THE GLOBAL STATE OF LMR SYSTEM MANAGEMENT

ADDRESSING THE NEW DEMANDS OF A SOFTWARE-CENTRIC ENVIRONMENT

2018 MOTOROLA SOLUTIONS LMR SYSTEM MANAGEMENT BENCHMARK SURVEY

MOTOROLA SOLUTIONS

THE RELIABILITY AND FUNCTIONALITY of land mobile radio (LMR) systems make them ideal for business- and mission-critical operations. However, because these systems are now software-based environments, maintaining them requires a whole new range of tools and expertise.

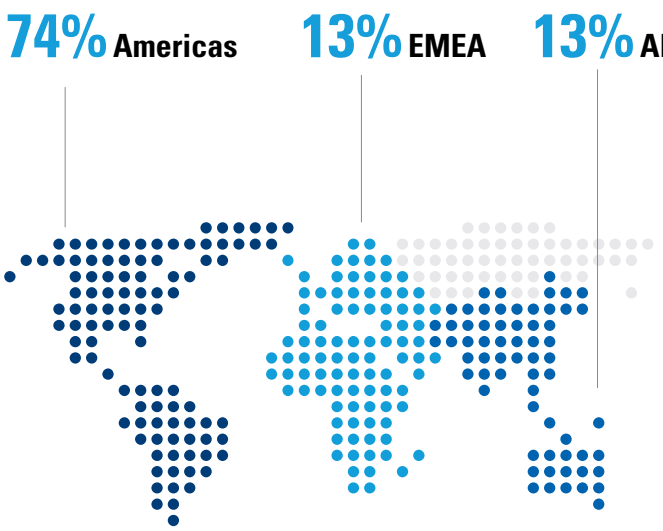
To understand the new trends and challenges associated with managing and supporting evolving LMR systems, Motorola Solutions conducted our inaugural LMR System Management Benchmark Survey in 2018. The survey queried LMR system managers from around the globe in a wide variety of positions and received 120 responses. Forty-one percent of respondents were from public safety, including police, emergency medical services, and fire personnel. Thirty-three percent were from other government agencies. The remaining 26 percent were from enterprise organizations in a range of business-critical industries, such as oil and gas, utilities, transportations, and mining.

Responses came from 24 countries. Seventy-four percent were from the Americas, including the United States, Latin America, and Canada. Asia-Pacific countries, including China, Bangladesh, India, Malaysia, Australia, and India, comprised 13 percent of responses. Another 13 percent came from Europe, the Middle East, and Africa.

Overall, 45 percent of all organizations are using digital-only two-way LMR systems. Another 26 percent are using analog-only systems, and the remaining 29 percent are using a hybrid of digital and analog. These numbers shed light on the industry's ongoing transformation from analog to digital—and the role hybrid systems play in aiding this process.

RESPONSE PROFILE

By Region



Americas: 74%

U.S.	87%
Canada	10%
Latin America/ Caribbean	3%

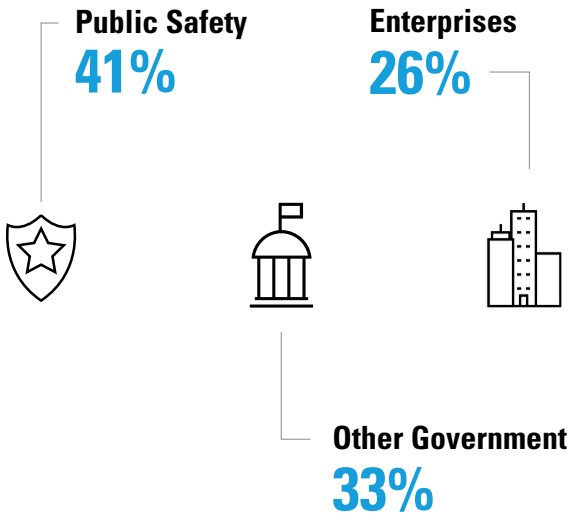
APAC: 13%

China	60%
Malaysia	20%
India	7%
Bangladesh	7%
Australia	7%

EMEA: 13%

Europe	50%
Africa	38%
Middle East	12%

By Industry



Public Safety: 41%

Fire	25%
Police	13%
Emergency Medical Services	3%

Other Government: 33%

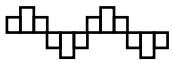
Enterprises: 26%

Other Non-Government	11%
Transportation	9%
Utilities	4%
Mining	1%
Oil & Gas	1%

By System

26% Analog Only

45% Digital Only



29% Hybrid

KEY FINDINGS

1. LMR system managers still give more support to traditional system management measures than they do to software-centric ones. However, those who focus more on software-centric activities such as network monitoring experience fewer outages.

