



CYBERSECURITY SERVICES

SECURING YOUR MISSION-CRITICAL OPERATIONS

CYBER ATTACKS ARE A REALITY. AND THE STAKES ARE HIGH.

For organizations tasked with mission-critical operations, system downtime endangers lives and failure is simply not an option. But cyber attacks continue to accelerate in number, frequency and impact. In fact, the annual cost of global cyber crime damage is expected to hit \$5 trillion in 2020.¹

Malware, ransomware, phishing, man-in-the-middle attacks, distributed denial-of-service attacks, SQL injections and zero-day exploits are some of the common attacks that can disrupt mission-critical operations without a moment's notice. Too often, security strategies are created to "check the box" on security compliance or as a reaction to a specific attack. Clearly, yesterday's strategies to secure mission-critical operations are inadequate to protect against today's advanced and accelerating cyber threats.

The uncertainty and the financial implications of a cyber attack have made cybersecurity a top concern for organizations. Advancement in cyber attack techniques and an ever-evolving IP-based system are putting relentless pressure on in-house resources. There is a constant need to update skills and expertise in order to manage a complex environment and bolster cyber resilience. In addition, investments in next-generation security tools to prevent and

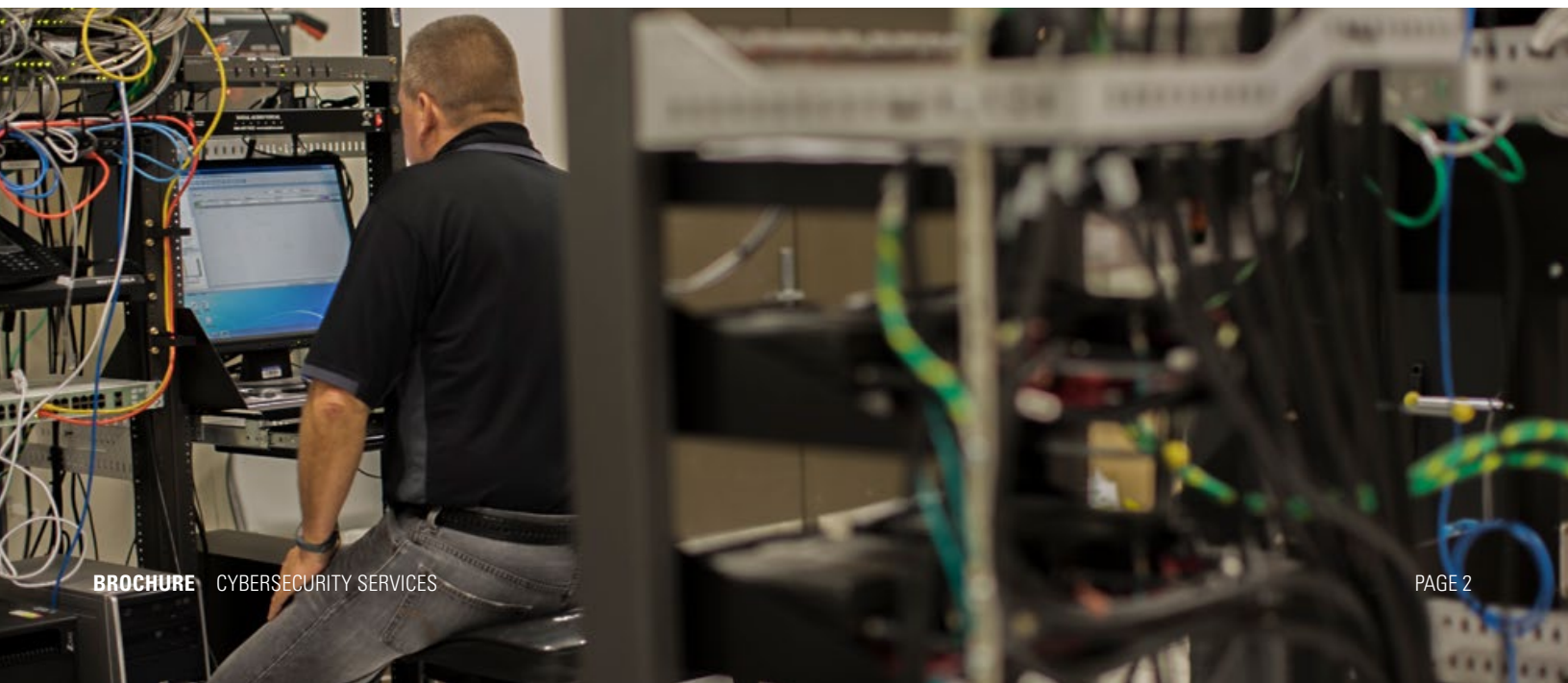
combat sophisticated threats continues to pose a challenge, as organizations face shrinking budgets.

