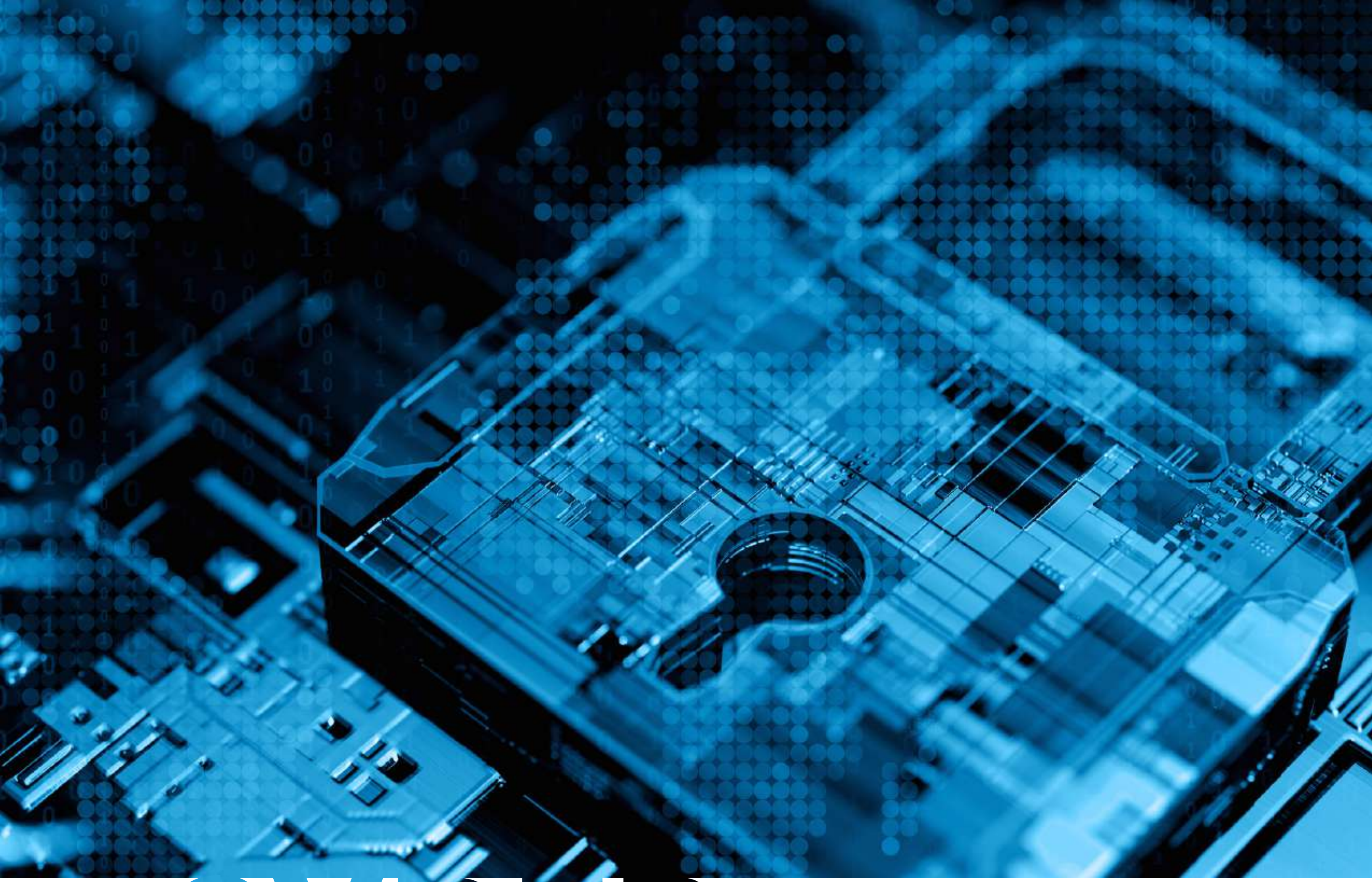


CYBER RESILIENCE

IMPLEMENTING A HOLISTIC, RISK-BASED APPROACH TO SECURITY

MOTOROLA SOLUTIONS

TABLE OF CONTENTS

A Holistic, Risk-Based Approach to Security

The frequency and sophistication of worldwide cyber attacks continues to surge. Today, it is widely recognized that no agency, company, or organization is immune.

