TOP 5 MOBILITY CHALLENGES GOVERNMENT CAN NO LONGER IGNORE

OVERVIEW

Mobility is transforming the way government enterprises and citizens interact with each other and share information. In fact, mobile devices are fast becoming one of the greatest public safety tools, with more than 400,000 wireless 9-1-1 calls made each day.[1]

Mobile applications are proliferating quickly, too. According to Gartner Inc., they are projected to increase tenfold by 2015. Yet while 71 percent of organizations already use or plan to use mobile applications, most are not confident about their mobility expertise.[2] Out of 11 key capabilities, IT departments rate themselves lowest on the skills and expertise needed to customize, manage and maintain mobile applications and platforms in-house.[3]

400 THOUSAND CALLS MADE TO 9-1-1 FROM MOBILE PHONES EACH DAY

71% OF ORGANIZATIONS LACK CONFIDENCE IN THEIR MOBILITY EXPERTISE

IT RATES THEMSELVES **LOWEST ON SKILLS** TO MANAGE MOBILE APPS AND PLATFORMS IN-HOUSE

TEXT

Meanwhile, citizens across the country are relying on mobile technology and social media to communicate and collaborate. They expect immediate access and instant engagement with government organizations – whether it's a text sent to 9-1-1 or access to a real-time public safety announcement video.
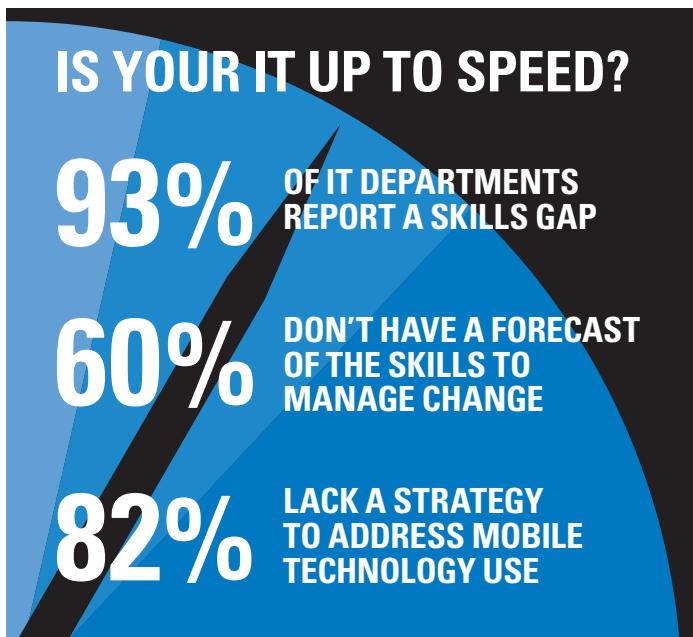
Government organizations are being pressed to be more responsive to citizens – to reduce crime, improve public safety and increase productivity. They must deliver more with diminishing dollars and fewer resources. Many simply do not have the infrastructure, people, processes and specialized skills to make it happen – or make it happen quickly enough.

As networks, devices and applications converge, they introduce a new level of capability, but simultaneously create a need for new skills to effectively manage this new environment. Maintaining mission critical readiness can become even more challenging as organizations work to deploy thousands of devices, stream sensitive data across an IP broadband network and connect hundreds of applications and databases.

GOVERNMENT IT LEADERS ARE ASKING

" **IN THIS DYNAMIC AND COMPLEX ENVIRONMENT, WHAT IS THE MOST EFFECTIVE WAY TO PLAN, IMPLEMENT AND RUN IT ALL?** "

THE CHALLENGE: MANAGING EVERY MISSION CRITICAL ASSET

If you're a government CIO, your purview covers a full spectrum of departments, from state IT management to the mayor's office, public service to public safety with its mission critical requirements. You may be responsible for governance over a mixed network environment – including radio, wireless LAN and both public and private LTE networks. How will you successfully deliver services built around new wireless technologies? Ensure these technologies perform in mission critical applications?

As the number of users expands, you need to manage mobility without losing focus on your core mission. And you are being challenged to keep up with the fast pace and broad spectrum of technologies your IT must manage. You may be wondering how your organization can best allocate resources or execute a successful strategy – especially if the bulk of resources are devoted to network, device and application maintenance.

IS YOUR IT UP TO SPEED?

