CYBERSECURITY ASSESSMENT SERVICE
YOUR FIRST LINE OF DEFENSE

Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and organizational information, disrupting critical operations, and causing substantial economic losses to individuals, corporations and governments. It has even negatively impacted the confidence of government agencies to manage citizen records as well.

Hostile actors, be it hackers, organized criminals, or foreign countries are rapidly improving their technical cyber capabilities. They will also continue to target governments and organizations operating critical infrastructure services, such as public safety agencies, health care, transportation and aviation with a single focus - to steal, manipulate sensitive data, and/or to disrupt everyday operations.

This scenario played out in 2018, when cyber criminals attacked the national healthcare body governing the largest cluster of healthcare institutions locally – SingHealth's IT system. The compromised system led to the data of 1.5 million patients, including records of outpatient medication given to the Prime Minister, being illegally accessed. For transport systems and services, cyber attacks could impact commuter safety with disruptions of signaling systems, or components that go into boards and cards put into railway systems that are not security certified.

RANSOMWARE AND PUBLIC SAFETY

In 2019, there was a notable increase in ransomware attacks against cities and public sector agencies. Motorola Solutions believes that the sheer criticality of emergency services will likely prompt cyber criminals to launch increasingly targeted and sophisticated ransomware extortion attacks directly against emergency services for potential financial rewards, or to cause disruption as a punitive action.

We anticipate more targets on critical systems such as the public safety answering points (PSAP), or managed service providers (MSPs) will take place in order to increase the scale of infection, and the likelihood of receiving a payout.

Additionally, as the demand increases for accessible ransomware options in criminal marketplaces, we predict that the Ransomware-as-a-Service (RaaS) model will grow in popularity to meet that demand.

The stakes are extremely high. Emergency services are a key component of critical infrastructure. Failing to protect the confidentiality, integrity and availability of the information systems that support them, as well as the information residing within them, puts lives at risk and endangers public confidence in the government itself.

UNDERSTAND YOUR CYBERSECURITY RISKS

Most public safety agencies do not have personnel with a deep knowledge of the latest cybersecurity policies and procedures, leaving vulnerabilities open to cyber criminals. Hiring outside consultants to periodically assess your network can bring your organization the critical information needed to make informed decisions like the latest security procedures for network access, vulnerability patching, operation continuity and incident response plans.

An essential initial step is to start off with a Cybersecurity Risk Assessment, which provides an informed overview of your organization's cybersecurity posture and offers data for cybersecurity-related decisions. Risk assessment is the building block on which your organization can establish the priorities for mitigating risk, implement protective programs and measure the effectiveness of those programs – to give you the peace of mind that your system is secure and resilient.

YOUR TRUSTED, VALUE-ADD PARTNER

While the technology infrastructure for public sector organizations can be diverse and complex – these systems must be secure and be able to rapidly recover from all hazards including physical and cyber events. Motorola Solutions' Cybersecurity Assessment Service has been used by many of the world's leading organizations, including public sector organizations. We can help you get a picture of vulnerabilities in your IT systems and prioritize remediation activities necessary based on overall risk to your operations.

Our team consists of highly knowledgeable personnel with industry certifications, knowledge of best-in-class organizational policies and procedures, and expertise in state-of-the-art automation and analytics tools. We are uniquely equipped to deliver enhanced cybersecurity solutions that address your needs today and in the future.

A HOLISTIC, RISK-BASED APPROACH

Our risk assessment professionals use a consultative approach to provide security resilience assessments. Our program follows a proven three-step approach: pre-assessment, onsite-assessment and post-assessment.

- **Pre-assessment:** Together we will define the scope and agree on the desired outcome to meet your operational needs, and finalize engagement scope and timelines.
- **Onsite-assessment:** We perform a National Institute of Standards and Technology (NIST) Aligned Risk Assessment to evaluate networks and applications across your mission-critical ecosystem, along with Technical Vulnerability and Threat Intelligence Assessments.
- **Post-assessment:** Data collected will be distilled using a set of sophisticated programs, including a Risk Scorecard report and recommendations.

MAXIMIZE AVAILABILITY
Manage risk and maximize the availability of your mission critical operation

MAINTAIN FOCUS
Focus on your core mission while Motorola Solutions assesses the risks to your operation

REDUCE COST
Minimize the impact of a cyber incident and implement efficient security controls based on risk

TECHNICAL PARTNERSHIP
Leverage Motorola Solutions technical expertise and experience to protect your operation

REDUCE CYBER RISK TO YOUR OPERATION

For more information about our Cybersecurity Risk Assessment Services, contact your Motorola Solutions representative or visit us online.

www.motorolasolutions.com/cybersecurity-apac

MOTOROLA SOLUTIONS

Motorola Solutions Australia & New Zealand PTY LTD. 10 Wesley Court, Tally Ho Business Park, Burwood East, Victoria 3151, Australia **motorolasolutions.com**