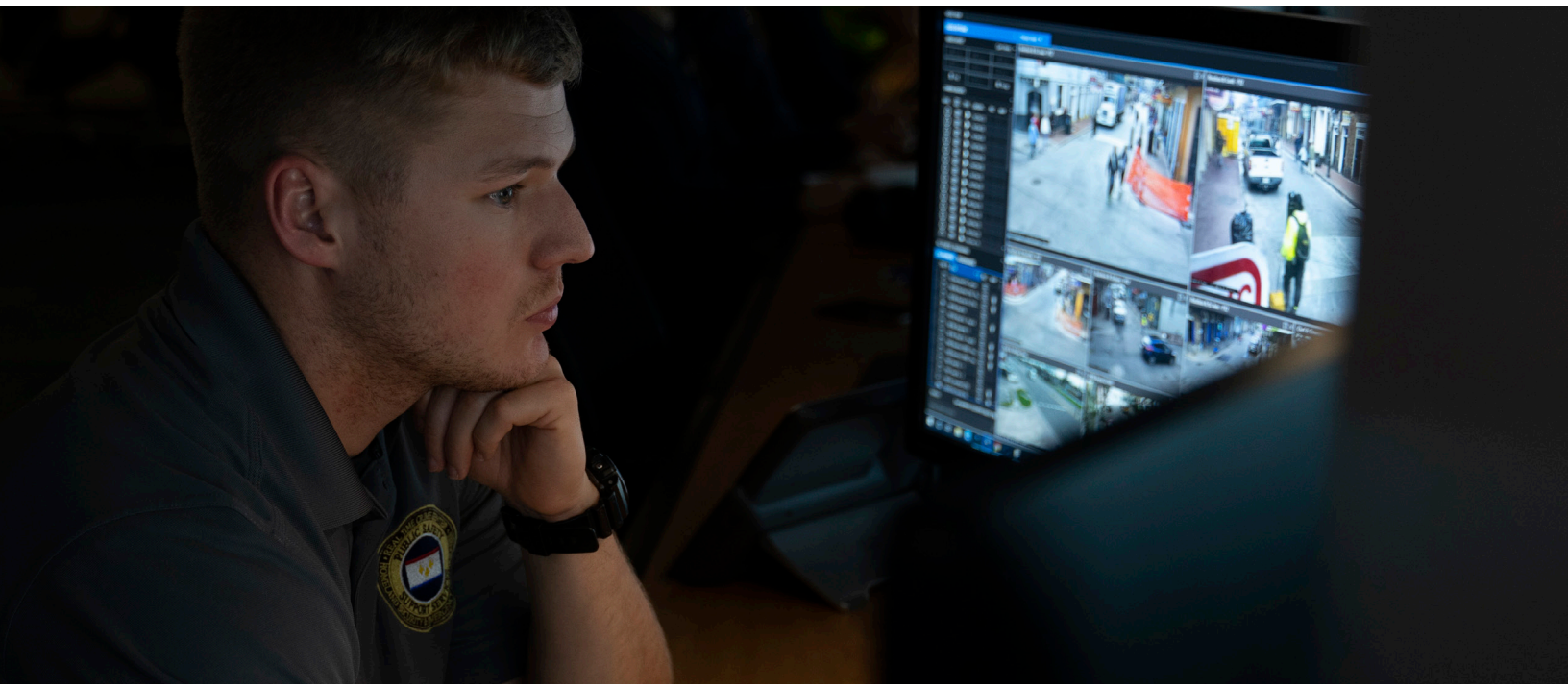
SECURING PUBLIC SAFETY ANSWERING POINTS

UNDERSTAND TODAY'S THREATS AND IMPROVE YOUR CYBER POSTURE

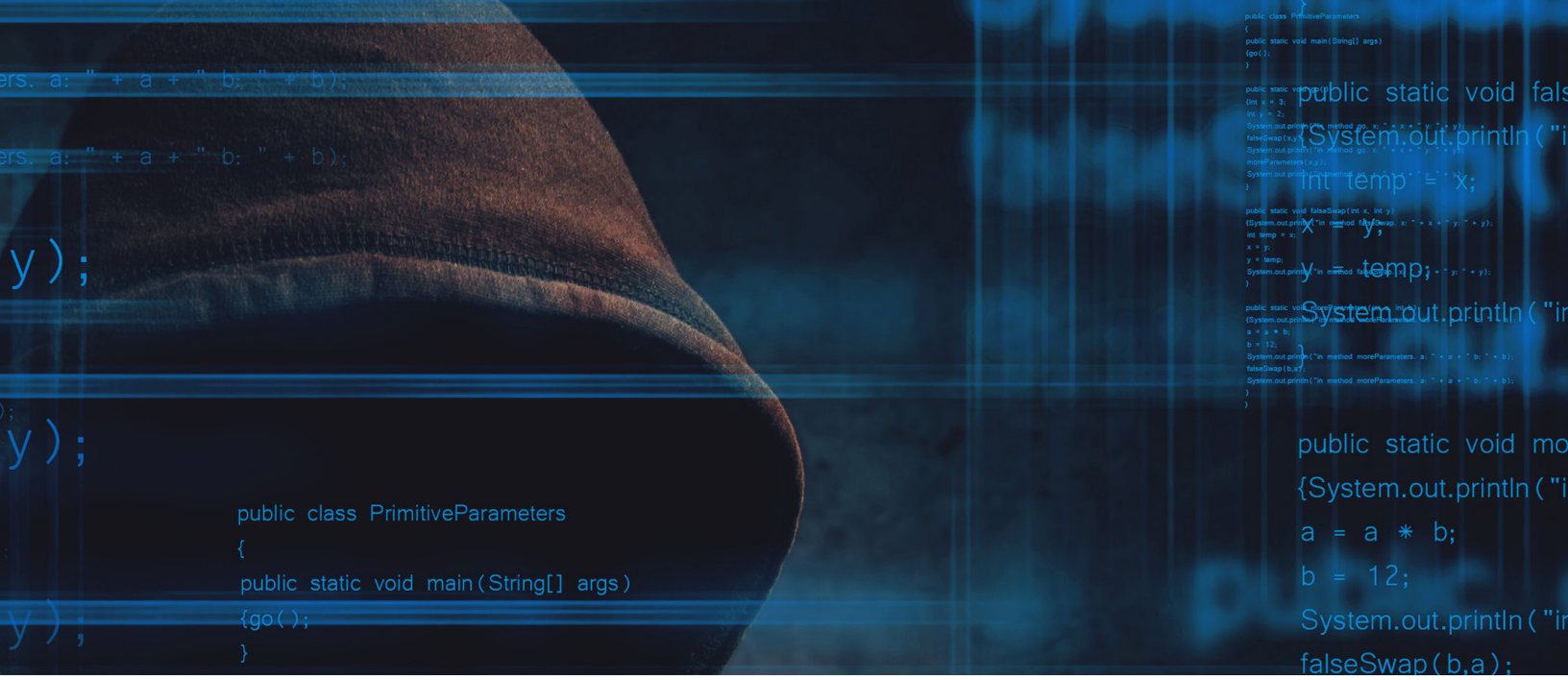
MOTOROLA SOLUTIONS

PUBLIC SAFETY SYSTEMS: MORE CONNECTED - MORE EXPOSURE TO VULNERABILITIES

Next Generation 9-1-1 (NG9-1-1) has reshaped the way Public Safety Answering Points (PSAPs) serve their community by providing communication that's more accurate, integrated and tailor-made for today's digital and wireless lifestyles. But with these technological advances, NG9-1-1 also introduces new challenges. As opposed to the legacy, radio-based systems used in the past, today's public safety systems are more closely related to IT systems, meaning they're more connected and can introduce more modern vulnerabilities.