93% OF IT DEPARTMENTS REPORT A SKILLS GAP

60% DON'T HAVE A FORECAST OF THE SKILLS TO MANAGE CHANGE

82% LACK A STRATEGY TO ADDRESS MOBILE TECHNOLOGY USE

THE REALITY: MULTIPLE FACTORS AFFECT MOBILITY IMPLEMENTATIONS

1. **Technology is changing rapidly** and with it comes a newfound level of power and capability. Citizens are embracing devices and expecting greater mobile access and use. Yet seasoned resources at the IT level are scarce as ever-changing technology requires an ever-changing set of specialized skills. Ninety-three percent of IT organizations report a gap between skills they have and those they need.[4] Over 60 percent lack a comprehensive forecast of the skills needed to manage change.[5]

2. **Resources are focused on maintenance,** making it difficult for government CIOs to execute a coherent strategy to progress their initiatives. Only 18 percent of organizations have a strategy in place to address the changes in mobile technology use and adoption.[6]

3. **Security concerns are impacting the ability to move quickly.** IT leaders are wondering how to maintain control and make security upgrades to their devices and applications as more employees bring consumer devices to work. 86 percent of IT leaders said police officers in their districts use their own devices for work-related activities.[7]

4. **Speed of deployment is slowed by the lack of standardized processes.** Technology roll-outs can be slowed by the time it takes an organization to evaluate, stage, establish logistical support and integrate new and existing processes.

5. **Predictable spending and forecasting are elusive** as government organizations seek to achieve the optimum financial structure for their services. Too often, a long wait for funding can hamper the ability to adapt.

THE FACT: GOVERNMENT ENTITIES ARE TRANSFERRING RISK AND GAINING RESOURCES

Government agencies are looking outside their offices to trusted providers with the expertise to manage their network infrastructure, devices and applications. They want to make sure all their powerful new technologies, tools and applications are most effectively utilized. When they gain access to a level of specialization, expertise and logistical support, then implementing new technologies – such as next generation command centers – becomes easier and trouble-free.

For example, your agency may be deploying a growing mix of devices, a number of new applications or grappling with the BYOD movement as employees use their own smartphones and tablets at work. Managing all those applications and devices can pose a tremendous challenge. Instead, you can mitigate the risk and optimize your resources by relying on the expertise of a service provider with a track record of successful implementation.

Or your P25 radio network may be in need of important technology upgrades as your footprint grows and your infrastructure faces unplanned obsolescence. By transferring the risk and complexity to a trusted provider, you address the issue with a predictable budget each year. They can help you plan and implement upgrades – assuring critical technology remains current and effective.

THE OPPORTUNITY: LEVERAGE TRUSTED TALENT AND EXPERTISE

Managing networks, devices and applications externally provides a level of specialized skills and advanced capabilities you may not have in-house. By leveraging the expertise of a trusted advisor, you bridge the gaps in people, skills, infrastructure, business process, logistics and financial resources. You benefit from astute guidance and specialized solutions – especially as the demand for wireless grows, the universe of mobile apps expands, and you are pressed to accommodate both trends.
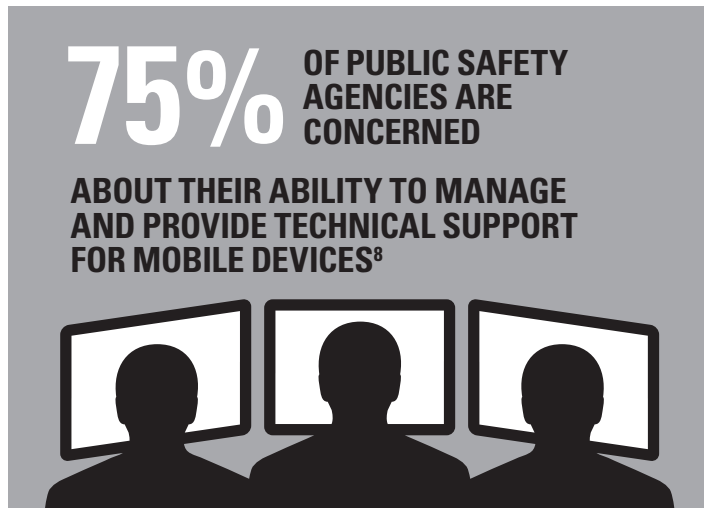
Managing networks, device and applications externally frees your IT teams to focus on your core mission. Rather than being held hostage by maintenance issues, they can redirect their attention to the strategic initiatives that build value for your citizens and spur innovation.

