GLBA Compliance Report

from 2009-09-17 16:16:53 to 2009-09-18 16:16:53

System Name: AirDefense
Domain: System
Generated: 2009-09-18 16:18:03
Version: 7.3.3-12
Time Zone: EDT - Eastern Daylight Time

GLBA Requirement Summary

(a) Designate an employee to coordinate your information security program.

The committed owners of information security must also be responsible for or delegate responsibility for WLAN security and rogue protection.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

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 customer information.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

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

(d) Oversee service providers by selecting service providers capable of maintaining appropriate safeguards and requiring them to implement and maintain such safeguards.

Require all service providers, especially those whom the FSP exchanges customer information with, to possess the same level of security safeguards, or higher, with regards to both wire and wireless security.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by element (c).

Take action to respond and remediate WLAN security risks identified by the monitoring equipment. Remediation must be done in a timely manner and in accordance with the identified threat.

Section 314.4 Element (a)

Designated person(s) name is:

Section 314.4 Element (b)

Rogue Access Points:	110
Insecure Station Connections:	0
Attacks Against Wireless Network:	69

Section 314.4 Element (c)

APs with Weak Authentication:	7
APs with Weak Encryption:	5
Rogue Stations:	15
Unauthorized Roaming Between APs:	0

Section 314.4 Element (d)

Domain: (The domain of the report is listed in the header.)

Section 314.4 Element (e)

Severe and Critical Events Unacknowledged: 466

Policy Violations (Up to 50 Listed)

Total Policy Violations 19

Criticality	Device	Device MAC	SubCategory	Type	Start Time	Location	Group	Cleared
85	Belkin:c2:ff:c3[b,g]	00:1c:df:c2:ff:c3	Advanced Key Generation	Advanced Key Generation Modes Violated	8/11/09 6:49 PM	Auburn, GA	Auburn	No
85	Belkin:c2:ff:c3[b,g]	00:1c:df:c2:ff:c3	Authentication	Extended Authentication Modes Violated	8/11/09 6:49 PM	Auburn, GA	Auburn	No
85	Symbol:4f:e4:1c[a,b,g]	00:15:70:4f:e4:1c	Authentication	Extended Authentication Modes Violated	8/5/09 5:05 PM	Atlanta, GA Office	1st Floor	No
85	Symbol:50:1f:40[a,g]	00:15:70:50:1f:40	Authentication	Extended Authentication Modes Violated	8/5/09 5:02 PM	Atlanta, GA Office	1st Floor	No
85	Symbol:4f:de:64[a,g]	00:15:70:4f:de:64	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
85	Symbol:50:1e:54[a,b,g]	00:15:70:50:1e:54	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
85	Symbol:4f:e4:80[a,b,g]	00:15:70:4f:e4:80	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
85	Nortel:76:7d:40[a,b,g]	00:18:b0:76:7d:40	802.11 Encryption	80211 Encryption Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
85	Nortel:76:7d:40[a,b,g]	00:18:b0:76:7d:40	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
85	Symbol:50:1f:40[a,g]	00:15:70:50:1f:40	802.11 Encryption	80211 Encryption Modes Violated	9/14/09 8:47 AM	Atlanta, GA Office	1st Floor	No
85	Symbol:50:1e:54[a,b,g]	00:15:70:50:1e:54	802.11 Encryption	80211 Encryption Modes Violated	9/14/09 9:48 AM	Atlanta, GA Office	1st Floor	No
85	Symbol:4f:e4:80[a,b,g]	00:15:70:4f:e4:80	802.11 Encryption	80211 Encryption Modes Violated	9/15/09 8:09 AM	Atlanta, GA Office	1st Floor	No
85	Askey:05:6f:39[a,b,g]	00:11:f5:05:6f:39	Environment	Ad-Hoc Network Violation Unauthorized Device	9/17/09 11:26 AM	Atlanta, GA Office	1st Floor	No
85	Symbol:27:e1:b0[a]	00:15:70:27:e1:b0	802.11 Encryption	80211 Encryption Modes Violated	9/17/09 5:13 PM	Atlanta, GA Office	1st Floor	No
85	Liteon:b0:82:2d[b]	00:22:5f:b0:82:2d	Environment	Ad-Hoc Network Violation Unauthorized Device	undefined time	Atlanta, GA Office	1st Floor	No
85	Liteon:b0:82:2d[b]	00:22:5f:b0:82:2d	Environment	Ad-Hoc Network Violation Unauthorized Device	9/18/09 11:46 AM	Atlanta, GA Office	1st Floor	No
20	Belkin:c2:ff:c3[b,g]	00:1c:df:c2:ff:c3	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/11/09 6:50 PM	Auburn, GA	Auburn	No
20	Nortel:76:7d:40[a,b,g]	00:18:b0:76:7d:40	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/5/09 5:02 PM	Atlanta, GA Office	1st Floor	No
20	Symbol:27:e1:b0[a]	00:15:70:27:e1:b0	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	9/11/09 1:55 PM	Atlanta, GA Office	1st Floor	No