



GOVERNMENT IT SURVEY RESULTS REVEAL KEY DATA PRIORITIES

BETTER DATA COMMUNICATIONS CAN IMPROVE PUBLIC SAFETY PERFORMANCE

OVERVIEW

Our government agencies ultimately align to one clear focus: to help our cities become places where people and businesses want to establish themselves. Government leaders understand the need to continually improve public safety performance in order for our cities to thrive.

However, these leaders continuously contend with the fact that taxpayers want to pay less, but still expect improvements and advancements in protection, safety and service – resulting in the economic challenge of doing more with less. And, with the growing ability for the public to view performance metrics, citizens are paying more attention and government leaders are facing increased scrutiny and added pressure to move performance numbers in the right direction.

One of the most aggressive changes in the government and public safety environment is technology's rapid acceleration; often, the public's access to and proficiency with technology exceeds that of first responders and government workers.

The first people on the scene are the victims and the witnesses.

They can capture images, send text, record video – creating data that government needs, and they expect public safety and service departments to be able to use what they provide. Just about every incident has someone there with a cell phone, ready to document it, and the public has a propensity to call the media. To add to the urgency, NG9-1-1 is now in process, forcing departments to think ahead about how they are going to respond to this change.

Criminals have increasingly sophisticated tools and it only gets harder and harder to keep up. Bombs are being detonated over cellular devices; offenders are getting good at hacking, leveraging data and communications off the public network to their advantage and to everyone else's detriment. The public network is now a target for bad actors; and it's accepted that we cannot rest public safety organizational performance goals on something this vulnerable.

Front line responders also have rising expectations. They know there is data out there that can help them do their jobs more effectively, or perhaps even save their lives. These first responders apply steady pressure on government leadership to provide them with that data and those tools. In many cases, responders are already using their own communication devices as workarounds while they wait for their departments to procure the tools they need.

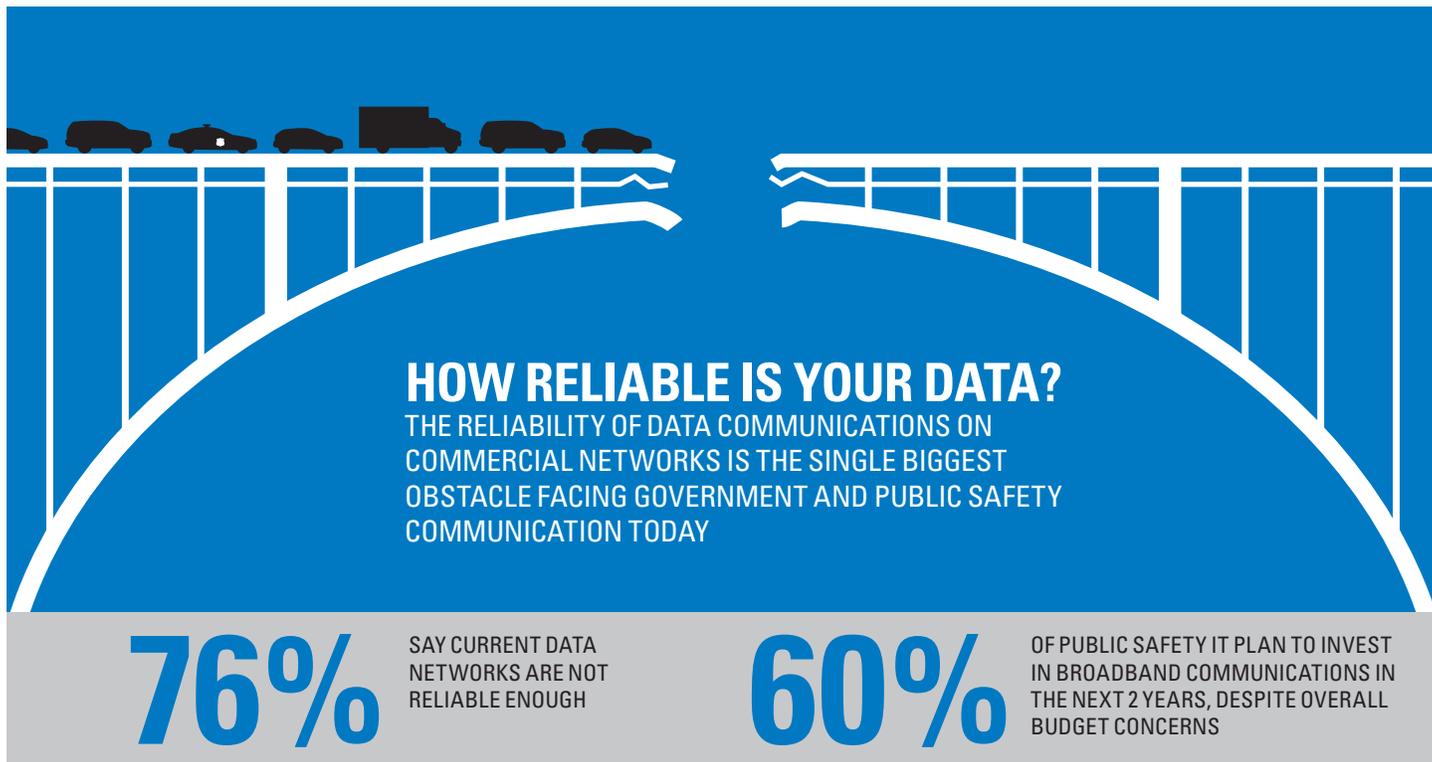
As communications technology evolves and next generation capabilities start to transform the functions of government and public safety agencies, Motorola continuously engages with US government and public safety IT decision makers to understand their top priorities.

