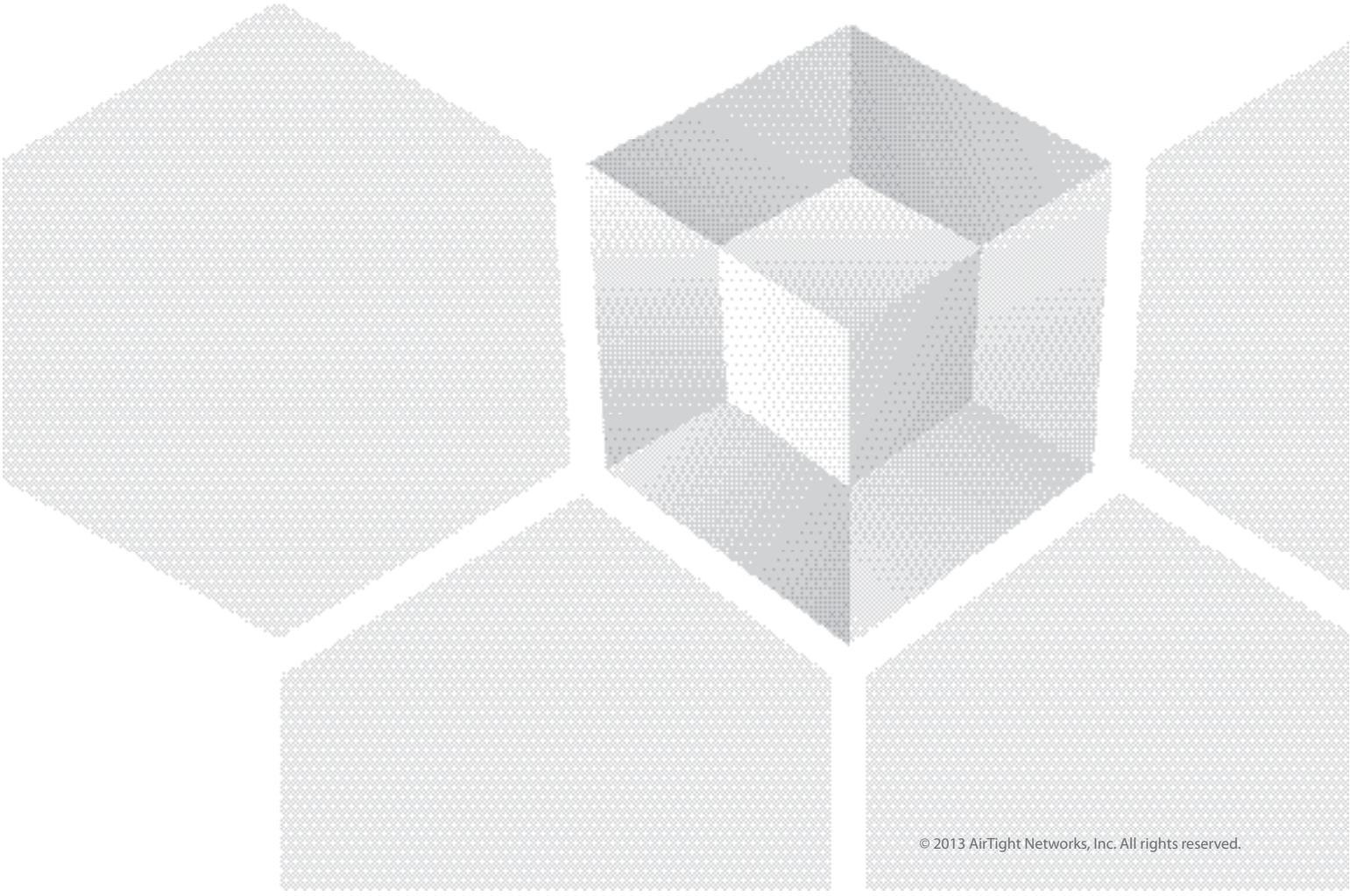
Complying with RBI Guidelines for Wi-Fi Vulnerabilities

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Mountain View, CA 94043
www.airtightnetworks.com



Complying with RBI Guidelines for
Wi-Fi Vulnerabilities

Reserve Bank of India (RBI) guidelines cover all aspects of information technology (IT) infrastructure - Governance, Operations, Security, Audit and Vulnerability Assessment, Cyber Frauds, Outsourcing Management, Business Continuity Planning, Customer Education and Legal issues for organizations providing banking services in India.

