



GETTING STARTED GUIDE: HOW TO PROTECT YOUR MISSION-CRITICAL LIFELINE IN AN INCREASINGLY VULNERABLE WORLD





CYBER THREATS TO MISSION- CRITICAL SYSTEMS: GROWING RISKS, CREDIBLE SOLUTIONS

Since their introduction, Land Mobile Radios (LMR) and the increasingly interconnected systems they rely on have become crucial to mission-critical services - essential to everyday operations and a lifeline in an emergency. Yet as the capabilities of mission-critical systems and technology have evolved, so have the

threats against them. In particular, there has been a significant rise in cyber attacks - when criminals or other threat actors gain unauthorized access to information, networks or devices and consequently compromise their security or availability.





CISA-IDENTIFIED CYBER AND PHYSICAL RISKS WITHIN LMR

Cyber attacks are not just limited to a network being breached or taken offline: they come in multiple guises. The Cybersecurity and Infrastructure Security Agency (CISA) recently published guidance that identifies the cyber risks to LMR, including:

- **RADIO FREQUENCY (RF) INTERFERENCE OR 'JAMMING':**
The unintentional or malicious disruption to the RF, preventing wireless, cellular, broadband or LMR communications.
- **INTERCEPTION:**
Eavesdropping on public safety transmissions to potentially acquire information using a web-based application or digital scanner.
- **DUPLICATE RADIO IDS:**
In a trunked radio system, duplicating radio IDs to gain access to and disrupt communications.
- **POOR CYBER HYGIENE:**
Lack of authentication or authorization applications, unpatched or outdated software, as well as poor password policies.
- **UNAUTHORIZED NETWORK ACCESS:**
When encryption keys are compromised or outdated, devices are lost or stolen, and digital scanners or online applications are used to access communications (interception).
- **UNAUTHORIZED DATA ACCESS:**
Attackers accessing sensitive databases to steal, adjust or corrupt data.

Additional risks include:

- **INTERCONNECTED SYSTEMS:**
The bridging of multiple systems, although beneficial to productivity and operations, if not carried out skillfully, can introduce further risks.
- **ADMINISTRATIVE ERRORS:**
Radio systems are highly complex and even minor mistakes can create configuration errors which leave them open to multiple vulnerabilities.
- **USB STICKS:**
Whether introduced into a device or environment by an unwitting employee or malicious insider, a USB infected with malware can quickly infiltrate an entire system.

The impact of these risks being exploited can be life-changing, if not life-threatening. Successful attacks can result in audio communications being lost or impaired, information being leaked (and altered), as well as the safety of first responders and the communities they serve being compromised.





ADVANCED AND EVOLVING CYBER THREATS

The tactics employed by malicious hackers and cyber criminals are growing increasingly sophisticated; last year, cyber attacks increased globally by 38 percent.¹ This can be attributed, in part, to criminals exploiting the digital tools and software used by remote workers, which may allow criminals to establish network connections while evading detection.

Ransomware attacks also continue to be a significant threat. In these attacks, cyber criminals install malicious software on devices and systems, preventing them from being used or information from being accessed until payment is made for their release. In some cases, cyber criminals threaten to publish confidential data online unless they receive additional payment. The past few years have also seen a rise in ransomware-as-a-service (RaaS), Artificial Intelligence (AI)

and machine learning being used to multiply and simplify the number of attacks performed, as well as an increase in hacktivism, in which attackers are motivated by a particular cause or ideology. These factors can also be linked to the growth in ransomware and other cyber attacks.

No business or organization - large or small - is immune to a cyber attack, and no organization can afford system downtime, rendering their services unusable for customers. While they can take only minutes, a cyber attack can cause millions of dollars in damage through lost services and the impact on an organization's reputation. Attacks can compromise the confidentiality of business information such as confidential product launch plans, Protected Health Information (PHI) and financial or legal records.

¹ LePree Anderson, Joy 'Global cyberattacks increased 38% in 2022', Security Magazine, 20.01.23
<https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022>





CYBER THREATS IN MISSION-CRITICAL AGENCIES

For mission-critical organizations reliant on multiple technologies to protect community safety, maintain public order and manage emergencies, a cyber attack that compromises their data, devices or networks does not just affect livelihoods, it threatens lives.

Studies have found that in the case of cyber attacks on hospitals, they can be directly attributed to an increase in mortality rates.² As a result of critical technology being compromised and the downtime to crucial networks this entails, communication breakdowns can lead to the wrong medicine being prescribed, insufficient checks being carried out on a patient, as well as emergency vehicles taking incorrect routes.

Similarly, in policing, conversations on unencrypted, non-trunked radio channels can be intercepted, and sensitive data, along with officers' personally identifiable information, can be retrieved, significantly compromising officer and victim safety and the confidentiality of police work.

For the public safety sector, the vast amount of personal data that agencies hold on individuals makes them more appealing to cybercriminals. Headline-making cases in the past few years include multiple instances of cyber criminals and hackers stealing and publishing — or threatening to publish — confidential personal details on officers, victims and informants as a result of ransomware attacks and online extortion schemes, also known as double extortion.