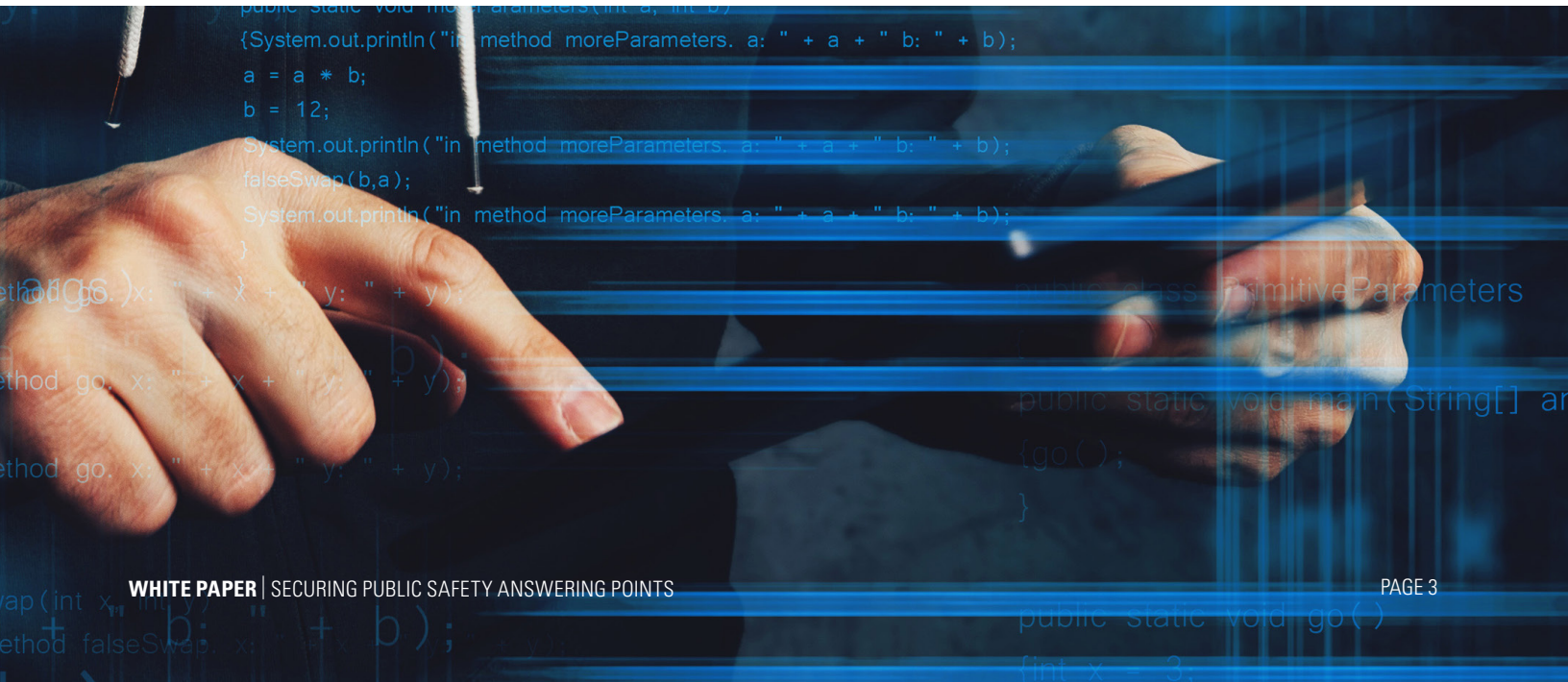


This fact is particularly worrisome as public safety agencies have begun to gather and retain more data than ever before. Traditionally, most PSAPs mainly handled telephone voice data; however, today they also store sensitive information such as video feeds from surveillance cameras, text-to-911 messages, photo evidence, social media engagement data and numerous other types of public safety communications. In addition to more data, as PSAPs have evolved, their systems often contain more interconnected devices, numerous vendors and higher levels of complexity that can be difficult to get a handle on. For instance, before mobile phones and Voice over Internet Protocol (VoIP), a telephone's location was consistent since it was hard-wired and the phone number correlated with a physical address. Today, there is no guaranteed correlation between a number and its location — a mobile phone can easily contact 9-1-1 from anywhere.



