CYBERSECURITY ADVISORY SERVICES

PREVENT ATTACKS, MEET COMPLIANCE REQUIREMENTS AND RESPOND QUICKLY TO SECURITY INCIDENTS

MOTOROLA SOLUTIONS

TABLE OF CONTENTS

Cybersecurity Services Snapshot 2-3

Risk Assessments 4

Penetration Testing 5

Incident Response Planning 6

Tabletop Exercises 7

Compliance Assessments 8

Building a Cyber Defensive Mindset 9

Resources 10

CYBERSECURITY SERVICES SNAPSHOT

To protect your systems, it's critical to have a complete understanding of where you might be vulnerable and which regulatory and compliance frameworks impact your organization.

Motorola Solutions Cybersecurity Services bring together an integrated portfolio of Managed Detection and Response (MDR) and Advisory Services aligned to the National Institute of Standards and Technology (NIST) framework.

As a trusted partner, we help you develop roadmaps to safeguard your information, employees and systems.

Our security advisors can assess your organization and deliver critical insights so you can make informed decisions on the best security procedures and controls to implement and build a robust cybersecurity strategy and roadmap in line with your business needs and industry best practices.

GLOBAL SCALE & EXPERIENCE

300+
Security experts focused on 24/7 monitoring and response

9B
Security events proactively monitored each day

20+
Years of experience developing cybersecurity solutions

PEOPLE

Experts with top industry certifications work hand-in-hand to ensure system availability and security

PROCESS

Mission-critical ITIL framework for scalable service operations that can easily handle peak load

TECHNOLOGY

Network to security operations, security orchestration and automation — designed to accelerate service response

100% co-managed approach for visibility and control

Cybercrime costs organizations an average of $2.9 million[1] every minute, with global ransomware damage costs predicted to exceed $265 billion[2] by 2031.

Motorola Solutions 90+ years of skilled experience, collaborative approach and use of scenario-based drills will prepare your organization to detect and respond to threats quickly in the event of a cyber attack.

RISK ASSESSMENTS

Our assessments provide your organization with useful insights by analyzing your current environment, systems and security program to identify critical vulnerabilities and gaps that need to be addressed. We use this information to develop a robust cybersecurity strategy that is mapped to key regulatory frameworks and provide a prioritized list of risks and vulnerabilities.

PRE-ASSESSMENT

Together we define the scope and agree on the desired outcome to meet your operational needs. Our cybersecurity experts collaborate with your team to define the statement of work and all deliverables. We develop an end-to-end understanding of your business operations including network architectures, security policies and controls, compliance and governance frameworks to finalize engagement scope and timelines.

ONSITE ASSESSMENT

Our onsite assessment, which includes data gathering and documentation, starts with one-on-one interviews with key stakeholders, understanding business profiles and analyzing annual statements and existing approaches to security. Workshops are conducted to close out any knowledge gaps. We can perform regulatory assessments along with vulnerability and threat intelligence assessments to evaluate network, applications and endpoints.

POST-ASSESSMENT

Once our consultants have collected the data, they distill it using a set of sophisticated programs including a Risk Scorecard report indicating low, moderate, high and critical severities for each finding. Then, working with your team, we produce a set of roadmaps and recommendations to strengthen your system's cyber resilience.

PENETRATION TESTING

Our experts evaluate the security of your IT and communications infrastructure by trying to exploit its vulnerabilities. By probing your systems for any potential gaps, we can reveal issues that could leave your organization at risk and recommend how to close them before a malicious actor exploits them. Motorola Solutions offers penetration testing, also known as pentesting, to ensure that your organization is aware of potential risks and how to best address them.

TYPES OF PENTESTING

EXTERNAL

An external network pentest is designed to test the effectiveness of perimeter security controls to prevent and detect attacks, such as physical premises security and digital authentication soundness. It can also identify weaknesses in internet-facing assets such as web, mail and FTP servers.

WIRELESS

A wireless pentest is performed by ensuring that all wireless connections between the business WiFi network and devices are secured from attacks.

