802.11 Wireless Security Report for Sarbanes-Oxley

from 2009-09-17 16:21:52 to 2009-09-18 16:21:52

System Name: AirDefense
Domain: System
Generated: 2009-09-18 16:23:02
Version: 7.3.3-12
Time Zone: EDT - Eastern Daylight Time

Based on COBIT IT Control Guidance
Define, monitor and enforce a wireless security policy

Implement WLAN monitoring and enforce WLAN policy. For approved WLAN deployments use monitoring to verify that these protective measures are effective.

Wireless Asset Inventory Report

COBIT Control Guidance summary (Ensure Systems Security, Manage the Configuration):

- Asset classification and control
- Ensure system infrastructure is properly configured to prevent unauthorized access

Baseline 802.11 wireless security practice: Identify all Access Points connected to the network

Identify and recognize wireless LAN risks such as rogue WLANs, insecure WLAN connections to unauthorized APs, and attacks against WLAN infrastructure that risk security and exposure of confidential information.

WLAN Environment

Authorized Access Points:	33
Authorized Stations:	53
Total Sensors Deployed:	6

Rogue Access Points and Stations Found

Rogue APs:	110
Rogue Stations:	15
Unauthorized APs:	233
Unauthorized Stations:	85

Authentication Report

COBIT Control Guidance summary (Ensure Systems Security, Manage the Configuration, Manage Data):

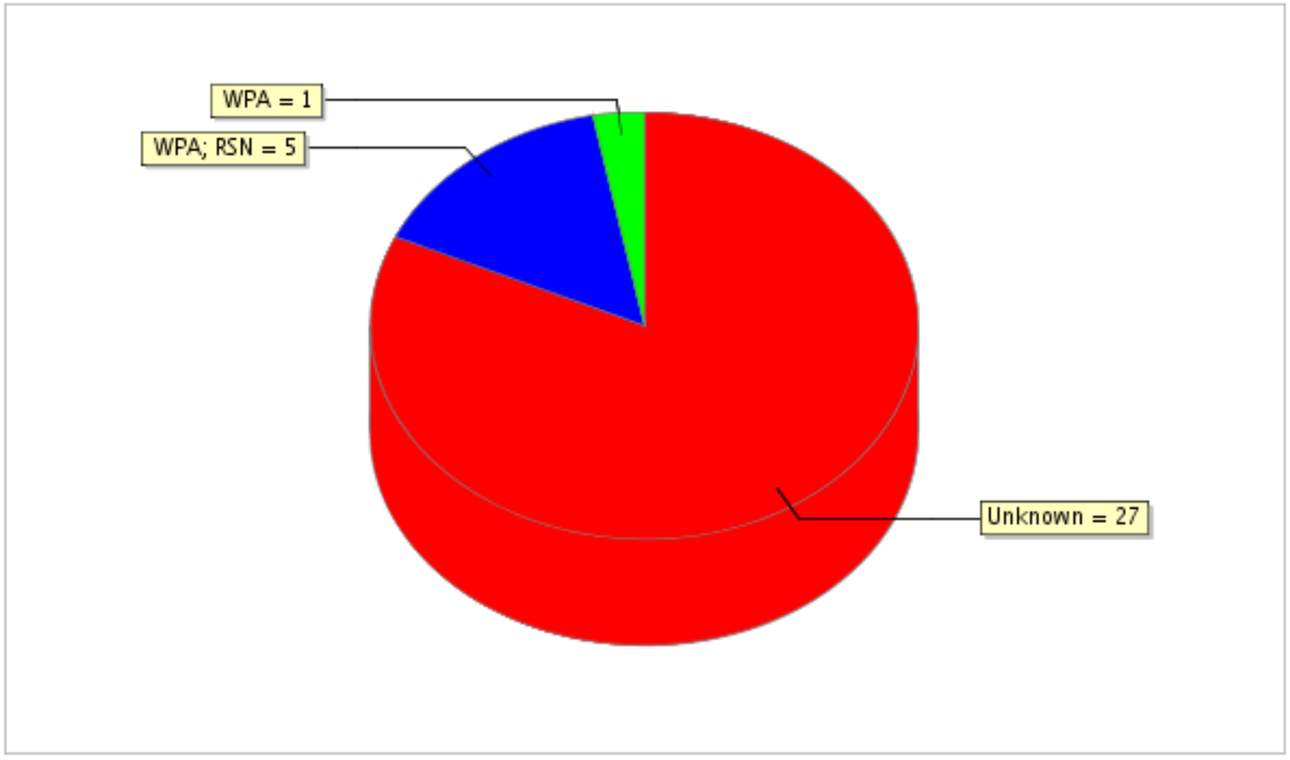
- Maintain effectiveness of authentication and access mechanisms
- Ensure system infrastructure is properly configured to prevent unauthorized access
- Protect sensitive information during transmission

