Airspace Confidentiality, Integrity, and Availability Compliance Requirements

Release Date: Autumn 2020

Copyright

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

The Orchestra Group Ltd logo and all Orchestra Group Ltd product and service names listed herein are either registered trademarks or trademarks of Orchestra Group Ltd or its subsidiaries. All other marks are the property of their respective owners.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Airspace Confidentiality, Integrity, and Availability Compliance Requirements

Wireless network access is relatively new to corporate campuses. Many companies operate wireless networks to allow greater flexibility through mobile computing.

Once it was nice to have, wireless is now becoming the default mechanism for most on-premises connectivity. Wireless is critical for supporting mobile workers (for example, hot desks), mobile customers (for example, mobile payments), and IoT devices (for example, smart rooms). As wireless networks proliferate, they can no longer be categorized as low impact from a security perspective[1], but should be considered at least having moderate impact[2]. That is, a security breach can be expected to have a serious adverse effect on the organization's operations, assets, or individuals, and need to be secured appropriately.

A lack of wireless security expertise causes many IT departments to ignore the unique dangers of WLAN (Wireless LAN) connectivity, relying only on existing network controls.

The problem is that wireless networks are much easier to attack and compromise than their wired counterparts because they are often accessible from public areas. Wireless devices are also more prone to Man-in-the-Middle type attacks because no physical access is needed, and attack hardware can be positioned anywhere nearby. Physical security does not prevent an attacker from attempting to eavesdrop on wireless communications or gain unauthorized access to internal networks.

The latest proof point is the September 2020 US Office of Inspector General report on their "wireless red team" that utilized easily-concealed units that cost less than $200 to attack government wireless networks from publicly accessible locations open to visitors. These simulated attacks went undetected by security guards and IT security staff and were highly successful. The "wireless red team" intercepted and decrypted wireless network traffic and, in two instances, gained access to internal networks. They also obtained credentials of an IT employee via wireless to log in to a help desk ticketing system.

Two well-known early compliance standards and guidelines for wireless network security are the PCI DSS Wireless Guideline [1] and the NIST Guidelines for Securing Wireless Local Area Networks [2]. These have been around for quite a few years. As a result of expanded interest in corporate wireless environments, a number of more up-to-date WLAN guidelines and standards have been published [3] [4] [5] [6] including two published this year (2020) [7] [8].

WLAN non-compliance has both security and privacy ramifications.

Survey of Guideline Control Objectives for WLANs

WLAN security and compliance have the following distinct components that need to be covered:

- WLAN airspace requirements
- WLAN connectivity requirements
- WLAN connected devices requirements
- WLAN infrastructure requirements

Each component has a unique set of requirements that need to be distilled and implemented from the guidelines. It is important to note that the airspace requirements are unique to WLAN and have no analogy in standard network compliance standards.

These requirements are related and have some overlap, but also have unique monitoring and enforcement needs.

In this document we focus on the airspace in order to integrate compliance, guidelines, and best practices together into an actionable security plan. Airspace protection is a critical, but typically misunderstood, factor that could place the organization and its digital assets at risk.

Every organization's risk appetite is different. That is why it is important to define guidelines as outcome-focused control objectives and not explicitly define how to satisfy the control.

Below is a summary of high-level control objectives for the WLAN airspace component of the relevant standards and guidelines. Please note that it does not cover other components that are related to internal networks and infrastructure or controls for managing wireless devices. Feel free to contact us at the Orchestra Group for more details on overall WLAN security, compliance, and privacy issues.

WLAN Airspace Confidentiality, Integrity, and Availability Control Objectives (distilled from SCP guidelines and best practices)

The following is distilled from listed compliance requirements.

- Monitor and enforce confidentiality of the corporate airspace.
    - Enforce SSID encryption level and multi-factor authentication protocols by segment.
    - Enforce WLAN-connected device separation.
- Monitor and enforce integrity of the corporate airspace.

- Ensure integrity of corporate SSIDs, APs, and hotspots accessible in the corporate airspace.
- Ensure integrity of the access path between a connected device and its associated AP.
- Ensure WLAN device separation.
- Monitor corporate airspace outside the organizational boundaries and enforce authorized access areas (and times).
- Monitor for unusual WLAN usage patterns.