This is especially true of public safety and government agencies, which are increasingly prime targets for cyber attacks of all types including malware, ransomware, and insider attacks.

A recent study by SecurityScorecard, a company that provides organizations with security risk ratings, analyzed the security postures of 552 local, state, and federal government organizations. Across all industries surveyed including transportation, retail, healthcare and more, government organizations received one of the lowest security scores. When compared to other industries government organizations especially struggled with endpoint security and patching cadence.[1]

Most agencies acknowledge the importance of protecting the continuity of their critical infrastructure and are stepping up efforts to put frameworks and policies in place to do so. This white paper outlines four security challenges facing public safety and government organizations, along with straightforward steps to implement a holistic, risk-based approach to addressing these challenges.

WHAT IS CYBER RESILIENCE?

According to the Department of Homeland Security, resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[2] Cyber resilience is a perspective that marries information security, business continuity, and resilience. It aims to help government and business prepare, prevent, respond and recover from cyber breaches. It is also a wholesale shift in thinking from earlier, individual cybersecurity efforts such as anti-virus programs, firewalls, and perimeter security that were touted as cure-alls that could be bought, installed, and essentially forgot. Cyber resilience counsels that security is an integral part of an agency or company's core business, its processes embedded in every level of day-to-day operations with complete buy-in from IT departments, all staff, and the most senior executives and board members.

CHALLENGE #1

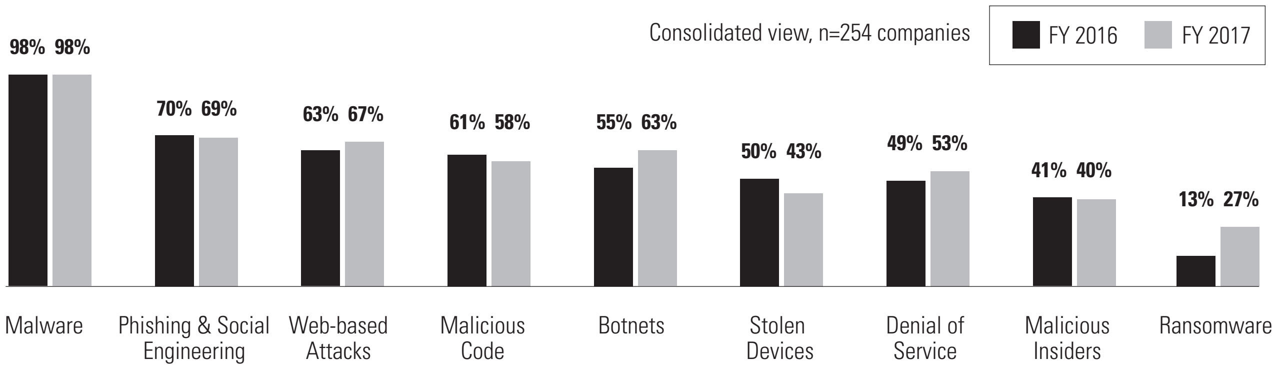
Advancement of Cyber Attack Techniques

Cyber resilience is critical to the daily operations of public safety agencies. If the confidentiality, integrity, or availability of communication systems is impacted, the consequences can be dire, even leading to loss of life.

