MOTOROLA SOLUTIONS

WHEN LIVES ARE ON THE LINE

PROTECTING PSAPS FROM CYBER ATTACKS

A FRANTIC CALLER QUICKLY DIALS 9-1-1. BUT SOMETHING ISN'T RIGHT.

Instead of a dispatcher promptly answering, there's a busy signal.

Throughout the community, the story is the same. Callers can't get through for hours as emergencies pile up and the situation becomes more chaotic as the result of an ongoing cyber attack that has disrupted 9-1-1 call center operations.

It's a nightmare scenario. It's also the real risk we're facing today in cities and towns across the country.

PSAPS: DESIGNED FOR SECURITY, YET INCREASINGLY TARGETED

Despite being engineered for security, Public Safety Answering Points (PSAPs) and the workstations housed there are increasingly being targeted by cyber criminals and other threat actors.

We last conducted a comprehensive review of the PSAP threat landscape in August 2020. Since then, attacks on PSAPs have increased. According to the Motorola Solutions Threat Intelligence Report, *2021 Threats to Public Safety: Criminal Operations Focus*, reported attacks on PSAPs increased almost 40 percent from August 2020 to the beginning of 2021.

That number included five Telephony Denial of Service (TDoS) attacks, affecting call-taking and handling services in each instance. These events are rarely disclosed, however, so it's quite possible this number is significantly higher. Ransomware, in which an attacker remotely locks systems or data and demands payment to unlock them, has also emerged as a primary method of attacking PSAPs.

A number of factors have driven the increase in threats. First, malicious hackers clearly understand the significance of call taking handling and dispatch software systems, which are critical for public safety. Without these systems, it would be difficult — if not impossible — to perform many modern critical response tasks, such as prioritizing and recording incoming calls, sending the right emergency personnel where they're needed most, and tracking responder location and well-being. This critical infrastructure makes PSAPs a prime target for threat actors.

In addition, as Next Generation 9-1-1 (NG9-1-1) systems come online, they're providing more accurate, integrated and useful communication, tailor-made for today's digital and wireless lifestyles and the needs of PSAPs. They allow citizens to send text, images, video and data to a PSAP. But because they're much closer to traditional IT networks than the radio-based systems used in the past, their interconnectedness creates new risks and requires new levels of vigilance.

With high potential payouts and a low chance of apprehension, much less prosecution, we can expect a steady stream of attacks to not only continue, but increase.

Further exacerbating the risks, response software like computer-aided dispatch (CAD), real-time intelligence and other systems aren't just used in fixed agency locations. Today, they can be found in mobile command centers, pop-up environments such as large events, or used by work from home and other remote employees who may not have the same protected environment as they would in the office.

For threat actors, the odds of getting caught are still low. In addition, many cyber attackers now use automated processes and "as a service" business models that have made it trivial for them to launch attacks. Ransomware-as-a-service, for example, is a subscription-based model that allows ransomware operators to "lease" malware to other bad actors for a fee. With high potential payouts and a low chance of apprehension, much less prosecution, we can expect a steady stream of attacks to not only continue, but increase.

