

Wireless Intrusion Detection & Prevention Services

Wireless network devices present risk to your network infrastructure, whether your organization allows them or not. CGI Managed Wireless Intrusion Prevention Service can help you manage risks by uncovering, locating and removing threats posed by unauthorized wireless devices.

Unmanaged Wireless Risk

Wireless network devices are now commodity items, and increasingly available for low cost. They are often deployed by employees at work looking for the same quick and mobile connectivity they enjoy at home. This effectively extends the range of network ports and mobile computing devices beyond the perimeter of your building, where physical security policy is unenforceable. Wireless technology built into laptops and tablets is typically enabled with promiscuously configured defaults to maximize connectivity. The backdoors to your network are no longer visible or manageable.

Path to Peace of Mind

CGI MSS Managed Wireless Intrusion Prevention Service provides a risk management solution to wireless network technology risks. The service provides regularly reported metrics that provides compliance evidence detailing the effectiveness of the risk management program in place.

CGI MSS begins the process with an analysis of the target office wireless security policy. The policy and site are assessed, including a report recommending the best coverage locations for sensor placement to support the policy. Sensors are deployed at the recommended locations with network connectivity. Our Security Operations Center monitors the sensors for health and security events, and alerts your computer security incident response team when policy violations occur. Using a centrally controlled procedure enables historical logging of wireless access that can provide granular wireless device information and store event logs and statistics for at least 90 days. This procedure is intended to demonstrate “due care” in the effort of providing a layered defense for industry acceptable security practices.

“Rogue” WLAN Access Point (AP)

A rogue Access Point (AP) is any device that adds an unauthorized (and therefore unmanaged and unsecured) WLAN to the organization’s network. A rogue AP could be added by inserting a WLAN card into a back office server, attaching an unknown WLAN router to the CGI network, configuring the workstation to serve as peer-to-peer WLAN AP, Smart phone hotspot, and/or by various other means. This creates a risk of unauthorized access into the CGI perimeter.

Unauthorized WLAN Stations

An unauthorized WLAN station is a laptop, tablet or smart-phone client with a WiFi interface that is not intended to be present in the environment. A rogue station can be configured to promiscuously connect to various wired networks AP or peer stations located outside of CGI premises. This creates a risk of data exfiltration from CGI’s perimeter.

Features

- Enforce wireless LAN policy
- Continuous monitoring and containment of violations
- Compliance reporting and incident handling
- Minimal on-site requirements

Benefits

- Industry leading MSSP with incomparable expertise
- Leading edge solutions and devices
- 99.5 % standard availability
- 24x7 coverage through the MSS SOC