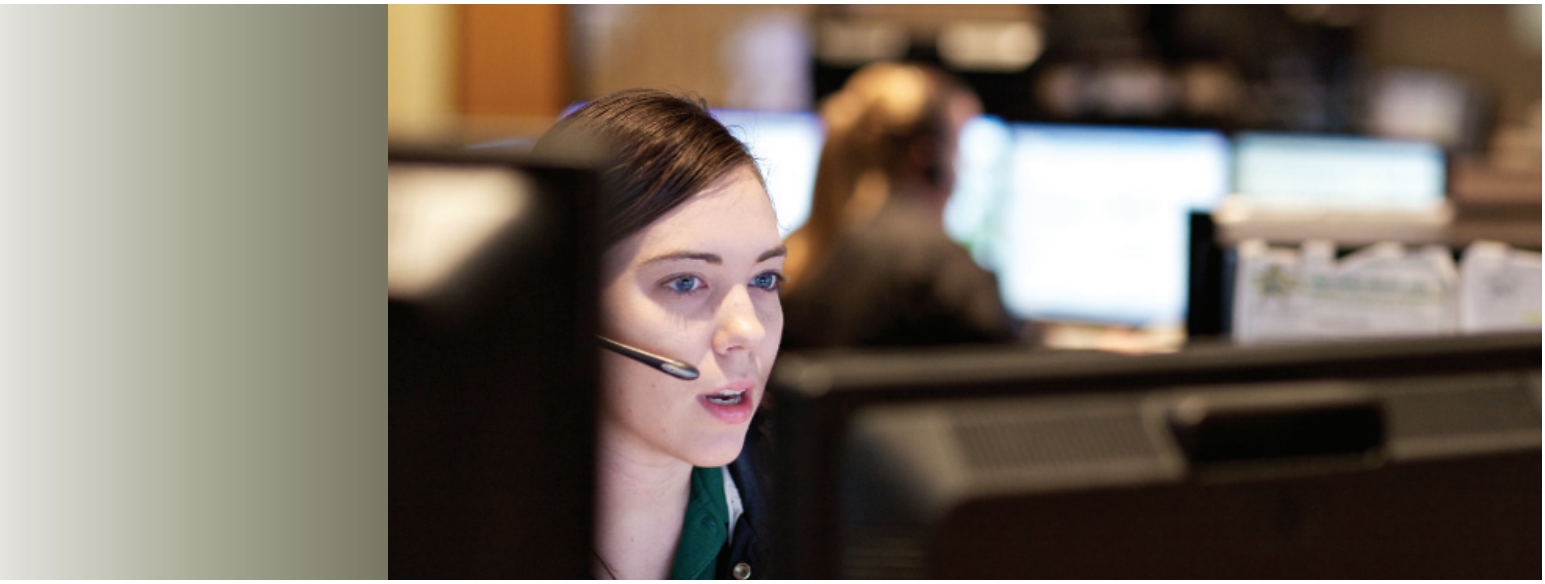


NETWORK SECURITY SOLUTIONS UNLOCK THE POWER OF WIRELESS LAN TECHNOLOGY FOR STATE AND LOCAL GOVERNMENT

TOP NEWORKING INVESTMENTS IN 2010

According to a recent study by the Enterprise Strategy Group, state and local governments will be among the biggest purchasers of network security and Wireless LAN equipment this year, followed by VoIP, WAN Optimization and 10Gb Core Network Upgrades.

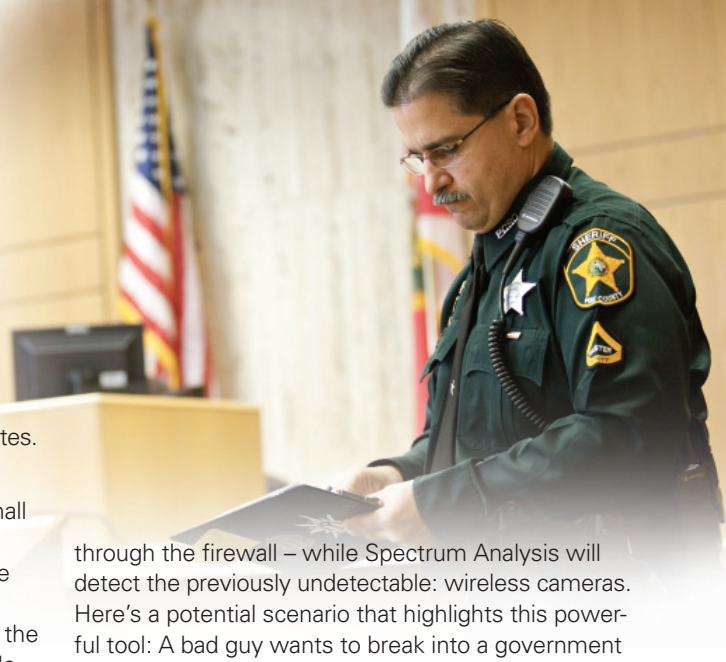
Source: Enterprise Strategy Group, 2010

Risk vs. reward. Most of us make decisions by weighing risks against achieving a desired outcome. As a government IT leader, you see the commercial sector using wireless network technology for real-time mobile connectivity and access to voice and data applications. Yet different risks and compliance standards have to be considered before making infrastructure investments. Network security is highly dependent on reliability – and mistakes can have a big impact on your operations and the public you serve.

