LMR CYBERSECURITY

BRIDGING THE DISCONNECT BETWEEN PERCEPTION AND ACTION

FINDINGS FROM OUR 2018 LMR SYSTEM MANAGEMENT SURVEY

WHITEPAPER

MOTOROLA SOLUTIONS

SAFEGUARDING LMR SYSTEMS: ACTION STILL NEEDED

With every new headline touting news of the latest cyber breach or vulnerability, it's clear that no entity is immune from the rising global threat of cybercrime. Agencies, companies and organizations around the world are taking notice. Global cybersecurity spending is estimated to reach a cumulative $1 trillion by the year 2021.[1] But behind the growing attention and increasing budgets, how are those responsible for supporting and maintaining land mobile radio (LMR) responding to the challenge? What measures are they taking to safeguard their systems and associated technologies? How confident are they in their organization's cybersecurity measures?

To answer these questions, we conducted the 2018 Motorola Solutions LMR System Management Survey—querying 120 LMR system managers around the world in public safety, government and enterprise organizations. The results of our survey reveal a disconnect between the perception of cybersecurity as a priority and actual measures being taken to safeguard LMR and associated systems.

CURRENT TREND

VS.

CURRENT PRACTICE

87%

are extremely or moderately confident in the cybersecurity of their LMR systems. But should they be? Only...

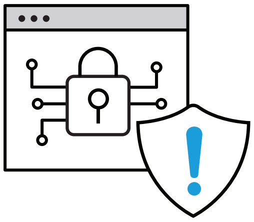
53% Conduct active security monitoring

48% Have documented security policies and procedures

42% Patch their LMR systems

30% Conduct periodic risk assessments

22% Do none of the above



Cybersecurity is the **4th** most important aspect needed for LMR network performance.

However, cybersecurity is the least supported aspect of system management.

18% surveyed do not take any cybersecurity measures.

78%

of organizations point to cybersecurity as extremely or very important. While only...

11%

of organizations cited establishing a cyber incident plan as a priority for the coming year.

IMPORTANCE IS RECOGNIZED

Respondents certainly acknowledge their LMR systems are susceptible to cyber threats. With 78 percent saying cybersecurity is extremely or very important, it ranked as the fourth most important aspect needed for LMR network performance.

When it comes to their confidence levels, 87 percent say they are extremely or moderately confident in the cybersecurity of their LMR systems. But should they be?

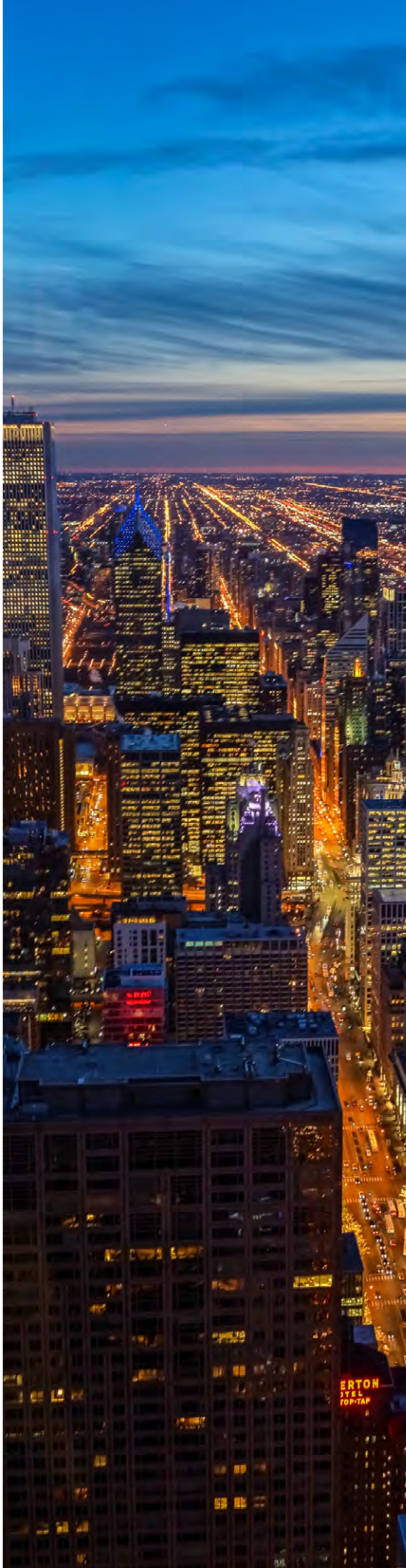
EXECUTION IS INCONSISTENT

When asked which security measures they apply to their LMR systems, active security monitoring is the most cited at 53 percent, followed by documenting security policies and procedures at 48 percent, security patching at 42 percent, and periodic risk assessment at 30 percent. Nearly a quarter—22 percent—say they are not applying any of these security measures.

The trends are similar for associated technologies. For dispatch systems or command center technologies, only 56 percent conduct active security monitoring, followed by documenting security policies and procedures at 53 percent, security patching at 47 percent, periodic risk assessment at 36 percent, and 20 percent not applying any of these security measures. The levels are also comparable for broadband networks, mobile devices, cloud solutions and vendor-hosted solutions.

Our survey reveals that cybersecurity is the least supported of all LMR services, behind activities such as network monitoring, hardware repair, configuration management, preventive maintenance, infrastructure and lifecycle management. Almost 18 percent of respondents say their organizations do not support any cybersecurity activities, and they don’t see that changing in the next 12 months.

Looking forward, respondents were asked what system management task they expect to address in the coming year. Establishing a cyber incident plan is the last item on their to-do list. Only 11 percent say it is a priority for the coming year.



SECURITY MEASURES THAT ENSURE CONFIDENCE

Although respondents rate cybersecurity as important and are confident in its application to their LMR systems and associated technologies, our survey reveals there is significant room to reduce system vulnerabilities to cyber threats. Organizations simply are not taking the required measures to reduce their risk. Additional actions can be taken by LMR system managers to mitigate risk, identify attacks, and move to swift remediation. So, what are they?

1 **Break free from a "set it and forget it" cybersecurity mindset.**

This is the thought process that once a security solution is in place, a system is protected with no further action needed. You cannot have this mindset. Cyber threats are constantly evolving. The strategy and solution you have in place today need to evolve with the changing threat landscape.

2 **Establish a comprehensive, proactive, risk-based security strategy.**

Monitoring is the most applied security measure in our survey. This practice is simply not enough. Managing and staying ahead of evolving threats requires consistently applying measures such as risk assessments, information assurance road maps, security patching, and active security monitoring to your LMR systems and associated technologies.

3 **Adopt and use proven cybersecurity frameworks and standards.**

The National Institute of Standards and Technology (NIST) framework and other standards, such as ISO 27001, are critical cybersecurity tools. They can help shed light on network vulnerabilities and risks, then guide users through each phase of cybersecurity: identify, protect, detect, respond, recover. This has proven to be an effective approach and should be adapted to an organization's individual security goals and resources.

UNDERTAKING YOUR CYBERSECURITY JOURNEY

Establishing and implementing a cybersecurity strategy comes with many considerations. If your organization has a lack of in-house cybersecurity experts, you can partner with us. Our experts are skilled, subject-matter professionals, ready to work with your organization to enhance your ability to identify, manage and respond to cyber threats.

To learn more, visit motorolasolutions.com/cybersecurity.

SOURCE

1. Cybersecurity Market Report, Cybersecurity Ventures, 2018

MOTOROLA SOLUTIONS

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