The unfortunate reality is that attackers now have the ability to lock critical systems and destroy data as part of their breach process, with security experts predicting this type of behavior is a precursor to devastating attacks. Other types of threats are growing as well. According to the 2017 Poneman Cost of Cybercrime Study, ransomware breaches increased significantly from 13% in 2016 to 27% in 2017. 69% of respondents experienced phishing and malicious social engineering and 67% of companies had Web-based breaches. Virtually all organizations had breaches relating to viruses, worms and/or trojans and malware over the four-week benchmark study period.[3]

To combat these threats, agencies must first break free from "snapshot thinking." This is the thought process that once a security strategy and solution are in place, all is well with one's IT environment. To manage and stay ahead of evolving threats, risk assessments, information assurance roadmaps, and other security measures must be continuous.

TYPES OF CYBER ATTACKS EXPERIENCED BY COMPANIES



Source: Ponemon 2017 Cost of Cybercrime Study

CHALLENGE #2

Spending on Cyber Tools Alone Does Not Ensure Security

The Ponemon Institute also looked at organizational spending on security and found that even though the average annual cost of cybersecurity for organizations across industries is $11.7 million — a 22.7% increase over 2016 — security capabilities have not delivered the desired efficiency and effectiveness.[4]

Successful breaches per company **increased 27%** from 2016 to 2017

The average time to resolve a malicious insider attack is **50 days**

Ransomware attacks doubled in frequency from **13-27%**

The average time to resolve a ransomware attack is **23 days**

To get the most value from their investment, organizations should ensure they are fully optimizing the capabilities of tools they already have, before buying new ones. They may find available updates enable new capabilities that were not originally present. But if spending alone doesn't ensure security, what does? A culture of good security processes across the organization and accountability at the executive level. A security team can help guide, prioritize, respond and inspect, but security must also live throughout an entire organization. Plus, because breaches are likely to happen despite an organization's best efforts, it's important to practice how the agency will respond to the public in the case of an intrusion, in addition to more technical responses.

CHALLENGE #3

New Attack Vectors from Open, Interconnected Networks

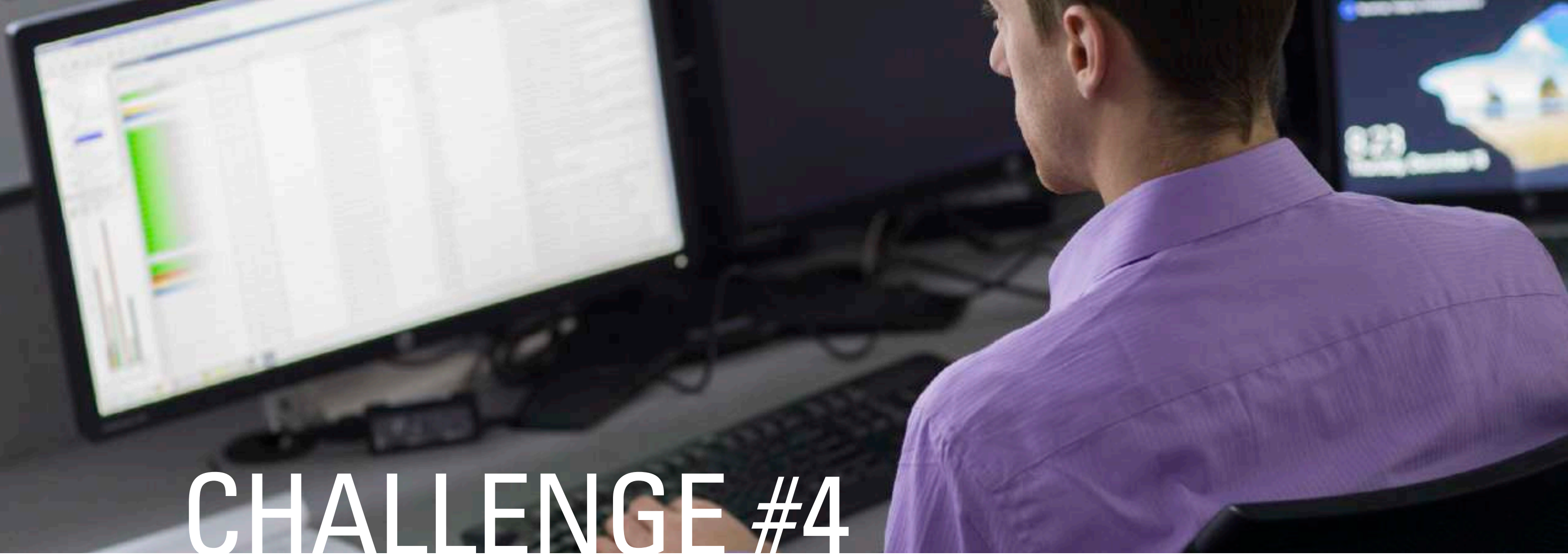
With the rapid pace of technology deployments and new data streams driven by operational enhancements such as video analytics and intelligent policing, public safety networks are becoming more interconnected.