As part of this effort, we conducted a comprehensive blind survey in February 2012, asking 250 US county, city and state level decision makers about their current technology needs, concerns and investment plans for data communications. This paper highlights their views on the reliability of existing data communications networks, the need for dedicated mobile broadband networks and their desire for devices built specifically to meet the unique needs of public safety communications.

94% BELIEVE INVESTMENTS IN PUBLIC SAFETY HAVE A POSITIVE IMPACT ON ECONOMIC GROWTH



KEY PRIORITY: RELIABILITY OF CURRENT DATA COMMUNICATIONS NETWORKS



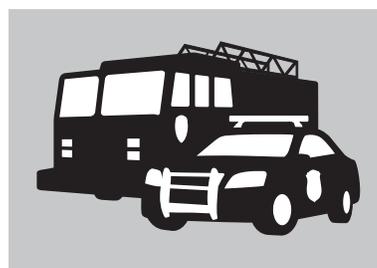
Survey respondents cite the reliability of existing data communications on commercial carrier networks as a significant concern. When asked how dependable their current carrier data communications network is in supporting all of their government data needs during emergencies, 76 percent indicated it is only “somewhat reliable” or “not reliable at all”.

Carrier networks are designed to serve the public during normal, peak demand periods, not in times of crisis. When a major disaster strikes, such as the 2011 East Coast earthquake, carrier networks, and the data applications depending on them, typically cannot sustain the massive call volume. Service disruptions from cell tower damage exacerbate the problem; in the aftermath of Hurricane Irene in 2011, 6,500 carrier network cell towers suffered damage, causing service disruptions along the East Coast from North Carolina to New Jersey. Private, dedicated, mission critical land mobile radio (LMR) networks,

on the other hand, continued to operate with minimal disruptions, allowing first responders to communicate and coordinate disaster response efforts with voice and data communications. That’s the level of data communication reliability that all first responder require in times of need.

Most government and public safety IT decision makers say they will invest in advanced broadband communications technology in the next two years.

- 60 percent indicate investments will likely include private mobile broadband to support advanced data communications capabilities
- That number grows to 70 percent in larger jurisdictions with 100+ public safety officers and government users



As they weigh options and investment strategies, agencies are turning to standards-based private Long-Term Evolution (LTE) networks to help achieve their future plans for mobile data applications. With the increased bandwidth delivered by LTE, first responders and mobile government workers will have access to high-speed connectivity and the ability to transmit large amounts of data and video to and from the command center, from patrol car to patrol car, or even from smart handheld device to smart handheld device in the field.

