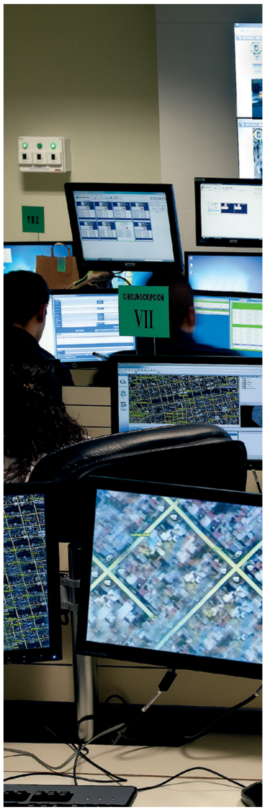
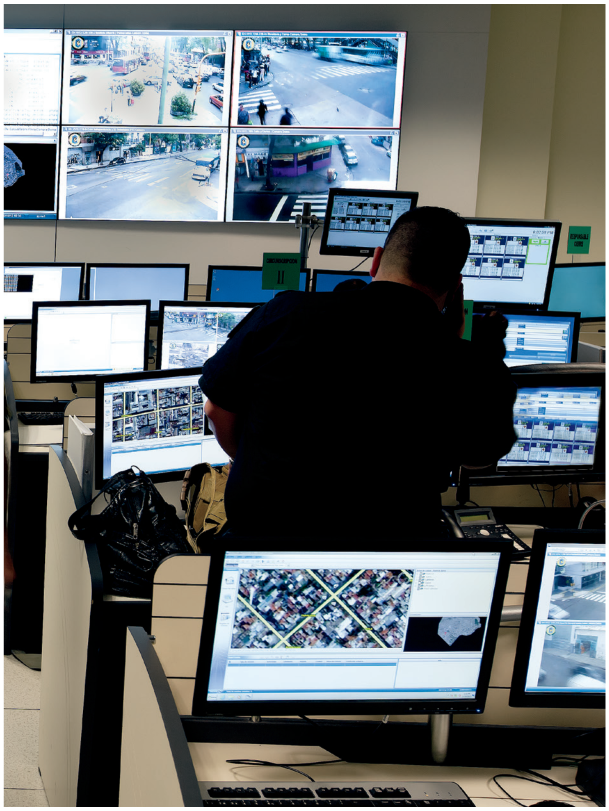


CYBER RESILIENCE: THE NEW CRITICAL MISSION FOR PUBLIC SAFETY

MOTOROLA SOLUTIONS



The frequency and sophistication of cyber attacks have surged to a point where businesses and governmental entities worldwide recognize that no one is immune. The search and implementation of cybersecurity best practices is a top priority. Public safety agencies are increasingly becoming prime targets for cyber criminals seeking to compromise their mission critical networks. Those responsible for securing these networks understand an attack can result in serious, life-changing ramifications. However, the path to cyber resiliency remains disjointed.

Cyber threats and attacks are as age-old as the computer itself. One of the first cyber intrusions can be traced back to 1986 to a virus simply known as "Brain." The effects from this attack were minimal in comparison to the malicious ones known today. The interconnectivity of devices, networks and systems have made organizations more attractive targets. Critical infrastructure sectors, which include public safety agencies, are now the target exploits for cyber criminals.

Governments acknowledge that protecting and promoting the continuity of critical infrastructure is essential to their security, public safety, health and economic vitality. They are stepping up efforts to put frameworks and policies in place to be cyber resilient.

CYBER ACTIVITIES SURGE IN PUBLIC SAFETY

Year after year, public safety has become one of the top sectors with the largest number of data breaches and confirmed data losses.[1] Government entities are being attacked at twice the rate of other industries across the board. Brute force attacks are most prevalent in the government sector.[2]

For public safety agencies, getting cyber resilience right is imperative to daily operations. The confidentiality, integrity and availability of mission critical communication systems can't be minimized or compromised. A cyber intrusion is a handicap no agency can afford because it impacts the responsibilities they are charged with carrying out each day. So where does an agency begin?