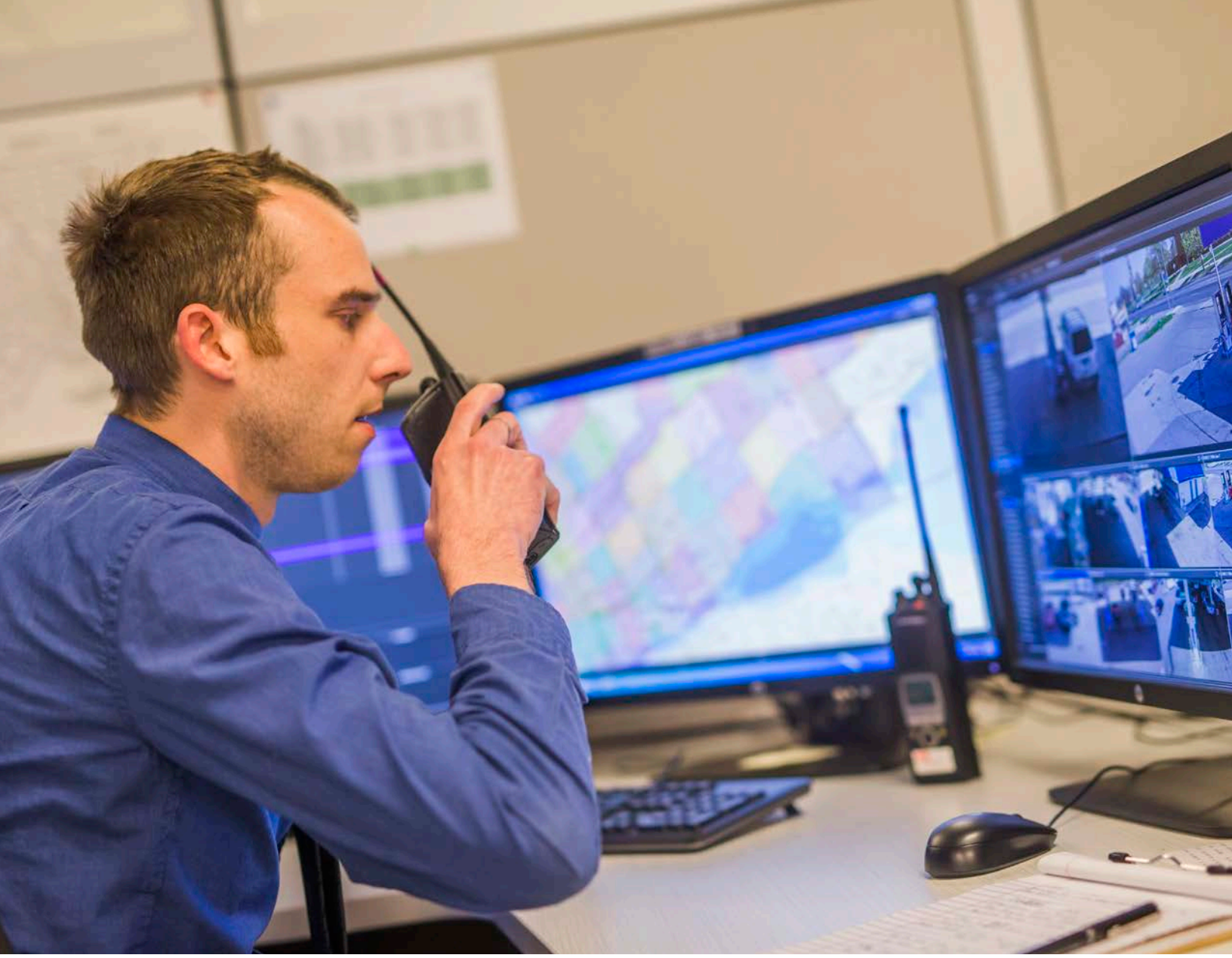
Today, many PSAPs simply don't have enough resources to devote to effective cybersecurity. Public safety agencies operate under limited budgets, making it difficult to fully staff for cybersecurity needs given other public safety priorities. Alarmingly, according to Motorola Solutions industry surveys, fewer than 50 percent of public safety agencies have documented security policies and procedures, regularly patch their systems or conduct periodic risk assessments.

Whether you're just starting out on your agency's cyber journey, or validating that your current program is optimally focused, Motorola Solutions can help.

This guide will help you answer foundational questions around PSAP cybersecurity, such as:

- *What are the best security and organizational practices to implement at your PSAP?*
- *How do you ensure a high level of security with available budget and resources?*
- *What's the best way to get started?*

To answer these and other important questions, we've outlined the most pressing threats to 9-1-1 and dispatch while providing recommendations for what to consider when exploring and evaluating solutions to keep your organization secure. While this information is not intended to be comprehensive, we hope that it will spark a conversation, making it easier for you to secure your PSAP in the most effective manner possible.



A "LOOMING" DANGER NO MORE: THREATS TO PSAPS HAVE ARRIVED

Public safety answering points process emergency calls in two primary ways: handling incoming calls and as NG9-1-1 rolls out, incoming SMS (text) traffic as well, then dispatching personnel where they're needed. Each use different underlying systems that are interconnected to function properly. While these CAD and call handling systems are designed for security, they connect to a variety of complex complementary systems. These interconnected systems, while providing important capabilities and automations to your operations, also contribute to the overall system's vulnerability.