These improvements are bringing great benefits to agencies, enabling business collaboration and innovation. However, they also come with added risk. Devices, software, and networks that were completely isolated are now managed in, or connected to, the cloud, creating new attack vectors. Adversaries looking to exploit the weakest points in systems and devices now have more entry points and can move laterally across networks without detection.

This increased level of interconnectivity creates new blind spots. Organizations do not always have complete visibility into what and how devices and software are connected to their network and their entire IT and operational ecosystem. Research by Lumeta found that a lack of visibility can lead to 20-40% of network and endpoint infrastructure becoming unknown or unmanaged by an organization.[5] Recent ransomware attacks show just how proficient attackers are at capitalizing on vulnerabilities across devices and networks for maximum impact.

Agencies need to take steps to safeguard enterprise software and connected devices and ensure continuous monitoring capabilities. Their objective must be to make it as difficult as possible for adversaries to achieve their goals while limiting damage done if vulnerabilities are exploited.

> “
> More than **2.5 quintillion bytes** of data are created every day. The sum of all knowledge will **double every 12 hours** in the future. That is a mind-boggling amount of data that will be created in the near future. And as we've seen over the past few years, it's becoming a liability for companies facing ever-more sophisticated cyber attacks.
>
> *— 2017 ASIS President Thomas J. Langer, CPP, in his opening remarks at ASIS 2017.*



CHALLENGE #4

Lack of Security Expertise

The availability of security experts is a constant challenge facing public safety and government agencies.

This is a problem that continues to get worse. According to the Global Information Security Workforce Study conducted by Frost & Sullivan for the Center for Cyber Safety and Education, the cybersecurity workforce gap is on pace to hit 1.8 million by 2022 — a 20% increase since 2015.[6] Agencies also have to compete with private organizations that can be more attractive to available talent.

This lack of security experts may slow an agency's ability to adopt and implement critical tools needed for cybersecurity efforts. For example, public sector organizations tend to fall short on threat investigation. According to the 2017 Motorola Solutions IT Services in Public Safety Survey, even with sizeable investments, many organizations still cannot keep pace with device and data security. 51% of respondents said they could use at least one more employee to cover necessary data security tasks.[7]