- Ensure availability of the corporate airspace.
  - Log all wireless access.
  - Audit and (penetration) test of airspace (contact us for more details).

Harmony IoT - Designed Specifically to Protect Your Airspace

Harmony IoT is foremost a detective control for the confidentiality, integrity, and availability of the corporate airspace by providing coverage for airspace compliance requirements. It can also be set to enforce airspace compliance requirements.

The moment a wireless device enters your airspace, it is identified and tracked. In addition, Harmony IoT compares what a device IS doing, with what it SHOULD be doing. These comparisons are based on the simultaneous analysis of a variety of device characteristics.

Harmony IoT uniquely combines positive detection, that looks at how a device should be behave, with negative detection capabilities, that identify known attack behaviors, to produce high-fidelity alerts that allow you to quickly understand and address airspace risk in your environment. Harmony IoT's cutting-edge data-science approach pinpoints airspace vulnerabilities that need to be addressed.

Harmony IoT interrupts or disconnects wireless connections to isolate threats in your environment. Harmony IoT can also enforce IoT policies that align with your business and compliance objectives.

SS019 [9], while not without issues, is currently the best WLAN compliance standard we have found. See Bibliography references (7) and (8) for our recommendations for WLAN security, compliance, and privacy.

Glossary

Airspace

The physical corporate premises extended to areas from which a corporate SSID is visible.

AP

WLAN Access Point.

Connected Device

A device connected to WLAN

Security Standard Wireless Network [7]

While not without issues, it is currently the most secure WLAN standard we have found. It is our recommendation for WLAN compliance.

SSID

Service Set Identifier. That is, the broadcast name of your WLAN. It defines the WLAN network segment.

WLAN

Wireless Local Area Network.

Appendix

	PCI-DSS	PCI-DSS CDE	CIS Controls 7.1	FFIEC	SS-19	Harmony IoT
Monitor and enforce confidentiality of the corporate airspace						
Enforce SSID encryption level and multi-factor authentication protocols by segment	Audit	Audit	X	X	X	X
Enforce WLAN-connected device separation			X		X	X
Monitor and enforce integrity of the corporate airspace						
Ensure integrity of corporate SSIDs, APs and hotspots accessible in the corporate airspace	Audit	Enforce	X	X	X	X
Ensure integrity of the access path between a connected device and its associated AP					X	X
Ensure WLAN device separation		X	X	X		X
Monitor corporate airspace outside organizational boundaries and enforce authorized access areas (and times)	X	X		X		X
Monitor for unusual WLAN usage patterns					X	X

	PCI-DSS	PCI-DSS CDE	CIS Controls 7.1	FFIEC	SS-19	Harmony IoT
Ensure availability of the corporate airspace					X	X
Log all wireless access			X		X	X
Audit and (penetration) test of airspace (contact us for more details)	Audit	Audit				Contact Us

Bibliography

(1). PCI - Data Security Standard (DSS). Information Supplement: PCI DSS Wireless Guideline. [Online] July 2009.

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

(2) NIST Special Publication 800-153. Guidelines for Securing Wireless Local Area Networks (WLANs). [Online] February 2012.

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

(3) NIST - SP 800-171 Rev. 2. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. [Online] February 2020.

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

(4) Federal Financial Institutions Examination Council's (FFIEC). Wireless Network Considerations. [Online] 2014.

https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic9-network-controls/iic9(a)-wireless-network-considerations.aspx

(5) NIST SP 800-53, REV. 5. Security and Privacy Controls for Information Systems and Organizations. [Online] September 2020.

(6) CIS - Center for Internet Security 7.1. [Online] April 2019.

https://learn.cisecurity.org/control-download

(7) Chief Security Office UK Department for Works and Pension. Security Standard Wireless Network (SS-019). [Online] March 2020.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882775/dwp-ss019-security-standard-wireless-network-v1.1.pdf

(8) Office of the Inspector General. Evil Twins, Eavesdropping, and Password Cracking: How the Office of Inspector General Successfully Attacked the U.S. Department of the Interior's Wireless Networks. [Online] September 2020.

https://www.doioig.gov/sites/doioig.gov/files/FinalAudit_WirelessNetworkSecurity_Public.pdf

(9) Computer Security Division Information Technology Laboratory. FIPS PUB 199. Standards for Security Categorization of Federal Information and Information Systems. [Online] 2004.

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf