also be secured, to prevent an employee from accidentally connecting to a neighboring Wi-Fi network, which might lead to malicious hacking of the employee's laptop or further access to the corporate network.

Control Types

Two types of IT controls must be checked during a Sarbanes-Oxley compliance audit: key controls and general controls. Key controls are those that ensure the values on the balance sheet are accurate and reliable. Expenses and transactions are items that must be validated and cross-checked using key controls. As an example, an entry in a database table for accounts receivable might automatically trigger the creation of an entry into the general ledger. It would be important to ensure that this trigger is in place, is correctly implemented and can only be changed by authorized personnel.

General controls go across all IT systems and are essential to ensuring the integrity and reliability of the systems. Security policies and procedures are an example of a general control that must be audited. Within security policies and procedures, the following is typically within the scope of an audit:

- Authentication/access controls
- Antivirus policies

- Laptop/workstation security
- Password policies
- Firewall/VPN policies
- Intrusion prevention and detection policies
- Physical access security
- Internet usage policy

For companies deploying wireless LAN infrastructure, the password, physical access, authentication/access controls and intrusion prevention policies are most applicable.

Recommendations for Wireless LAN Capabilities to Meet Sarbanes-Oxley Security Control Requirements

To meet Sarbanes-Oxley IT security controls, organizations installing a wireless LAN should look for a system that delivers the following security features:

Physical Access

Within the building, access points should be secured to prevent theft. Ensure your vendor supports plenum rating so access points can be placed above a suspended ceiling, if allowed by your building infrastructure. In addition, external antenna connectors should be available so that antennas can be brought out below the ceiling to ensure the best range. Physical locking mechanisms can also be employed to physically attach the access point. The access point should also not reveal any security settings in the event that it is stolen.

Authentication/Access Controls

Wireless LANs by their nature transmit signals beyond the physical perimeters of a building. Given that, it is imperative that the wireless LAN infrastructure support strong over-the-air and authentication controls to prevent those outside the building site from gaining access.

WPA2 or WPA Security

WPA2 and WPA provide strong over-the-air encryption (AES or TKIP, respectively) coupled with mutual authentication based on IEEE 802.1x between the client and the network.

Proven Interoperability with a WPA2 or WPA-compliant RADIUS Server

RADIUS servers such as Cisco ACS, Funk Software Odyssey and Meetinghouse AEGIS provide the back-end authorization capabilities for users trying to access the wireless network. They also provide a method which allows for auditing the users accessing the network.

Support for Multiple VLANs with Independent Security Settings

Many different types of users may need to access the wireless LAN network. Order administrators require access to the order entry and shipping systems. Accounting and finance staff require access to accounts receivable and payable as well as other financial systems. Marketing and sales teams may require access to sales performance data. Virtual LANS (VLANS) allow each authorized wireless LAN user to gain entry to only the network resources they need to access. In addition, many corporations may use barcode scanners for inventory tracking or in shipping and receiving. These types of devices often do not support today's WPA2 or WPA security, but the less secure WEP encryption. They too can be segregated on a specific VLAN which only allows access to the specific database or application they are associated with. This, along with frequent encryption key changes and MAC address control lists, mitigates potential security risks.

Password Protection and Secure Management Interfaces

The wireless LAN system should support secure, authenticated methods of management. Reconfiguring the access point through the management port is one method a malicious hacker might try to access the corporate network. Wireless LAN systems should provide SNMPv3, SSH (secure Web), and SSL (secure Telnet) interfaces. Furthermore, the system should be configurable such that management is not possible over-the-air, and ideally a management VLAN is available such that only stations on a specific VLAN can modify the WLAN network settings.

Intrusion Detection and Prevention

Wireless intrusion detection is a limited capability of some wireless LAN systems. Only recently have wireless LAN systems been advertising the ability to detect other wireless activity and report it. Most systems simply detect the intrusion, but do not have any means to automatically prevent it. In a large enterprise environment with many hundreds of Wi-Fi devices, and with possible neighboring Wi-Fi networks, the IT organization can be overwhelmed with false alerts and miss the real security issues.