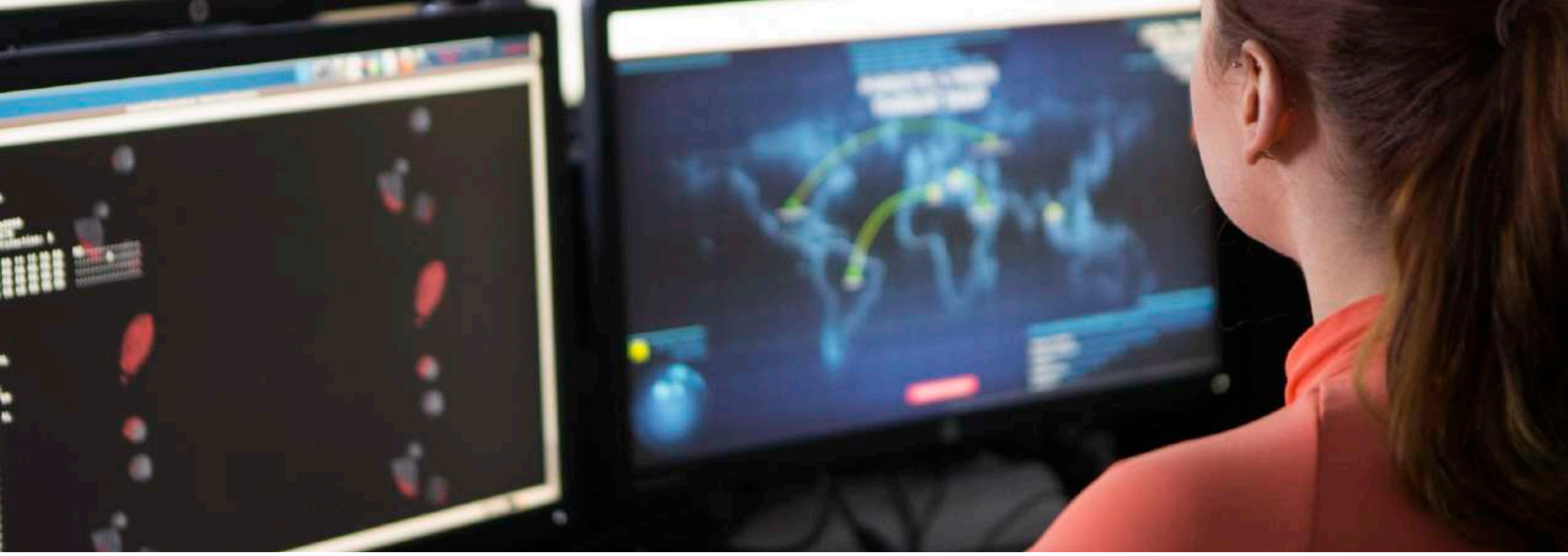
The seemingly ever-increasing need for security professionals arises, in part, because security is often not built into systems and organizational culture from the beginning. Ensuring solutions are implemented correctly the first time is much cheaper than having to hire additional resources to fix it afterwards.

Software as a Service and third-party support options should also be considered. These SaaS and support solutions place the responsibility of protecting the systems and data on the vendor, who are accountable to you.

In addition, it's important to track malicious cyber trends and plan against those trends. Then, adjust as needed and exercise again. These can take the form of condensed table top exercises, but going through the entire process from start to finish is even better. A real-world breach scenario is not the time to discover your teams can't actually act as fast as you thought they could during a table top exercise.

The cybersecurity workforce gap is on pace to hit **1.8 million** by 2022 – a **20% increase** since 2015.[6]

51% of survey respondents said they could use at least **1 more employee** to cover necessary data security tasks.[7]



From Compliance-Focused to a Holistic, Risk-Based Strategy

On average, hackers spend 146 days on a victim's network before they're discovered.[8]

This finding validates that organizations may be directing their attention to the wrong places. In effect, closing an open window or door, but never checking to see if someone had come in.

Security strategies and implementation are often driven by the response to attacks or the need to meet compliance requirements and deadlines—not by a holistic approach to risk-based security. Forward-looking security conscious organizations are shifting to a risk mindset, focusing on mitigation options, continuous monitoring, diagnosis and remediation to evolve security practices.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework, which Motorola Solutions endorses, serves as a guide to help organizations manage their cyber risk awareness and security and detection, response and recovery. In May 2017, an executive order requiring federal agencies responsible for the safety of the nation's technical infrastructure to follow the NIST framework was signed into law in the U.S. This order impacts public safety networks such as NG9-1-1 and i3 networks. The NIST Framework has proven to be an effective approach and should be adapted to an organization's individual security goals and resources.