2. LMR system managers are confident that their LMR systems are being safeguarded against security threats. This confidence may be misplaced given the security measures they say they are applying.

3. There is a "performance gap" between the activities that improve system health and system managers' reported level of satisfaction.

4. Looking toward the future, there is a clear intention to focus on improving the software-centric aspects of LMR systems in the next 12 months.

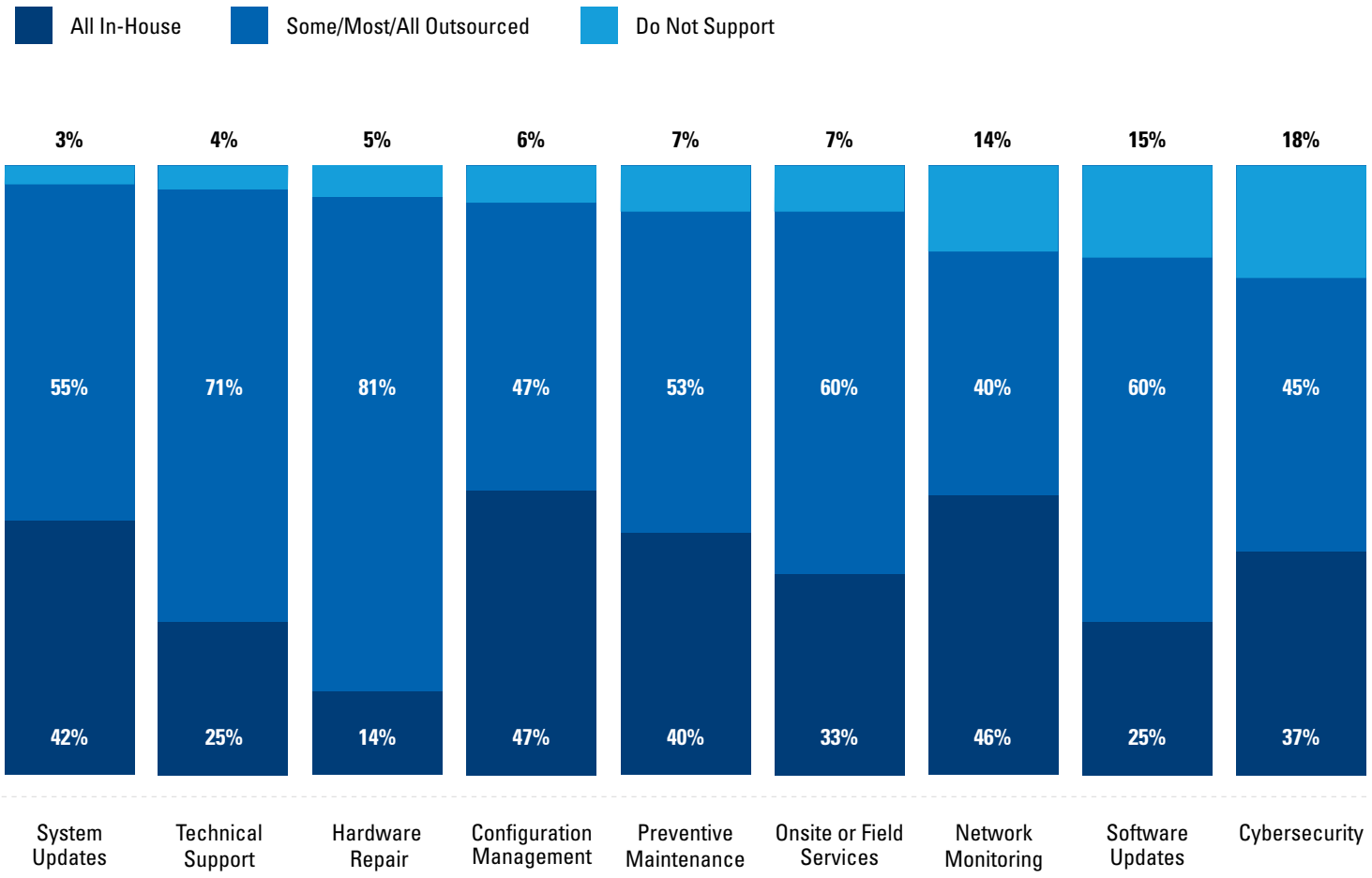
SUPPORT FOR MODERN SYSTEM MANAGEMENT ACTIVITIES LAGS TRADITIONAL MEASURES

When we developed the LMR 2018 System Management Benchmark Survey, we wanted to gather insights about the resources that system managers are using to maintain and support their networks.