More importantly, it is important to understand the implication of the infrastructure itself providing the control. In wireline networking infrastructure, the control is provided by a separate system. Witness today the clear separation of firewalls and IDS/IPS solutions for the wireline market. With the extreme penalties associated with failure to comply with Sarbanes-Oxley, organizations are advised to carefully consider third generations of wireless intrusion prevention systems now available.

Wi-Fi Vulnerabilities Exist, Even in a 'No Wi-Fi' Organization

Despite all of the above precautions taken to secure the wireless LAN network, a serious security risk can still exist, exposing the organization to Sarbanes-Oxley violations. Even a "no Wi-Fi" policy is no guarantee of security against these threats. Rogue access points can be brought in by employees. Laptops with embedded Wi-Fi can connect to neighboring networks. Both are real, significant risks. Traditional wireline security methods such as firewalls and VPNs do not detect these types of threats. And once the device is behind the corporate firewall, it is viewed as trusted. In this new era of almost ubiquitous Wi-Fi, the corporate air space itself must be considered an asset and protected. The eight major categories of wireless threats are described below.

Common Wireless Threats

Rogue Access Points

The most common, as well as most dangerous, wireless threat is the rogue access point. The rogue access point is typically a low cost, SOHO-class access point brought in by an employee who desires wireless access. The default access point settings typically have no security enabled, and thus when plugged into the corporate network create an entryway for anyone with a Wi-Fi client within range.

Mis-configured Access Points

For those enterprises with a wireless LAN infrastructure, one potential threat can arise from their own equipment. An access point which becomes mis-configured can potentially open up a door to the corporate network. In particular, if the access point is reset to network defaults or the security settings are turned off. If the access point is not centrally managed, then the likelihood of it going unnoticed is high. Employees will still be able to connect so no problem will be reported.

Client Mis-associations

Embedded Wi-Fi clients in laptops are now relatively common. Even for those enterprises with a "no Wi-Fi" policy, a Windows XP laptop with a wireless client will automatically try to connect to an SSID that it has successfully connected to before. This scenario is very common for two reasons.

If the employee has connected to a Linksys, Netgear or other home or hot spot access point using the default SSID, it will automatically connect to another AP with the same SSID without the user being aware of the connection.

Secondly, neighboring Wi-Fi networks can spill into the enterprise and curious users connect to these open, insecure, and distrusted networks while still connected on the wired side of the trusted network. Users may also connect to these networks if their internal network firewall does not permit POP email accounts, does not permit access to certain web sites, or they do not want their outbound traffic monitored.

Ad Hoc Connections

Wireless clients can also create peer-to-peer connections. A peer-to-peer connection can be exploited by a malicious hacker who may try to then inflict a variety of attacks on the client such as port scanning to explore and exploit client vulnerabilities.

Malicious Wireless Threats

Evil Twin/Honey Pot Access Points

Malicious hackers are known to set up Honey Pot APs with default SSIDs (e.g. Linksys, Netgear, default, any etc), hotspot SSIDs, and even corporate SSIDs outside of buildings and watch a large number of clients automatically connect to the AP. These APs can then inflict a variety of attacks on the client or attempt password stealing by presenting a login page to the client over the mis-associated wireless connection.

Rogue Clients

Rogue clients are those that are unauthorized to attach to an authorized corporate wireless network. This may occur through an authorized access point that has been mis-configured with encryption turned off, or through an access point that has had its encryption/authentication compromised and uses the key to connect to a properly configured authorized access point.

Denial of Service Attacks

A danger to any enterprise, denial of service attacks are a threat that can wreak havoc on a large number of users simultaneously. There are various forms of wireless denial of service attacks, but they typically involve flooding a channel or channels with deauthentication or similar packets that terminate all current and attempted client associations to access points. Denial of service attacks can be particularly destructive to voice over Wi-Fi applications, completely halting the conversation.

