MOTOROLA SOLUTIONS: YOUR TRUSTED CYBERSECURITY PARTNER

BECAUSE SUCCESSFUL OUTCOMES DON'T HAPPEN BY CHANCE

This report was commissioned by Motorola Solutions, Inc. and executed by LookingGlass Cyber Solutions.
So you’ve already acknowledged the importance of protecting the continuity of your critical systems and devices from cyber attack. Now you are ready to take the next step, but where do you begin?

Maybe you’ve dabbled in creating a cybersecurity plan but want to ensure it will stand up over time. What comes next?

To ensure a successful outcome, you need a trusted partner to work with you on your cybersecurity journey. Motorola Solutions, the leader in mission critical communications, knows the cybersecurity ecosystem inside and out: the networks, devices and software. Cybersecurity knowledge can be hard to come by, hard to keep up with and expensive to maintain. Our cybersecurity professionals are second to none. We can manage the complexity, so you are free to focus on running the rest of your business.
GETTING STARTED

When you partner with us, we’ll begin by determining and prioritizing your risks: which ones are the most important and which ones will do the most to reduce your risk.

Working together we’ll then put an end-to-end process in place to mitigate those risks and use proven technology to get you there. Our cybersecurity experts will help you every step of the way—from risk assessment, process improvement, selection of our key technology products / purchase guidance and implementation—to on-going cybersecurity management for today and tomorrow.

THE CYBERSECURITY ECOSYSTEM: PEOPLE, PROCESS AND TECHNOLOGY

Let’s have a look at the three parts of the cybersecurity ecosystem that we can help you put together: people, process and technology.

At the heart of the ecosystem are cybersecurity services. Depend on the knowledge of our skilled experts to safeguard your operational integrity.
People

Lack of cybersecurity expertise is a constant challenge facing public safety and government agencies today.

Organizations that find themselves with a shortage of cybersecurity personnel are at risk of slowed adoption and implementation of the critical tools and processes needed for cybersecurity protection—opening them up to breaches and attacks. For companies in need of cybersecurity expertise, partnering with an organization like Motorola Solutions that can provide cybersecurity support and services may be the solution.

This critical need underscores why we created the Motorola Solutions Products & Services Cybersecurity Team to oversee and guide cybersecurity across all of our products, solutions, and services. The team holds top industry cybersecurity certifications and stays sharp with comprehensive, ongoing training. They provide valuable, actionable advice on the entire range of cybersecurity products and services, from security monitoring solutions and notification services to cybersecurity assessments, patching, and updating services.

A SHORTAGE OF CYBERSECURITY PERSONNEL

The cybersecurity expertise shortage is estimated at just under 3 million professionals with roughly 500,000 of those positions located in North America. Asia-Pacific, with its growing economies and new privacy regulations, is experiencing the biggest shortage—2.14 million positions.1
Our holistic, organization-wide, risk-based process approach to security has the National Institute of Standards and Technology (NIST) Cybersecurity Framework at its core.

While many organizations are focused solely on prevention, prevention alone is an ineffective strategy. The NIST approach focuses on mitigation options, continuous monitoring, diagnosis and remediation to secure and protect systems and networks.

Motorola Solutions uses the NIST Cybersecurity Framework as we’re thinking through the cybersecurity and development of our own solutions.

Your critical systems and devices are seen as high value targets by cyber criminals who continue to get more technologically savvy. Our market-leading end-to-end security solutions have you covered every step of the way.

**PROCESS**

**IDENTIFY: ASSESS RISKS**
- Provide a thorough risk analysis
- Uncover potential vulnerabilities

**PROTECT: DEVELOP SAFEGUARDS**
- Develop policies and procedures
- Implement appropriate access and auditing control

**DETECT: MAKE TIMELY DISCOVERIES**
- Continuous monitoring 24x7x365
- Enable auditing capabilities

**RESPOND: TAKE ACTION**
- Establish a robust response plan
- Create, analyze, triage and respond to detected events

**RECOVER: RESTORE FUNCTIONALITY**
- Institute a recovery plan
- Create improvements to prevent future attacks

**TECHNOLOGY**

**ENCRYPTION**
We have purpose-built solutions to protect LMR voice and data that are compliant to LMR standards, FIPS 140-2 validated and provide AES 256 encryption. Link encryption to remote endpoints while traveling across intervening networks is also supported.