What's needed? A holistic approach to cybersecurity centered around a risk mindset, that focuses on mitigation options, continuous monitoring, diagnosis and remediation. We can help.

We bring a range of security products and services that span your mission-critical ecosystem - networks, command center software, video and radios.

We're continuously evolving our portfolio to ensure you have the cyber resilience to stay a step ahead of increasingly sophisticated attacks.

With the seamless orchestration of highly specialized talent, industry-leading security processes and cutting-edge tools, we help manage the complexity of cybersecurity so you can focus on your core mission.



SECURED BY MOTOROLA SOLUTIONS: SERVICES FOR CYBER RESILIENCE

Our approach to cybersecurity includes a holistic set of services spanning Risk Assessment and Consulting, Security Patching and Security Monitoring. In addition, we are expanding the portfolio to include Respond and Recover services and Cybersecurity Training. All of our offerings closely follow the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is aimed at helping organizations manage cyber risk awareness, detection, response and recovery.

INDUSTRY-LEADING NIST CYBERSECURITY FRAMEWORK



IDENTIFY



PROTECT



DETECT



RESPOND



RECOVER

Assess risks	Develop safeguards	Make timely discoveries	Take action	Restore functionality
Inventory critical assets and systems	Develop policies, procedures; introduce protective tools	Continuous monitoring 24/7/365	Establish a robust response plan	Institute a recovery plan
Provide a thorough risk analysis	Implement appropriate access and auditing controls	Enable auditing capabilities	Create, analyze, triage and respond to detected events	Create improvements to prevent future attacks

CYBERSECURITY SERVICES



RISK ASSESSMENT AND CONSULTING

Based on decades of experience working closely with public safety, government and enterprise customers we've refined a systematic and reproducible risk management assessment that helps you better understand your specific security environment. This spans your technology ecosystem including the command center, LMR networks, radios and video cameras.

We start with a pre-assessment to understand your unique requirements and needs, applying a mix of physical observation, in-person interviews and both commercially available and customized tools. Then, we conduct an on-site assessment to ensure alignment with the NIST Cybersecurity Framework, evaluate potential threat scenarios and assess potential risks to the confidentiality, integrity and availability of

your organization's communication system.

Post-assessment, we deliver a clear roadmap of mitigation steps such as security architecture changes, integration of specific products or implementation of new procedural controls. All risks are identified, clearly understood and prioritized.

At the conclusion of the assessment, you receive a risk scorecard report that prioritizes each finding based on low, moderate, high and critical severity. A remediation or risk acceptance recommendation follows each finding. Finally, based upon the gaps identified, we can introduce new technologies and provide services that help you withstand security threats on an on-going basis.

REPEATABLE PROCESS, CONTINUOUS AWARENESS AND EVALUATION



SECURITY PATCHING

Security patching is one of the most important, but often overlooked, tools to defend against cyber attacks. All software, systems and devices need continuous patching to stay secure. We work with you in three phases - identification, testing and installation - to ensure your patching procedures are as efficient and secure as possible.

First, our dedicated Information Assurance Lab identifies and validates required security updates to identify any gaps in your system patches. All hardware and software assets, network and communication flows and dependencies are identified, mapped, classified and managed according to criticality. While it's important to apply patches as soon as possible once released, for mission-critical systems it's absolutely essential to thoroughly test them before

deployment. Motorola Solutions' Security Update Service pre-tests the latest anti-malware definitions and all applicable software patches in dedicated testing labs. Once validated as safe, we work closely with you in the installation phase. We either make the updates for you or make them accessible on our secure extranet for implementation, so your organization can easily deploy them on its own terms.

You cannot effectively patch aging systems. Today's IP-based mission-critical networks require periodic upgrades to stay current. Motorola Solutions provides system upgrades to enable both software and hardware technology refresh across your infrastructure while ensuring system availability.