Preventing Wi-Fi Vulnerabilities with a Wireless Intrusion Prevention System

The benefits of wireless LANs are so compelling – improving efficiencies, lowering costs and increasing customer satisfaction - that doing without a Wi-Fi network is not a viable alternative for many corporations.

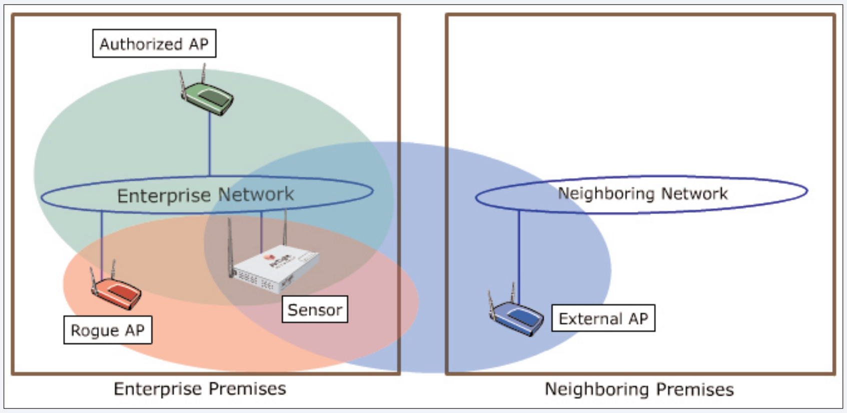
Fortunately, a new breed of security solution, the wireless intrusion prevention system (WIPS), provides a trusted 3rd party security system that prevents these Wi-Fi security risks. Much like an intrusion prevention system for wireline systems, a wireless intrusion prevention system both detects threats and automatically prevents them. WIPS solutions detect all wireless transmissions over-the-air, classify them and based on rules set up by the administrator, can automatically quarantine dangerous devices.

Wireless intrusion prevention systems stop attacks before they penetrate and harm the enterprise. WIPS solutions detect each category of attack using deterministic techniques involving a combination of device and event auto-classification, protocol analysis and association analysis. Signatures are only used to provide additional details and are not necessary for detection.

Key attributes of a wireless intrusion prevention system are:

1. **Monitoring/Detection:** All channels in the 2.4 GHz (802.11b, 802.11b/g) and 5 GHz (802.11a) bands should be scanned. It needs to analyze, aggregate, and correlate information reported by different sensors.

2. **Auto-Classification:** With increasing penetration of WLANs, there is a need to accurately and automatically sort harmful activity from the harmless activity in the shared wireless medium. As an example, in organizations with official WLAN infrastructure, the intrusion prevention system must be able to differentiate between authorized, rogue, and external wireless activities. This type of classification minimizes annoying false alarms and volumes of irrelevant alerts from the security standpoint, both of which make the security system unusable.



A Wi-Fi Intrusion Prevention System should automatically and precisely classify access points as Authorized, External and Rogue to eliminate false alerts.

3. **Prevention:** The WIPS must automatically and instantaneously block harmful wireless activity detected by its wireless sensors. For example, it must block any client from connecting to a Rogue AP or a MAC spoofing AP, prohibit formation of ad-hoc networks, and mitigate any type of DOS attack. Furthermore, it must block multiple simultaneous wireless threats while continuing to scan for new threats.

Prevention of Wi-Fi threats must be carried out with surgical precision to avoid disturbing legitimate WLAN activities. A well implemented WIPS Firewall should not stop traffic on the authorized wireless network or a neighboring Wi-Fi network.

4. **Visualization:** The spatial layout as well as materials within the enterprise (walls, columns, windows, furniture, etc.) interact with the radio coverage of the security sensor in a complex way creating a significant gap between rule-of-thumb placement and reality. A systematic, scientific, and scalable RF planning process is therefore required for determining the right placement of access points and wireless sensors. This must be site-specific and not require time consuming manual surveys. Live RF maps should provide real time information on coverage of both authorized Wi-Fi access points and security sensors.

