THE REAL COST OF OPERATING LMR SYSTEMS

WHITE PAPER

MOTOROLA SOLUTIONS

Maintaining a land mobile radio (LMR) system for business- and mission-critical operations requires a multitude of resources. From regular maintenance and upgrades to third-party vendors and security services, your total system management cost will vary depending on your organisation's operational needs.

ARE YOU INVESTING TO ACHIEVE YOUR DESIRED PERFORMANCE OUTCOMES?

A comprehensive look at your system support and maintenance not only gives you a detailed overview of known expenses, but also exposes undocumented costs.[1] This total cost of ownership (TCO) for managing your LMR system accounts for all costs associated with ensuring that your system can support your ongoing operational needs throughout its life. This essential information creates a sound understanding of the investment and resources needed to maximise network continuity and improve performance. It also allows you to budget accordingly and determine if these efforts should be supported in-house or managed by a trusted partner.

The following is a construct of the resources and tools required to manage a LMR system, based on the performance levels required for public safety agencies and business-critical enterprises. A thorough assessment of the information below can help you develop an accurate picture of associated costs and determine if a managed services provider is the most cost-effective approach for your LMR system management needs.

UNDERSTAND YOUR CAPITAL EXPENSE CYCLE

With today's LMR systems adopting IP-based technology, applications and data for critical operations, continuous support and maintenance are required to ensure the system is up to date. The longer you let the system age, the more significant and expensive the required upgrades become. Even with a top-notch up-to-date system, you must plan for upgrades that require capital expenses and factor in unforeseen costs such as network components that become faulty and need to be replaced. Addressing such situations require having a spare parts inventory and a management process. This also comes at a cost.

CAPITAL EXPENDITURES

- Configuration changes
- Hardware
- Land and geographic needs
- Network Management System
- Software
- Spare parts

CAPTURE ONGOING MAINTENANCE AND MANAGEMENT COSTS

As with any technology, your LMR system will have performance issues and parts will need to be repaired, replaced or updated. System security and operating software will require updates to avoid system vulnerabilities, improve performance, and give your users access to the latest functionalities. Preventive maintenance will need to be performed to preserve system reliability. Capacity and coverage will fluctuate as your operation evolves.

Neglecting any of these tasks can eventually lead to communication disruptions or network downtime. Most agencies and organisations use a network operations center (NOC) to facilitate and oversee ongoing system management needs. However, for most, acquiring and maintaining the right NOC resources and technology has been challenging. As a result, some have shared these responsibilities with, or have outsourced them to, a trusted partner to reduce cost and take advantage of state-of-the-art network management tools and system experts.[2]

Critical operations require around-the-clock network monitoring. Your NOC system management procedures and acumen must be exceptional, operational 24x7x365 and able to address all of the tasks mentioned above. With the right team, you will be able to pinpoint critical network failures amid thousands of daily system events. To address system incident issues faster, your NOC must also have the capabilities to assess and remotely resolve these events whenever possible.

ONGOING EXPENSES

- Infrastructure hardware repairs
- Network monitoring
- Preventive maintenance
- Provisioning and subscriber management
- Software licenses
- System software updates