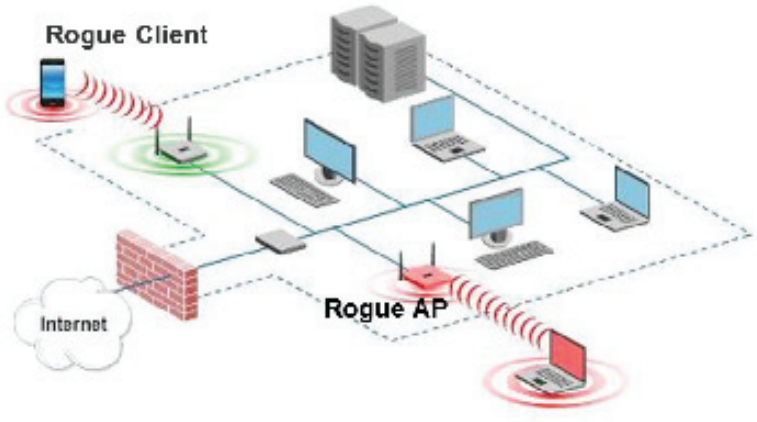
This whitepaper presents a detail action plan for compliance with RBI Guidelines for security.

Security Challenges with Wireless Local Area Networks (WLANs or Wi-Fi)

IEEE 802.11 based wireless (popularly known as Wi-Fi) presents new security challenges for IT administrators, which easily bypass traditional network security measures, such as a firewall, and compromise the network security perimeter. Internal users namely, employees, contractors, and visitors carry Wi-Fi enabled devices and can connect to external untrusted networks, or Bluetooth-like peer to peer Wi-Fi connections, thereby, endangering identity theft and even data leakage. Besides laptops and smartphones, printers, projectors, and cameras are Wi-Fi enabled creating security risks that were not observed before.

With Wi-Fi, outsiders can reach a bank's network and an internal user can reach out to external untrusted Wi-Fi bypassing the bank's security infrastructure. Consider the following scenarios:

Unauthorized Wi-Fi on Enterprise LAN



Scenario 1: An unauthorized Wi-Fi Access Point (AP) is connected to a bank network enabling external untrusted users to listen to the data traffic on a bank's internal wired network, obtain IP addresses, gain access to bank's servers, and even obtain customer data. Such unauthorized Wi-Fi APs plugged onto a bank's private network without permission are called "Rogue APs" and often are inadvertently installed by internal users to enjoy Wi-Fi access without realizing the security implications.
A Rogue AP need not be an external device; even an internal user's Windows 7 laptop can be easily converted into a Wi-Fi AP using built-in or readily available free public domain tools, and used to share the access to a bank's private network with unauthorized users over Wi-Fi.

Scenario 2: An internal user creates a Wi-Fi hotspot on a smartphone, or a hacker creates a Wi-Fi hotpot, using the same Wi-Fi network name (also known as SSID) as that of the bank Wi-Fi or any Wi-Fi that internal users use, such as their home Wi-Fi (their wireless devices often probe for home Wi-Fi even when the user is in the office). It's easy to sniff the air and obtain Wi-Fi networks being probed by wireless users and then mimic these networks. Bank users will inadvertently connect to such an external, untrusted Wi-Fi network without even realizing it and can result in data leakage as data from their devices (personal or those provided by the bank) passes through the hotspot.
These connections bypass the bank's firewalls and other controls and can happen even when users may not be trying to explicitly use Wi-Fi on their laptops, tablets or smartphones.

