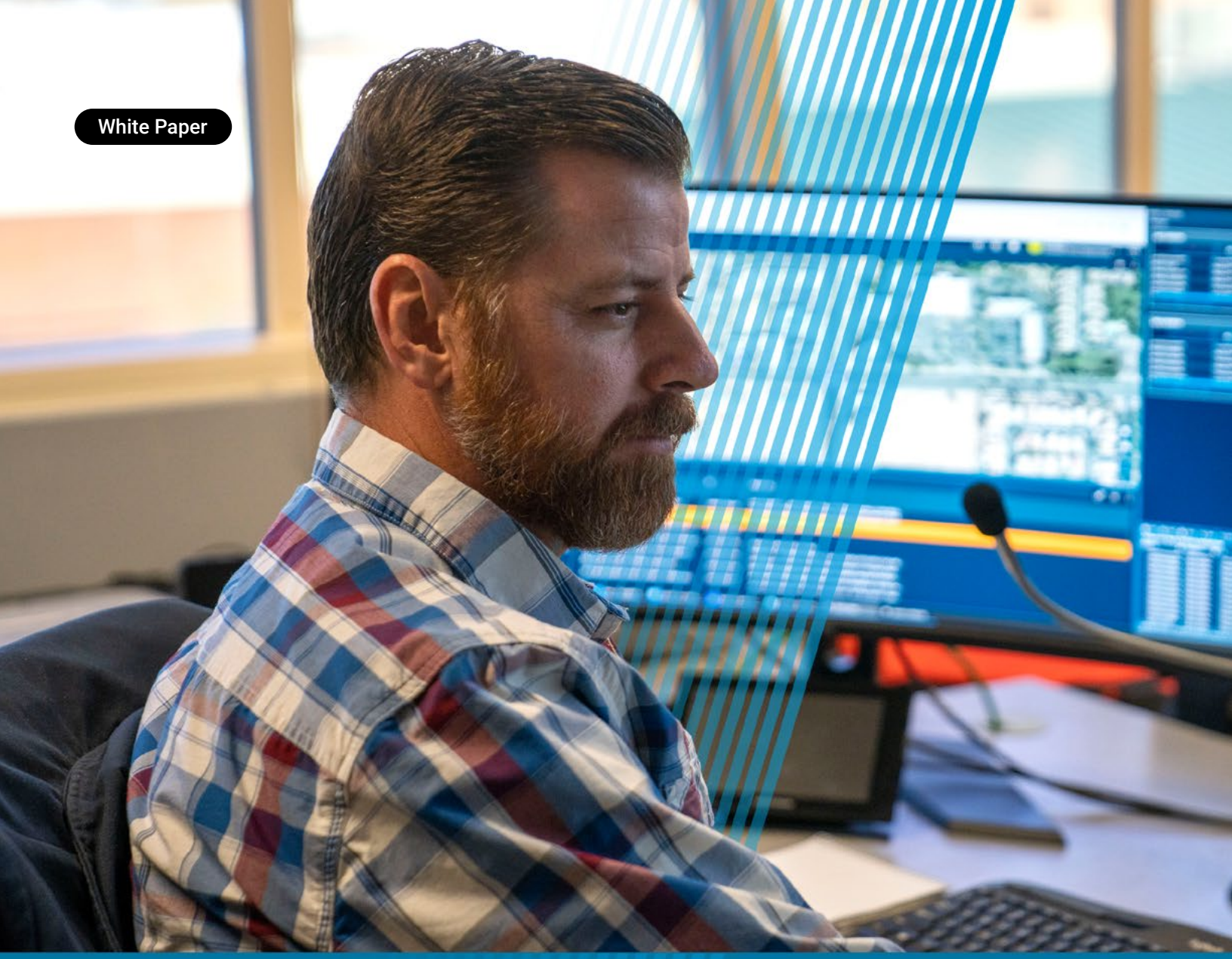
White Paper



Mitigating cyber threats to critical communication systems

MOTOROLA SOLUTIONS

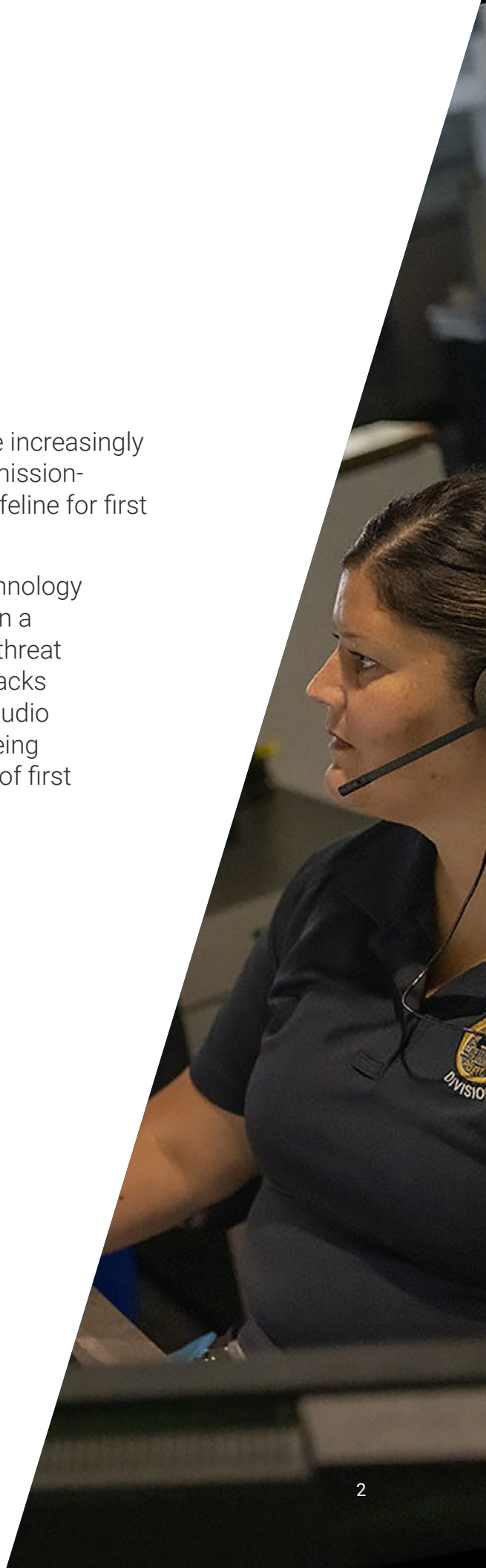
Cyber threats to mission-critical systems: growing risks, credible solutions

Since their introduction, Land Mobile Radios (LMR) and the increasingly interconnected systems they rely on have been crucial to mission-critical services — essential to everyday operations and a lifeline for first responders in emergencies.

Yet, as the capabilities of mission-critical systems and technology have evolved, so have the risks. In particular, there has been a significant rise in cyber attacks — when criminals or other threat actors gain unauthorized access to information. These attacks may consequently impact system availability, resulting in audio communications being lost or impaired and information being leaked or compromised, ultimately jeopardizing the safety of first responders and the communities they serve.

64%
increase

Cyber attacks against public safety are only growing, with a 64 percent increase globally in 2023[1]