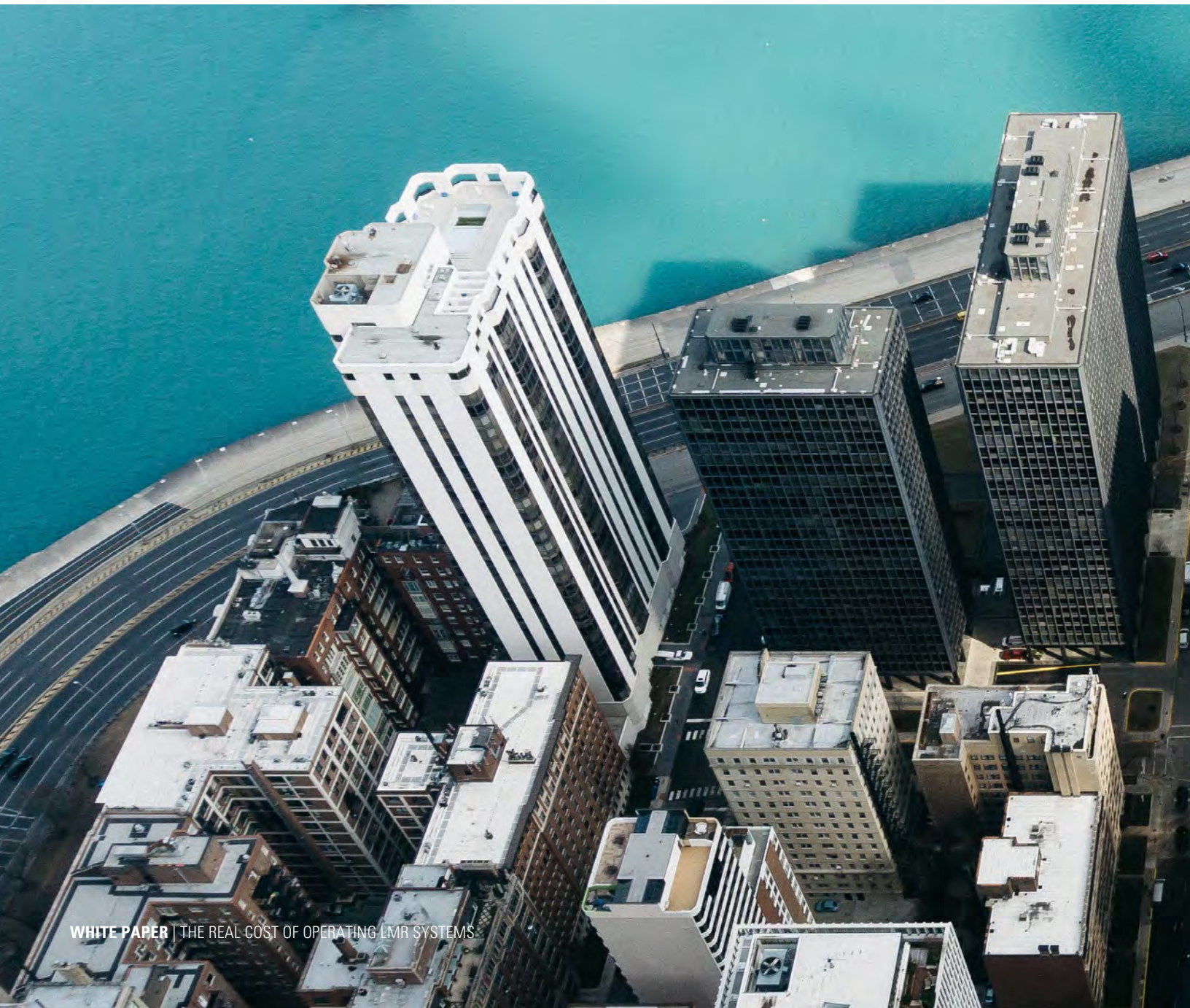
INVEST IN SAFEGUARDING YOUR SYSTEM FROM VULNERABILITIES

Another often neglected aspect of ongoing costs is security. Critical infrastructures are high-priority targets for hackers. The luxury of a closed LMR network is long gone, as hackers now have means to penetrate networks without a direct connection to the Internet. The ransomware incidents that have crippled mission-critical operations around the world reveal that no one is immune from a cyber attack. To prevent an intrusion and safeguard your system, you need consistent patching of your system with pre-tested security software, active security monitoring, well-understood policies with internal team members and external partners, as well as periodic cybersecurity risk assessments. Omitting even one of these security elements can leave your system vulnerable.

Cyber crime has increased by 23 percent in the past year. It is costing the utilities and energy sector $17.20 million, the manufacturing sector $10.22 million, the transportation sector $7.37 million and the public sector $8.28 million.[3] If your system is compromised, is your team prepared to handle not only operations and finances but also the public relations fallout?