Given this growth in complexity and their high availability requirements, PSAPs are increasingly becoming an inviting target for attacks. Recently, the US has seen an uptick in a type of cyber attack on PSAPs (known as ransomware) where cybercriminals encrypt critical customer files and demand a ransom for the decryption key. For the perpetrator, attack scans can be automated to scour the Internet looking for available vulnerabilities to exploit. Currently, the odds of getting caught are fairly low and even the more basic cyber attacks have become increasingly lucrative. With high potential payouts, a diverse set of attack vectors and a low chance of apprehension, we can expect a steady stream of attacks to continue.

We've already seen the destructive effects these types of attacks can have on public safety systems. In 2018, a ransomware attack on the city of Baltimore had serious operational impacts on the city's 9-1-1 dispatch services and served as a wake-up call for PSAPs and municipalities around the country. According to the Motorola Solutions Threat Management Group, this type of monetized attack is one of the largest cyber threats to public safety agencies. In addition to the theft and destruction of important public safety data, hostile actors often also look to prevent access to emergency services. Distributed Denial-of-Service (DDoS) and Telephone Denial-of-Service (TDoS) attacks seek to overwhelm 9-1-1 systems which are often already working at full capacity. These attacks can uniquely impact PSAPs and their mission due to their commitment of having direct, uninterrupted access to the public.



Just as concerning, many PSAPs simply don't have enough resources to devote to effective cybersecurity protection. Agencies often have limited budgets along with trouble recruiting and retaining top cybersecurity personnel. Given the stakes involved with the operation and maintenance of NG9-1-1 systems, properly securing PSAPs can seem like a daunting task and raise a number of questions:

What are the threats directed towards PSAP systems? How do you know if your system is vulnerable? What are the best security and organizational practices to implement at your PSAP? How do you ensure a high level of security with limited budget and resources? What's the best way to get started?

To answer these and other important questions, we've outlined PSAP cybersecurity best practices and a recommended threat modeling framework to identify and prioritize threats. While this information is not intended to be comprehensive, we hope that it will spark necessary conversation, making it easier for you to begin the journey of securing your PSAP in the most effective manner possible.

PSAP CYBERSECURITY: 7 BEST PRACTICES

When it comes to securing your PSAP, time and budget resources aren't unlimited, which is why threat modeling is a useful tool to efficiently identify likely adversaries, evaluate potential threats and allow you to properly focus your resources. To get started, it's important to prioritize the most vital aspects of security: confidentiality, integrity and availability. While each of these information security focuses are important, for PSAP organizations, availability must be the top priority. If your system is breached and inaccessible, your mission to serve the public is severely hindered. But how do you make sure your emergency services remain available 24x7x365, while also taking advantage of the latest PSAP solutions? Then, how do you continue to maintain the integrity and confidentiality of your system while opening it up to the increased opportunities for interconnectivity and improved service?

Here are seven best practices to help get you started with threat modeling, system security and data protection.

1. KNOW YOUR ADVERSARY

One of the first steps of threat modeling involves understanding the most likely motivations of a PSAP attacker. Today, most are motivated by the financial benefits seen through money paid as ransom. Hackers aim to seize and hold your system, data and services hostage until you pay. The more of your system they can seize, the more money the attacker can try to extort. Encrypting your files so you can't access them and then charging a ransom can take as little as a few minutes. It's a high-margin, illegal business and the odds of getting caught and prosecuted are slim due to the emergence of anonymous payment methods like Bitcoin, an often used cryptocurrency. Given the stakes, there's tremendous pressure for PSAPs, especially, to pay the ransom to try to quickly restore services (note: the FBI and DHS advise to NEVER pay the ransom). Unfortunately, the odds a cyber criminal will actually restore your system once you pay are not good. A report from software company SentinelOne says that only 26 percent of companies who paid at least one ransom had their files unlocked. Moreover, these same companies who pay the ransom are two-thirds more likely to again become the target of ransomware.[1] The best way to thwart these ransom attacks is to put in place proper defenses to prevent becoming a victim in the first place.