RISK-BASED STRATEGY: DEFINED

A Risk-based strategy begins with the process of identifying and reviewing the complete range of risks an organization faces. By first assessing risks, you become actively aware of where uncertainty surrounding events or outcomes exists. Then, based on risk prioritization, steps are identified to reduce risk or remediate a situation to protect the organization, people and assets concerned. Forward-looking security conscious organizations are shifting to this risk mindset, focusing on mitigation options, continuous monitoring, diagnosis and remediation to evolve security practices. Ultimately, this approach saves both time and money by proactively, not reactively, confronting potentially hazardous situations before they become acute threats.

A Simplified Framework for Maximum Results

To create a comprehensive security approach that improves an organization's security posture, focus on the five core functions of the NIST framework by breaking each into smaller activities that are easier to implement.

CYBERSECURITY FRAMEWORK	SYSTEMATIC ANALYSIS AND PLAN
IDENTIFY Assess Risks	• Provide 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 • Create, analyze, triage and respond to detected events
RECOVER Restore Functionality	• Institute a recovery plan • Create improvements to prevent future attacks

Using the NIST Framework to Prepare for Cyber Threats

Whether from targeted attacks, ransomware, advanced persistent threats (APTs), or insider exfiltration, agencies must be proactive and prepared to handle an increasing array of attacks, both internal and external in nature. This point was highlighted in March, 2018 as a major US city experienced a breach of their CAD system. Using the five core functions of the NIST framework, agencies can begin to prepare for almost any cyber threat, including the below hypothetical CAD breach scenario.

CAD Ransomware Attack

IDENTIFY

- All System hardware and software assets identified, inventoried, classified and managed according to criticality.
- All network and communication flows are identified, mapped, classified and managed according to criticality.
- All external Systems dependencies are identified, inventoried, classified and managed according to criticality.
- System mission, objectives, resiliency requirements, and activities are defined and prioritized.
- Cybersecurity policies are established and institutionalized.
- Roles and responsibilities, including cybersecurity, are defined and coordinated for all internal personnel and external stakeholders for operation of the System.
- Risk/Threat assessment and management practices are established for the System, external Systems, Suppliers, Partners, and Supply Chain. Priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Vulnerability assessment and management practices are employed for the System. Ongoing vulnerability and security testing, monitoring, tracking, and remediation practices are established.

PROTECT

- Physical and environmental controls are employed to meet the mission and operational requirements of the System. Effective protection technologies and controls are employed, covering Network, Platform, Application, etc. The controls employed ensure meeting the mission and operational requirements of the System.
- User identity and access management controls are employed. Secure remote access and maintenance (local and remote access) controls are employed. Network access and integrity protection employed through network access controls and segregation. Access controls follow least privilege, least functionality, and separation of duties.
- Ensure sufficient network and compute capacity to meet availability requirements of the System.
- Data-at-Rest and Data-in-Transit security controls employed to support CIA of data at rest / transit. Data loss prevention mechanisms are implemented. Removable media is blocked or protected.
- Employ change, configuration, and lifecycle management practices of all assets during their lifespan: install/update/patching, operation, removal, transfer, and disposition.
- Employ integrity and authenticity mechanisms to verify software, and to protect against malicious software installation.
- Auditing/logging controls are defined and implemented.

DETECT

- Employ mechanisms to ensure anomalous activity is detected in a timely manner. Mechanisms must be tested.
- Employ physical controls with monitoring and alerting capabilities.
- Employ host controls, such as HIDS, host firewalls, asset whitelisting, anti-malware and malicious code protection, etc., with alerting mechanisms.
- Employ network controls such as NIDS, network firewalls, router ACLs, network anti-malware detection, and 802.1x/MPL, with alerting mechanisms.
- Employ application protective and detective controls, such as robust error/exception reporting, WAFs, API gateways, etc.
- Employ logging/auditing, event monitoring and event correlation (SIEM). Events, event sources, behaviors, behavior thresholds, and impacts must be well understood.
- Employ activities monitoring of internal personnel, external stakeholders, and external service providers for cybersecurity events.
- Employ vulnerability assessment and management practices for the System. Ongoing vulnerability and security testing, monitoring, tracking, and remediation practices established.