For example, your agency's CAD workstations often serve multiple purposes, like checking email, browsing the web and accessing various platforms to accomplish other day-to-day tasks. Even if your agency or local government is fortunate enough to have an in-house IT and security team, it's a complex environment with dozens of security tools to manage. It's easy to miss actual security threats in the thousands of daily automated notifications from applications, hardware, software and devices. As NG9-1-1 systems with the ability to accept multimedia roll out, threats are likely to grow further.

According to the Motorola Solutions Threat Intelligence Team, PSAPs largely encounter two main threats: ransomware and TDoS attacks.

RANSOMWARE

Call handlers, 9-1-1 operators, and dispatchers rely on CAD systems to send emergency personnel where they're needed most. Dispatchers also use CAD systems to identify first responder location and status, in addition to prioritizing and recording incoming emergency calls.

Today, ransomware is the most common threat, impacting CAD systems in two ways. The first is via indirect attacks on municipal and public safety networks, which often work as the backbone networks for CAD systems. In the event of a ransomware attack, defenders may disable network services as a precaution, as part of incident response, or during later data restoration activities.

In these instances, even when the PSAP network itself is not directly compromised, degradation of services or even outages may occur. As such, dispatch centers should expect that extortion attacks on municipal networks have a significant chance to also impact 9-1-1 call-taking and handling, CAD, or other functions.

Ransomware can also directly compromise public safety networks themselves. Direct compromise is typically rarer, but does occur, especially in the case of misconfigurations or unsecured services. Direct network compromises often come from trusted connections between multiple environments and adjacent municipal or police networks.

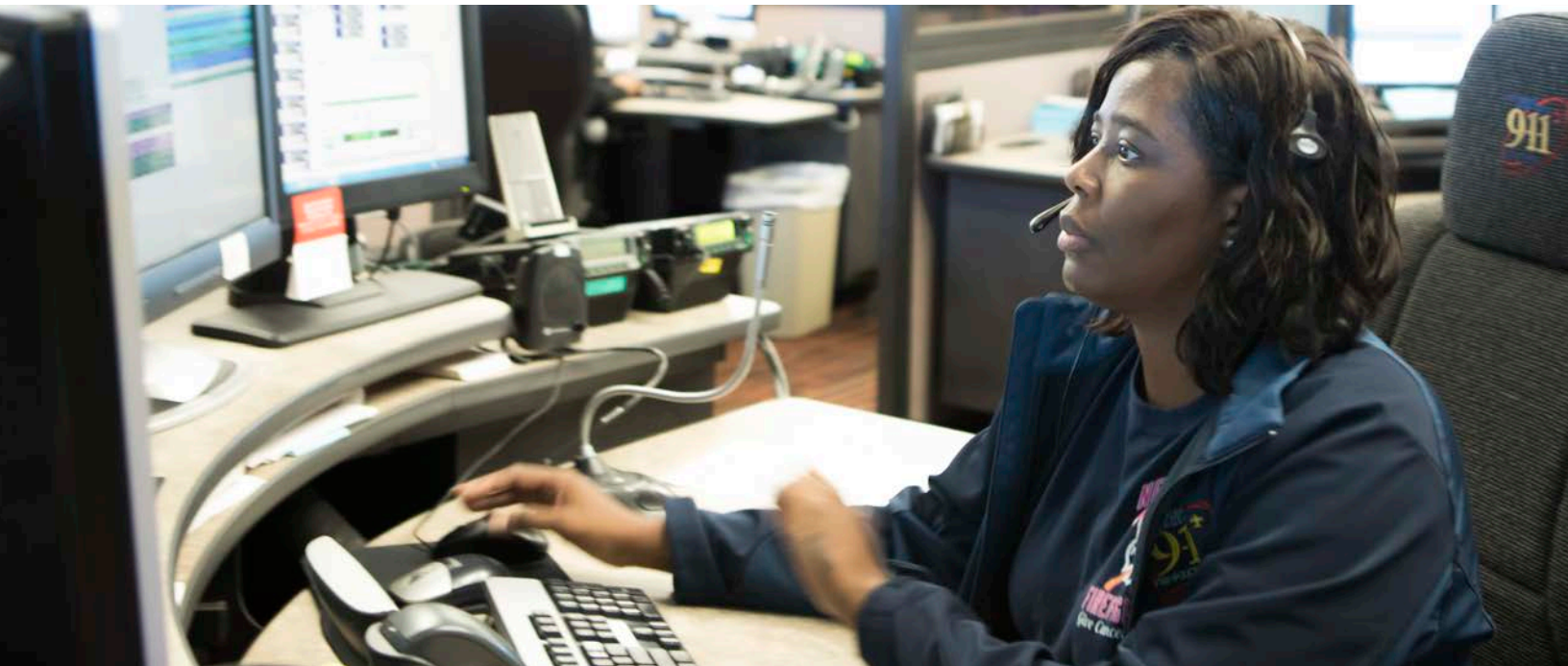
They also occur when CAD workstations are enabled with outbound internet connectivity, which is when activity originates from inside the network, and connects to external services on the internet or outside network. This practice is not the standard and is not recommended. Finally, inbound services such as VPN connections can be compromised in rare instances, leading threat actors to access CAD systems from the open internet or other networks.

