Wireless Security Assessment

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Wireless technology has introduced a number of complications and additional security risk into traditional network management. BYOD, signal jacking, the proliferation of public Wi-Fi and most recently, expanded work-from-home has made securing the corporate network much more challenging. Securing the wireless component of your organization's network requires well-documented policies as well as strong technical controls.

To help your organization achieve this, TPx offers a comprehensive Wireless Security Assessment that results in actionable recommendations for a robust, high-performing, and secure wireless environment.

Assessment Benefits

- Enable mobile and remote work productivity gains without sacrificing corporate security
- Validate use of Best Practices in authentication and encryption protocols
- Secure your network against attack and compromise from rogue DHCP clients
- Ensure your BYOD and Acceptable Use policies meet your organization's needs
- Visualize your location's wireless coverage through a saturation map — ensure signal is getting to where it needs to be

Overview

TPx's Wireless Security Assessment is founded on industry standards such as ISO 27001, ISO 27033, NIST 800-153, CIS "Top Twenty" and current best practices. It is designed to evaluate your organization's wireless infrastructure and configuration, the security posture, and functional capabilities. The assessment will be divided into three phases, covering the following:

- **Documentation & Visualization** of the existing wireless network environment. TPx will inventory and catalog your existing wireless network assets and architecture.
- **Security Strategy** TPx will assess the network policies, standards and procedures as well as all the security management processes, and roles and responsibilities related to the wireless network.
- **Operational Function & Hygiene** TPx will assess the technical measures implemented in your network infrastructure.

Assessment Activities

The approach for the wireless security assessment is to evaluate your organization's wireless network security posture and profile. Posture refers to your organization's current ability to transfer, maintain and protect data within the wireless network. Profile refers to the minimum target of capability required to protect information and manage associated risks, which an organization should aim to achieve.

Your information security posture will be assessed based on a set of categorizations (e.g., access controls and network protections). The categorizations covered for the assessment focus on areas of cybersecurity that have the highest likelihood of incidents and breaches for your organization.

The objective of this effort is to assess your infrastructure's adherence to industry standards of ISO 27033. TPx will review the organization through interviews, policy review, validation and investigation of process to provide a numerical rating that reflects that maturity/resiliency of your security infrastructure. The assessment will focus on the following areas:

Phase 1: Documentation & Visualization

Physical Inventory

- Hardware Inventory Spreadsheet
- Layer 1-2 Diagrams/Documentation (will create during the engagement if doesn't exist)
- Layer 3 Diagrams/Documentation

Design & Architecture Review

- Network Overview Architecture
- Layer 3 Routing
- Layer 2 Optimization

Phase 2: Security Strategy

Network Infrastructure Security

- Weak wireless authentication or encryption protocols
- Centralized authentication, authorization, and accounting
- Rogue DHCP/client detection
- Validate network access (ingress and egress) to the WAN via port scan

Performance Monitoring & Analysis

- Recommend improved hygiene and integration with MSS/SOC
- Review acceptable usage policies and ensure WAN enforces policy details
- Validate performance on WAN and off WAN
- Validate performance via different network protocols
- WAN heatmap available (as scoped)

Phase 3: Operational Function & Hygiene

Infrastructure Monitoring & Management

- Central Monitoring/Alerting Capabilities
- Syslog Capabilities
- Host End Monitoring/Management
- Software Management (networking)
- Wireless configuration validation capabilities

Configuration Management

- Centralized Configuration Backup
- Centralized Configuration Automation
- Configuration Change Management Workflow

Reporting

Upon completion of the assessment, TPx will provide two reports: an Executive Summary and a detailed Best Practice report. The reports will speak to two different levels of resources at the Customer: the leadership and the security practitioner. A detailed recommendations report will be provided and validated with your personnel. The objective of this report is to present the results and observations related to your wireless network security posture.

In addition, you will receive recommendations by TPx for your top three priorities based on your business, your sensitive data, your exposure landscape and the wireless network state. TPx will also provide an updated wireless network diagram, wireless saturation for the primary location (as scoped) and recommendations on how to best create or update your security-related documentation.

The average mobile device connects to two to three insecure Wi-Fi hotspots per day

Verizon Mobile Security Index, 2020