What we found is that there is a common trend of using third-party service providers for traditional management activities such as hardware and technical support. Meanwhile, aspects such as software updates, network monitoring, and cybersecurity were split between in-house support and using a service provider. Overall, these same software-centric activities, were among the least supported tasks.

This raises some interesting possibilities. Organizations may simply be struggling to support or understand the relevance of software-centric tasks. In addition, many organizations face resource challenges, both in budget and in talent, that may be impacting their ability to support more software-based activities. Investing in the required talent, knowledge, and tools is not easily attainable for most organizations.

> Overall, modern LMR management activities such as LMR system software updates, network monitoring and cybersecurity were among the least supported.



24x7x365 NETWORK MONITORING IMPROVES SYSTEM UPTIME

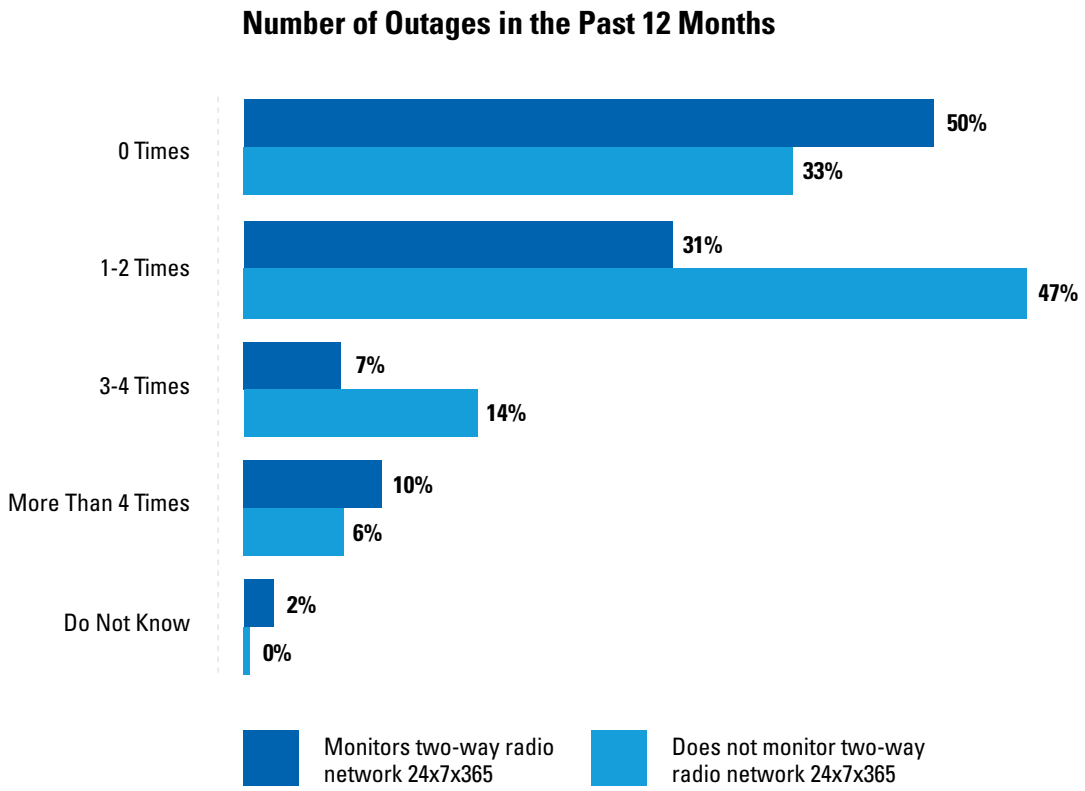
LMR networks, like similar communication environments, generate thousands of system alarms on a daily basis. Network monitoring is the proactive process to watch for these alarms and resolve the critical ones that can disrupt end-user communications. Given the business- and mission-critical requirements of LMR systems, network monitoring must be performed around the clock.

