# Keeping Your WLAN Safe and Secure

By Anne McCarthy Strauss

An ever increasing number of WLANs are being deployed in public companies, hospitals and retail environments, all of which have standards with which they must comply to stay in compliance with legislation and standards that have been adopted by their industries. Public companies must conform to the mandates of the Sarbanes-Oxley Act (SOX), enacted to protect shareholders and the general public from accounting errors and fraudulent practices in the corporation. In healthcare, one of the Healthcare Information Portability and Accountability Act's (HIPAA) efforts is to ensure that health data is kept private and secure. Finally, the Payment Card Industry (PCI) Security Standard is a set of requirements meant to ensure the security of credit cardholder personal information throughout the processes of purchase and transaction.

Each regulation carries penalties for failure to comply. A wireless protection system must have the ability to provide compliance reporting by collecting historical data on system activity and perform advanced forensic analysis of past network events. Such an ability to replay events and provide proof of compliance can save a company thousands of dollars in fines should a breach occurs while their system is operating in compliance.

Securing a WLAN requires diligence, but it can be accomplished with policy definition and enforcement of that policy with the appropriate tools. Begin by defining your security policy and determining who will be permitted to use wireless tools to support business activities. All user devices should be examined to ensure against their accidental misuse or intentional attack. Assess the cost or damage that would be incurred by your business if security was breeched. A thorough WLAN vulnerability assessment and business risk analysis helps determine where to focus your security budget. Next, provide your IT department with the proper monitoring tools. Then, enforce your policy by having IT step in when compliance is threatened.

Keeping the Network Secure

The advantages of the wireless enterprise are many. Convenience tops the list of benefits with mobile users being able to access network resources from virtually any location within their primary networking environment. Mobile access enhances productivity by enabling workers to access enterprise tools from remote locations. The networks can be deployed via a single access point and expanded with no need a lay cable to various locations. But along with the convenience comes the possibility of security breeches that must constantly be keep in check.

Monitoring software allows administrators to view all devices on the network and assess their status. In fact, IT can proactively identify and troubleshoot performance issues even before users report the problem. Such software generates reports on using defined KPIs, helping to prevent

**Motorola RF Management Suite**

Motorola's solution to the challenges of deploying, managing, monitoring and securing your WiFi network is the Motorola RF Management Suite. By providing complete visibility into your Wi-Fi network, the RF Management Suite simplified the complex task of managing your network.

Each of the four modules can be used individually or in concert with the others to create a network management system tailored specifically to the needs of your network and the enterprise it serves. Because the suite of network management tools enables data sharing across modules for a more complete picture of the state of your Wi-Fi network, it is more powerful when the tools are used together.

The RF Management Suite is comprised of the following modules:

**LAN Planner**
Enables the enterprise workforce to stay seamlessly mobile.
**MSP RF Management Edition**
Controls your end-to-end enterprise mobility solution from top to bottom.
**RF Management Software**
Speeds planning and monitoring of your Wi-Fi network.
**Wireless Intrusion Protection System**
Next-generation split intelligence architecture

costly network downtime. User intuitive GUI tools give administrators an immediate view of administrative problems, load balancing and throughput.

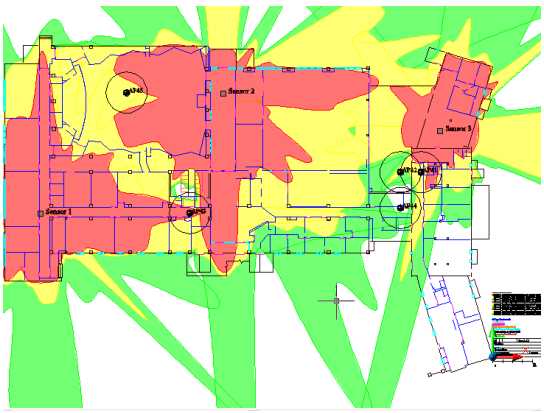
"Monitoring software allows network administrators a total view of the WLAN and showing the performance of all access points," said Kevin Goulet, Senior Director of Product Marketing at Motorola. "When intrusions are detection, rogues are located and disabled remotely, and forensics are provided that determine the root cause of an intrusion so that future incidents can be prevented. The device threat level varies from low, between neighboring APs, increasing to moderate for unauthorized APs in the building, higher when transferring date via a connected station and highest when there is a rogue on the network."

If a device is lost it can be locked down remotely by IT, preventing its unauthorized use or the procurement of confidential data. The monitoring system must detect and locate rogue devices, preventing intrusions to your WLAN. Beyond that, the intrusion protection system must also protect against denial-of-service attacks, providing an additional layer of defense from wireless attacks.

Growing Your Network

Many wireless LANS inched their way into the enterprise, starting as departmental solutions. As the enterprise began to realize the value of the wireless approach, many of these networks were incrementally deployed, often without a clear, long-term strategy. As organizations cobbled together these ubiquitous devices, they faced the challenges of optimizing and securing these networks and maintaining compliance.

Although disparate networks can be joined to create an enterprise solution, homogeneous networks are less difficult to manage. In fact, some experts advise against them. "A 'cobbled together' 802.11 WLAN is a security, performance, and support nightmare," said Devin Akin, Chief Technology Officer at The CWNP Program. "When improperly implemented, 802.11 WLANs can pose a significant risk to the security of any organization, and the cost of support alone can far outweigh the cost of implementing a new, single WLAN infrastructure."



*A tool such as Motorola LAN Planner, part of the Motorola RF Management Suite, simplifies the planning and design of a WLAN.*
*In this image of a building, designers can built a network identifying users and the clients they deploy.*

Ideally, WLANs are designed from the ground up using software tools that model coverage, and configuration is verified onsite via walk through. This approach is faster than manual methods, and can be done remotely. In addition, it reduces the number of costly changes that must be made post deployment. Single vendor management tools have the added appeal of enabling sharing of data and access through a single console, providing one point of contact for end-to-end WLAN infrastructure and device management.

For configuration and deployment, a device management software program allows IT to centrally apply firmware and configuration changes to a large number of mobile devices and WLAN infrastructure and, alert IT when devices are out of compliance. The days when devices have to be shipped to IT for software downloads are over; WLAN devices can be configured with information set over the wireless network in batches.

"The 802.11 standard has provided a Robust Security Network (RSN) platform flexible enough to address SOHO, SMB, and Enterprise market needs," said Akin. "Strong and scalable authentication and encryption mechanisms are easily implemented and interoperable across almost all vendors. The next big hurdle, addressed in the 802.11r draft amendment, is providing a fast, secure roaming mechanism suitable for real-time applications."

Gartner Security and Privacy analyst John Pescatore added, "When enterprises begin to deploy and support ubiquitous WLANs, they typically find significant overlap between their need for radio frequency (RF) monitoring to manage the wireless network and their need for such monitoring to detect security vulnerabilities and potentials intrusions. Many enterprises using third-generation WLAN systems have found that their monitoring needs can be met by integrated solutions that use the operational access points. But enterprises using older "fat" access points have more rigorous security need, requiring overlay WLAN monitoring approaches that use dedicated receive-only sensors."

According to Gartner, the number of mobile applications deployed by enterprises to their employees will continue to grow by 30 percent per year through 2011. A holistic WLAN management solution simplifies the transition from planning to ongoing monitoring, whatever the origins of the WLAN. By providing tight integration among components, such a system can secure even the most ubiquitous WLAN.