Ransomware attacks are not hypothetical threats; they're being actively deployed against PSAPs. A typical case looks like one that happened in 2020.[1]

On a late spring evening, the operations manager on duty for a county PSAP got an alert that someone had logged into a dispatch center workstation using a remote desktop access program. He rushed to the 9-1-1 center and immediately realized someone had launched a ransomware attack against it.

The attackers had locked multiple files and sent an encrypted message with specific instructions for how to unlock them. The operations manager didn't make contact, however, and instead, immediately shut off servers and workstations to minimize the impact of the attack. He also notified state and federal investigators.

Although the attack didn't affect radios or phone communications, it impacted the county's CAD system. Due to the attack, dispatchers had to go back to pen and paper methods to handle calls until the system was brought back online. This no doubt caused a great deal of stress to the dispatchers on duty and the teams in charge of bringing the systems back online.



TELEPHONY DENIAL OF SERVICE ATTACKS: TDOS

Distributed Denial of Service (DDoS) attacks are a well-known type of cyberattack that tries to make a website or network resource unavailable by flooding it with malicious traffic so that it is unable to operate. For PSAPs, that typically takes the form of Telephony Denial-of-Service (TDoS) attacks, which continue to represent a significant threat.

Threat actors leverage TDoS attacks against 9-1-1 and administrative systems via their physical and IP-based telephony lines, both of which can result in disruptions to call handling ability. While these attacks often go unreported, they remain the most common attack type observed involving PSAPs.

