



HARRIS COUNTY ADOPTS PROACTIVE SECURITY STRATEGY TO ENSURE AVAILABILITY OF MISSION-CRITICAL SYSTEMS

CASE STUDY



Seated in the third most populous county in the nation, Motorola's ASTRO® 25 network in Harris County, Texas is unique in that it supports a vast region comprised of 13 counties surrounding Houston and Galveston. Harris County works with providers across 1,788 square miles in every aspect of public safety, including military and federal (U.S. Coast Guard, U.S. Army, FEMA, FBI) and state and local (law enforcement, fire, EMS) authorities, as well as other first responders.

Its mission is straightforward—to protect citizens from danger and save lives—but crucial success depends on reliable, real-time voice and data communications between over 400 dispersed public safety agencies in the midst of a major disaster, as well as on a day-to-day operational basis. This region is home to international shipping ports as well as petrochemical and nuclear power facilities, and frequently experiences severe weather along the Gulf Coast. First-responder access to the right information at the right time translates into reduced emergency response times and fewer fatalities.

Balancing Benefit and Risk



Harris County demonstrates a long history of proactively managing security concerns via its comprehensive and far-reaching Information Technology Center. Recently, the county recognized the need to extend its aggressive security strategy from the IT world to its public safety radio network, addressing a unique security frontier. Expanding the functionality of its public safety radio network allows it to take advantage of advanced IP-enabled technologies that support improved coverage and uninterrupted communications in both large rural and dense urban areas.

While recognizing the benefits of improved interoperability among first responders, county officials also understood that expanded capabilities would introduce new security threats to its mission-critical network. Protecting the specialized radio network and its related technologies clearly required the expertise of a trusted partner familiar with managing security in that environment. Simply applying established IT solutions would be ineffective for the public safety network, which has a unique purpose and, therefore, requires different policies to govern behavior.



Motorola Security Services helps government, enterprise, and network service provider customers identify and mitigate security risks that threaten the business, operational and productivity benefits of enterprise mobility.

Working With a Practitioner

Motorola offers a practitioner-based approach to security, whereby the day-to-day operational security of its own networks is managed by the same professional team that manages security for its clients—bringing operational experience to the forefront to better understand customer concerns and pain points. “Motorola designs these networks, operates equipment on these networks, and constantly monitors the security of technologies that run on these networks,” explains Sam Cattle, Engagement Manager for the Harris County assessment team.

With an ASTRO 25 network already in place, Harris County is a well-recognized Motorola reference customer in the government sector. Given its unwavering commitment to provide first responders with the best available tools and technologies to do their jobs effectively,

Harris County added digital IP-based voice and data services to its ASTRO 25 network—brand new territory for many radio networks. The resulting convergence of voice and data IP-based services provided a perfect opportunity to showcase Motorola’s ASTRO 25 Security Evaluation and Design Service (ASED). This service is designed for customers that have or are planning to implement an ASTRO 25 network. It evaluates the customer’s overall deployment environment, including existing IT network infrastructure, from a security perspective to identify issues that could impact or threaten the business and mission.

