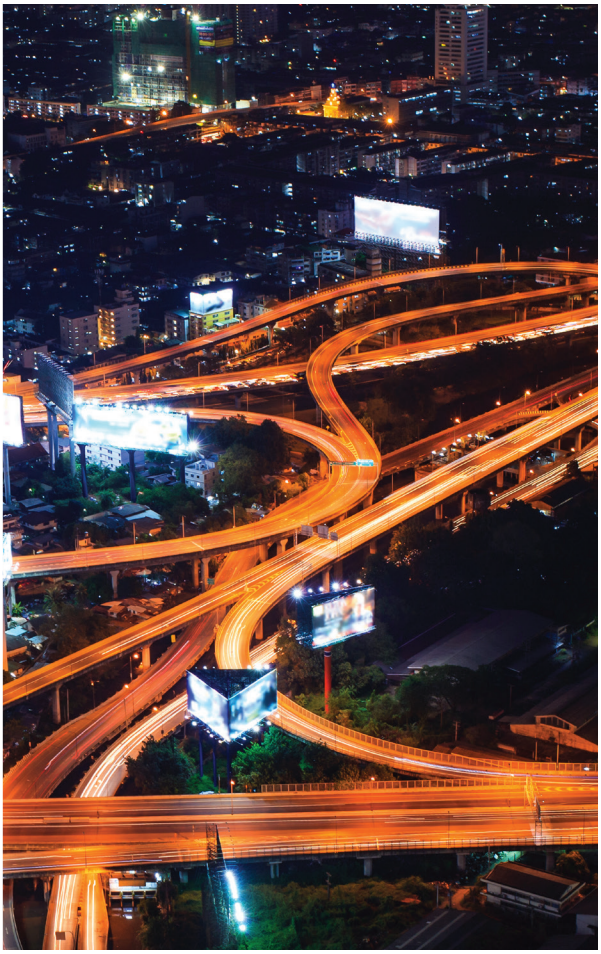
ASCERTAIN YOUR RISK BEFORE IT BECOMES REALITY

MOTOROLA



CYBERSECURITY PROFESSIONAL SERVICES

A COMPREHENSIVE AND SYSTEMATIC APPROACH TO RISK MANAGEMENT AND PROTECTION OF CRITICAL INFRASTRUCTURE

BUILDING MORE RESILIENT NETWORKS IN AN ERA OF INCREASING CYBER ATTACKS

The digital world has brought to life unprecedented ways to increase productivity, maximize value, and ultimately improve the lives of billions of people. At the same time, an explosion of cybersecurity incidents has brought unique challenges to businesses and government agencies alike. Today, polymorphic attacks capable of modifying themselves with every execution are ubiquitous. While many organizations would like to think their most sensitive mission-critical information is inoculated, it is becoming increasingly clear that no one is immune. Cybersecurity goes beyond hacker attacks and technical controls.

The cybersecurity regulatory and enforcement landscape is also dynamic and rapidly evolving, creating more challenges in complying with a myriad of industry standards while managing appropriate security controls. As mission-critical networks evolve into dynamic systems of interconnected networks with more open-source platforms and cloud-based solutions, governance and oversight throughout the system's operational lifecycle is required. This encompasses a coordinated and regular re-evaluation of people, processes and technology to assure organizational readiness to protect, detect and respond to evolving threats.

UNDERSTANDING YOUR CYBERSECURITY RISK POSTURE

Motorola's Cybersecurity Professional Services provide a comprehensive and systematic process for identifying, assessing and managing cybersecurity risk throughout enterprise systems. With Cybersecurity Professional Services, you will be able to fully understand your cybersecurity risk posture related to your organization's operational environment. Motorola provides a comprehensive assessment of your attack surface profile; a cost/benefit evaluation and detailed remediation recommendations. With ever-changing technologies and business processes, security threats are always changing and your organization's security posture is never static. Periodic security posture assessments help to maintain a current record of vulnerabilities and help to prioritize remediation activities necessary based on overall risk to your operations.

In 2014, the National Institute of Standards and Technology (NIST) issued the Framework for Improving Critical Infrastructure Cybersecurity for organizations to achieve specific cybersecurity outcomes. The Framework comprises leading practices from various standards bodies that have proved to be successful when implemented. Motorola Solutions participated alongside government and industry partners to help develop this framework. As a result, Motorola's assessment leverages the NIST recommendations by mapping the NIST Cybersecurity Framework to your organization's current risk management processes and procedures to determine your current cybersecurity profile risk levels and recommendations.

NIST CYBERSECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Business Environment	Policies	Anomalies and Events	Response Planning	Recovery Planning
Risk Governance	Processes	Detection Processes	Communications	Improvements
Asset Management	Data Security	Continuous Monitoring	Analysis	Communications
Risk Assessment	Access Control		Mitigation	
Risk Management	Protective Technology		Improvements	
	Awareness and Training			

Critical infrastructure is diverse and complex—these systems must be secure and able to rapidly recover from all hazards including physical and cyber events. Our efforts to drive risk reduction and management activities are based upon identifying assets; assessing risk based on consequences, vulnerabilities, and threats; establishing priorities for mitigating risk; implementing protective programs; and measuring effectiveness.