Finally, you can opt for a payment model that is flexible and spread out over an extended period. You get recurring, predictable payments you can budget for, along with regular and planned migrations, plus the confidence your networks, devices and applications are operational around-the-clock.
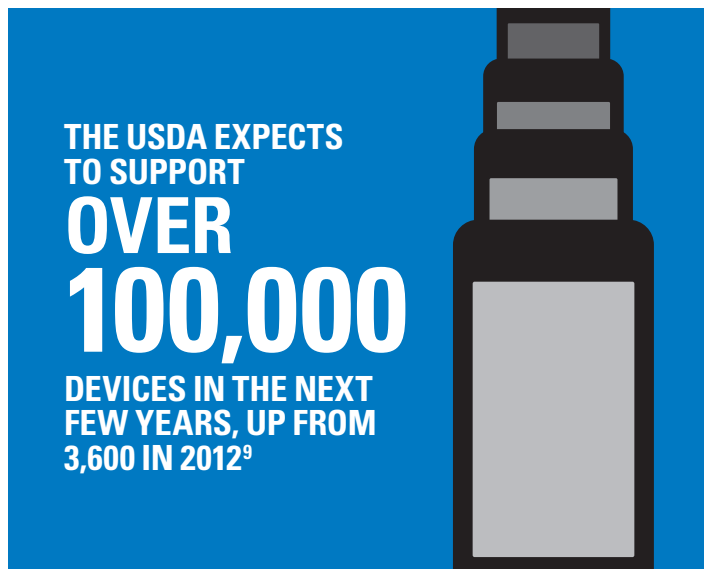
86%
OF IT DECISION MAKERS SAY PUBLIC SAFETY OFFICERS ARE USING THEIR OWN CONSUMER GRADE DEVICES

OVER 50%
WANT OFFICERS TO USE DEVICES SPECIFICALLY DESIGNED FOR PUBLIC SAFETY PURPOSES[8]

75% OF PUBLIC SAFETY AGENCIES ARE CONCERNED
ABOUT THEIR ABILITY TO MANAGE AND PROVIDE TECHNICAL SUPPORT FOR MOBILE DEVICES[8]

THE USDA EXPECTS TO SUPPORT **OVER 100,000** DEVICES IN THE NEXT FEW YEARS, UP FROM 3,600 IN 2012[9]

84% OF IT DECISION MAKERS SAY OUTDATED TECHNOLOGY PRESENTS A SIGNIFICANT CHALLENGE TO THEIR ABILITY TO ENSURE PUBLIC SAFETY[8]

IMPROVE THE LEVEL OF SERVICE TO YOUR COMMUNITY

A managed services model is a compelling approach for planning, implementing and running operations. By working with a trusted advisor, your organization gains access to technology, maintenance and management, as well as processes, documentation and reporting capabilities that may be unavailable through your internal resources. A trusted advisor can keep you up-to-date while preparing your technology to be future-ready.

A managed services model can help your government enterprise keep up with technology with less capital expenditure and deliver comprehensive network and operations support for every public safety user. Bottom line, it mitigates your risks, improves your performance and contains your costs.

A major State, for example, turned to a managed services provider to fund their public safety-grade communications system. The provider furnished the resources for 24x7x365 system operations and support,

supplied the expertise to expand the system as needed, kept pace with changing technology and shifted operations, service level commitments and support responsibility outside.

IMPROVE YOUR DECISION-MAKING AND RESPONSIVENESS

By using a managed services model, you get optimized capabilities for better decision-making, improved responsiveness, expected governance and increased performance from your technologies. You increase the speed and flexibility of your government enterprise – so you can implement solutions faster, use smarter mobile technologies and manage your fleet of devices and assets more efficiently.

You reduce your operational risk and benefit from assured outcomes you have established – whether it is running mission-critical applications in a secure data center or making sure your wireless LAN system is properly maintained. Since success is defined in terms of a Service Level Agreement (SLA), both you and your provider are aligned in targeted goals and expected performance.

Now more than ever, as mobile technologies evolve, agencies strive to improve safety and citizens demand more, government entities are discovering the powerful advantages of partnering with a proven provider to manage their network infrastructure, devices and applications.

A managed services solution delivers expert capabilities, promised performance and assured outcomes. It is the best practice approach more government entities are relying on to cut through the confusion, manage the complexity, and help them plan, implement and run it all.

SOURCES

1. CTIA Research, 2012

2. State of Mobility Survey, Symantec 2012

3. Mobile Survey, VDC Research, April 2011

4. State of the IT Skills Gap, CompTIA, February 2012

5. "Evolving IT Skill Sets: Seven roles that should be on CIOs' radar", Corporate Executive Board, 2012

6. www.sap.com/solutions/technology/enterprise-mobility/resources/mobilecio.epx

7. Motorola Solutions "Public Safety Data Communications Technology Survey", January-February 2012

8. Motorola Solutions Public Safety Communications Technology Survey, KRC Research 2012

9. http://gcn.com/articles/2012/08/21/usda-next-generation-mobility.aspx

For more information on how to manage network, applications and devices, visit **motorolasolutions.com/services**.

MOTOROLA