SECURITY MONITORING

Remote security monitoring delivers the most cost-effective and secure way to monitor your networks. Our remote monitoring capabilities allow 24/7/365 protection, are delivered by technical experts and are backed by automation.



We use a systematic process to detect, analyze, investigate, resolve and report on incidents to protect your system.

DETECT POTENTIAL THREATS - Your Motorola Solutions systems are pre-configured with intrusion detection sensors, authentication and logging server integration, and antivirus integration to detect worms, viruses and other forms of malicious software. Threat intelligence from global and social media news is also constantly fed into the system. Tools are in place to capture and examine system logs throughout your network infrastructure, devices, operating systems, software and applications. If a malware or intrusion event is detected on your system an alert is generated and appropriate action is taken.

ANALYZE DATA AUTOMATICALLY - Using machine learning algorithms, all events on your system are automatically filtered to actual incidents, omitting false threats. This system is programmed and trained to identify intrusion attempts, malware infection, network-based scanning and authentication activity.

INVESTIGATE INCIDENTS - Incident details are generated automatically and sent to security analysts who thoroughly research and analyze the incident, leveraging the knowledge base for skilled triaging and troubleshooting.

RESOLVE AN INCIDENT - If an incident is confirmed on your system, our technologists will work quickly to identify and implement a fix. They will monitor the event until it is fully resolved and the incident is closed to your satisfaction. To close out the case they will provide on-site assistance to make sure the situation is remedied and your system returns to full operational mode.

REPORT INSIGHTS - We want to keep you informed of any changes to your system health. Our post incident reports are quickly generated, used to implement preventive measures, shared with your team and leveraged in future security operations to better protect your network.

MYVIEW PORTAL

We understand that it is critical for you to have full visibility into the performance of your entire technology ecosystem. Our web-based management portal provides actionable insights into your system status and health, allowing you to keep an eye on the health of your mission-critical ecosystem. Known as the MyView Portal, it provides you quick, easy insight into your security incidents and service delivery status from a single web-based platform.



YOUR MOTOROLA SOLUTIONS EDGE: PEOPLE, PROCESS AND TOOLS

Effective cybersecurity goes beyond technology. Our industry-leading talent, security processes and cutting-edge tools are part of an integrated approach that streamlines complexity and makes it easier for your organization to manage risk.

PEOPLE

Lack of cybersecurity expertise is a constant challenge facing many organizations today. This can slow adoption and implementation of the critical tools and processes needed for effective cybersecurity protection.

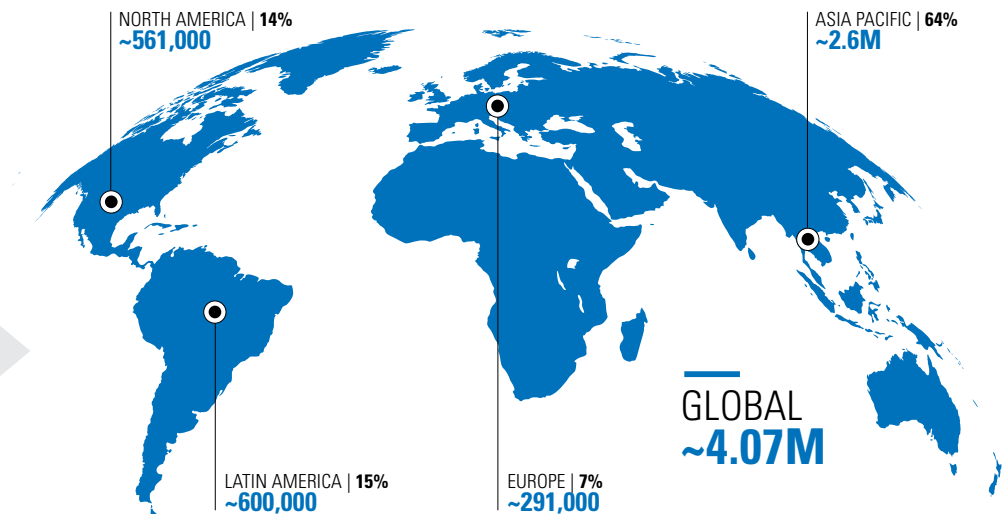
Our people are the driving force of our security culture, one that's fully integrated in everything we do. Our cybersecurity experts guide the entire range of our cybersecurity solutions, constantly striving for more predictive and proactive cybersecurity. They hold top industry cybersecurity certifications such as Criminal Justice Information Services (CJIS), Federal Information Processing Standards (FIPS) and Federal Information Security Management Act (FISMA) and stay sharp with comprehensive, ongoing training. We created the Motorola Solutions Cyber Champions Program, which instills cybersecurity principals and knowledge at a grassroots level throughout every facet of the company.