SECURITY-RELATED COST

- Active security monitoring
- Documented security policies and procedures
- Periodic risk assessments
- Security patching



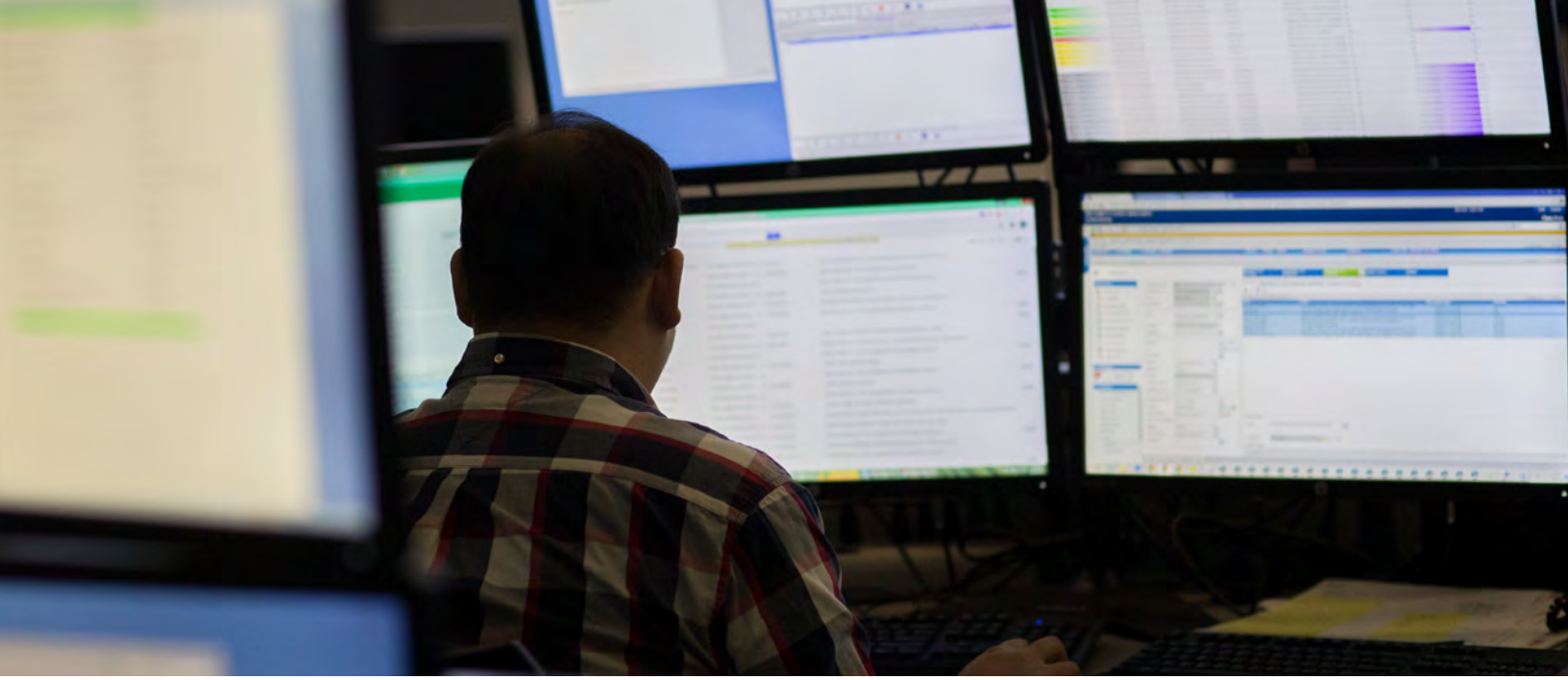
HAVE YOU CAPTURED YOUR CYBERSECURITY TCO?

Best-in-class cybersecurity requires a dedicated security operations center, a lab to validate patches and certified security experts. Are you capturing all of these costs?

RESOURCE OR TOOL	YEAR 1 COST	YEAR 2 COST	YEAR 3 COST
Patching test lab	$1,000,000		
Patching test engineers (at least two)	$200,000	$200,000	$200,000
Patching operations sustainment cost	$250,000	$250,000	$250,000
Security operations center	$1,000,000		
Security operations center sustainment	$2,000,000	$2,000,000	$2,000,000
Security operations center analysts (two or three)	$180,000	$180,000	$180,000
Security team training	$10,000	$10,000	$10,000
TOTAL	**$4,640,000**	**$2,640,000**	**$2,640,000**

*Actual TCO savings will vary by system size and operational requirements.