The system managers in our survey clearly demonstrate the importance of around the clock monitoring: 70 percent say they monitor their systems 24 hours a day, seven days a week and they had nearly 50 percent fewer outages in the past year than those that lack 24x7x365 monitoring. While networking monitoring software now allows system managers to pinpoint critical alarms at a faster rate, these resources require a large investment in tools and staff, including a sophisticated network operations center (NOC).

70% of LMR system managers say they monitor their LMR system 24x7x365.

THE CLEAR BENEFIT OF 24x7x365 NETWORK MONITORING

Organizations that monitor their systems 24x7x365 had nearly **50%** fewer outages in the past year than those that do not.



TOP IMPEDIMENTS TO 24x7x365 TWO-WAY RADIO NETWORK MONITORING

Despite the importance of network monitoring, almost a third of system managers (30 percent) say their organizations do not monitor their networks around the clock. There were a range of reasons cited, but the top two represented more than two-thirds of all specific reasons given: **budget constraints** and **staffing challenges**. Budget constraints, cited by 50 percent of system managers, include not being able to pay for staff with the necessary skills or for third party providers. In addition, almost 20 percent say their internal IT support staff is simply too small to provide around-the-clock service.

28% Budget constraints on available internal IT support staff

22% Budget does not allow for a third-party provider

19% Internal IT support staff is too small

8% Third-party provider does not provide 24x7x365 coverage

MISPLACED CONFIDENCE IN SAFEGUARDING LMR SYSTEMS AND ASSOCIATED TECHNOLOGY

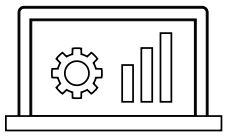
Unsurprisingly, cybersecurity is a top priority for agencies and companies across the globe. In our survey, 78 percent of system managers say cybersecurity is extremely or very important, and 87 percent are extremely or moderately confident in the cybersecurity of their LMR systems. *But should they be?*

Almost 20 percent say their organizations do not support any cybersecurity activities, and they do not see that changing in the next 12 months. Plus, in the next 12 months, establishing a cyber incident response plan is at the bottom of the list of planned activities.

The story is validated by the actual security measures being applied to LMR systems. Only 53 percent of system managers perform active security monitoring. Plus, only 42 percent apply software patches to their LMR systems—the first and most important step to keep LMR networks safe. Even fewer, 30 percent, are conducting periodic risk assessments. 22 percent are doing nothing at all. This practice level are similar for associated technologies such as dispatch systems/ command center tools.

While system managers view cybersecurity as important and they are confident in the measures they are applying, our survey highlights the gulf between that perception and the reality that organizations simply are not taking the necessary steps to secure their LMR systems and associated technologies.

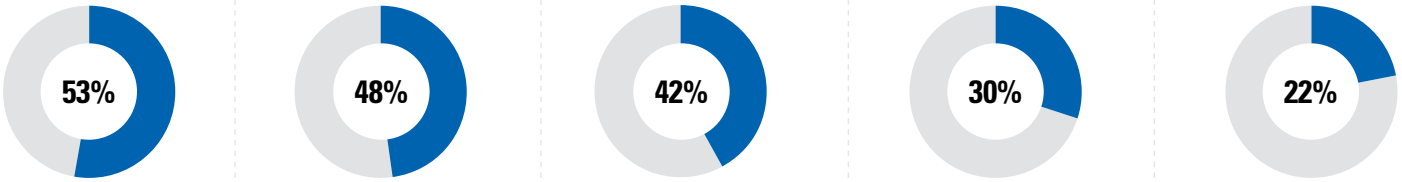
Safeguarding LMR systems and associated technologies requires a holistic risk-based security strategy. According to the 2017 Ponemon Cost of Cyber Crime Study, ransomware breaches increased significantly from 13 percent in 2016 to 27 percent in 2017. 69 percent of respondents experienced phishing and malicious social engineering and 67 percent of companies had Web-based breaches. Virtually all organizations had breaches relating to viruses, worms and/or trojans and malware over the four-week benchmark study period.[1]