Employees Bypassing Enterprise Security

Scenario 3: An internal user connects her bank laptop to a personal smart phone using computer-to-computer Wi-Fi protocol and creates what is commonly called as an "ad-hoc network" to download some data, or say connects to a projector or printer that's Wi-Fi enabled. Such ad-hoc networks create a parallel channel of communication that does not pass through the bank's wired network security controls and without appropriate security measures in place, the bank has no visibility into how such connections are being misused. An external untrusted user could sniff such connections or even lure bank employees to directly connect to their device.

These scenarios are only a few examples of how Wi-Fi can inadvertently or maliciously compromise a bank's security perimeter and are possible irrespective of whether or not the bank has installed Wi-Fi. Even in case of a stated 'No Wi-Fi policy', users carry Wi-Fi enabled devices and a Wi-Fi AP can be plugged into a bank's network easily. So unless a bank is actively monitoring and enforcing a "No Wi-Fi policy", the policy is rendered useless.

Automatic
Device Classification

Comprehensive
Threat Coverage

Reliable
Threat Prevention

Accurate
Location Tracking

BYOD
Policy Enforcement

Automated
Compliance Reporting

Wi-Fi Security Best Practices

Following best practices can secure a bank's network and data from Wi-Fi based vulnerabilities:

- Definition of a comprehensive Wi-Fi security policy that designates locations for Wi-Fi access and and specifies types of users, such as employees and visitors, who have access to Wi-Fi internally and when away from work place such as travelling or at home.
- Employing best in class encryption for authorized Wi-Fi networks , and enforcing proper user authentication.
- Use a wireless intrusion prevention system (WIPS) for 24x7 monitoring of a bank's airspace and wired network. WIPS should detect all Wi-Fi devices including smartphones, tablets, printers, projectors, and security cameras and their activity or connections; automatically classify these for conformance to the bank's Wi-Fi security policy; and in real-time prevent all connections that violate the stated policy so that the Wi-Fi misuse – inadvertent and malicious – is stopped before any damage is done.
- Periodic security audit for compliance with bank's Wi-Fi policy and other applicable regulations.

What About Network Access Control (NAC) for Wi-Fi

Banks should not assume that implementation of a NAC remediates Wi-Fi threats. A NAC or other conventional wired security measures, such as firewall, have no visibility into the wireless medium and, hence, cannot protect a bank's data and network from wireless vulnerabilities and threats. While the use of strong encryption and authentication (e.g., WPA2/802.1x) for authorized Wi-Fi connections is a form of NAC, it cannot block unmanaged devices, e.g., Rogue APs, mobile hotspots, and the resulting unmanaged connections.

Complying with RBI Guidelines

RBI guidelines outline a detail plan for a bank's IT infrastructure. While Section 28 is dedicated to wireless security, threat from Wi-Fi based attacks is not only to the Wi-Fi infrastructure but the entire IT infrastructure. Consequently, wireless threat management needs to be woven into entire IT security fabric – policies, assessment, audit, firewalls, intrusion prevention, end point security, and forensics. The table below provide a cross reference between the best practices and RBI Guidelines. Please contact AirTight Networks at **rbicompliance@airtightnetworks.com** for a detailed clause-wise compliance metrics.

