PROTECT CRITICAL INFRASTRUCTURE FROM CYBER THREATS

A MULTIFACETED CYBERSECURITY APPROACH TO SAFEGUARD YOUR OPERATIONS

BROCHURE | CYBERSECURITY SERVICES

MOTOROLA SOLUTIONS

CYBER ATTACKS INFILTRATE CRITICAL INFRASTRUCTURE SECTORS

Government and enterprise critical infrastructure sectors such as energy, communications and emergency services have become prime targets for cyber criminals. The Aspen Institute surveyed 625 IT executives in charge of critical infrastructure worldwide and 72% believe cyber attacks are increasing. Almost 9 out of 10 have had at least one breach in the past year. Almost half believe there will be a cyber attack that may result in a potential loss of life.[2]

At one point just a buzzword, ransomware is now an all-too-real threat to businesses, governments, and individuals worldwide. 2017 gave us a very sharp reminder that patching of critical infrastructure is essential.

The sophistication of threats are increasing and organizations may need to adapt processes and practices in order to safeguard against it in order to maximize system configuration, integration and availability.

As an organization in charge of managing critical infrastructure systems, safeguarding your system against cyber attacks is top of mind. From the employee who unknowingly inserts a virus laden USB flash drive into a laptop infecting a network to organized cyber criminals aiming to take down critical infrastructure, crippling a city, town or country, cyber attacks are coming from every direction and have become an everyday occurrence.

Leveraging the skills and tools of cybersecurity experts can provide you with a robust, systematic approach to cyber resiliency.

$3.8 MILLION IS THE AVERAGE COST OF A DATA BREACH TO A COMPANY[1]

146 DAYS IS THE MEDIAN NUMBER OF DAYS AN ATTACKER STAY WITHIN A NETWORK BEFORE DETECTION[2]

60 PERCENT OF MALWARE PAYLOADS IN Q1 2017 WERE RANSOMWARE[3]

SIXTEEN SECTORS TOP THE TARGET LIST

Department of Homeland Security (DHS) identified 16 National Critical Infrastructure (NCI) Sectors[3] that could impact a nation's stability and our everyday lives if they were to fall victim to a cyber intrusion. The importance of safeguarding these systems against cyber threats and potential attacks are at the top of the agenda for managers in charge of keeping them operational.

Chemical

Commercial Facilities

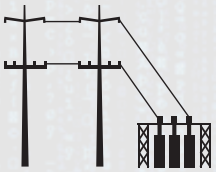
Communications

Critical Manufacturing

Dams

Defense Industrial Base

Emergency Services



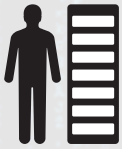
Energy

Financial Services

Food Agriculture

Government Facilities

Healthcare and Public Health



Information Technology

Nuclear Reactors, Materials and Waste

Transportation Systems

Water and Wastewater

MORE THAN 50%

OF U.S. BUSINESSES EXPERIENCED A CYBER ATTACK IN THE PAST YEAR.[4]

HOLISTIC APPROACH TO CYBER RESILIENCE
RISK ASSESSMENT SERVICE

Establishing and implementing a cybersecurity strategy comes with many considerations. As a critical infrastructure organization, you need to understand and apply the cybersecurity industry standards and risk governance frameworks pertaining to your sector. Staying current with rapidly changing cyber threats and network vulnerabilities adds another layer of complexity to being cyber resilient. The security measures you took yesterday may not be right for tomorrow's cyber assault.

CERTIFIED, TRAINED EXPERTS CURRENT ON LATEST TRENDS

Our cybersecurity experts stay abreast of the continuously changing frameworks and standards worldwide. Working with framework including DISA STIGs, NERC, NIST 800-53, ISO27001, CES, or CIS we can work with your organization to develop a plan to meet a necessary level of compliance. Our comprehensive approach does not stop here even though this is an important step. We work hand-in-hand with you to understand your risk posture, develop a prioritized plan focused on safeguarding your operational integrity, and identify the right tools and services needed to address on-going threats and vulnerabilities.

CYBERSECURITY FRAMEWORK	SYSTEMATIC ANALYSIS AND PLAN
IDENTIFY **ASSESS RISKS**	**Perform a thorough risk analysis** **Uncover potential vulnerabilities**
PROTECT **DEVELOP SAFEGUARDS**	**Develop policies and procedures** **Implement appropriate access and auditing control**
DETECT **MAKE TIMELY DISCOVERIES**	**Continuous monitoring 24x7x365** **Enable auditing capabilities**
RESPOND **TAKE ACTION**	**Establish a robust response plan** **Correlate, analyze, triage and respond to detected events**
RECOVER **RESTORE FUNCTIONALITY**	**Institute a recovery plan** **Create improvements to prevent future attacks**

PRE-TESTED SECURITY UPDATES ASSURES SYSTEM CONTINUITY

Today's IP-based mission critical LMR systems use multiple third party software programs from anti-virus to Microsoft®. Each one has a different update cadence. Routinely patching with the latest software updates is critical to protecting your LMR systems from known vulnerabilities and potential cyber attacks.