In the wake of both routine and large-scale weather emergencies and disasters, public safety agencies worldwide are looking for network technology that delivers needed insurance, along with the capacity, interoperability and reliable access, required to keep them connected when it matters most. While commercial wireless networks can’t always ensure these needs are met, Public Safety LTE solutions offer the control, reliability and security at the core of dedicated, mission critical technology.

CRITICAL TOOLS FOR PUBLIC SAFETY OPERATIONS



KEY PRIORITY: ACCESS TO SECURE, PRIVATE MOBILE BROADBAND

Two of the most important tools in public safety and government operations are reliable communications and relevant information. The ability to provide up-to-date information to the right resources at the right time over a secure network is critical to keeping first responders and citizens safe. Some agencies are using 3G and 4G commercial networks to deliver information to first responders today; however, many of them are concerned about data security and reliability, and would prefer the added safety of a dedicated, private network.

- In fact, 97% of the government and public safety IT decision makers surveyed cited the importance of having a dedicated and private mobile broadband communications system to support their operations.
- In addition to the need for reliability, survey respondents also shared their data security concerns: 87 percent indicate they are worried about the threat of criminals hacking government information over a public network that they don't control.

Dedicated networks provide a reliable way to deliver citizen-generated multimedia content to first responders. 72 percent of survey respondents want the ability to use the video and text messages provided by citizens at the scene of an incident to help mobilize public safety officers and make smarter, faster decisions. And, 60 percent of them say they have already experienced how text messages and pictures captured by the public have helped meet public safety needs in their jurisdiction.

At the same time, a dedicated public safety network can capture public safety's own records about an incident, which can be very important if multimedia information is used to question public safety response performance. In our survey, 60 percent of decision makers recognized that user-generated content such as texts, Web posts and photos could be used by the media to criticize their response time and effectiveness.

Seeing the new capabilities that Public Safety LTE offers, agencies in the US are interested in deploying LTE to get more reliable and secure mobile data access.



KEY PRIORITY: RUGGED, SECURE DATA DEVICES

While waiting for access to dedicated broadband networks and broadband devices specially designed for public safety use, many jurisdictions are relying on carriers and consumer-grade devices such as smart phones and tablet computers for their data connections.

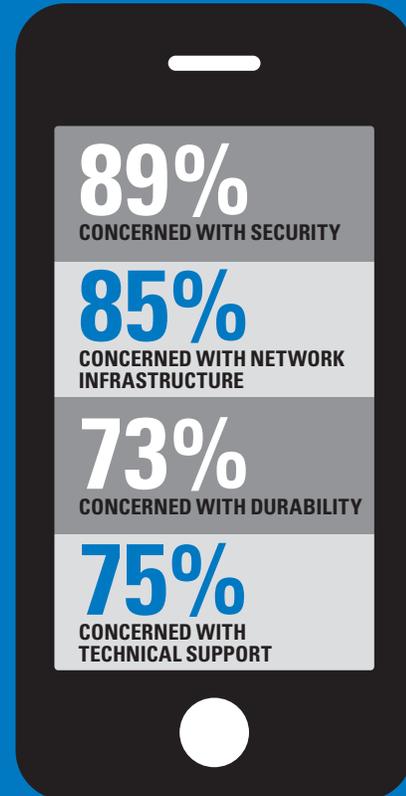
- 86 percent of survey respondents said police officers in their jurisdictions currently use their own consumer-grade devices for work-related activities
- 89 percent of government and public safety IT decision makers are worried about allowing the use of consumer-grade devices without an advanced and unified communications infrastructure
- More than 9 in 10 (95 percent) in city jurisdictions are concerned about the security of consumer-grade devices, including the unauthorized access to confidential data that could result from a lost phone
- More than half (51 percent) would prefer to invest in communication devices specifically designed for public safety

During mission critical operations, devices specifically built for public safety offer not only security, but also a number of other advantages over their consumer/commercial counterparts. A rugged form factor stands up to heat, cold, rain, and dust as well as the challenges of prolonged daily street use. And rugged, secure, devices built for public safety can also cost less to operate.