Wireless Security Best Practice	RBI Guidelines Index
Defining Wi-Fi Security Policy Definition of a comprehensive wireless policy describing guidelines for properly securing bank's enterprise networks wired and Wi-Fi and a No-Wi-Fi policy; best practices for employees for their Wi-Fi enabled devices, as well as for visitors and contractors when working in bank's premises;	**Information Technology Governance** Risk Management (Pages 4,5,8,9) **Information Security** Risk Assessment (Page 16) End User Awareness & Training (Page 19, 22) Data Center Policy (Page 22) **Wireless Security** **Information Security Assurance** Audit, Penetration Testing & Assurance (Page 51)
24x7 scanning for Wi-Fi threat detection and protection 24x7 scanning of bank's air space and wired network for detection of all wireless devices including smart devices and connections, automatically classifying these for conformance to the wireless security policy; automatically building a list of internal users' smart devices for approval; determine which Wi-Fi access point devices are on bank's enterprise network; comprehensive assessment of wireless vulnerability & threat assessment (WVA) and blocking all connections violating bank's wireless security policy	**Information Security** Information Security Governance (Page 12) Critical Components of Information Security (14,15) Threat Assessment (Page 16) Access Control: Smart Devices Provisioning & Approval (Page 19, 20) DLP – Data leak Prevention (Page 30) Automated Vulnerability Scanning (Page 31) Monitoring for events and patterns (Page 31) Networks Design for monitoring (Page 32) IDS & IPS (Page 33) Anomaly Detection Tools (Page 33)

Wireless Security Best Practice	RBI Guidelines Index
	Network Behaviour Analysis (Page 33) Traffic Logging (Page 37) Security Event Management (Page 37) Security Measurement Metrics (Page 38, 39) Network Security (Page 38, 39) Network Perimeter Security (Page 39) IDS (Page 42) Security Hardening (Page 45) Backdoor Medium Control (Page 45) Network Control & Access (Page 46) **Wireless Security** Implementation of WIDS (Page 49) Scanning for wireless (Page 49) Encryption & Security (Page 50) **Information Security Assurance** Penetration Testing (Page 51) **Cyber Fraud** Fraud Vulnerability Assessment (Page 114) Data/Information/System Security (Page 115) Customer awareness (Page 118) Employee Awareness (Page 119)
End Point Security for Mobile Users Enforcing policy on bank's mobile users who carry corporate wireless devices away from work and connect to Wi-Fi at airports, home.	**Information Security** Critical Components of Information Security (14,15) Access Control: Smart Devices Provisioning & Approval (Page 19, 20) Security Hardening (Page 45) Access from Remote Locations by users (Page 46) Analysis of remote accesses (Page 47) **Wireless Security** Restrict Wireless Access on clients (Page 49) Wireless Vulnerability Assessment (Page 51) Wireless Penetration Testing (Page 51) **Cyber Fraud** Fraud Vulnerability Assessment (Page 114) Data/Information/System Security (Page 115) Customer awareness (Page 118) Employee Awareness (Page 119)

Other Regulations

The chapter on legal issues covers the civil and criminal liabilities of bank with respect to the IT act. Given below are MCIT and MHA Guideline that need to be considered when banks consider Wi-Fi security.

Complying with RBI Guidelines for
Wi-Fi Vulnerabilities

Ministry of Communication & Information Technology (MCIT) Regulation

MCIT regulation requires provider of Wi-Fi infrastructure to know the identity of wireless users. While other methods do exist, the only reliable way is 24x7 scanning of the environment, comprehensive detection of Wi-Fi and maintenance of Wi-Fi users data. It is applicable for Wi-Fi as well as No Wi-Fi zones as an unmanaged Wi-Fi AP can be plugged in easily making the bank responsible for this unauthorized Wi-Fi network.

Ministry of Home Affairs (MHA) Guidelines

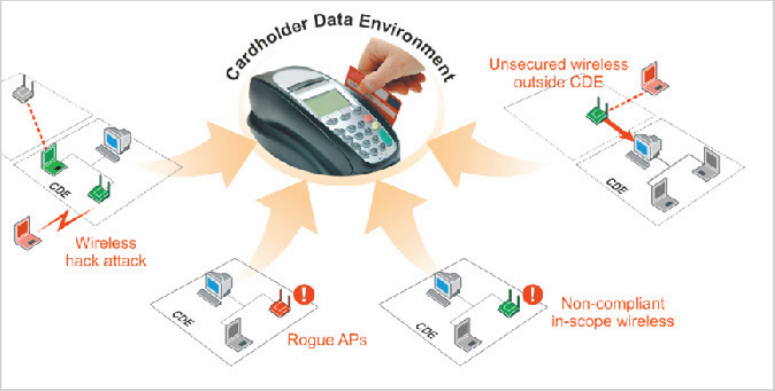
Ministry of Home Affairs (MHA) issued following guidelines after incidents of terror mails sent around the time of blasts in Jaipur, Ahmedabad, and Delhi.