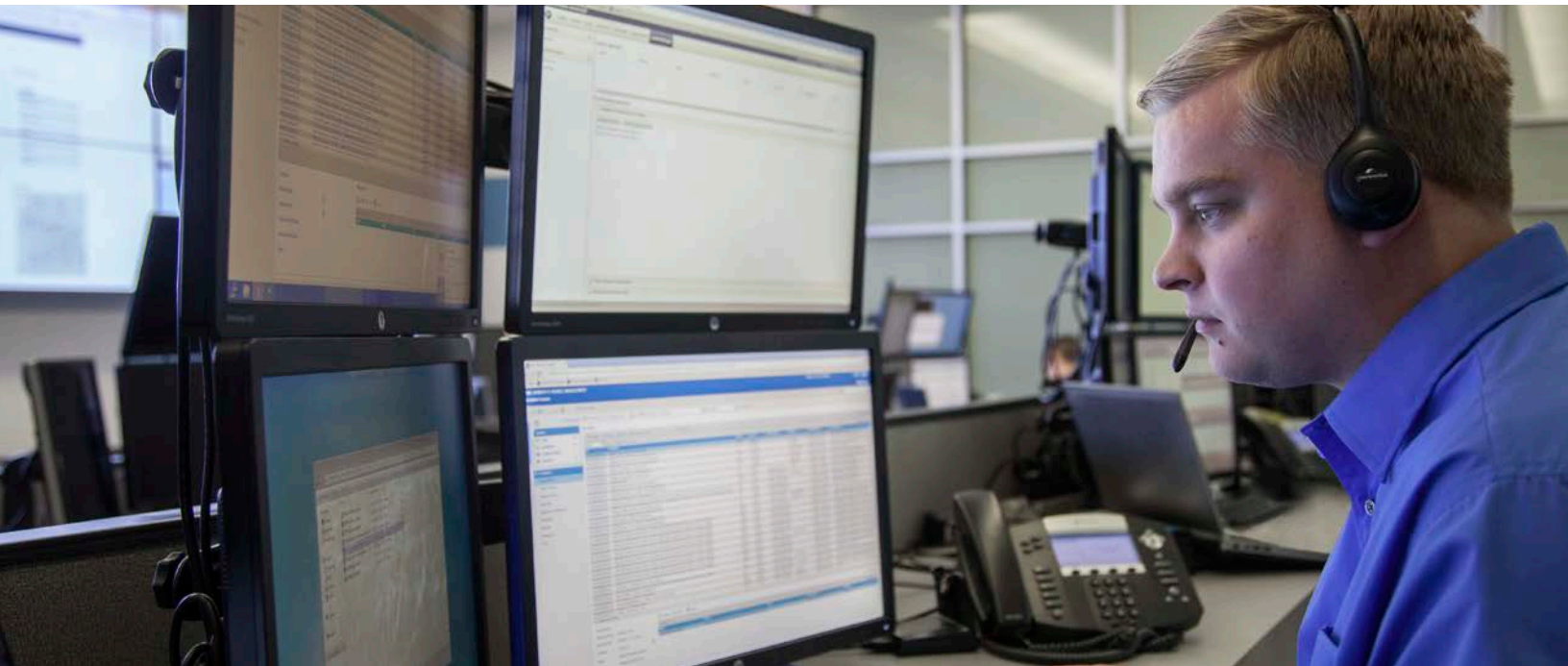
Both manual and automated TDoS attacks are extremely easy to conduct, requiring little to no sophistication. For manual TDoS attacks, threat actors must access an arbitrary, but often high, number of phones. These are either prepaid disposable phones or phones compromised with malware. In either scenario, the attacker can leverage these devices by having them dial emergency numbers, flooding PSAPs with manually-generated calls.

Automated attacks are easier to conduct. They only require access to a virtual telephony system capable of fielding a large number of computer-generated calls. This can be accomplished by renting access to low-cost botnets or even by running simple programs via desktops or other workstations.

The motivations behind TDoS attacks range from ideological to financial or even notoriety. However, according to the Motorola Solutions Threat Intelligence Team, available reporting from victims suggests it's likely that low-sophistication attackers primarily seek to make money in TDoS schemes by extorting PSAPs for a ransom. These financially-motivated TDoS attackers are often unaffiliated with specific groups, instead choosing to act alone. TDoS attacks can occur on both legacy and newer NG9-1-1 systems. However, NG9-1-1 systems are more resilient to TDoS attacks than legacy systems since they are capable of handling a much higher number of simultaneous calls than older systems. However, TDoS attacks are still a problem for NG9-1-1. While NG9-1-1 systems are able to withstand the flood of calls fielded by TDoS attackers, PSAP employees on the receiving end of these calls are not so lucky.

In older, non-NG9-1-1 systems, TDoS attacks impacted service provider phone lines due to higher call loads than telephony bandwidth. In NG9-1-1, those fraudulent calls go through, resulting in call-takers having to answer them. "Real" calls intermingle with these fake ones, as everyday citizens attempt to contact emergency services. This result is that people have to wait longer for their calls to be answered, which often lead to abandoned calls and redials, effectively creating another TDoS within the original attack.

When conducting TDOS attacks against PSAPs, threat actors may position calls during times in which defenders are unable to proactively respond due to high call volume or low staffing. Statewide protests or natural disasters like wildfires can result in a high number of legitimate 9-1-1 calls. Meanwhile, off-hours and some holidays can mean fewer dispatch personnel at work. Either of these situations will worsen the disruptive effects of TDoS attacks.



PSAP CYBERSECURITY: THE BASICS

When it comes to PSAP security, time and budgets are limited, so it's important to prioritize investments that protect the most critical parts of your mission. For PSAPs, that means being available 24x7x365. But how do you make sure your PSAP remains available in the face of rising cyber threats, while also taking advantage of the latest technologies? Here are seven foundational best practices to help get you started.

1 KNOW YOUR RISKS

First, you must understand where your risks are. In order to prepare an effective response and develop a roadmap to protect your system, you need a complete understanding of your vulnerabilities to make informed decisions. This can be done through regular third-party assessments of your people, processes and technology that begin with understanding your unique security environment and concerns.