5. **Location:** Physical remediation is a final step in permanently preventing the Wi-Fi threat and requires knowledge of the physical location of these devices. The WIPS Firewall must provide the location co-ordinates of such a device inside and around the perimeter of the enterprise premises without need for any specialized client side software or hardware.

How a WIPS Solution Maintains Network Integrity and Controls

Wireless IPS solutions can assist a corporation in maintaining network integrity and passing the security compliance audit as required by Section 404 of Sarbanes-Oxley. Unique user identification and over-the-air encryption is a first level of security that IT administrators can use to ensure proper authentication and access controls to meet Sarbanes-Oxley Section 404 control requirements for access over a wireless LAN infrastructure. The WIPS system can monitor and enforce the requirement for unique user identification and encryption. By using WPA or WPA2 security on the wireless LAN network, a user-based authentication process is enforced before access to network resources is allowed. WPA or WPA2 also provide very secure TKIP or AES encryption.

In addition, Section 404 may be violated by other Wi-Fi vulnerabilities. A WIPS solution can ensure that proper Access Control protocols stay in place by:

- Reporting and quarantining any mis-configured access points; i.e. those access points that are authorized but no longer support WPA or WPA2 security due to mis-configuration or intentional tampering. This will prevent unauthorized clients from accessing the network. It will also prevent any authorized client from accessing the network without a proper audit trail.

- Reporting and quarantining any rogue access points. Any access point that attaches to the network and is not authorized should be quarantined, whether or not it has encryption enabled. This will prevent any client, authorized or unauthorized from accessing the network and potentially accessing or tampering with confidential corporate financial data.

- Reporting and quarantining any client mis-associations; i.e. preventing authorized Wi-Fi clients from accidentally connecting to neighboring networks. This will prevent an employee's laptop from connecting to a neighboring Wi-Fi network that uses a default SSID. If the employee laptop uses Windows XP and has associated with a default SSID at home or in a public hot spot, in searching for the strongest connection it can find it may associate with another neighboring network. In doing so, it leaves the laptop open to port scanning or other malicious activity that may compromise the corporate network and allow unauthorized users to gain access or tamper with confidential corporate financial data.

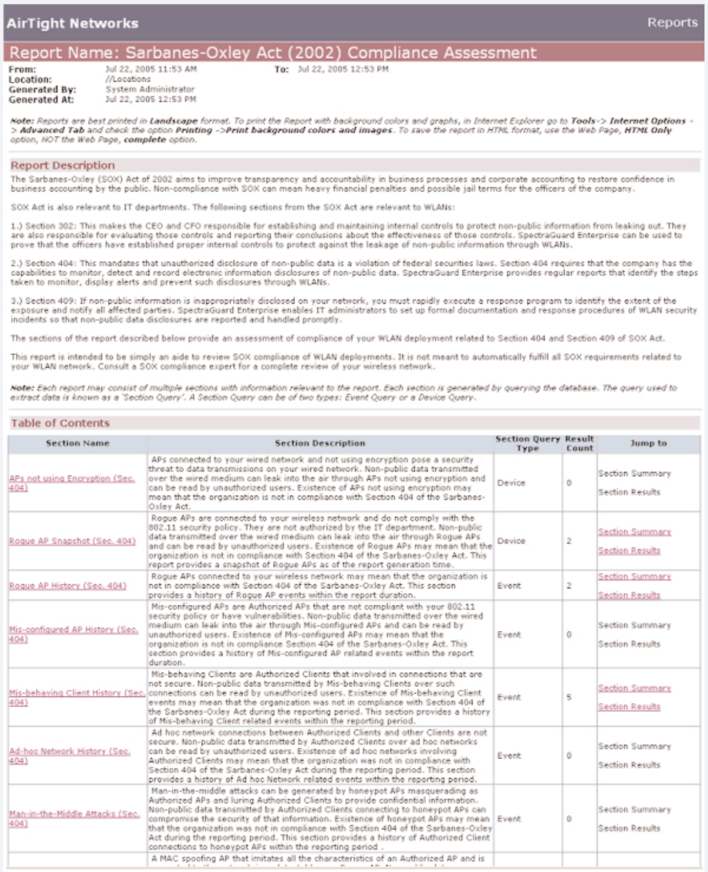
- Reporting and quarantining any honey pot or Evil Twin access points. Malicious hackers might try to emulate authorized access points in an attempt to gain user credentials to log into the corporate WLAN network. The WIPS system should identify these types of attacks and stop any authorized client from associating with these devices.