CYBER ATTACKS: IT'S NO LONGER A QUESTION OF IF, BUT WHEN



ACCOUNT FOR SKILLED RESOURCES

Your staff is vital to your system management operations. From network monitoring to field services and security, your team's skills are the driving force behind the system performance outcomes achieved. You need a team that is proficient in everything from classic radio frequency to IP-based technology and data analytics.

For network monitoring, you need a team equipped with the right tools and technologies to monitor and maintain your system. This team must have the skills to configure your tools for your operations—from configuring system rules and detecting critical alarms to identifying root causes. With the right team, you can optimise system coverage, capacity and availability while also preventing and predicting outages. And, do not forget about the remote operations required with field services and preventive maintenance. You also need to address your subscribers' needs when it comes to call-group management and provisioning.

In addition to network management specialists, you need security experts for patching, monitoring and risk assessment. Finding, attracting and retaining qualified individuals can be difficult. These individuals maintain the integrity, confidentiality and availability of the communication and data that is traveling across your network. Without them, your system is vulnerable to intrusions that can disable your network.

Last but not least is your communications director. This person orchestrates your system operations and is your champion with cross-functional stakeholders and budget authorities. Having an advocate with intimate knowledge of your operations and evolving technology needs is essential to keeping your system current and performing at target levels.

These skilled resources are indispensable. When you review your system operations, ensuring you have the means and capital to recruit, train and retain these individuals is key to your operations. However, this kind of talent comes at a cost.

TALENT

- Communications director
- Field services
- Network monitoring team
- Network provisioning
- Security team
- Subscriber technicians