Developing a high-level understanding of your organization and operational needs is a critical first step. What technologies are you using? What does the architecture of your system and network look like? How are those systems distributed? These considerations help to establish a baseline for your operations and the components that need to be assessed.

It's also important to understand your current approach and practices. What are the roles and responsibilities within your IT organization? What policies and procedures are in place? Have you completed any previous assessments? Are there specific areas of concern that you want to pay special attention to? The answers to these questions provide insights into your current state and what's needed to get to your desired state.

2 TAKE OWNERSHIP OF SECURING YOUR ORGANIZATION'S TECHNOLOGY

For emergency call centers, complexity is only increasing as modern features around NG9-1-1 begin rolling out. To ensure everyone is communicating around security issues, it's important to proactively designate one person within your PSAP to own the operational side of your system. This is similar to a general contractor role; they ensure 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, such as detection and monitoring services. There should be constant communication with one another, streamlining operations and IT.

Although PSAP software and communications systems are designed with security in mind, the shared security responsibility model dictates that emergency call centers take proactive measures to protect those systems once they are deployed.

3 EMPOWER YOURSELF WITH KNOWLEDGE ABOUT SECURITY STANDARDS

The National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, has established a common framework for cybersecurity under Special Publications (SP) 800-53-revision 5. For those requiring international standards, the International Organization for Standardization also addresses cybersecurity under Standards 27001-27002.

In addition, the American Institute of CPAs (AICPA) provides a structure for effective third-party validation of a service organization's controls. This enables auditors to confirm whether or not the vendor is providing the services and standards they claim and provide a detailed report assessing the vendor's performance.

4 PATCH, PATCH, PATCH

Patching is the single most important way for PSAPs to limit the threat of cyber attacks. Regular patching is one of the most efficient and cost-effective actions an organization can take to lower its exposure to cybersecurity threats. Check for software updates and end-of-life (EOL) notifications, and prioritize patching known exploited vulnerabilities. Externally-facing systems and services, such as VPNs, firewalls, and applications should also be prioritized. Regarding cloud systems, ensure that virtual machines and third-party services are patched regularly as well.

It's critical to develop a patching plan, which should consist of written operational strategies and tactics so that patching isn't delayed because of personnel constraints and schedules.

5 UPGRADE HARDWARE

Along with regular patching, upgrading hardware is essential to reduce security vulnerabilities.

Many older systems and OSs, like Windows XP, are no longer supported by the manufacturer. 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.

Another essential upgrade is employing "encryption-in-motion" (i.e., protecting 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.

6 MONITOR SECURITY ALERTS FROM CAD ENDPOINTS 24/7

By deploying endpoint security agents to monitor for attacks on CAD workstations and servers, security analysts can see potential threats in real time and remediate them quickly. Endpoint security services can provide protection against known threats, identify anomalies quickly and enable investigation if there is a suspected incident. Endpoint security services can be applied to any workstations that are required to access critical applications, including CAD, records and evidence and other workstations.

Continuous network monitoring can help defenders spot and remediate problems before they become an emergency, or understand when they should begin incident response as a result of a potential network compromise. When coupled with a team that can realistically interact with and review alerts on a 24/7 basis, network security monitoring can be useful for identifying a significant portion of threats. However, many law enforcement agencies do not have the resources required to devote hours a day to reviewing security logs, and thus should consider using a managed service for 24/7 monitoring.

7 UNDERSTAND ATTACKER MOTIVATIONS VIA THREAT INTELLIGENCE

Finally, it's important to understand the motivations of threat actors. Most are criminals motivated purely by financial gain, which is why ransomware has become the attack of choice for many. The more of your system they can take control of, the more money they can try to extort. Given the stakes, there's tremendous pressure for PSAPs to pay the ransom. But the odds an attacker will actually restore your system once you pay are not good. Many threat actors combine ransomware with demands to pay additional money or face the threat of sensitive information such as criminal case data, informant names or even personal details of first-responders being publicly posted online.