76%
CISOs SAY ATTACKS ON INFRASTRUCTURE ARE MORE SOPHISTICATED[3]

#1 TARGET
GOVERNMENT SECTOR HAS MOST DESTRUCTIVE ATTACKS[3]

2X
RATE OF ATTACK ON GOVERNMENTS VERSUS OTHER INDUSTRIES[2]

WHAT ARE YOU PROTECTING, AND FROM WHOM?

Countries are establishing frameworks that focus on what's needed for a comprehensive cybersecurity program to safeguard critical infrastructure, entities and businesses and lower risk. From the National Institute of Standards and Technology (NIST) Cybersecurity Framework in the U.S. to the EU Cyber Defence Policy Framework in Europe, critical elements of cybersecurity are outlined and linked to proven standards for organizations to consider. With the staggering array of public safety assets that must be protected, the complexity can be overwhelming.

As public safety and government agencies focus on which framework to adopt, they can't forget the fundamentals. They should ask "what are we protecting" and "from whom are we protecting ourselves" before developing and executing a strategy. These steps are crucial to being effective in addressing the ever-changing cybersecurity landscape.

DEBUNKING THE MYTH OF THE CLOSED NETWORK

For decades, public safety agencies enjoyed the benefits of a "closed" and "secure" network within their operational environment. With the rapid pace of technology and new data streams (social media, body worn cameras, intelligent policing and more – see Figure 1), the luxury of a closed network is long gone. Public safety networks are interconnected and the mission critical information they contain are highly prized by criminals.

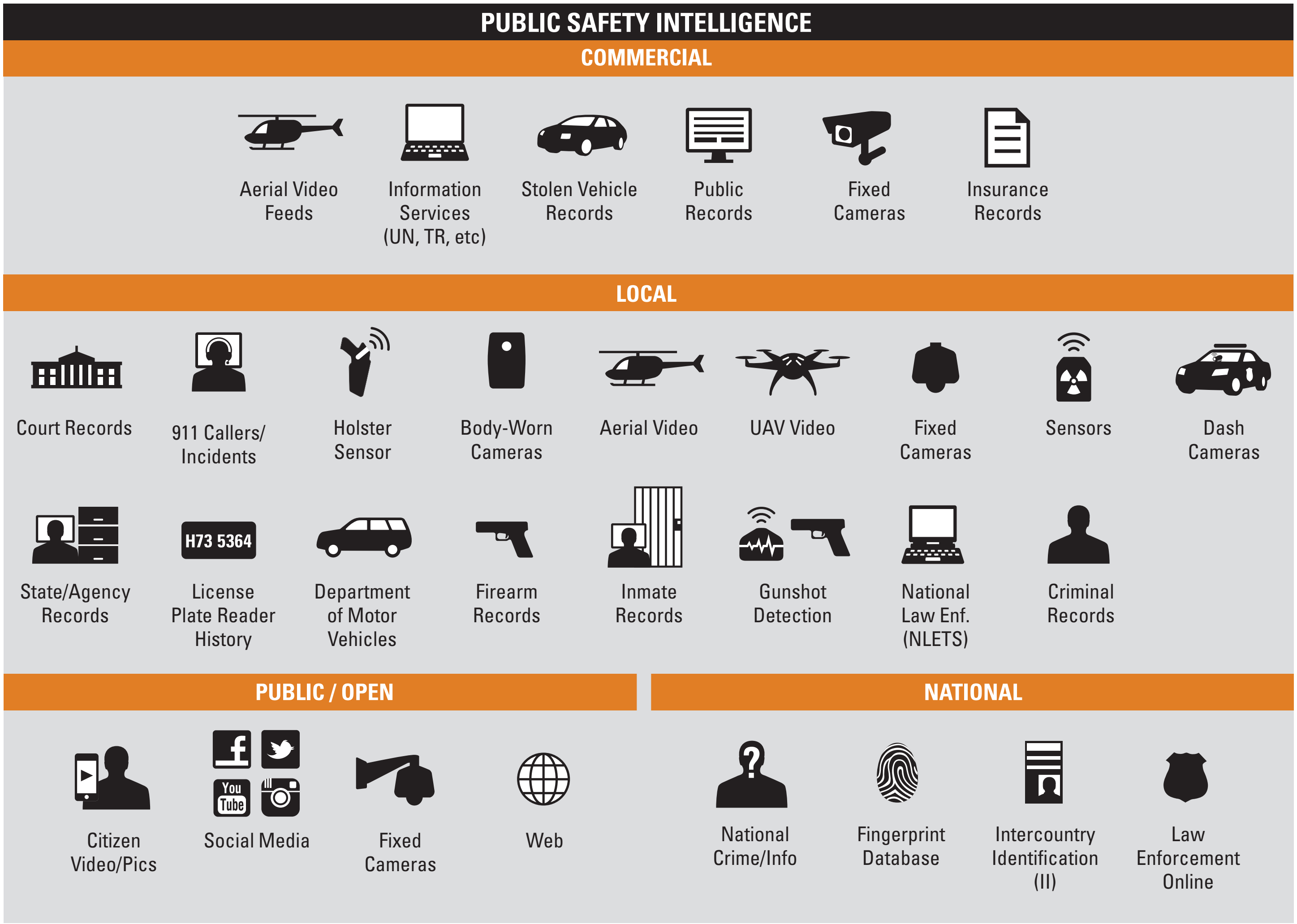
No longer is it a matter of if – but when, how and what are the consequences of a cyber attack.

