



## Five Wireless Facts a CIO Should Know

**In 2005 alone, there were 10,511 mergers & acquisitions in the U.S.** (FactSet MergerStat)

With corporate merger and acquisition activity near an all-time high, a Fortune 1000 corporation can expect to acquire several companies in the next twelve months. Following a merger, today's all-Cisco Wi-Fi network can instantly become a heterogeneous wireless LAN with hardware from Symbol, ProCurve, Proxim, Aruba, and others. According to Accenture, "infrastructure incompatibility" is the single greatest impediment to a successful post-merger IT integration. To overcome this obstacle without AirWave, you would need to decide whether to (a) spend hundreds of thousands of dollars to replace existing hardware to maintain a homogeneous network or (b) maintain multiple management systems to support a heterogeneous network. With an open, multi-vendor wireless management solution like the AirWave Management Platform, you will be able to control your diverse network from a single console – freeing you and your staff to handle more pressing post-merger issues.

Years ago, Wi-Fi hardware vendors promised that 'thin' wireless access points would be like lightbulbs: inexpensive, disposable, and easy to replace. In fact, today's thin APs are as expensive as intelligent, stand-alone access points – and the cost of installing and provisioning a new AP can be higher than the price of the device itself. Instead of replacing APs frequently, cost-conscious organizations are doing everything they can to extend the life of their existing infrastructure. *NetworkWorld* reports that the average life expectancy of a wireless AP is three years. Yet, while your organization seeks to extend the life of your existing investment, vendor-proprietary management tools often cannot support even that same vendor's legacy products. The AirWave Management Platform™ provides unparalleled support for legacy products, allowing your staff to manage the Cisco Aironet 350 access point you installed two years ago from the same console they use to configure your newest Airespace AP.

**The average life expectancy of Wi-Fi hardware is 3 years or more** (NetworkWorld)

**90 percent of WLAN security incidents will be the result of misconfigured systems** (Gartner)

A misconfigured wireless access point can be an open door that allows an outsider directly onto your network, exposing your corporate data and jeopardizing your compliance programs (SOX, HIPAA, PCI, etc.) Yet, with hundreds or thousands of devices on your network, attempting to locate a misconfigured device through manual reports and processes is truly like searching for a needle in a haystack. The AirWave Management Platform automates configuration audits and compliance management for wireless network. At a specified interval, AMP compares the configuration of every device to your policies, immediately alerting you when a violation is detected and automatically repairing the configuration before it can be exploited by an intruder.

According to NetworkWorld's 2005 salary survey, help desk salaries average \$53,000 per year, compared to \$80,000 for a network analyst and \$66,000 for a network admin. With wireless networks, support calls are often escalated directly to the network engineer, because the help desk lacks the tools to resolve the issue. This costs you money and, even worse, prevents your skilled network specialists from tackling other higher priority tasks. The AirWave Management Platform has specially designed Help Desk views that allow them to quickly locate users on the network, assess the cause of their problems, and resolve the issue quickly. And with AMP's role- and responsibility-based security levels, you know that the Help Desk staff will not inadvertently change network settings or access data they are not authorized to see.

**It costs 25-50% more for a support call to be handled by a Network Engineer than by the Help Desk** (NetworkWorld)

**Companies with 10,000 or more employees average 645+ separate physical facilities** (u.s. Census Bureau)

With hundreds of facilities, ranging from large campuses to small remote sales offices and stores, most Fortune 500 organizations are still years away from having wall-to-wall coverage with Wi-Fi or with RF sensors. This simultaneously gives your employees in remote offices an incentive to install their own (unsecured) rogue APs on your network and also makes it extremely difficult to detect those rogues since they are out of range of your APs and sensors. Unlike other solutions, AirWave's RAPIDS rogue detection module conducts scans across your wired network as well as RF scans with your own APs. This means you can detect and remove unauthorized rogue APs anywhere on your network, whether they are connected in your corporate headquarters or in one of your hundreds of remote sites.