INTERNAL

An internal network pentest helps organizations detect what an attacker could achieve with insider access to their network. An internal network pentest can mirror threats that can come from within an agency, such as an employee intentionally or unintentionally performing malicious acts or an external malicious threat actor who gains access to the same privileges as an employee.

WEB APPLICATION

A web application test ensures that any public facing web application, such as a website, is secure and that any data connected or submitted to that page is safe.

PHASES OF PENTESTING

PRE-ENGAGEMENT

Establish Rules of Engagement (ROE)

ENGAGEMENT

Perform pentests aligned with ROE

POST-ENGAGEMENT

Document and submit applicable findings

INCIDENT RESPONSE PLANNING

With cyberattacks on the rise, it's increasingly important to have an incident response (IR) plan ready in the event that your systems are compromised. Our incident response services are tailored to your needs and organizational structure to optimize how your agency will handle a cyber attack. Motorola Solutions custom IR plans are designed to be the best fit for your employees, processes and technology so you have a well-defined plan in the time of need.

BE PREPARED FOR ANY SITUATION

Industrial Control Incidents

Natural Disasters

Internal/External Threats

PROVEN APPROACH TO SECURITY INCIDENT MANAGEMENT

Motorola Solutions can help contain or prevent an incident by recommending and implementing safeguards. Through an array of technologies and skill sets around cloud analytics, endpoint threat hunting, log and data analytics, system forensics, malware analysis and more, our incident response planning provides assistance developing an integrated response to cyber attacks and data breaches. This can also include advanced threat hunting and post-incident analysis.

TABLETOP EXERCISES

Tabletop exercises are a type of emergency preparedness planning exercises that enable a broad group of participants to evaluate the effectiveness of your organization's incident response plan, as well as walk through the who, what, when, where and how of a situation in a safe environment.

Cyber exercises like this provide a valuable real-world scenario to see how prepared your team is and where improvements should be made, as well as ensuring that key stakeholders across the organization understand their role in the event of an emergency. These exercises improve the team's ability to detect, respond and recover to cybersecurity incidents faster.

20%

Of employees are likely to click on phishing email links[3]

95%

Of cybersecurity breaches result from human error[4]

BE PREPARED FOR ANY SITUATION

- RANSOMWARE
- PHISHING
- MALWARE
- DATA BREACH

COMPLIANCE ASSESSMENTS

Our compliance assessments give you data-driven, prioritized recommendations to inform better cyber risk management and decision-making. We ensure your team adheres to the regulatory cybersecurity requirements that are in line with your unique organizational needs and follow industry best practices.

ASSESSMENT OPTIONS

Our experts can provide gap analysis preparation and pre-audit verification. Audit reports* evaluate the strength and thoroughness of compliance preparations, security policies, user access controls and risk management procedures over the course of a compliance audit. Our experts are also approved to assess your agency or organization as meeting certain compliance certifications.

CYBERSECURITY MATURITY MODEL CERTIFICATION

The **Cybersecurity Maturity Model Certification (CMMC)*** program includes cyber protection standards for companies in the defense industrial base (DIB). By incorporating cybersecurity standards into acquisition programs, CMMC provides the Department assurance that contractors and subcontractors are meeting DoD's cybersecurity requirements.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 800-171

National Institute of Standards and Technology (NIST) 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT 800-53

Federal Information Security Modernization Act (FISMA)(NIST) 800-53 is the guideline established for federal agencies to uphold regulatory requirements regarding the management of their information security systems.

STATERAMP

StateRAMP provides a comprehensive security framework designed to improve cloud security for state and local governments.

FEDRAMP

FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 2700X/9001

International Organization for Standardization (ISO) 2700X/9001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.

CENTER FOR INTERNET SECURITY CONTROLS

Center for Internet Security (CIS) Controls are a set of 20 best practices that can guide you through the process of creating a layered cybersecurity strategy.

* Motorola Solutions can currently only provide audit reports for CMMC.