ATTACKS ABOUND – INADVERTENT OR INTENTIONAL

Hackers attack public agencies to disrupt services, acquire critical information and create a form of terrorism. These causalities keep information security leaders up at night. Over the past year, their concerns have increased: 37 percent for nation state attackers, 24 percent for cyber warfare/terrorism, and 15 percent for breaches involving high-value information.[4] Those responsible for securing critical information must pay attention to the significant increases in top cyber attacks directed at public safety.

Agencies should consider internals threats just as seriously. Threats from insiders – those with immediate access to "closed" networks – are often due to inadvertent actions, human error and internal misuse. Almost one-third surveyed said insider crimes are more costly or damaging than incidents perpetrated by outsiders.[5] The most costly cyber crimes are caused by malicious insiders, denial of services and web-based attacks – a whopping 55 percent of all cyber crime costs per company each year.[6]

FIGURE 1



A CLOSER LOOK AT INTERNAL THREATS

Whether a former technician who knowingly breaches a network or a current employee who unwittingly infects it with malware, agencies must be proactive and prepared to handle an increasing array of insider attacks.

INSIDER ATTACKS

A disgruntled employee has access to confidential information about a mission critical radio network. He text messages the system configuration to malicious outsiders to disrupt communications.

ACTIONS

Regularly review organizational policies (those governing access to and handling of confidential information and proper use of personal communication devices) with legal, HR, and employees.

Consider behavior-monitoring technologies and practices to legally monitor employees with access to confidential information.

Educate personnel and establish processes to control the network.

Consider deploying "honey pot" technologies and continuously monitor your network for anomalies.

MALWARE PROPAGATION

A dispatcher unknowingly brings an infected USB stick – one of the devices in the BYOD category – to work. Malware spreads throughout the network, shuts down dispatch positions and infects other agencies.

ACTIONS

Continuously update anti-malware software.

Harden and patch the system.

Regularly review router access control lists (ACLs) and firewall rules.

Monitor the system to detect malware and other unusual activity.

Address immediately to neutralize the infection and contain the outbreak.

UNAUTHORIZED CONNECTION

An IT technician installs an unauthorized and unsecured Wi-Fi access point (AP) for "convenient" remote access into his agency's system. The Wi-Fi AP becomes an attack vector and is discovered by malicious actors.

ACTIONS

Enable network switch port security controls.

Harden systems to prevent unauthorized activation of Wi-Fi interfaces on servers and end-user devices.

Monitor the system for unauthorized asset additions to the network.

Monitor to detect unusual network traffic.