According to a report on Mobile Computing by the International Association of Chiefs of Police (IACP), the percentage of savings in time, personnel, money, consumables, accuracy, and safety can be a lot more than you might expect, often between 20-40 percent. A 2010 report from VDC Research notes that the average five-year total cost of ownership (TCO) for a consumer device is 33% more than a rugged, enterprise-designed handheld; the variation in TCO is based on the maintenance cost for supporting, securing and managing the device, as well as the cost of lost productivity.

With the range of device choices that will be available to government and public safety agencies, it is likely that a mixed fleet of rugged and more consumer-like devices will be in service for differing user environments and needs. Although over half of the respondents preferred purpose-built devices, 39 percent are still considering consumer-grade devices while

CONCERNS WITH CONSUMER GRADE DEVICES



expressing security concerns. For a complex mixed-device environment, a simplified and unified device management tool will help ensure consistent security policies are enforced and application performance can be more consistently managed.

51% PREFER TO INVEST IN DATA DEVICES SPECIFICALLY DESIGNED FOR THE UNIQUE PUBLIC SAFETY ENVIRONMENT

51% WANT DEVICES SPECIFICALLY DESIGNED FOR PUBLIC SAFETY USERS

39% CONSIDERING CONSUMER-GRADE DEVICES

7% PREFER MIX OF BOTH

PAVING THE WAY FOR NEXT GENERATION INVESTMENTS

Access to robust data and mission critical applications has become as vital to first responders and mobile government workers in the field as voice communications, moving from a “nice to have” to an essential capability. The reason is clear. With the public more connected and data savvy than ever, their expectations of what’s possible have changed dramatically along with the rapid advance of technology.

Today, government and public safety IT decision makers face a number of critical communications challenges to meet those growing expectations. This survey shines a light on many of them. It also validates just how important having reliable data communications, dedicated private mobile broadband and mission critical purpose-built devices are to their operations. Intelligent connectivity helps prioritize user access, supports mobile devices, ensures maximized interoperability and keeps officers in the field more productive and safe no matter where a call may take them. That’s the real power of next generation government and public safety communications networks.

As a leader in innovation, Motorola Solutions conducts surveys like this along with other ongoing engagement activities to further deepen our understanding of customers’ needs, concerns and technology investment goals.

GOVERNMENT AND PUBLIC SAFETY DATA COMMUNICATIONS TECHNOLOGY SURVEY METHODOLOGY



Respondents covered a diverse group of government and public safety IT decision makers with 51 percent in technology roles and 49 percent in public safety leadership roles. 92 percent of respondents have six or more years experience in managing communications technology, with 56 percent reporting 16 or more years of experience.



The telephone survey was designed and executed by KRC Research, a leading public opinion and strategy firm, based in Washington, D.C., and conducted among 250 government and public safety IT decision makers between Jan. 25 – Feb. 27, 2012. To participate in this blind survey, respondents had to be responsible for purchasing decisions, or planning and acquisition decisions, for technology used by public safety personnel in their jurisdictions, as well as be familiar with the data communications used by public safety officers in their jurisdictions.

WHITE PAPER

GOVERNMENT IT SURVEY RESULTS REVEAL KEY DATA PRIORITIES

SOURCES

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

http://www.computerworld.com/s/article/9219567/Irene_s_wrath_leaves_6_500_cell_towers_out_FCC_says

"Mobile Computing Technologies", IACP Technology Desk Reference, International Association of Chiefs of Police, 2006, page 135

"Total Cost of Ownership Models for Mobile Computing and Communication Platforms, Third Edition, Track II, Volume 4: Public Safety", VDC Research Group, 2012, page 24

Next generation technologies are transforming government and public safety organizations by allowing you to collect the information flowing between citizens, responders and agencies, make this information actionable and securely distribute it across mission-critical devices and easy-to-manage networks. To learn how you can operationalize the data that surrounds you and make your city safer, contact your Motorola representative or visit motorolasolutions.com/safercities.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2012 Motorola Solutions, Inc. All rights reserved. GO-36-122