INDUSTRY-LEADING NIST CYBERSECURITY FRAMEWORK

IDENTIFY

Assess Risks

Inventory critical assets and systems

Provide a thorough risk analysis

PROTECT

Develop Safeguards

Develop policies, procedures; introduce protective tools

Implement appropriate access and auditing controls

DETECT

Make Timely Discoveries

Continuous monitoring 24/7/365

Enable auditing capabilities

RESPOND

Take Action

Establish a robust response plan

Create, analyze, triage and respond to detected events

RECOVER

Restore Functionality

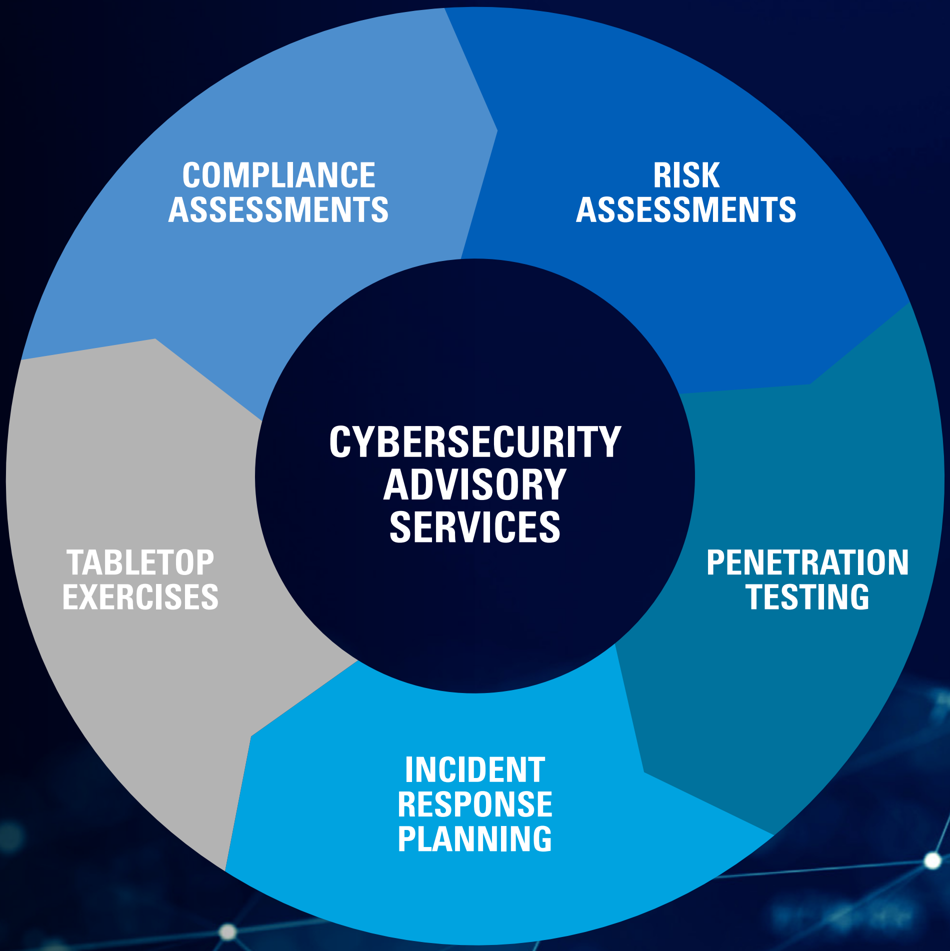
Institute a recovery plan

Create improvements to prevent future attacks

BUILDING A CYBER DEFENSIVE MINDSET

When a cybersecurity incident occurs, what will you do? With cyberattacks growing in number and intensity, businesses and public safety agencies must be prepared to keep critical operations running smoothly by detecting and handling security incidents and breaches. Our experts are ready to work with your agency to create a comprehensive cybersecurity strategy plan.

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions Cybersecurity Services empower agencies to take control of their security and instill confidence in employees to handle cyber risks.