2. TAKE OWNERSHIP / MODEL THE PSAP SYSTEM

Once you better understand what malicious actors are after, you then must make sure you understand your complete system from end-to-end. To do this, it's important to proactively designate one person within your PSAP to own the operational side of your NG9-1-1 system from a business point of view. This individual is responsible for understanding the PSAP environment from start to finish including applications and systems across different platforms and vendors. Until the entire PSAP ecosystem is understood, it can't be properly protected. This role would also be similar to that of a general contractor, ensuring everyone is coordinating, working together and communicating. Ideally this person owns operational and business functions of your system and works closely with any external resources who own the technical functions. There should be constant communication with one another, streamlining both operations and IT to close any functional gaps. If budget doesn't allow for an external resource, it's still important to designate an internal point person who can ensure that everyone playing a role in securing the PSAP is properly working in coordination.

Two Common Types of PSAP Hackers

The Cyber Criminal

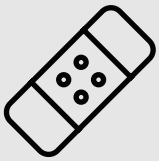
- May be scanning for types of victims or specific victims
- Does research on targets through social media, news articles and websites
- Usually technically advanced
- Professional, conducts criminal cyber operations as a living or as a dedicated hobby
- Typically works solo, with assistance from criminal forums for guidance and support, or operate as an organized crime group, comprised of numerous cyber criminals
- Engagement times can be brief, or long, up to years in some cases

The Hacktivist

- Typically targets specific municipalities or departments
- Attacks often occur during or around contentious or controversial current events
- Often moderate to advanced technical ability
- Individuals or groups may be linked ideologically
- May have societal or political motivations
- Attempts to steal confidential information, deface websites, deny emergency services or embarrass the competency and abilities of victims

3. SEEK STANDARDS TO EVALUATE AND PRIORITIZE YOUR THREATS

Another important step is to conduct a comprehensive risk assessment before your PSAP system goes live. 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 including identification, protection, detection, response and recovery. The NIST Framework provides an outline of best practices that organizations can adopt to focus their time and money while catering to their specific business and security goals. For those requiring international standards, the International Organization for Standardization (ISO) also addresses cybersecurity under Standards 27001-27002. Lastly, when using third-party support, the American Institute of CPAs (AICPA) provides a structure for effective third-party validation of a service organization's controls.



4. PATCH, PATCH, PATCH

In virtually all cyber attacks studied over the past few years, failure to regularly patch systems was the primary reason hackers were successful. That's why patching is the single most important way for PSAPs to limit the threat of cyber attacks. Thus, it's critical for organizations to develop and implement a detailed patching plan, which should consist of written operational strategies, tactics, roles and responsibilities so that patching isn't delayed because of situations like critical personnel going on vacation. It's also important to use a system architecture that allows for both automatic patching and testing of patches to prevent any negative impact on the PSAP's services. Still, as time goes on, it becomes harder and more costly to patch older systems which often are the most vulnerable and require the most frequent patch updates. It's important to track these costs to understand when it's become more cost effective to replace older systems than to maintain them. PSAPs may also want to consider cloud solutions which place the burden of patching on the vendor, freeing PSAP resources.

5. UPGRADE YOUR SYSTEMS

Along with regular patching, upgrading hardware is essential to reduce security vulnerabilities. Many older systems and OSs, for example Windows XP, are no longer supported by the manufacturer, thus they rarely, if ever, receive security patches even though many vulnerabilities are well known. Upgrading old hardware and software can both reduce an organization's attack surface and allow it to make use of new security features. For example, the latest smart firewall technology includes intrusion detection systems (IDS) or, as an upgrade, are capable of understanding what applications are running on the network and how they should be communicating, sometimes called "Next Generation" or Layer 7 firewalls. While an IDS can detect bad actors based on signatures of known bad traffic, Layer 7 firewalls go even further, sensing bad actors based on behavior even if it's not recognized by signature.