- Reporting and stopping any denial of service attacks. Denial of service attacks can disable the wireless LAN infrastructure. While not causing a direct access control problem, they do compromise the reliability and integrity of the network.

An Example Compliance Report

As discussed above, a properly configured wireless IPS system can not only provide constant monitoring, but also automatic prevention of the many threats that Wi-Fi poses to the confidentiality and integrity of healthcare records. Compliance reports tailored for all levels of management can be automatically generated. A high level view, as shown in the report below from AirTight Network's SpectraGuard Enterprise, can provide an immediate understanding of the areas that the organization faced risks.

Detail on each area can be provided by simply clicking on the appropriate section. This enables understanding of the exact nature of the security incidents, their location, dates, time and devices involved.



Report Name: Sarbanes-Oxley Act (2002) Compliance Assessment

From:	Jul 22, 2005 11:53 AM	**To:**	Jul 22, 2005 12:53 PM
Location:	//Locations		
Generated By:	System Administrator		
Generated At:	Jul 22, 2005 12:53 PM		

Note: *Reports are best printed in* ***Landscape*** *format. To print the Report with background colors and graphs, in Internet Explorer go to* ***Tools-> Internet Options -> Advanced Tab*** *and check the option* ***Printing ->Print background colors and images****. To save the report in HTML format, use the Web Page,* ***HTML Only*** *option, NOT the Web Page,* ***complete*** *option.*

Report Description

The Sarbanes-Oxley (SOX) Act of 2002 aims to improve transparency and accountability in business processes and corporate accounting to restore confidence in business accounting by the public. Non-compliance with SOX can mean heavy financial penalties and possible jail terms for the officers of the company.

SOX Act is also relevant to IT departments. The following sections from the SOX Act are relevant to WLANs:

1.) Section 302: This makes the CEO and CFO responsible for establishing and maintaining internal controls to protect non-public information from leaking out. They are also responsible for evaluating those controls and reporting their conclusions about the effectiveness of those controls. SpectraGuard Enterprise can be used to prove that the officers have established proper internal controls to protect against the leakage of non-public information through WLANs.

2.) Section 404: This mandates that unauthorized disclosure of non-public data is a violation of federal securities laws. Section 404 requires that the company has the capabilities to monitor, detect and record electronic information disclosures of non-public data. SpectraGuard Enterprise provides regular reports that identify the steps taken to monitor, display alerts and prevent such disclosures through WLANs.

3.) Section 409: If non-public information is inappropriately disclosed on your network, you must rapidly execute a response program to identify the extent of the exposure and notify all affected parties. SpectraGuard Enterprise enables IT administrators to set up formal documentation and response procedures of WLAN security incidents so that non-public data disclosures are reported and handled promptly.

The sections of the report described below provide an assessment of compliance of your WLAN deployment related to Section 404 and Section 409 of SOX Act.

This report is intended to be simply an aide to review SOX compliance of WLAN deployments. It is not meant to automatically fulfill all SOX requirements related to your WLAN network. Consult a SOX compliance expert for a complete review of your wireless network.