CYBERSECURITY ADVISORY SERVICES

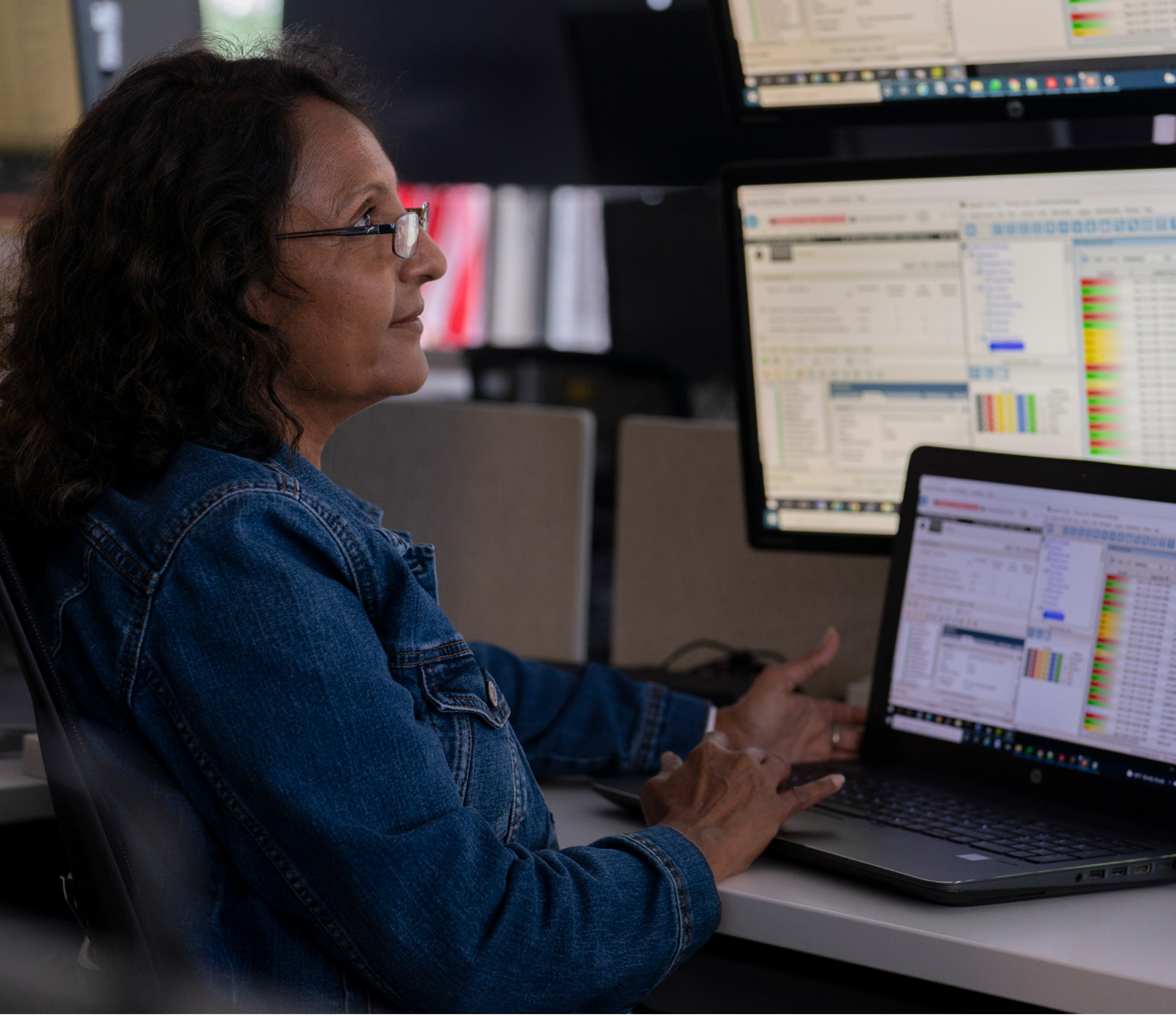
COMPLIANCE ASSESSMENTS

RISK ASSESSMENTS

PENETRATION TESTING

INCIDENT RESPONSE PLANNING

TABLETOP EXERCISES



RESOURCES

1 https://www.forbes.com/sites/joeljohnson/2020/08/11/what-costs-29-million-every-minute-and-how-to-protect-yourself-from-it/?sh=509e33ed7764

2 https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

3 https://www.techrepublic.com/article/phishing-emails-more-than-25-of-american-workers-fall-for-them/

4 https://www.cybintsolutions.com/cyber-security-facts-stats/

MOTOROLA SOLUTIONS

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