Threat actors publish this stolen data on name-and-shame blogs as a way to punish agencies that chose not to pay ransoms. The tactic is prevalent across most industries, with a 47 percent increase in stolen company data found on ransomware leak sites in the first three quarters of 2021 compared with all of 2020. However, within the realm of public safety, double extortion has specifically coincided with an increased use of offline backups, which allows municipal victims to more reliably recover from ransomware attacks.³

² Miller, Maggie 'The mounting death toll of hospital cyberattacks,' Politico, 12.28.22
<https://www.politico.com/news/2022/12/28/cyberattacks-u-s-hospitals-00075638>

³ 2021 Cyber Threats to Public Safety: Criminal Operations,
https://blog.motorolasolutions.com/en_us/cyber-criminals-target-public-safety/





PLANNING FOR THE UNPREDICTABLE: A TRUSTED CYBERSECURITY PARTNER

We've used our 90 years' experience building mission-critical technology, and over 20 years' experience of developing cybersecurity solutions, to create the first and only ecosystem built for both public safety and enterprise. As well as computer-aided dispatch (CAD) and VESTA® 9-1-1 systems, our cybersecurity solutions are designed to protect our industry-leading ASTRO P25 radio systems - our communication system which supports first responders in the most challenging of environments. As a trusted cybersecurity partner, Motorola Solutions can provide the technology and services necessary to improve your agency's cyber resilience. From ensuring you're prepared for an attack to training your employees to better understand and recognize cyber threats, we help to ensure your focus is on your mission, not your system security.

Our cybersecurity services include an integrated portfolio of solutions aligned to the National Institute of Standards and Technology (NIST) framework.

ADVISORY SERVICES

Getting a thorough understanding of where your system's vulnerabilities lie and which regulatory and compliance frameworks will impact your organization is essential to its protection. Our highly trained security advisors will assess your organization and deliver critical insights against structured frameworks, helping you make informed decisions on the most effective security procedures and controls you can implement now and in the future. They will also support you in building a robust cybersecurity strategy and roadmap which aligns with your business needs and the latest industry best practices.

Our Advisory Services include Risk Assessments, Penetration Testing, Vulnerability Assessments, Incident Response Planning and Tabletop Exercises, as well as services to help you get the most out of our Managed Detection and Response (MDR) services. These services are designed to help you identify potential areas for improving your security posture and prepare your team for threats like ransomware.

Our Advisory Services team works independently from but collaborates closely with the ASTRO product team to address any findings that may impact your system. We have direct access to vital data, such as patching cycles and releases, ensuring we provide precise results and guidance on how to mitigate any vulnerabilities found.

Our experts utilize vulnerability scanners that are specifically fine-tuned for your system. With extensive experience in both ASTRO and cybersecurity, our team focuses on the most important aspects of your deployment and environment.

Finally, we strongly recommend incident response planning - creating a regularly updated documented plan that outlines how you will identify, contain, eradicate and recover from a cyber attack or data breach, including an element on lessons learned for future reference.





MANAGED SECURITY SERVICES

Agencies have an ongoing need to detect and remediate security issues quickly, preventing minor security threats from evolving into major incidents. A service provider with the right people, technology and proven processes can proactively monitor and manage your security needs to stop small issues from becoming big ones. Our Managed Detection and Response (MDR) solutions, powered by our ActiveEye platform, deliver 24/7 threat management and data protection across networks, endpoints, cloud infrastructure and applications, as well as mission-critical systems like ASTRO, VESTA and CAD.

ActiveEye is the only MDR solution specifically designed and supported by Motorola Solutions for ASTRO LMR radio systems. Our MDR services have been extensively tested for compatibility with Motorola Solutions products for optimal performance and enhanced security. As a co-managed and transparent service, ActiveEye offers real-time visibility into what our Security Operations Center (SOC) analysts see, providing peace of mind and actionable insights. Our dedicated team of analysts provide actionable recommendations to prevent incidents, minimize risk and ensure best practices.

SECURITY PATCHING

Vulnerabilities in software security leave you open to a cyber attack. Our security patching services help you identify and fix weaknesses in your mission-critical systems, safeguarding them against potential attacks. The breadth of these services include patch identification, along with testing and flexible deployment - both remotely and on-site.

Our engineers track all available anti-malware definitions and software patches. Only the applicable patches needed for your system are identified and selected for testing. Before applying patches to your production system all potential patches are first implemented in a dedicated Information Assurance lab to identify any possible risks or issues.

Once validated as safe we offer multiple ways to implement patches. You can deploy patches or we can implement them for you by setting up a deployment cadence on a weekly, monthly or quarterly basis.

CYBERSECURITY TRAINING

We encourage all our partners to invest in their frontline defenses by regularly participating in cyber learning. It provides employees with the means to develop their existing skills and learn new ones, ensuring that their knowledge is current and that employees remain confident in addressing cyber attacks.

GET IN TOUCH

As an established service provider, Motorola Solutions delivers unified security management and visibility across networks, devices, software and video, ensuring mission-critical responsiveness, resiliency and availability — while enabling a predictable investment. To discuss a robust cybersecurity program for your agency, [get in touch](#) and we'll be happy to help.

In partnership with the grant experts at Lexipol, we help organizations across law enforcement, fire, government, education and many more find grant funding, including grants for [cybersecurity](#) and [police radios](#). Learn more about our [grants assistance program](#).





Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](https://www.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. ©2023 Motorola Solutions, Inc. All rights reserved. 11-2023 [JP06]