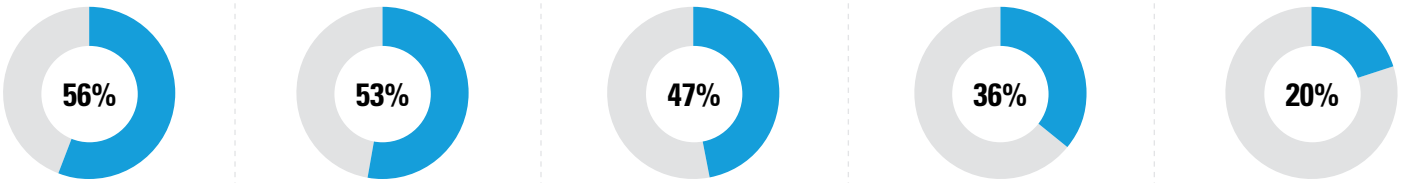
Only **42%** of LMR system managers say they patch their LMR system.

Guidelines such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the ISO 27001 standard are essential for understanding, detecting, responding to and recovering from these types of attacks. These resources provide practical insights for securing your system as well as ensuring the integrity of data and any associated technologies.

SECURITY MEASURES APPLIED TO LMR SYSTEMS



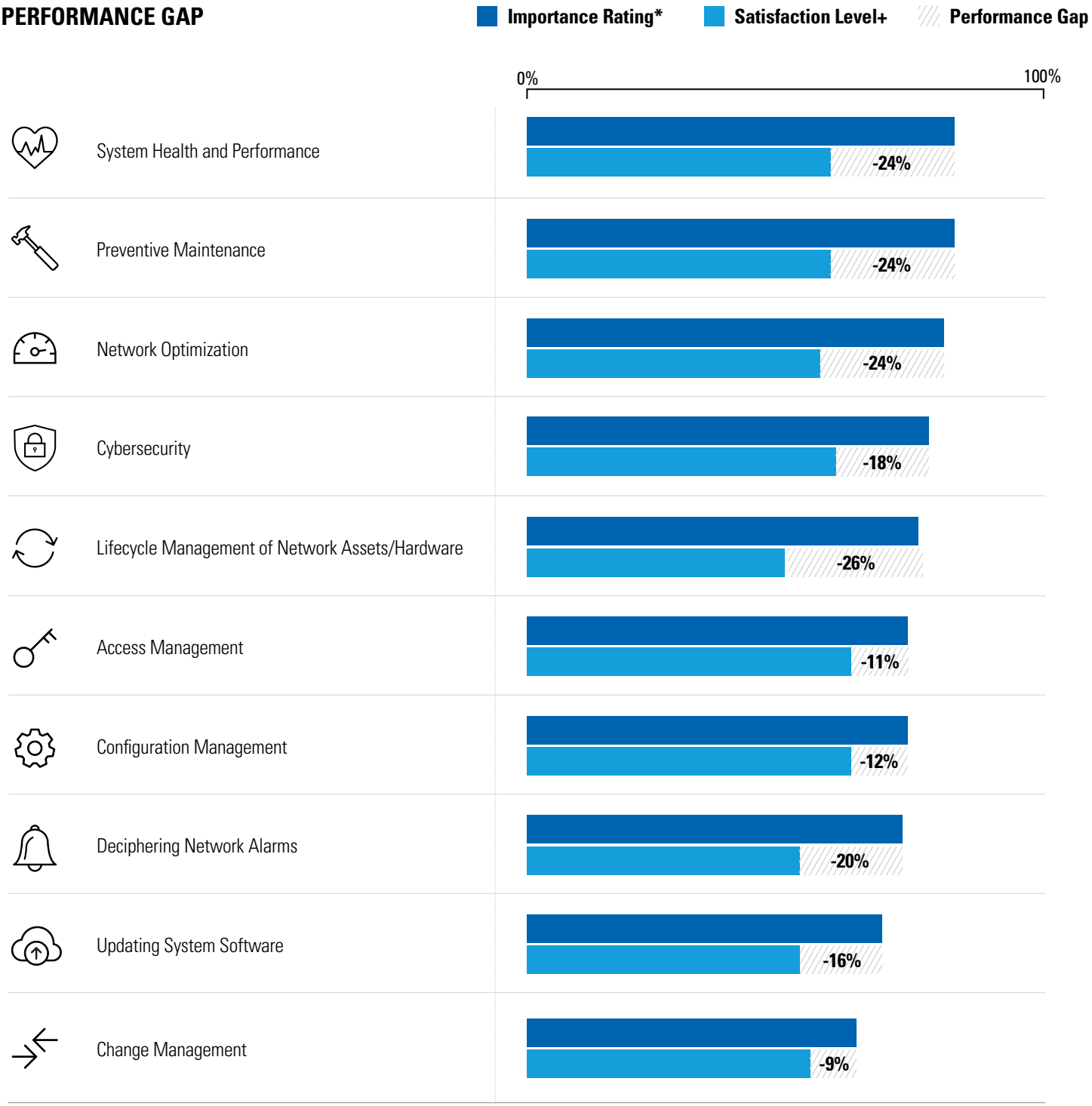
SECURITY MEASURES APPLIED TO DISPATCH SYSTEM/COMMAND CENTERS



A CLEAR"PERFORMANCE GAP" EXISTS BETWEEN THE MOST IMPORTANT MANAGEMENT ACTIVITIES AND SATISFACTION LEVEL

We asked system managers about the LMR managed and support activities they deem important to their systems' health—tasks that must be addressed on an ongoing basis because of the systems' modern software-centric environment. The aspects they rank as most important are understanding overall system health and network performance, preventive maintenance, optimizing network performance, cybersecurity, and lifecycle management of network assets. However, these same areas had lower