CISA-identified cyber and physical risks within LMR

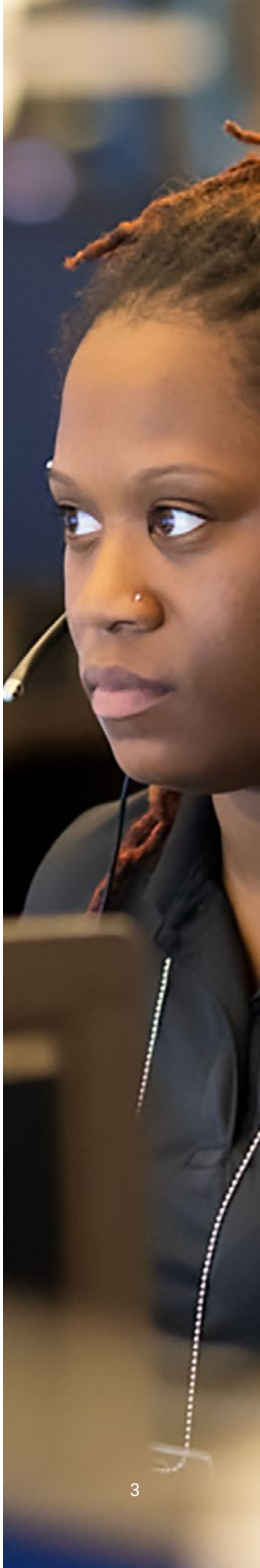
Cyber attacks come in multiple guises. The Cybersecurity and Infrastructure Security Agency (CISA) recently published guidance that identifies multiple key risks to LMR, including:

- Radio frequency (RF) interference or 'jammin': 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 a software defined radio
- Duplicate radio IDs: in a trunked radio system, duplicating radio IDs to gain access to and disrupt communications
- Poor cyber hygiene: which can include missing authentication/authorization, unpatched/outdated software and poor password management or 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)
- Supply chain attacks: which can occur when the victim's supply chain partners (e.g., customers, suppliers) are compromised in some way, and the use of the "legitimate" product or service compromises the victim's system

Additional risks include:

- Interconnected systems: while beneficial to productivity, the interconnections between LMR and other networks and systems can introduce opportunities for exploitation if they are not properly configured
- Administrative errors: radio systems are highly complex. Even minor mistakes can create configuration errors, which can 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

In this whitepaper, we provide mitigation strategies to address many of the CISA-identified risks listed above. For the complete list of all cyber risks identified by CISA, including vulnerabilities in the P25 standard and additional physical/environmental risks, view the full report



Advanced and evolving threat actors

Malicious hackers and cyber criminals are using increasingly sophisticated tactics to take advantage of weaknesses found in software, hardware, systems and devices. Last year, the average number of security vulnerabilities across organizations in multiple industries increased 589 percent[2].

Ransomware continues to be a significant threat, making up 24 percent of all cyber attacks[3]. 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 threat actors using ransomware-as-a-service (RaaS), Artificial Intelligence (AI) and machine learning to conduct attacks, as well as an increase in hacktivism, in which attackers are motivated by a particular cause or ideology.

No business or organization — large or small — is immune to a cyber attack, and any downtime can have a significant impact on the safety of first responders and the communities they serve.

The impact of cyber threats on public safety

For organizations that rely on mission-critical systems 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 can also threaten lives.

For the public safety sector, the vast amount of personal data that agencies hold on individuals — coupled with the fact that agencies must have systems available 24/7 to fulfill their mission — makes them especially appealing to cyber criminals. Headline-making cases in the past few years include multiple instances of threat actors 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 choose not to pay. Many of these attacks also impact the operations of mission-critical systems, causing them to go offline for hours, days or weeks[1].

Due to the appeal that the public safety sector presents to threat actors, cyber attacks against public safety are only growing, with a 64 percent increase globally in 2023[1]. Ransomware continues to be one of, if not the most popular tactic, with a 63 percent increase in ransomware attacks against public safety agencies in the United States[1].

Planning for the unpredictable: a trusted cybersecurity partner

We've used our 90+ years' experience building mission-critical technology and more than 20 years' experience developing cybersecurity solutions to create services that are deeply integrated with and designed for ASTRO LMR systems that support first responders in the most challenging environments.

Motorola Solutions is committed to providing the most innovative and reliable mission-critical emergency communications systems. Maintaining that reliability, especially while adding new, innovative capabilities, also requires a focus on mitigating cybersecurity threats.