We continuously invest in cyber education and training because when our cybersecurity experts are set up for success, so are you. We use the NIST Cybersecurity Workforce Framework to guide our cyber education and training efforts.

In addition, the Motorola Solutions Threat Intelligence team creates a holistic view of the cyber threat landscape and how it impacts our customers' business priorities and infrastructure. The team analyzes and communicates the capability, opportunity and intent of a cyber threat targeting Motorola Solutions' products and customers. This level of situational awareness provides stakeholders and decision makers with the information needed to prioritize resources and enable better security decisions. Our experts are here to help you navigate a complex technology environment so that your people can focus on the mission, not the technology.

THE CYBERSECURITY PERSONNEL CRISIS

The global cybersecurity expertise shortage is estimated at just over 4 million professionals with over 500,000 of those positions located in North America. Asia Pacific, with its growing economies and new privacy regulations, is experiencing the biggest shortage - 2.6 million positions.³





PROCESS

Our cybersecurity processes are guided by three core objectives: confidentiality, integrity and availability. Data and information must be confined to people authorized to access it and not be disclosed to others; data must be kept intact, complete and accurate, with IT systems operational; and all information must be available to authorized users whenever needed. While many organizations simply focus on prevention, in today's threat climate, every enterprise must be thoroughly prepared for a "worst-case" cyber attack scenario.

TOOLS

Criminals and state actors are always evolving the technology they use in cyber attacks. To stay a step ahead, we constantly become more predictive and proactive with investments in sophisticated tools such as automation and analytics. When properly applied, automation and analytics can lower operational costs, accelerate service response and augment predictive decision-making by eliminating many of the time-consuming manual processes involved in managing threats. In addition, using advanced analytics to examine threats and failure patterns across the system can eventually prevent

With the NIST Cybersecurity Framework at its core, our approach to cybersecurity focuses on mitigation options, continuous monitoring, diagnosis and remediation to secure and protect systems and networks. In addition, we are aligned with the principles of industry recognized ITIL management practices, Service Design, Service Transition and Service Operations for service delivery. Our experienced team draws on extensive global knowledge to develop a service delivery model, architecture and policies that meet your needs.

security incidents more effectively by addressing their root causes before they impact the system. Based on a rich data lake, these tools continuously optimize system performance.

We also continuously invest in other advanced technologies such as security incident and event management (SIEM); network intrusion detection and vulnerability scanning. We employ the most advanced cybersecurity tools so you can always keep up with complex technology trends, without investing additional time and resources.

CYBER RESILIENCE DONE RIGHT

Cyber attacks can happen to anyone at any time. Are you ready? Our cybersecurity services offer the expertise, cutting edge technology and responsiveness to help you get there. Partnering with Motorola Solutions for cybersecurity allows your team to focus on your mission, not systems upkeep. We manage the complexity for you, which means you are always on pace with innovation at a predictable cost. Our team of specialists will become your team, holistically securing your most important communication assets, anticipating issues

before they become problems and continuously improving plans to prevent future attacks.

Motorola Solutions is the mission-critical communications leader for a reason. We bring the same trust and commitment you've relied on for over 90 years to every cybersecurity service we offer. With industry-leading people, processes and tools we're redefining what it means to ensure resilience for mission-critical operations.

GLOBAL SCALE AND EXPERIENCE

4M

USERS UNDER OUR
MANAGED SERVICE

20M

EVENTS PROACTIVELY
MONITORED EACH DAY

13K

SYSTEMS
INSTALLED

100K

CUSTOMERS ACROSS
100 COUNTRIES

90+

YEARS OF
EXPERIENCE

NOTES

1 Cyber Defense Magazine

2 2018 Motorola Solutions LMR System Management Benchmark Survey

3 ISC2 2019 Cybersecurity Workforce Study, 2019

See how Motorola Solutions can help keep your organization secure.
Visit www.motorolasolutions.com/cybersecurity to learn more.



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. 800-367-2346 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. © 2020 Motorola Solutions, Inc. All rights reserved. 03-2020a