RESPOND

- Response Plan processes and procedures are executed during and post incident.
- Response Plan is improved and maintained to ensure timely response to detected cybersecurity events.
- Roles and Responsibilities are well defined in the Response Plan, with contingencies for delegation of authority.
- Effective communications, information sharing, and situational awareness practices areas employed with internal / external stakeholders. External communications and notifications are in compliance with applicable regulatory requirements.
- Incidents are categorized and handled consistent with Response Plan.
- Employ effective analysis and forensics techniques.
- Mitigate the incident by containment of the attack and initiating corrective actions and controls.

RECOVER

- Execute Recovery Plans processes and procedures to restore the System and associated assets to operation.
- Recovery Plan is improved and maintained to ensure timely recovery from cybersecurity events.
- Effective communications, information sharing, and situational awareness practices areas employed with internal / external stakeholders. External communications and notifications are in compliance with applicable regulatory requirements.

The latest cyber headlines offer fresh warnings: agencies must be ready for breaches to critical networks such as CAD systems. As states and municipalities are finding out, the best protection is a proactive, holistic, and risk-based approach using the five core functions of the NIST framework as a guide.

Build Resiliency to Protect Mission-Critical Assets

Public safety and government agencies fully acknowledge that it's no longer a matter of if, but when and how they become prime targets for adversaries.

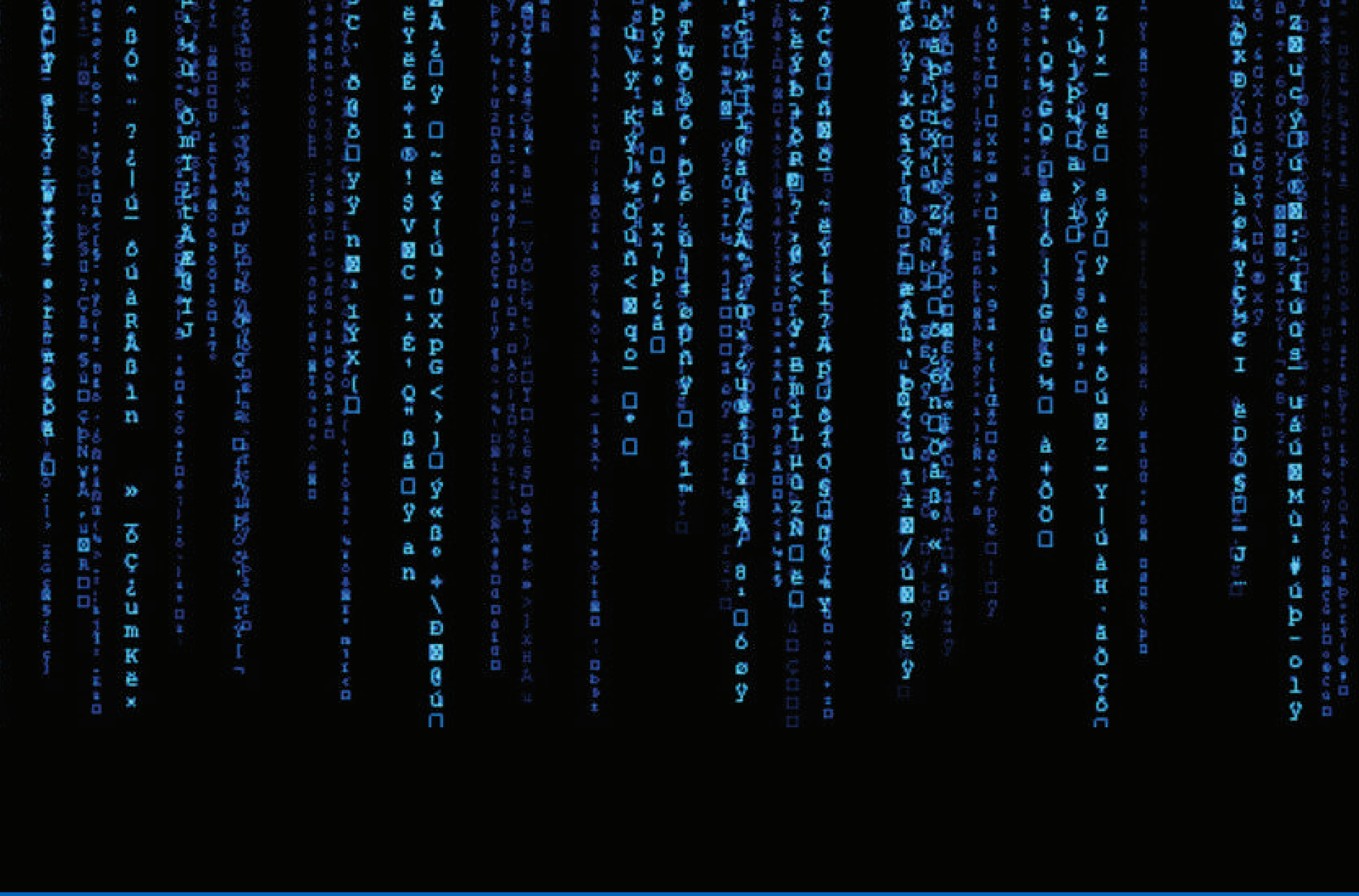
Safeguarding critical communication networks and technologies requires a comprehensive — yet simplified — approach to address existing vulnerabilities, assess risk posture, take proactive measures to monitor threats and understand how to respond and recover from intrusions.