Baseline 802.11 wireless security practice: Use strong Authentication & Encryption protocols for 802.11 wireless access and strong Encryption protocols for wireless communication

For approved WLAN deployments deploy strong encryption and authentication protocols for protection and use monitoring to verify that these protective measures are effective.

Authorized Access Points by Authentication Type

Authorized Access Points by Authentication Type



Authorized Access Points with Authentication Violations

AP	Criticality Level	Alarm Name	SSID	Location	Group
Belkin:c2:ff:c3[b,g]	Critical	Advanced Key Generation Modes Violated	ralphsnart	Auburn, GA	Auburn
Belkin:c2:ff:c3[b,g]	Critical	Extended Authentication Modes Violated	ralphsnart	Auburn, GA	Auburn
Symbol:4f:e4:1c[a,b,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:50:1f:40[a,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:4f:de:64[a,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:50:1e:54[a,b,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:4f:e4:80[a,b,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Nortel:76:7d:40[a,b,g]	Critical	Extended Authentication Modes Violated	Chris_Nortel_WPA	Atlanta, GA Office	1st Floor

Encryption & Authentication Report

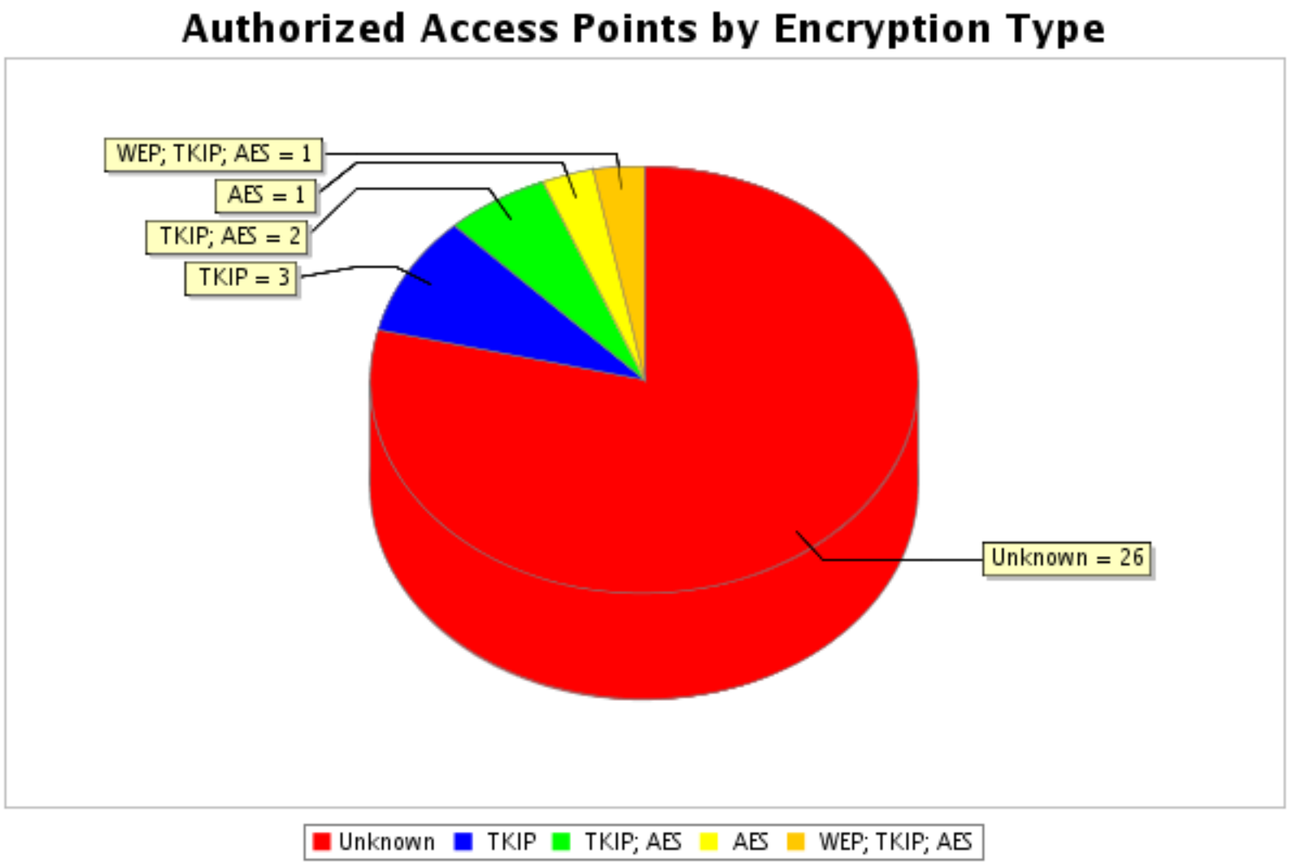
COBIT Control Guidance summary (Ensure Systems Security, Manage the Configuration, Manage Data):