**KEY LOADING**
Quickly and easily create, store, and deliver encryption keys while on the move with our key variable loader. Offering the highest levels of protection, our FIPS 140-2 level 2 validated key fill device ensures robust and secure key management while in the field. In fact, our key loading products are the preferred solution for 3rd party radios.

**HARDWARE SECURITY MODULE**
Prevent lost or stolen radios from being hacked to lift encryption keys and intercept your private communications. The FIPS 140-2 level 3 validated encryption modules available in our devices act as a trust anchor, providing a tamper-proof secure environment for storing encryption keys.

**AUTHENTICATION**
Motorola Solutions’ radio authentication ensures only authorized users can communicate on your network. It prevents compromised radios from hijacking your network’s resources and sending unauthorized messages, and eliminates the ability of cloned radios to masquerade on your system as real users.

**KEY MANAGEMENT**
Respond faster to changes in your environment with enhanced visibility and greater control over your encryption keys across devices deployed in the field. Generate, load, and delete keys on-demand so you can stay ahead of your adversaries and better insulate yourself from attacks.

Ensure all your voice and data communications are secured with encryption keys that update over-the-air. Over The Air Rekeying (OTAR) avoids the delays, inconvenience and costs of having personnel bring their devices into the shop for manual rekeying.

**CENTRALIZED ACCESS MANAGEMENT**
Our identity and access management solutions supplement Active Directory-based centralized access management for improved security.
CYBERSECURITY SERVICES - BE PREPARED FOR WHAT'S NEXT

Our Services offer the expertise, vigilance and responsiveness that give your people back the time and peace of mind they need to be their best. In particular, our Cybersecurity Services help to alert and defend your network against hacks and data breaches while allowing you to keep pace with innovation at a predictable cost. Our Cybersecurity Services include:

RISK ASSESSMENT
Using industry standards and frameworks, we perform a comprehensive assessment to help you understand your risk posture and steps that should be taken to mitigate, react and respond to cyber threats.

PATCH INSTALLATION (SECURITY UPDATE SERVICE)
Pre-tested security updates are deployed onto your radio network system to address known vulnerabilities as soon as they are available and validated to avoid network disruption.

NETWORK SECURITY MONITORING
Our team of experienced network security professionals remotely monitor your system from our Security Operations Center (SOC) for security events and apply countermeasures whenever necessary.

ON-PREMISE SECURITY OPERATIONS CENTER
Remote security monitoring delivers the most cost-effective and secure approach. If it is not a viable option our On-Premise Security Operations Center provides you with a reliable means to proactively monitor your network for unusual security activities.

SURVEY RESULTS REVEAL CYBERSECURITY PREPAREDNESS

Our recent survey of customers with LMR systems found that most respondents feel quite confident in their cybersecurity preparedness, but in fact many do not engage the required best practices for true security. Organizations need to adopt a holistic, risk-based security strategy and apply the recommended measures required to protect, detect and respond to evolving cyber threats.

87% of LMR system administrators 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
WHEN COMPLEXITY IS MANAGED, CALM PREVAILS.

As technology advances, so does the complexity of your devices and networks. Supporting them doesn’t have to be a burden—we can manage the complexity for you.

Off-loading the seamless deployment and management of your communication system to a trusted, capable partner can leave your team free to focus on your operations, the mission and not the systems you use. A team of specialists will work side-by-side with your team, anticipating problems before they are problems and putting corrective actions into place. Now you can simplify the complexity of deploying and managing technology with support from mission-critical communication experts, who deliver an always on, resilient, private and secure communication network.

100+ COUNTRIES
Our expertise and footprint expands around the globe.

500+ NETWORKS
We mitigate risk and minimize downtime to ensure peak performance.

10k+ SITES
We deliver ‘always-on’ resilient, private and secure communications.

500k+ SUBSCRIBERS
We keep your workforce mobilized, end-to-end.
For more information about our Cybersecurity Products and Services visit: motorolasolutions.com/cybersecurity

Sources
1 https://www.isc2.org/research
2 2018 Motorola Solutions LMR System Management Benchmark Survey