While the challenges created by new attack vectors, a severe shortage of cybersecurity professionals, and a lack of desired effectiveness from existing security solutions are real, there are tangible actions agencies can take to significantly reduce risk, identify attacks and move to swift remediation. Implementing a holistic, risk-based approach to cyber security, starting with the five core elements of the NIST framework, will give mission-critical organizations the necessary tools to win the battle for information assurance in this evolving threat climate.

TRUSTED CYBER RESILIENCE EXPERTISE

Increasing cyber threats require a more continuous, end-to-end approach to protecting your critical communication environment. The security measures you took yesterday may not be right for tomorrow's cyber assault. When you need to protect your systems from cyber intrusion, trust the leader in mission critical communication, Motorola Solutions. Leveraging the skills and tool sets of our cybersecurity experts, trained to stay actively informed of the rapidly changing landscape of security threats and compliance requirements, the cybersecurity services available through our land mobile radio (LMR) service packages are designed to help safeguard your operational integrity. They are Security Patch Installation, Remote Security Monitoring, On-Premise Security Operations Center and Cybersecurity Risk Assessment.

To learn more, visit:
motorolasolutions.com/cybersecurity



1. 2017 U.S. State and Federal Government Cybersecurity Report, SecurityScorecard https://cdn2.hubspot.net/hubfs/533449/Images/Security-Scorecard%202017%20Govt%20Cybersecurity%20Report.pdf

2. What Is Security and Resilience? https://www.dhs.gov/what-security-and-resilience

3. 2017 Poneman Cost of Cyber Crime Study, https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

4. 2017 Poneman Cost of Cyber Crime Study, https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

5. Eliminating 100% of Your Blind Spots to Secure the Entire Network and Optimize Security Operations Across the Entire Threat Defense Lifecycle with Lumeta and McAfee. http://www.lumeta.com/resources/analyst-coverage/frost-sullivan-wp-lumeta-mcafee-integration-elimina-tes-blind-spots-network-endpoint-infrastructure

6. The Global Information Security Workforce Study, June 2017

7. 2017 Motorola Solutions IT Services in Public Safety Survey

8. The Global Information Security Workforce Study, June 2017

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