- Maintain effectiveness of authentication and access mechanisms
- Ensure system infrastructure is properly configured to prevent unauthorized access
- Protect sensitive information during transmission

Baseline 802.11 wireless security practice: Use strong Authentication & Encryption protocols for 802.11 wireless access and strong Encryption protocols for wireless communication

For approved WLAN deployments deploy strong encryption and authentication protocols for protection and use monitoring to verify that these protective measures are effective.

Authorized Access Points by Encryption Type



Authorized Access Points Encryption Violations (Top 50)

Device	Criticality Level	Alarm Name	SSID	Location	Group
Nortel:76:7d:40[a,b,g]	Critical	80211 Encryption Modes Violated	Chris_Nortel_WPA	Atlanta, GA Office	1st Floor
Symbol:50:1f:40[a,g]	Critical	80211 Encryption Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:50:1e:54[a,b,g]	Critical	80211 Encryption Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:4f:e4:80[a,b,g]	Critical	80211 Encryption Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:27:e1:b0[a]	Critical	80211 Encryption Modes Violated	MXAP	Atlanta, GA Office	1st Floor

Vulnerability Assessment Report

COBIT Control Guidance summary (Ensure Systems Security, Manage the Configuration, Manage Problems and Incidents):

- Where network connectivity is used, appropriate controls (including firewalls intrusion detection and vulnerability assessment) exist and are used to prevent unauthorized access.
- Ensure system infrastructure is properly configured to prevent unauthorized access
- Incidents, problems and errors are recorded, analyzed and resolved in a timely manner

Baseline 802.11 wireless security practice: Monitor the RF airwaves to detect intrusions

Monitor to detect intrusions and perform vulnerability assessments to prevent unauthorized access. Take action to respond and remediate WLAN security risks identified by the monitoring requirement. Remediation must be done in a timely manner and in accordance with the identified threat.

Attacks

Identity Theft Attacks:	0
Denial of Service Attacks:	0
Reconaissance Activity:	2
Time Of Day Violations:	0
Authentication Failures:	0
Station on Watch List Present:	2

Misconfigurations

Access Points Using Unauthorized Channel:	0
Access Points wth SSID in Beacon:	3
Access Points without Strong Authentication (policy):	8
Access Points without Strong Encryption (policy):	5
Access Points Using Unauthorized Data Rates:	0
ESSID Change on Access Point:	1
CF Change on Access Point:	0

Top 5 Stations with Attacks

Station	Criticality Level	Type	Location	Group

Top 5 Misconfigured Access Points

Device	Criticality Level	Type	SSID	Location	Group
Belkin:c2:ff:c3[b,g]	Critical	Advanced Key Generation Modes Violated	ralphsnart	Auburn, GA	Auburn
Belkin:c2:ff:c3[b,g]	Critical	Extended Authentication Modes Violated	ralphsnart	Auburn, GA	Auburn
Symbol:4f:e4:1c[a,b,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:50:1f:40[a,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor
Symbol:4f:de:64[a,g]	Critical	Extended Authentication Modes Violated	M-Wireless	Atlanta, GA Office	1st Floor