Another essential upgrade for NG9-1-1 systems is employing "encryption-in-motion" (i.e., on data as it moves through the network). This type of encryption makes automated hacking much more difficult to execute because attackers can't easily identify which data is important to a potential target. Finally, be sure to also upgrade to a security monitoring solution that is both proactive and encrypted. Real-time network monitoring can combine cyber threat intelligence, event correlation and analytic tools to reduce risk and apply active countermeasures to keep systems protected. The monitoring solution's network protocols must also be encrypted as this makes it far more difficult for either hackers or insider threats to access your system and gain an understanding of your PSAP's operations.

Threat Modeling Terms and Concepts

Threat Modeling
Helps proactively identify threats and reduce attack surfaces to focus cybersecurity investments

Risk Mitigation
A systematic reduction in exposure to a risk

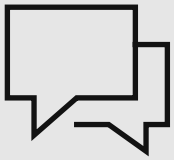
Attack Surface
The total sum of vulnerabilities in a given system or network

Attack Vector
The path or means by which a hacker can gain access to a system or network

6. BACKUP AND RECOVERY

Backup and recovery are often overlooked functions in cybersecurity. Whether combating hardware failures or ransomware attacks, backup strategies must be developed specific to each PSAP's business needs and resources. Ensuring that there are reliable and up-to-date backups available are the biggest factors in a timely recovery. Backups should be stored offline and undetectable as hackers typically target the backups first in a ransomware attack. The backups should also be tested in periodic drills to increase IT staff's familiarity and ensure their ability to recover in a cyber attack/disaster.

Organizations must also make sure their PSAP is part of the wider Business Continuity/Disaster Recovery Plan for the location where the data is stored. Ensuring there is an established recovery plan in place can be the key differentiator to resuming service in a timely manner.



7. ENGAGE AND SEEK HELP WHEN NEEDED

According to a 2018 study conducted by the International Information System Security Certification Consortium (ISC), the cybersecurity workforce gap currently stands at nearly 3 million globally with almost 500,000 needed in North America alone.[2] With such a shortage of qualified cyber professionals, don't hesitate to engage, demand and seek clarification when the latest NG9-1-1 IT advancements become confusing. Be certain to engage help early in the process of developing a cyber readiness plan to ensure that you are making good decisions from the start and properly preparing your PSAP to respond and recover from any attack.

Cybersecurity can be complicated, especially in an industry as critical as public safety and working with experts can greatly reduce that complexity while improving decision making.

ADAPTING THE NIST FRAMEWORK

The NIST Cybersecurity Framework is a powerful tool to help you manage cyber risk with a few straightforward steps: Identify, Protect, Detect, Respond and Recover. It has proven to be an effective and flexible approach that can easily be adapted to your organization's individual security goals and resources. To create a comprehensive security approach that improves your PSAP's security posture, focus on the five core functions of the NIST Cybersecurity Framework by breaking each into smaller activities that are easier to implement.

IDENTIFY
Assess Risks

- Inventory critical assets and systems
- Perform a thorough risk analysis

PROTECT
Develop Safeguards

- Develop and disseminate security policies and procedures
- Implement appropriate access and auditing control