From helping you prepare for potential attacks to training your employees to better understand and respond to cyber threats, we can equip you with the services you need to focus on your mission, not your system's security. Our cybersecurity services include an integrated portfolio of solutions aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Find and respond to cyber threats faster to prevent incidents

Our Managed Detection and Response (MDR) service, powered by our ActiveEye platform and supported by our 24/7 security operations center (SOC), has been extensively tested for compatibility with Motorola Solutions products for optimal performance and enhanced security. It has been specifically designed and supported by Motorola Solutions for ASTRO LMR systems to provide early detection and response capabilities to mitigate cybersecurity threats. The service can cover the entire LMR system, including Motorola Solutions and third-party components.

Endpoint security blocks many common threats with active policies tuned for the ASTRO network, without any human interaction required. This includes ransomware and other types of malware, even if it has not been seen before. With antivirus no longer being sufficient to detect advanced threats, Endpoint Detection and Response (EDR) services can proactively identify and remediate threats on endpoints within the radio system, dispatch and the related enterprise network.

Many agencies are seeking to improve their LMR communication systems with enhancements such as increased interoperability and command centers. MDR provides advanced monitoring and insights to instill confidence in implementing the new connectivity required by these services. MDR also provides key monitoring controls mandated by NIST and Criminal Justice Information Services (CJIS) guidelines set for federal IT systems and those communicating criminal justice information.

As a co-managed and transparent service, ActiveEye MDR offers real-time visibility into what our SOC analysts see, providing actionable insights. Our dedicated team of analysts provides recommendations to help your team prevent incidents, minimize risk and ensure best practices.

Understand potential risks to your system

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 can conduct a Risk Assessment for 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 can also support you in building a strong cybersecurity strategy and roadmap which aligns with your organization's needs and the latest industry best practices.

Identify potential security gaps and how to fix them

Our Advisory Services also include Penetration Testing (aka Ethical Hacking). Penetration testing and technical assessments are excellent ways to see how your cybersecurity strategy will fare in the real world. In many cases, a third-party pentest is also a mandatory requirement to meet compliance regulations or industry standards.

Proactively identify and fix vulnerabilities

Vulnerabilities in your systems can leave you open to a cyber attack. Our experts utilize vulnerability scanners that are specifically fine-tuned for your system to look for known weaknesses and security flaws. Our Security Patching services help you resolve weaknesses in mission-critical system software, safeguarding them against potential attacks. Services include patch identification as well as 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 the patches are validated as safe, you can deploy them on your own or we can set up a deployment cadence and implement them for you.

Gain expert assistance to protect your critical communications

Our Advisory Services team works independently from but collaborates closely with the ASTRO development teams to address any findings that may impact your system. We have direct access to vital information such as patching cycles and releases, ensuring we provide precise results and guidance on how to mitigate any vulnerabilities we find. In addition to Risk Assessments, Penetration Testing, Vulnerability Scanning and Security Patching, our professional services include Tabletop Exercises and Incident Response (IR) Planning. With extensive experience in both ASTRO and cybersecurity, our team focuses on the most important aspects of your deployment and environment.