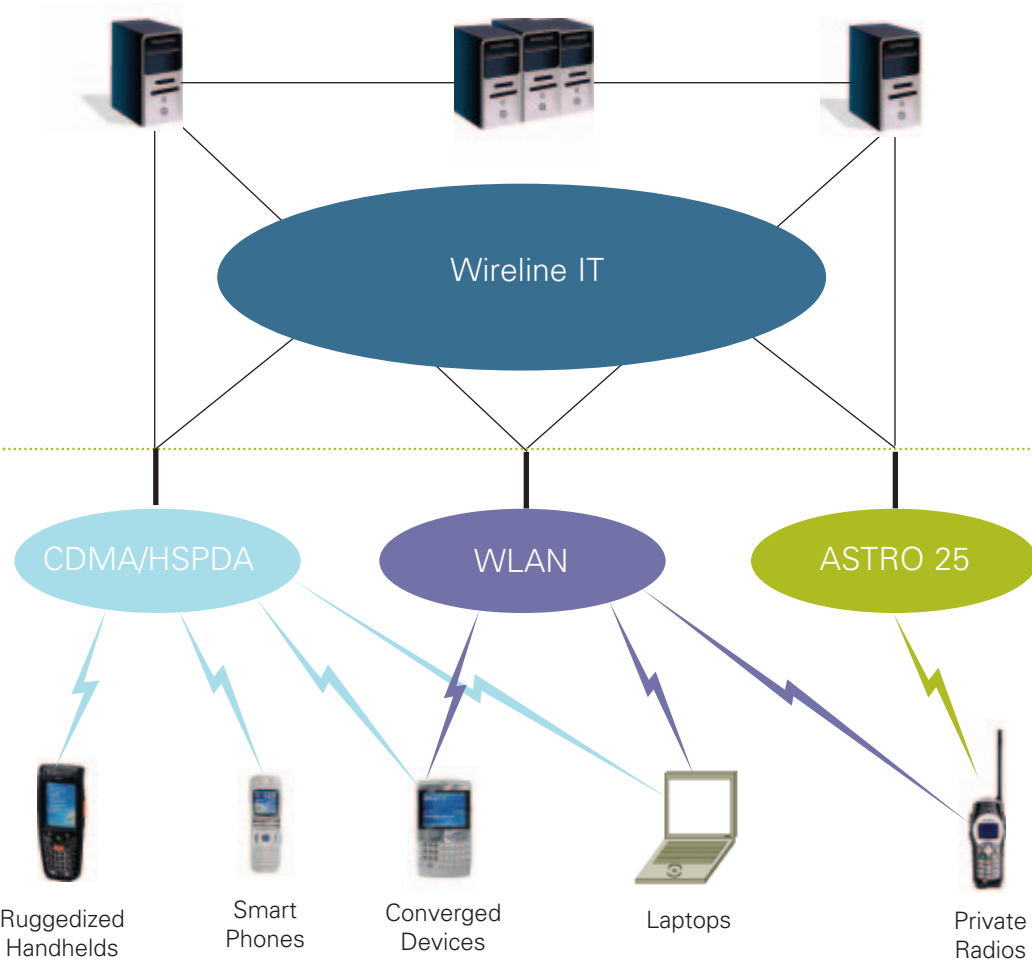


“Ours is a growing system in a constantly evolving environment, so there are always security issues.

When Motorola approached us with the concept of a security assessment, we were very receptive. It’s easy to get bogged down in your daily routine, with the mindset that ‘this is the way we’ve always done things, and it works’... but, things change. I was very open to having Motorola look over our shoulders and help us bring our security deficiencies to light.”

**-David Dodson, Division Chief,
Harris County Regional Radio**

Data Center and Emergency Management Resources



Networks attached to the Harris County core network include: the ASTRO 25, 802.11 WLAN, CDMA 1xEV-DO (Verizon), HSDPA (Cingular), and a wireline IT network supporting over 30,000 first-responder subscribers.

A Unique Engagement

The Motorola Security Services team performed its high-level Security Evaluation and Design Service in conjunction with Harris County's deployment of an upgrade to its public safety communications network in the form of Motorola's ASTRO 25 network—a third-generation digital wireless solution specifically designed for mission-critical applications.

The team identified security configuration and design vulnerabilities that could lead to system outages in the core network, as well as system compromises exposing sensitive government

data and communications. Given the size and scope of this network, and the number of access technologies involved, Motorola examined all the interconnection points to obtain a true sense of potential security weaknesses. Networks attached to the Harris County core network include: the ASTRO 25, 802.11 WLAN, CDMA 1xEV-DO (Verizon), HSDPA (Cingular), and a wireline IT network supporting over 30,000 first-responder subscribers.



Objective Perspective Promotes Awareness

Although Harris County already possessed a good sense of most of its potential security vulnerabilities, many were perceived as small, individual concerns that could be addressed if and when they became critical. Missing from this perspective, and revealed in the Motorola assessment, was the understanding that all these individual vulnerabilities could converge and together threaten the availability of the mission-critical network at large. Thus, an immediate customer benefit of the engagement was a significant increase in awareness regarding the magnitude and impact of specific security issues in this particular environment.

While many findings in a security assessment report involve objective evaluations of technology that suggest corrective action, internal political elements often are stronger catalysts in driving decisions. For example, a security technician may perceive an assessment as a threat to his/her position, but, essentially, the evaluation aims to identify gaps in policy and resources, and reduce complexity, with the end goal of making the technician's job easier.

Also, friction and power brokering between government agencies and jurisdictions can hinder implementation of new policies and processes. So, when the Motorola team—external, independent experts—makes authoritative recommendations (in written report form), security concerns previously voiced internally often gain additional credibility.

Securing networks is about more than applying security controls and devices. It involves users, end-to-end applications, and the total environment. A holistic approach to security encompassing people, process, policy and technology is essential to securing a customer's networks and information. Otherwise, the "solution" is just a box—a Band-Aid with short shelf life. In addition, even though customers may not control all the devices on a network, they need to assume a level of authority that justifies requiring all subscribers to have a minimum level of security since there are critical resources on the network that could be compromised by corrupt devices. Motorola can help customers implement and manage this more holistic approach to security.

"Anytime you have government entities working together in a complex organization involving multiple agencies, you potentially run into territorialism issues. But, when a third-party validates a security vulnerability issue, for example, it becomes easier for one internal agency to ask another for help securing the network."