Note: *Each report may consist of multiple sections with information relevant to the report. Each section is generated by querying the database. The query used to extract data is known as a 'Section Query'. A Section Query can be of two types: Event Query or a Device Query.*

Table of Contents

Section Name	Section Description	Section Query Type	Result Count	Jump to
APs not using Encryption (Sec. 404)	APs connected to your wired network and not using encryption pose a security threat to data transmissions on your wired network. Non-public data transmitted over the wired medium can leak into the air through APs not using encryption and can be read by unauthorized users. Existence of APs not using encryption may mean that the organization is not in compliance with Section 404 of the Sarbanes-Oxley Act.	Device	0	Section Summary Section Results
Rogue AP Snapshot (Sec. 404)	Rogue APs are connected to your wireless network and do not comply with the 802.11 security policy. They are not authorized by the IT department. Non-public data transmitted over the wired medium can leak into the air through Rogue APs and can be read by unauthorized users. Existence of Rogue APs may mean that the organization is not in compliance with Section 404 of the Sarbanes-Oxley Act. This report provides a snapshot of Rogue APs as of the report generation time.	Device	2	Section Summary Section Results
Rogue AP History (Sec. 404)	Rogue APs connected to your wireless network may mean that the organization is not in compliance with Section 404 of the Sarbanes-Oxley Act. This section provides a history of Rogue AP events within the report duration.	Event	2	Section Summary Section Results
Mis-configured AP History (Sec. 404)	Mis-configured APs are Authorized APs that are not compliant with your 802.11 security policy or have vulnerabilities. Non-public data transmitted over the wired medium can leak into the air through Mis-configured APs and can be read by unauthorized users. Existence of Mis-configured APs may mean that the organization is not in compliance Section 404 of the Sarbanes-Oxley Act. This section provides a history of Mis-configured AP related events within the report duration.	Event	0	Section Summary Section Results
Mis-behaving Client History (Sec. 404)	Mis-behaving Clients are Authorized Clients that involved in connections that are not secure. Non-public data transmitted by Mis-behaving Clients over such connections can be read by unauthorized users. Existence of Mis-behaving Client events may mean that the organization was not in compliance with Section 404 of the Sarbanes-Oxley Act during the reporting period. This section provides a history of Mis-behaving Client related events within the reporting period.	Event	5	Section Summary Section Results
Ad-hoc Network History (Sec. 404)	Ad hoc network connections between Authorized Clients and other Clients are not secure. Non-public data transmitted by Authorized Clients over ad hoc networks can be read by unauthorized users. Existence of ad hoc networks involving Authorized Clients may mean that the organization was not in compliance with Section 404 of the Sarbanes-Oxley Act during the reporting period. This section provides a history of Ad hoc Network related events within the reporting period.	Event	0	Section Summary Section Results
Man-in-the-Middle Attacks (Sec. 404)	Man-in-the-middle attacks can be generated by honeypot APs masquerading as Authorized APs and luring Authorized Clients to provide confidential information. Non-public data transmitted by Authorized Clients connecting to honeypot APs can compromise the security of that information. Existence of honeypot APs may mean that the organization was not in compliance with Section 404 of the Sarbanes-Oxley Act during the reporting period. This section provides a history of Authorized Client connections to honeypot APs within the reporting period .	Event	0	Section Summary Section Results
	A MAC spoofing AP that imitates all the characteristics of an Authorized AP and is			

Conclusion

Wireless LAN infrastructure is now an increasingly common part of corporate enterprises. With wireless LAN infrastructure, new productivity gains can be realized. With this infrastructure though comes a new threat to corporate security. Wi-Fi threats can compromise the corporate infrastructure integrity and security, whether or not the corporation has their own wireless LAN network. These threats combined with the need for Sarbanes-Oxley compliance require new solutions to protect the network integrity and security. A Wi-Fi IPS solution can provide a 24 x 7 monitoring and prevention solution for all categories of Wi-Fi threats. Using a Wi-Fi IPS solution can ensure that proper authentication and access controls for the wireless LAN infrastructure remain in place. It also will prevent unauthorized access points and clients from compromising the corporate network. Both of these areas are critical for maintaining Sarbanes-Oxley IT security controls and thus ensuring integrity of the corporate network.