IMPROVING RISK MANAGEMENT BY IDENTIFYING AND REDUCING THREATS

Through years of working with public safety, government and enterprise customers, the Motorola Cybersecurity Professional Services team has developed a holistic and methodical risk management approach that offers a comprehensive, risk-prioritized and informative outcome. Risk owners and decision makers receive carefully calculated and factual appreciation of applicable risk factors.

SCOPE	Only applicable controls spanning Technical, Management and Operational categories are selected to conduct a tailored risk analysis. Mitigation steps such as security architecture changes, integration of specific products or implementation of procedural control are recommended and discussed with the stakeholders only after the environment is methodically evaluated, risks are identified, analyzed, clearly understood and risk prioritized.
APPROACH	Using physical observation, in-person interviews, manual, computerized, commercially available and custom tools, Motorola will evaluate potential threat scenarios and assess potential risk implications to confidentiality, integrity and availability of the organization's mission.
METHODOLOGY	All applicable risk factors are considered and taken into account prior and during the assessment. After capturing all necessary data pertaining to the scope of the assessment, a threat profile is developed and prepared as a Risk Scorecard report indicating low, moderate, high and critical values for each finding/issue identified. A remediation or risk acceptance recommendation will follow each finding/issue.

CYBERSECURITY PROFESSIONAL SERVICES DISCIPLINES

MANAGEMENT

- Business Impact Analysis
- Asset Identification/Classification
- NIST Framework Readiness Assessment
- Framework Governance Structure and Institutionalization
- Cyber Risk Scorecard and Organizational Key Performance Indicators (KPIs)
- Organizational Policy and Standards Development
- Operational Processes Effectiveness
- Threat Modeling/Threat Intelligence
- Intellectual Property Risk Assessment
- Off-shore Manufacturing and Software Development Risk Evaluation
- Secure Development Lifecycle
- Threat Analysis/Research
- Regulatory Compliance Impact Evaluation
- Third-Party Vendor Management Policy Process
- Training and Awareness

OPERATIONAL

- Ad-hoc Customer Inquiries
- Operational Security Assistance
- Incident Response Assistance
- Digital Forensics Investigation
- Tailored Security Monitoring
- Customized Anomaly Detection Monitoring
- Social Engineering Testing

TECHNICAL

- Technical Risk Cybersecurity Assessments
  - Vulnerability Scans
  - Web Application Security
  - LAN and Wireless Penetration Testing
  - Physical Penetration Testing
  - Cloud Implementation Assessment
- Compliance Evaluation
- Network Architecture Review
- Identity and Access Management Solutions
- Third-Party Connectivity Evaluation
- SCADA Environment Risk Assessment
- Network Discovery/Asset Inventory
- Application Audit/Code Review
- Security Reference Architecture
- Enterprise Architecture Security
- Cryptographic Services
- Secure Mobile Technology Adoption
- "Honey Pot" Deployment and Monitoring
- Open Source Software Licensing Compliance

CYBERSECURITY PROFESSIONAL SERVICES DELIVERY OPTIONS

Motorola's Cybersecurity Professional Services team is comprised of certified, security professionals trained to stay actively informed of the rapidly changing landscape of security threats and compliance technologies. We will work with you to establish the best assessment methodology to meet your desired business outcomes. Options include:

MOTOROLA EXECUTED	JOINT ENGAGEMENT	INDEPENDENT THIRD PARTY COORDINATION
Motorola's Cybersecurity Professional Services Team conducts the comprehensive assessment and provides risk-prioritized recommendations.	Motorola lead engagement working alongside your IT staff to ensure program sustainability, information sharing and expert collaboration.	A reputable third-party entity designated to conduct impartial assessment with MSI oversight to ensure successful execution and delivery to meet your objectives.

RELY ON MOTOROLA SOLUTIONS FOR PROACTIVE CYBERSECURITY RISK MANAGEMENT SERVICES

As a global leader providing secure technologies for mission-critical operations in more than 100 countries, we fully understand the importance of designing, developing and deploying innovative technologies that are most effective and secure.

Expectations are increasingly demanding a more comprehensive approach for cybersecurity throughout the solution development, implementation and operational lifecycles. Technology advancements in mission-critical communications result in a wider attack surface that can leave you vulnerable to security breaches.

Your critical systems are seen as high-value targets by cyber criminals who continue to get more technologically savvy. These compounding trends lead to increased risks to availability, confidentiality and integrity of your mission-critical voice and data. Taking a holistic approach to system security with proactive threat detection, real-time response and corrective actions can give you the peace of mind that your system is secure and resilient.

For more information about Security Services, contact your Motorola representative or visit **motorolasolutions.com/services**.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorolasolutions.com**

MOTOROLA