Making Investments Count

Despite its pervasiveness in other industries, Wireless LAN implementations at the government level are still met with a bit of trepidation. Funding remains a challenge, so investments must be made carefully. Many state and local agencies first deploy wireless infrastructure as a trial across a small portion of their network. Once the value of mobility is realized, they may roll it out in phases to other departments, buildings, conference rooms, hallways and public spaces. While increased access and mobility deliver tremendous operational efficiencies and productivity gains, they also bring increased security threats and a number of government-specific compliance and regulatory requirements. Network security can't be compromised for new wireless capabilities being deployed.

One large state government administration in the Southwest U.S. sought to build an 802.11n wireless footprint to cover 22 municipal buildings, but wanted to prove the security and reliability of the Wireless LAN first, as the network was being accessed by government employees for administrative work and by guest users throughout the work day. The State



Bar Association also requested to have wireless connectivity added to courtrooms. This expansion meant having to comply with security standards at the federal, state and local level, including FIPS 140-2, SoX, HIPPAA, the Identity Theft Act and State Department of Information Resources mandates.

Numerous proprietary and overlay solutions were evaluated and beta tests were conducted over small portions of their infrastructure for several months. Our Motorola AirDefense Security and Compliance solution was part of this process, and we helped assess their existing infrastructure, current use of the network and future needs. We formulated a nimble, responsive and robust security solution that they ultimately selected to implement over other competitive offerings.

LEVERAGING "n"

This particular state administration had already made the decision to invest in 802.11n wireless technology. Given the advanced capabilities this network delivers, it's critical that the right security solution is deployed to monitor legacy equipment, support multiple vendor solutions and scale to cover advanced applications as needs demand. They wanted to make sure that if and when they had a network problem or coverage issue, it could be quickly addressed before impacting day-to-day operations and/or users. It also had to be easy to manage. Our AirDefense Security and Compliance solution with Advanced Forensics, Wireless Vulnerability Assessment and Spectrum Analysis modules fits the bill.

Initially, the AirDefense system rolled out in six buildings, with an average of five sensors in each building. For sensing, Motorola dual-radio AP-7131 access points were deployed. These band-unlocked radios can monitor the RF environment across the full spectrum, pose as a rogue client as part of a Vulnerability Assessment and offer the flexibility of being used for supplemental Wi-Fi access if desired to fill in coverage gaps.

THE BEST DEFENSE: OFFENSE

With our Advanced Forensics module, the IT team can monitor current and historical relationships and behaviors, making unusual access or activity easy to identify. The Wireless Vulnerability Assessment tool uses a simulated rogue client to test potential paths through the firewall – while Spectrum Analysis will detect the previously undetectable: wireless cameras. Here's a potential scenario that highlights this powerful tool: A bad guy wants to break into a government facility. He places a concealed wireless camera nearby and watches for traffic patterns and gaps in physical security. When a non-authorized wireless device transmits in such fashion, an automated alarm trips, the device is flagged and classified (for example, frequency hopping device X-10 cameras) while providing ample data points for device location tracking and extraction.

ENSURING THE PROPER AIR COVER

After putting the AirDefense Security and Compliance solution to the test, our customer overcame the risks associated with building a larger wireless network and has new confidence in the security and reliability of their Wireless LAN. As a result, they have already identified their next objective – making it their primary network. We look forward to helping them achieve that goal and enjoy the rewards of adding VoIP and new applications for streaming multi-media interviews and communications.

ABOUT MOTOROLA WIRELESS NETWORK SOLUTIONS

Motorola delivers seamless connectivity that puts real-time information in the hands of users, giving customers the agility they need to grow their business or better protect and serve the public. Working seamlessly together with its world-class devices, Motorola's unrivaled wireless network solutions include indoor Wireless LAN, outdoor wireless Mesh Wide Area Networks, Point-to-Multipoint, Point-to-Point networks and Voice over WLAN solutions. Combined with powerful software for wireless network design, security, management and troubleshooting, Motorola's solutions deliver trusted networking and anywhere access to organizations across the globe.

OUT WITH THE OLD…

The Wi-Fi Alliance deems Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) to be inherently insecure and is now instituting a phased plan to prohibit older protocols from its product certification testing. Here are the phases:

- **Jan. 1, 2011:** The Alliance will prohibit WPA (the version with TKIP for encryption) as a sole encryption method in the APs it certifies. However, WPA2 Mixed Mode (TKIP + AES) will be allowed in the devices.
- **Jan. 1, 2012:** The Alliance will prohibit WPA/TKIP in client devices in addition to APs.
- **Jan. 1, 2013:** WEP will be prohibited from Alliance-certified APs.
- **Jan.1, 2014:** WEP will be prohibited from Alliance-certified clients, in addition to APs. WPA2-Mixed Mode will also be prohibited.

MOTOROLA

www.motorola.com/airdefense