MOTOROLA SOLUTIONS

CYBER RESILIENCE

IMPLEMENTING A HOLISTIC, RISK-BASED APPROACH TO SECURITY

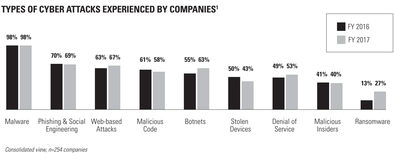
As the frequency and sophistication of worldwide cyber attacks surges, public safety and government agencies are increasingly prime targets. Outlined below are four security challenges facing public safety and government organizations, along with steps to implement a holistic, risk-based approach to addressing these challenges.

CHALLENGE #1

Advancement of Cyber Attack Techniques

Attackers now have the ability to lock critical systems, hold data for ransom, and destroy files as part of their breach process. Security experts predict continued growth for these types of attacks.

TYPES OF CYBER ATTACKS EXPERIENCED BY COMPANIES[1]



Consolidated view; n=254 companies

Cyber Resilience, "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions"[2] is critical to the daily operations of public safety agencies. Agencies must break free from "snapshot thinking" — 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, security measures must be continuous.

CHALLENGE #2

Spending on Cyber Tools Alone Does Not Ensure Security

The average annual cost of cybersecurity for organizations across industries is $11.7 million, however security capabilities have not delivered the desired efficiency and effectiveness:[2]

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

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

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

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

CHALLENGE #3

New Attack Vectors from Open, Interconnected Networks

The rapid pace of technology deployments and operational enhancements bring great benefits and they also create new blind spots. Agencies need to take steps to safeguard enterprise software and connected devices and ensure continuous monitoring capabilities.

Lack of visibility can lead to **20-40% of infrastructure becoming unknown or unmanaged** by an organization.[3]

CHALLENGE #4

Lack of Security Expertise

The availability of security experts is a constant challenge facing public safety and government agencies.[4,5]

The cybersecurity workforce gap is on pace to hit **1.8 million** by 2022 — a **20% increase** since 2015

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

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

A Risk-based strategy begins by identifying and reviewing the complete range of risks an organization faces. Then, based on risk prioritization, steps are identified to reduce risk or remediate a situation.

A Simplified Framework for Maximum Results

The National Institute of Standards and Technology (NIST) Cybersecurity Framework, serves as a guide to help organizations manage their cyber risk awareness and security and detection, response and recovery. Focus on the five core functions of the NIST framework below 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

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. Our land mobile radio (LMR) service packages help safeguard your operational integrity and include Security Patch Installation, Remote Security Monitoring, On-Premise Security Operations Center and Cybersecurity Risk Assessment.

To learn more, visit motorolasolutions.com/cybersecurity.

1. 2017 Ponemon Cost of Cyber Crime Study. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017
2. What Is Security and Resilience? https://www.dhs.gov/what-security-and-resilience
3. 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-eliminates-blind-spots-network-endpoint-infrastructure
4. 2017 Global Information Security Workforce Study
5. 2017 Motorola Solutions IT Services in Public Safety Survey