satisfaction levels in terms of how they are being addressed. This "performance gap" indicates system managers are challenged executing software-based solutions. Partnering with an outside service provider could provide a better outcome.

PERFORMANCE GAP



*Percentage of system managers who ranked task as extremely or very important.

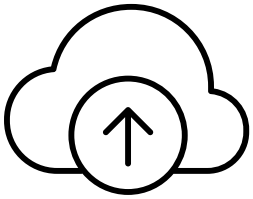
+Percentage of system managers who are extremely or very satisfied with how activity is being addressed.

THE FUTURE OF LMR SYSTEM MANAGEMENT

So, what does the future hold for LMR system management? Respondents' top focus areas in the next 12 months are software-centric activities that help them improve their system, such as updating software and improving their networks' overall health and performance.

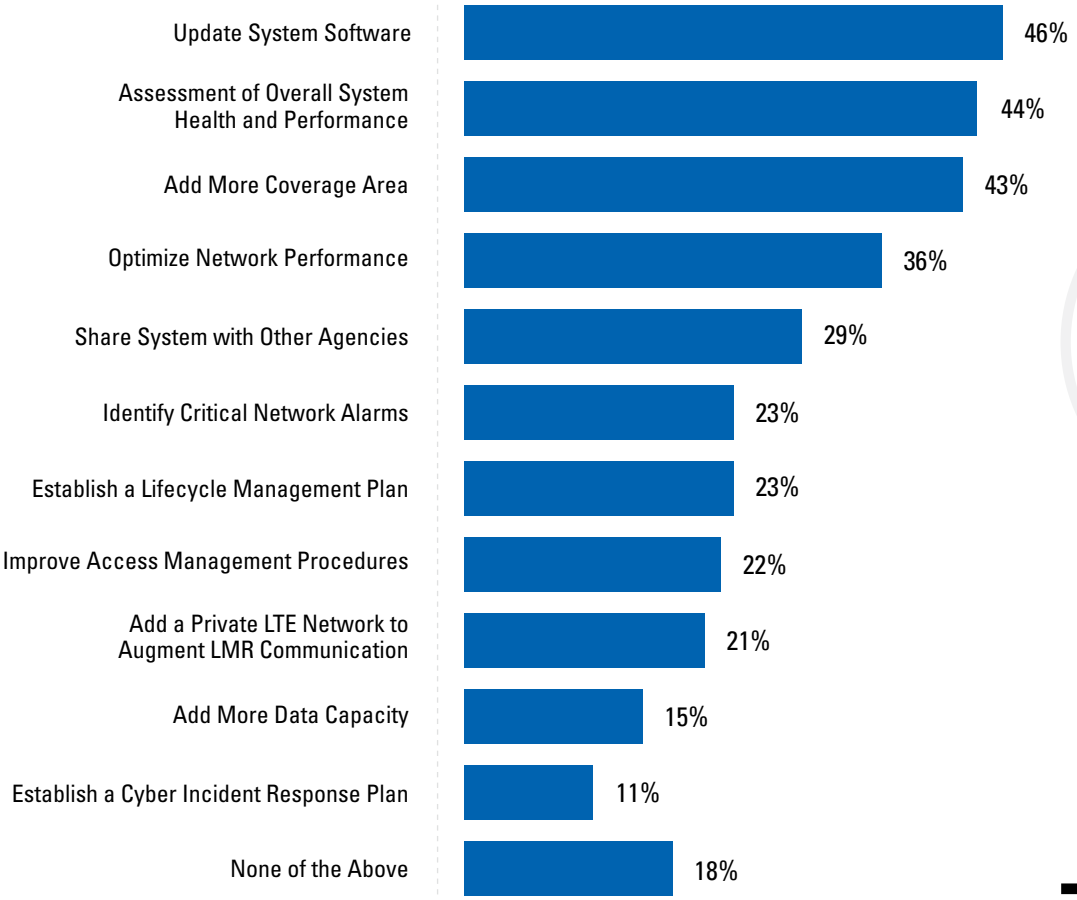
In addition, adding broadband LTE to augment LMR networks is in the plans for 21 percent of organizations. Of these organizations, 80 percent want to move forward with this effort in the next year with the help of a third-party provider. Although augmenting LMR with LTE is clearly important for system managers, core LMR-based activities are still the main focus.