Before these security updates can be added to your system, they need to be tested to make sure they will not cause havoc. Our certified security experts help validate security updates – alleviating this burden from your staff. All security updates are pre-tested in our dedicated system test lab to make sure there will be no issues when the patches are applied to your system. Once verified, we can install the updates for your organization or your IT staff can download and install the updates.

THE RIGHT DELIVERY OPTION FOR YOUR ORGANIZATION

SELF-INSTALLED SECURITY PATCHES

Once the patches have been certified by our security experts, you can download the latest updates from a secure extranet site and install the software on your timeline using your technicians.

REMOTE SECURITY UPDATE SERVICE DELIVERY

Our technicians will install the software patches on your system: verify all patches are working optimally, test your mission critical system performance and provide status reports.

WHY PATCHING IS NECESSARY

85 PERCENT OF SUCCESSFUL HACKS USED THE TOP 10 EXPLOITS[5]

PROACTIVE MONITORING
FOR CONTINUOUS THREAT ASSESSMENT

Cyber criminals do not work 9 to 5. It is not enough to simply barricade your network with advanced firewalls, anti-malware, encryption algorithms and sophisticated access controls. You need to continuously monitor your system 24x7x365, looking for unusual activities, traffic anomalies, suspicious logs, too many failed log-on attempts, and so on. However, monitoring alone is not enough. System trends also need to be analyzed to diagnose potential cyber incidents in real time. According to the Center for Strategic and International Studies (CSIS), 85% of breaches take months to discover — on average 5 months[5].

Our Security Monitoring Service provides a comprehensive methodology to remotely monitor your system against malicious attacks from external and internal vectors. When a potential incident is suspected, our experienced and highly trained security experts take decisive countermeasures to respond.

TWO APPROACHES TO PROTECT YOUR NETWORK

REMOTE MONITORING

Dedicated cybersecurity analysts in our Security Operations Center (SOC) monitor your network 24x7x365 and take corrective action as needed.

- Deploy the latest analytical tools on your system
- Correlate events across multiple systems and establish intelligence needed for a comprehensive response
- Identify, investigate and resolve potential cyber incidents

ON-PREMISE MONITORING

Monitor your network via tools provided by Motorola.

- Tailored tool set to continuously monitor your system within your isolated network environment
- Regularly updated dashboards reflecting vital information required by your team to identify security events of interest and respond accordingly – including an overview of system status from the homepage
- 24x7 access to Motorola's certified security experts

ROBUST SECURITY OPERATIONS CENTER CAN DO THE WORK

At the Motorola Solutions Security Operations Center (SOC), our trained analysts work around the clock to protect your network from impending cybersecurity threats with a three prong approach; real-time monitoring, proactive analytics and decisive action in the event an incident is detected. When a potential threat is identified, we put in place actions to mitigate the threat and notify your organization.

146 DAYS IS THE MEDIAN NUMBER OF DAYS AN ATTACKER STAYS WITHIN A NETWORK BEFORE DETECTION[5]

ARE YOU PREPARED FOR A CYBER ATTACK?

Increasing cyber threats requires a more continuous, end-to-end approach for protecting your critical communication environment. The security measures you took yesterday may not be right for tomorrow's cyber assault.

Leveraging the skills and tool set of our cybersecurity experts, trained to stay actively informed of the rapidly changing landscape of security threats and compliance requirements, the cybersecurity services which are available through our service packages are designed to help safeguard your operational integrity. They are:

Security Patch Installation. Pre-tested security updates are deployed onto your radio network system to address known vulnerabilities as soon as they are available and validated to avoid network disruption.

Security Monitoring. Our team of experienced security professionals remotely monitor your system from our Security Operations Center (SOC) for security events and apply countermeasures whenever necessary.

On-Premise Security Operations Center. If remote security monitoring is not a viable option for you, our On-Premise Security Operations Center provides you with a reliable means to proactively monitor your network for unusual security activities.

Cybersecurity Risk Assessment Services. Using industry standards and frameworks, we perform a comprehensive risk assessment to help you understand your risk posture and steps that should be taken to mitigate, react, and respond to cyber threats based on your unique operational requirements.

AT-A-GLANCE: CYBERSECURITY SERVICES BY SERVICE PACKAGES

SERVICES	ESSENTIAL	ADVANCED	PREMIER
Cybersecurity Risk Assessment Services			
Security Monitoring			
Remote Security Patch Installation			
Self-Installed Security Patches			

MOTOROLA SOLUTIONS UNDERSTANDS CRITICAL INFRASTRUCTURE AND THE IMPORTANCE IT PLAYS IN KEEPING OUR COMMUNITIES SAFE

Cyber attacks are the reality of the world we live in. Making sure you are ready to respond is every organization's responsibility. When you need to protect your systems from cyber intrusion, trust the leader in mission critical communication, Motorola Solutions. Our cybersecurity experts are skilled, subject-matter professionals, ready to work with your organization to enhance your ability to identify and manage cyber risks. To learn more about our cybersecurity services, contact your Motorola Solutions representative.

SOURCES:

1,2. Microsoft Advanced Threat Analytics 2016
3. Malwarebytes
4. Insurance Journal, September 29, 2017
5. Verizon 2018 Data Breach Investigations Report

For more information about our Cybersecurity Services, contact your Motorola Solutions representative or visit **motorolasolutions.com/cybersecurity**.

MOTOROLA SOLUTIONS

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