General Vulnerabilities

Ad Hoc Stations:	2
Ad Hoc Networks:	4
Software Based Access Point:	2
Missing Access Point:	0
Rogue AP	110
Rogue Stations:	16

Unauthorized Associations

Accidental Associations:	0
Roaming Policy Violations:	0

Top 5 Access Points or Stations with Alarms

Count	Device	Location	Group
4	Symbol:ea:c2:e1[a]	Atlanta, GA Office	1st Floor
4	Symbol:e0:c4:f1[a,b,g]	Atlanta, GA Office	1st Floor
4	Symbol:bb:c4:1d[a]	Atlanta, GA Office	1st Floor
4	Microsoft:2a:ee:ad[b]	Atlanta, GA Office	1st Floor
4	Symbol:bb:fa:ac[b,g]	Atlanta, GA Office	1st Floor

Policy Violations Report

COBIT Control Guidance summary (Ensure Systems Security, Manage the Configuration, Manage Problems and Incidents):

- Maintain effectiveness of authentication and access mechanisms
- IT security administration monitors and logs security activity and identified security violations are monitored.
- Ensure system infrastructure is properly configured to prevent unauthorized access

Baseline 802.11 wireless security practice: Monitor the RF airwaves to ensure policy compliance

Monitor to enforce wireless security policy compliance to prevent unauthorized access. Take action to respond and remediate WLAN security risks identified by the monitoring requirement. Remediation must be done in a timely manner and in accordance with the identified threat.

Policy Compliance Summary

Wireless Access Points Without Encryption:	0
Insecure Connections:	0
Unauthorized Access Points:	264
Unauthorized Stations:	231
Unauthorized Roaming Between Access Points:	0
Suspect After-Hours Activity:	0
Severe Events Unacknowledged:	365
Critical Events Unacknowledged:	100

Specific Policy Violations (Top 50)

Device	Criticality Level	Alarm Name	Category	Group	Location
Symbol:bb:c6:2c[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bb:fa:ac[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:ce:73:ad[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:ce:73:ac[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bb:c8:a9[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:4e:91:f4[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office

Device	Criticality Level	Alarm Name	Category	Group	Location
Symbol:bb:c8:aa[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:4e:bc:2c[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:27:36:19[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bf:ed:3c[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bf:ef:bc[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bf:ef:bd[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Motorola:0e:c7:20[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:31:89:6d[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:54:33[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:56:d1[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:54:31[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bb:c8:ab[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Intel:07:ae:1e[a,b,g]	Severe	Rogue Station	Rogue Activity	1st Floor	Atlanta, GA Office
Hon:4c:4e:1b[a,b,g]	Severe	Rogue Station	Rogue Activity	1st Floor	Atlanta, GA Office
Gemtek:d8:0f:ff[a,b,g]	Severe	Rogue Station	Rogue Activity	1st Floor	Atlanta, GA Office
Nathan Station[a,b,g]	Severe	Rogue Station	Rogue Activity	1st Floor	Atlanta, GA Office
Intel:07:88:2c[a,b,g]	Severe	Rogue Station	Rogue Activity	1st Floor	Atlanta, GA Office
Intel:0f:63:c0[a,b,g]	Severe	Rogue Station	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e5:b4:e1[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Motorola:0e:c8:e0[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:ce:06:53[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:ce:06:52[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:d5:11:a0[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Motorola:07:1a:a8[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:54:30[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:ce:0a:68[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e5:b4:e3[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e0:66:a0[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e0:c4:f1[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e5:b4:e2[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office

Device	Criticality Level	Alarm Name	Category	Group	Location
Cisco:68:53:7c[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:56:d0[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e0:c4:f0[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:53:7a[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e3:ac:e0[a,b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Cisco-linksys:54:57:2a[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:53:79[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Cisco-linksys:54:57:2b[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:ce:06:50[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:bb:fa:ad[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:e5:b4:e0[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Cisco:d5:96:dc[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:cf:3e:64[a]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office
Symbol:6e:53:7b[b,g]	Severe	Rogue AP on Wired Network	Rogue Activity	1st Floor	Atlanta, GA Office