38%

INTRUSIONS DETECTED IN GOVERNMENT NETWORKS[7]

55%

CYBER CRIME COSTS DUE TO MALICIOUS INSIDERS, DENIAL OF SERVICES AND WEB ATTACKS[6]

31 DAYS

AVERAGE TIME TO CONTAIN AN ATTACK[6]

SIMPLIFY RISK AND EXECUTION FOR MAXIMUM IMPACT

Agencies can simplify their risk management framework by focusing on these key areas to help assure continuity and operational integrity of critical services:

1. **Simplified governance and oversight model** should focus on the entire ecosystem. This includes people, process, policy and technology. Each by itself cannot protect the mission critical environment; only by working together cohesively can it be achieved.
2. **Simplified risk management scope** should clearly define tangible technical risks and how to mitigate them. Risks should be categorized as factual and specific.
3. **Simplified execution model** should focus on practical risk areas across all organizational entities and not get overburdened by resource-intensive compliance efforts. In most cases, compliance objectives will be met transparently when practical risk management aspects are addressed.

For example, when agencies harden their system in accordance with higher-tier industry-accepted best practices, such as DISA STIGs and NIST 800-53, they can meet less stringent compliance requirements at the same time they address the most critical technical risks.

SIMPLIFY THE SCOPE OF RISK MANAGEMENT

Start by considering what you are really protecting – mission critical data, robustness of operational integrity, or something else? Assess your understanding of the threat landscape and the potential risks impacting your organization's operations – from third-party dependencies to insider threats.

Then ask "whom are we protecting the organization from?" Specifically, look at the risk, possible attack vectors, likelihood of occurrence, and skill set needed to successfully carry out an attack on your system.

Once you have identified related systems and assets, the next step is to baseline your cybersecurity capability and implementation. It is critical to simplify the framework and clearly define a delivery for satisfying compliance objectives versus technical risks.

FOCUS ON MONITORING AND RESPONDING, NOT FORTRESS-BUILDING

Most adversaries use a very simple approach to breach the system and are often active on a breached network for months before being detected. On average, hackers spend 243 days on a victim's network before they are discovered.[8] Yet organizations direct attention to the wrong places; in effect, securing the windows while leaving the doors unlocked.

Even when agencies comply with all regulatory requirements, a seemingly innocuous error can lead to a breach that has a cascading impact, compromising mission critical operations. An organization that is 100 percent compliant can still get compromised the same day.

Rather than building fortresses to safeguard perimeter and other assets, agencies can benefit by looking seriously at the feasibility of robust and comprehensive security monitoring and incident response capabilities.

SECURE CRITICAL INFRASTRUCTURE WITH A HOLISTIC APPROACH

ANALYSIS AND ASSESSMENT: Identify and categorize assets, then assess and evaluate vulnerabilities

IMPACT: Build a clearly structured framework for establishing priorities and procedures and allocating funds for mitigation

CORRECTIVE ACTION: Have a systematic plan for addressing risks, business continuity and disaster recovery

VIGILANCE: Perform ongoing risk assessment and development of cost-effective processes

TRUSTED ADVISOR: Collaborate with industry experts to create a security ecosystem where all entities work together for total protection

SAFETY IS WHAT YOU CAN'T SEE. EXPERTISE IS WHAT YOU CAN'T OVERLOOK.

As a global leader in mission-critical communications in over 100 countries, Motorola is intimately aware of how critical it is to design, develop and deploy technologies that are absolutely effective and secure. We work with public safety agencies worldwide to manage cybersecurity challenges, partner with their internal resources, and provide the training and tools to help them be cyber resilient in an intensifying threat climate.

SOURCES

1. 2015 Data Breach Investigation Report, Verizon Wireless
2. 7. Post-Intrusion Report, Vectra, June 2015
3. Report on Cybersecurity and Critical Infrastructure in the Americas, Trend Micro, 2015
4. 6. 2015 Ponemon Global Megatrends Report
5. Managing cyber risks in an interconnected world, PWC, September 2014
8. Cybersecurity Roadshow, IBM 2014

To find out how Motorola is helping public safety agencies work better, smarter and faster through next generation technology, visit **motorolasolutions.com/cybersecurity**.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. 800-367-2346 **motorolasolutions.com**

MOTOROLA SOLUTIONS