-Ben Zotyka
Motorola Account Manager



A carefully integrated security strategy involving people, process, policy and technology ensures the availability of mission-critical networks, which allows first responders to fulfill their mission to protect lives and property.

Availability Most Critical Aspect for ASTRO 25 Network

“Understanding wireless security threats and their resulting system impact is critical to the success of ASTRO 25 and other wireless technologies that render mission-critical services,” explains Cattle. He notes that even minimal downtime can equate to delayed emergency response times and the potential loss of life.

Availability is the most critical aspect of security for ASTRO 25 and its mission in a public safety or first-responder environment, as evidenced in the

Harris County engagement, where a security glitch in the network leading to possible shutdown would be catastrophic given the number of touchpoints involved in such an extensive coverage area. “When uniting multiple networks into one end-to-end network environment, each technology involved has associated security concerns. It is at the point of integration that significant security mistakes can be made,” observes Cattle.



Motorola's Security Evaluation and Design Service

"ASTRO 25 offers robust security features, but the environment where the system is deployed often can introduce security-related vulnerabilities," emphasizes Cattle. That's why Motorola recommends performing this security service with system deployment. Motorola's ASTRO 25 Security Evaluation and Design Service analyzes the customer's environment, evaluating architecture, as well as policy and procedure.

The Motorola team examines points of vulnerability in the core IP network environment and recommends actions to prevent remote hacker and insider attacks. Security breaches can result when companies skip Motorola's Security Evaluation and Design Service prior to system installation. Proactively identifying security gaps early on, prior to a potential crisis, is far more effective and less costly than the alternatives.

"We were fully satisfied with every aspect of this engagement," said Dodson. "The Motorola team's project management, quality of service, responsiveness to our needs, technological knowledge, professionalism, and recommendations offered in the findings report met or exceeded our expectations. We were impressed with how well Motorola Security Services understands our business and the mission of our network, and how the team's security findings impact both."



Conclusion

Harris County used the data in Motorola's assessment summary to enhance its network security policies and bolster evidence to requisition additional resources and equipment. Among Motorola's major findings was an understaffed security organization. "We're doing the best with what we have, but it was certainly helpful to have an objective third-party entity validate our resources situation," remarked Dodson.

"Our assessment specified the additional resources needed to provide the appropriate level of service, as well as the potential ramifications of not taking action," explains Zotyka. The cost associated with additional employees usually is far less than the expense associated with a crisis like system failure.

"The Motorola documentation stood on its own," says Dodson. "The Motorola team provided a straightforward look at our vulnerabilities and recommended actions. The information was delivered supportively, rather than as criticism, encouraging us to take the necessary steps to further secure our already reliable system to maintain it as a rock-solid network for the future."

The Harris County engagement highlights the additional complexities, and therefore vulnerabilities, inherent in networks and systems that serve a broad user population, dispersed geographically, functionally, or both. In these environments, Motorola's proactive approach to security proves to be particularly invaluable.

About Motorola Security Services

- Proven expertise in voice and data security for service providers, governments and enterprises
- Established track record of delivering design and implementation of complex infrastructure networks that are supported by a full range of professional and managed security services
- Holistic security framework that operationalizes security across the people, process, policy and technology foundations of each organization
- Practical hands-on experience with vulnerability assessment and mitigation, as they relate to threats associated with converged networks
- Onsite Security Assessments: Two-Way Radio Network, WLAN, WWAN, UMA, IMS, CDMA, GSM/GPRS, UMTS, Physical and Facilities
- Defense-in-Depth Threat Management (Design, Managed Service, Integration) expertise
- Policy Design and Related Services (Incident Response Planning, Risk Management, Compliance)

About Motorola Services

Motorola Services, based on innovative technologies, delivers optimal solutions and managed services for service providers, governments and businesses. Motorola offers a comprehensive portfolio of cost-effective, high-performance services and applications that are robust and operational in critical multi-vendor,

multi-technology environments. We leverage deep expertise in mobility, security and systems integration to deliver seamless communications. Motorola Services collaborates with customers to understand their needs and help them achieve their organizational objectives.

About Harris County

The largest county in Texas and the third largest in the nation, Harris County, supports a vast region comprised of 13 counties surrounding Houston and Galveston. Harris County works with over 400 public safety agencies dispersed across 1,788 square miles of the state in every aspect of public safety, including military, federal, state and local

authorities. Its mission is to protect citizens from danger and save lives in a region that is home to international shipping ports, petrochemical and nuclear power facilities, and severe weather along the Gulf Coast. Harris County Regional Radio is a division of the county's Information Technology Center (ITC).



MOTOROLA

Motorola, Inc.

www.motorola.com/services/government

MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. All other product or service names are the property of their respective owners. © Motorola, Inc. 2007

0107HCCS