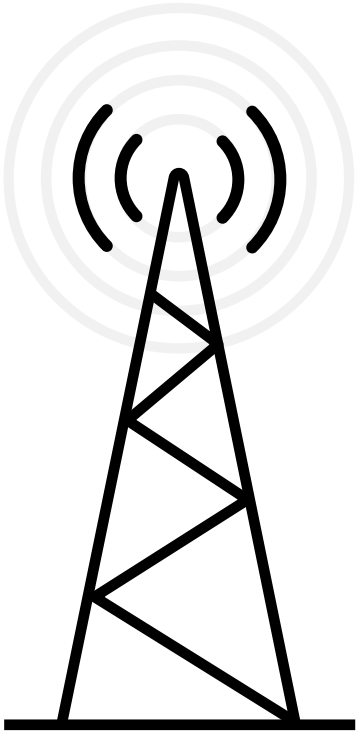
These focus areas for the next year highlight the growing importance of software-centric LMR network and maintenance activities. Indeed, activities such as updating system software are integral to network and application performance. Software updates fix identified programming errors, enhance features, and address known vulnerabilities, providing end-users with access to the latest features, functionality, and enhancements so they can communicate more effectively.



Executing LMR system updates is the top priority for system managers in the coming year.

System Services Organizations are Planning to Address in the Next 12 Months





EVOLVING LMR SYSTEM MANAGEMENT TO ADDRESS ITS MODERN SOFTWARE-CENTRIC ENVIRONMENT

Today's business- and mission-critical LMR systems are increasingly software-centric. This evolution has enabled leaps in functionality, performance and interoperability. But these systems are only as good as their maintenance allows. Managing them, especially as they become more complex and as more bad actors aim to do them harm, requires dedicated resources, specific tools and deep expertise.

Organizations that best adapt to managing the evolving software-centric LMR network, from using network monitoring to incorporating cybersecurity and regular security patching to talent procurement, will gain a powerful advantage. End users will reap the rewards in the form of network security, availability, and performance gain. Forward-looking system management will be vital to the health and innovation of these end-users' communication tools and ultimately in the success of the mission or business itself.

PREPARE FOR EXCELLENCE. OVERCOME THE UNEXPECTED.

As the leader in LMR communication systems, Motorola Solutions' mission is to ensure that your LMR system works seamlessly, is safeguarded, and can adapt to new operational complexities and technology changes.

To accomplish this, we collaborate with you to pinpoint your system management needs and goals. Then, we partner with you on a service level that meets your specific needs. We offer best-in-class universal support, maintenance tools, resources and a global team of experts who have an intimate knowledge of LMR systems and associated technologies. To learn more about our service packages, visit: **motorolasolutions.com/services**.

SOURCE

1. 2017 Ponemon Cost of Cyber Crime Study, https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

LOOK	See which LMR system services solution is right for your operation.
LISTEN	Learn about the best practices for avoiding network downtime and maintaining a secure and reliable LMR system.
LEARN	Discover which managed and support service level can help you with your performance goals.
INTERACT	Explore the right level of services to help you achieve your performance goals.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**