DETECT
Make Timely Discoveries

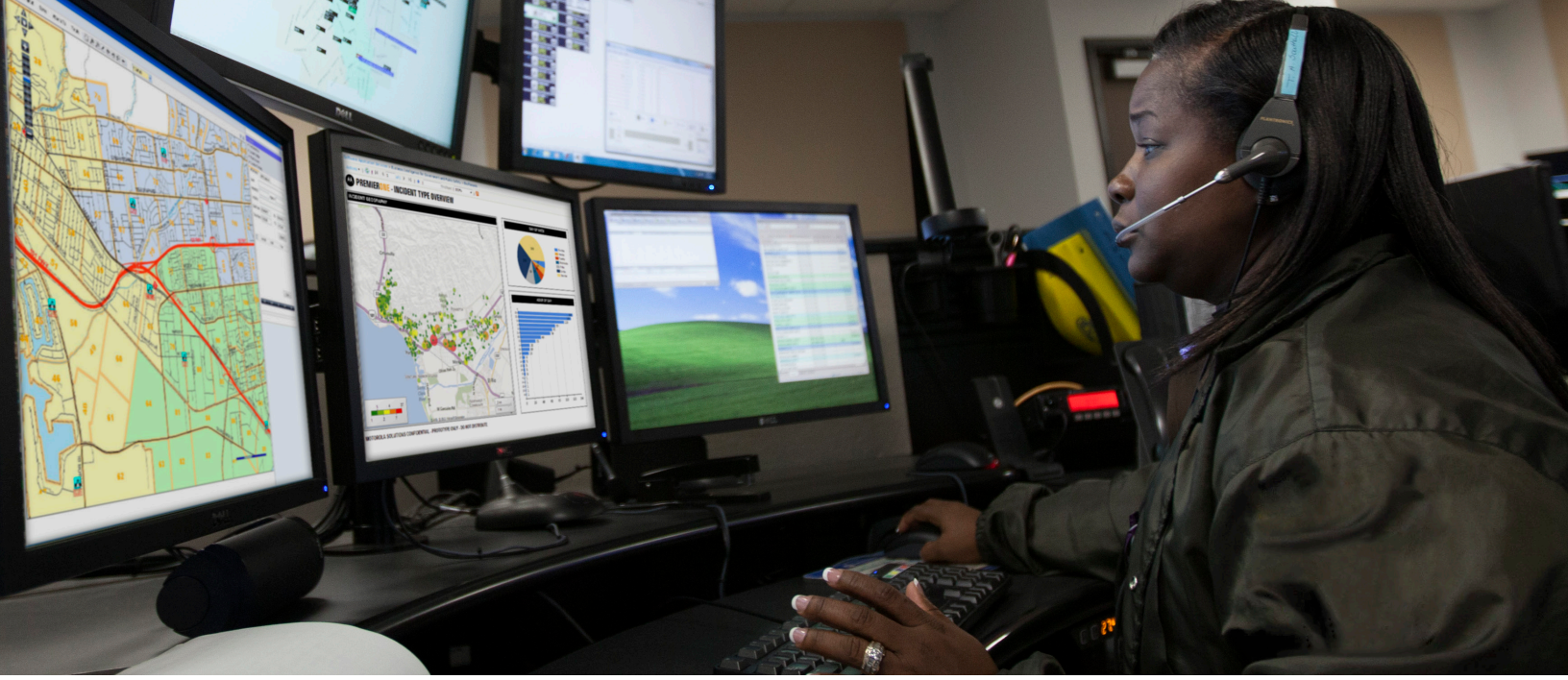
- Conduct continuous monitoring 24x7x365
- Enable auditing capabilities

RESPOND
Take Action

- Establish a robust response plan
- Analyze, triage and respond to detected events

RECOVER
Restore Functionality

- Institute a recovery plan
- Create improvements to prevent future attacks



THE ROAD TO ROBUST PSAP SECURITY STARTS HERE

Today, it's no longer a matter of if, but when and how your PSAP will become a target. Public safety organizations provide services that communities depend on which give them great value to the public and, consequently, to hostile actors trying to score a quick payday. The good news is that following cybersecurity best practices can greatly reduce your risk levels and potential vulnerabilities. Adhering to our 7 industry best practices and leveraging the NIST Cybersecurity Framework will help you find answers to your most pressing cyber questions and get you started on the road to robust PSAP security.

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. Our cybersecurity services leverage the skills and tool sets of our cybersecurity experts, who are trained to stay actively informed of the rapidly changing landscape of security threats and compliance requirements. Our cybersecurity services include: Security Patch Installation, Remote Security Monitoring, On-Premise Security Operations Center, Cybersecurity Risk Assessment and many others all designed to help safeguard your operational integrity.

To learn more, visit: **motorolasolutions.com/cybersecurity**

Notes

1. SentinelOne: Global Ransomware Study 2018 https://go.sentinelone.com/rs/327-MNM-087/images/Ransomware%20Research%20Data%20Summary%202018.pdf
2. ISC2 Workforce Study reference: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

MOTOROLA SOLUTIONS

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