"In view of the vulnerabilities associated with the usage of Wi-Fi and their exploitation by terrorists / criminals and unscrupulous hackers, sensitive ministries and departments are advised not to install or use any Wi-Fi network in their offices. The ministries will have to install best available Wi-Fi intrusion detection system and carry out regular audit o their airspace to detect hotspots and rogue access points."

National Cyber Security Policy (NCSP)

NCSP issued by Department of Information Technology, Ministry of Communication & Information Technology caters to the whole spectrum of ICT users and providers including medium and large enterprises. It requires entities to put in place a 24x7 mechanism for cyber security emergency response and resolution. In critical sectors like banking, it requires organizations to carry out periodic IT Security Risk Assessment, evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks.

Payment Card Industry (PCI) Wireless Security Guidelines



Complying with RBI Guidelines for Wi-Fi Vulnerabilities

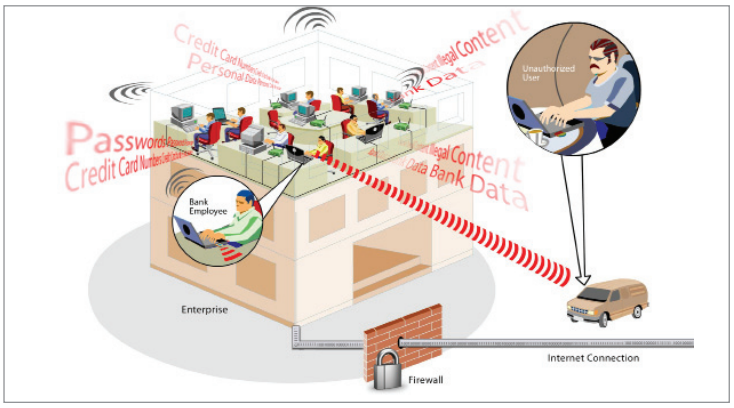
PCI DSS (Data Security Standards) is about securing credit card data. PCI DSS Wireless Guideline mandates a quarterly wireless scan throughout the organization, monitoring alerts and an incident response system. This is applicable irrespective of presence of WLANs. Further PCI DSS Wireless Guideline mandates presence of usage policies, maintenance of wireless logs, IEEE 802.1i security and physical security for known WLANs inside credit card data environment.

While a scan may take place quarterly, a PCI auditor can ask for information from any time period during the quarter. PCI DSS recommends use of automated scanning enabled by a wireless intrusion prevention system (WIPS) for large organizations and Tier 1 merchants.

In Summary…

Existing IT Security architecture works on the premise that only trusted users can physically access an enterprise network. All others have to come through security gates, such as enterprise firewalls and intrusion prevention systems. Wi-Fi breaks this premise as the network is now in the air and the invisible radio waves cannot be confined to a building or forced behind a firewall, blurring the enterprise network perimeter. A hacker does not need to physically enter the building to access an enterprise network. RBI Guidelines mention diminishing boundaries between internal and external networks and the consequent vulnerabilities. Wi-Fi destroys the perimeter because it operates in an unlicensed frequency spectrum, thereby making external networks visible and accessible from inside the bank and also exposing the banks Wi-Fi network for access by outsiders.

In view of all of these, securing against Wi-Fi threats requires additional security architecture at Layer 2 beyond traditional firewalls and other wired security controls.



AirTight Networks, Inc. 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 | **www.airtightnetworks.com**
India Office: +91.020.66407050 | **contact@airtightnetworks.com**

White Paper: Complying with RBI Guidelines for Wi-Fi Vulnerabilities [Doc ID: ATN-WP-0913-002-00-EN]

AirTight® NETWORKS

Comprehensive Cloud - Managed Wi-Fi