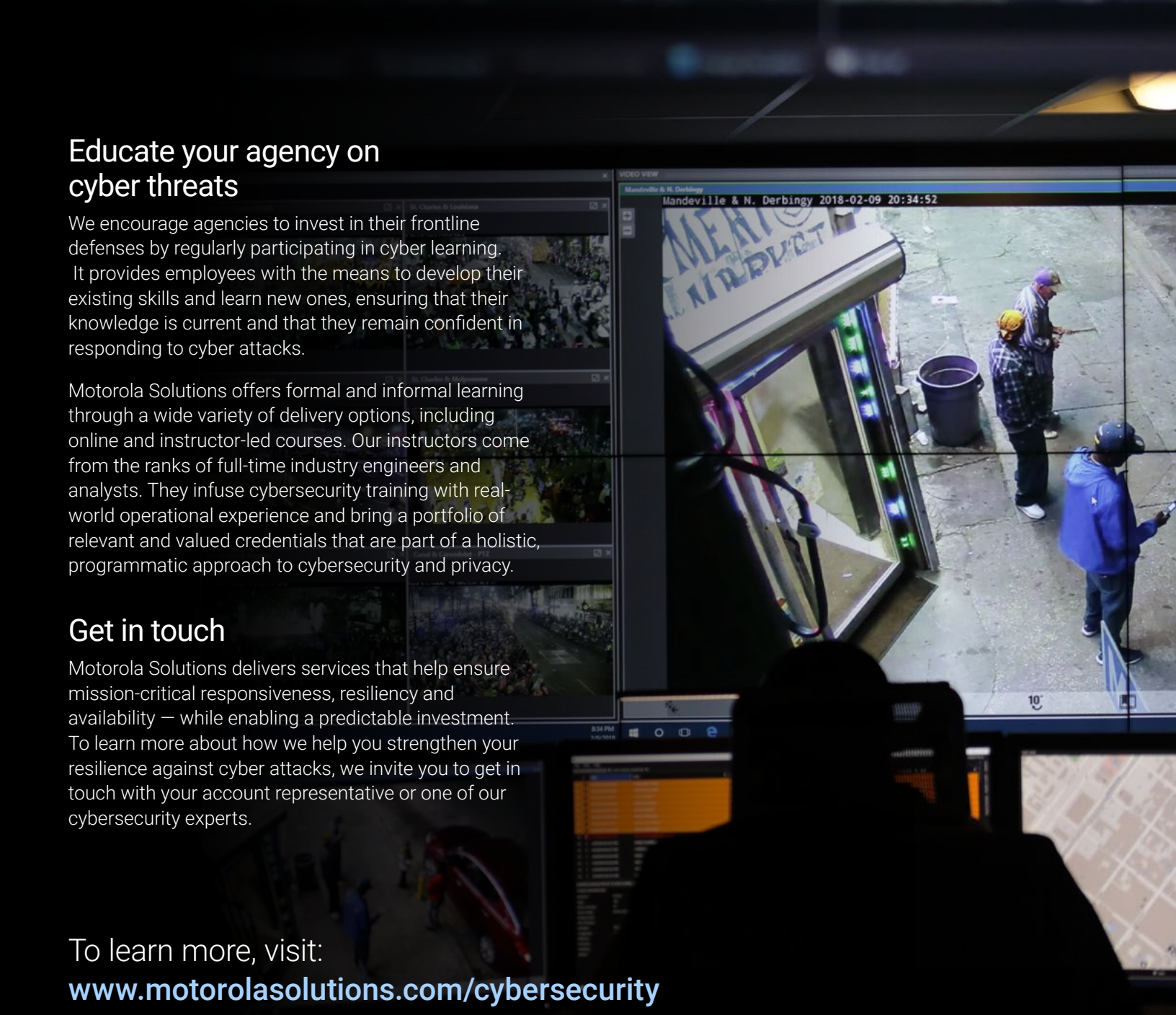
Educate your agency on cyber threats

We encourage agencies 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 they remain confident in responding to cyber attacks.

Motorola Solutions offers formal and informal learning through a wide variety of delivery options, including online and instructor-led courses. Our instructors come from the ranks of full-time industry engineers and analysts. They infuse cybersecurity training with real-world operational experience and bring a portfolio of relevant and valued credentials that are part of a holistic, programmatic approach to cybersecurity and privacy.

Get in touch

Motorola Solutions delivers services that help ensure mission-critical responsiveness, resiliency and availability — while enabling a predictable investment. To learn more about how we help you strengthen your resilience against cyber attacks, we invite you to get in touch with your account representative or one of our cybersecurity experts.



To learn more, visit:
www.motorolasolutions.com/cybersecurity

Sources

1. PSTA Finished Intelligence Report: Defending Against the Top Threats to Public Safety
2. Brooks, Chuck. Cybersecurity Trends & Statistics; More Sophisticated And Persistent Threats So Far In 2023." Forbes, 5 May 2023, https://www.forbes.com/sites/chuckbrooks/2023/05/05/cybersecurity-trends--statistics-more-sophisticated-and-persistent-threats-so-far-in-2023/
3. Verizon, 2023 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/dbir/

MOTOROLA SOLUTIONS

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