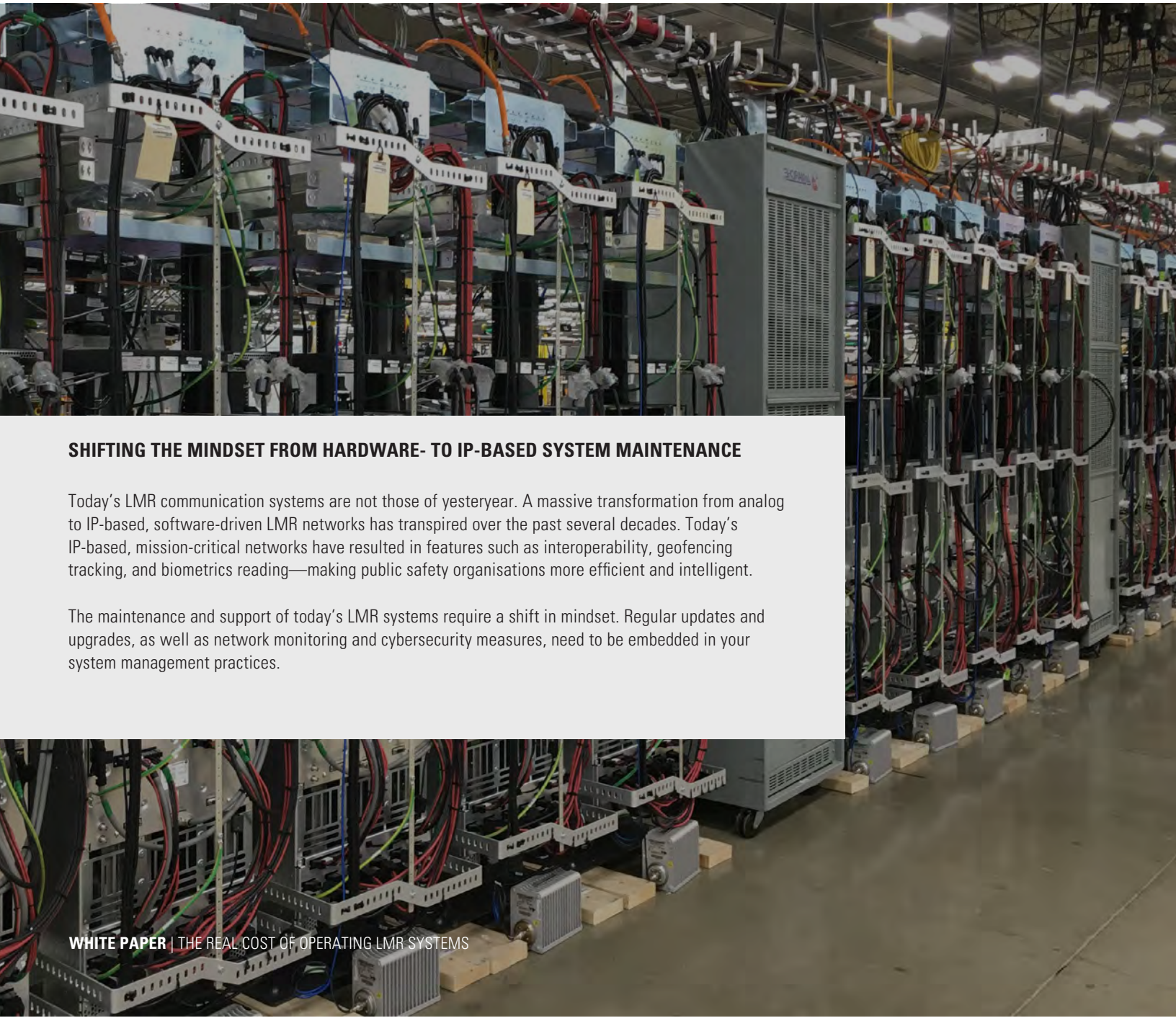
RECOGNISE YOUR MISCELLANEOUS EXPENSES

There are plenty of other system management expenses that are integral to system maintenance, but are they being captured in your TCO? Some are outsourced because of a lack of in-house resources. Others are just part of doing business, including Frequency License Management, grounds and facility maintenance, HVAC, utilities, tower inspection, backhaul maintenance and monitoring, fuel and power supply and much more. These services are crucial to keeping your system up and ensuring that your operations meet public safety standards.

MISCELLANEOUS ITEMS

- Antenna and lines
- Backhaul solutions*
- Fuel and power supply
- Frequency license management
- Grounds and facility
- HVAC services and utilities
- Site leases
- Training
- Tower inspections and lighting

*Maintenance, preventive maintenance and tech support



SHIFTING THE MINDSET FROM HARDWARE- TO IP-BASED SYSTEM MAINTENANCE

Today's LMR communication systems are not those of yesteryear. A massive transformation from analog to IP-based, software-driven LMR networks has transpired over the past several decades. Today's IP-based, mission-critical networks have resulted in features such as interoperability, geofencing tracking, and biometrics reading—making public safety organisations more efficient and intelligent.

The maintenance and support of today's LMR systems require a shift in mindset. Regular updates and upgrades, as well as network monitoring and cybersecurity measures, need to be embedded in your system management practices.

WHERE DO YOU STAND?

Have you been accounting for all of these costs? If not, you now have a more comprehensive view of what it really costs to maintain your LMR system, ensure availability, and achieve the performance outcomes required for your end users. You can better assess your operations and identify gaps and improvement opportunities. This knowledge will help you make a well-informed decision about keeping your system management operations in-house or outsourcing them to a managed services partner as a more cost-effective solution.

As a global leader in mission-critical communication products and services, Motorola Solutions has the expertise to take care of your system operations. Having managed more than 500 LMR systems worldwide, we understand it is not just about having the right technology, but helping our customer networks achieve their target performance outcomes. When every second counts and network availability is a must, we are ready and able to serve your organisation today, tomorrow and into the future.

Contact us to find out how we can help you achieve your performance targets and desired outcomes. We have a team of dedicated managed services experts prepared to free up your time and resources so you can focus on your core mission: saving lives.

SOURCES:
1. Total Cost of Ownership TCO Analysis, Business-case-analysis, 2017
2. Network Operations Centers: Understanding Your Options, Milestone, 2017
3. Cost of Cyber Crime Study, Accenture, 2017

MOTOROLA SOLUTIONS

Motorola Solutions, Nova South, 160 Victoria Street, London, SW1E 5LB, United Kingdom. **motorolasolutions.com**