Other threat actors may be motivated by political beliefs or causes such as social injustice. Nation-state actors may attack PSAPs to undermine the stability of communities and trust in government services, or potentially take down emergency response systems as part of a terrorist attack. The best way to thwart these attacks is to not become a victim in the first place. Threat intelligence customized for public safety agencies can offer valuable knowledge on motivations and insights into the threats other PSAPs are facing.

SELECTING THE RIGHT MANAGED DETECTION AND RESPONSE (MDR) SOLUTION

With so many documented ongoing threats to PSAPs, it's critical that agencies commit to implementing a holistic cybersecurity approach. This approach should be centered around a risk mindset that focuses on regular assessments and incident response readiness exercises, deploying modern Endpoint Detection & Response (EDR) solutions, and continuous monitoring to enable rapid threat detection and remediation.

Most importantly, this approach helps better detect zero-day exploits, the methods used by threat actors to take advantage of a vulnerability the vendor themselves have not discovered and therefore have had no time (zero days) to patch. Agencies will also be better prepared to discover adversaries escalating privileges within an IT network or PSAP system and prevent data exfiltration or compromise.

This "gold standard" approach requires experienced professionals to monitor systems, investigate alerts and determine how to implement and update policies and technology specific to your environment and needs. That can be difficult, since finding, hiring and retaining staff with cybersecurity expertise is a constant challenge facing agencies of all sizes that can slow adoption and implementation of the critical tools and processes required for effective protection.

Many agencies are partnering with an MDR provider focused on the specific, unique needs of PSAPs as the most cost-effective way to share or offload the complexity of modern cybersecurity.

When evaluating vendors, look for one that excels in the three critical areas of people, processes and technology. Here are some key questions to ask:

- Are their analysts and advisory services staff trained and certified on an ongoing basis?
- Where are their security operations centers (SOC) located?
- What types of advisory services do they provide specific to public safety?
- Do they offer a robust, co-managed platform with visibility into what their analysts see, as well as advanced analytics, threat intelligence and human expertise to speed incident investigation and response?
- Can they support 24/7 monitoring for your cloud applications and infrastructure, traditional IT networks and firewalls, and endpoints outside of the CAD system?
- How do they correlate security data from these devices and systems with security data from your core PSAP systems?

3 QUESTIONS:

How Can MDR Complement Your Security Team?

1

Are you confident your cybersecurity team can differentiate between a routine and critical system alert?

Many security teams are overwhelmed

by the high volume of alerts from multiple security solutions like EDR, firewalls and web applications. An advanced MDR solution can eliminate most false positives so their security analysts or yours—or a combination of the two—can focus their attention on actual security incidents.

2

Is your cybersecurity team experienced in determining the threat level of suspicious activity, then initiating response actions within 30 minutes?

Initial entry into a system can usually be contained if responded to within 30 minutes. Yet, most teams don't have enough experience with advanced threats to be ready to take action that fast. In contrast, an MDR provider's SOC is typically staffed by highly experienced analysts who battle ransomware and other threats daily, so they're ready to act quickly and effectively whenever needed.

3

Is investigating alerts the best use of time for your internal cybersecurity staff?

Agencies typically have a limited number of cybersecurity professionals on staff. With so many threats and the rapid movement of technology, their work is likely to be most impactful when focused on more strategic cybersecurity projects, instead of day-to-day threat detection and investigation.

PEOPLE

Staffing and training an internal cyber security team can be expensive for public safety agencies. With salaries for cybersecurity experts rising to more than $150,000 on average, it can be prohibitively expensive for agencies to staff and train a security team. Working with a managed security services provider (MSSP) with MDR capabilities can help by providing access to top cyber practitioners, but with a predictable budget.

Any security vendor is only as effective as the people it employs. Look for an MDR provider that offers 24/7 protection delivered by specialists and backed by some level of analytics and automation. The best MDR providers operate as an extension of your team, managing complexity, anticipating issues before they become problems and continuously improving plans to prevent future attacks. These practitioners don't just protect your systems in a vacuum — they offer system transparency while educating and bolstering those in your organization dedicated to security. Make sure your MDR provider offers security advisories, bulletins and extensive reporting so your team can better understand active threats, how to best take action and where to find further information.

In addition, look for a provider that employs experts with top industry cybersecurity certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+ and Certified Ethical Hacker (CEH) . In such a fast-moving industry, where new attack methodologies and threat actors are constantly evolving, it's also important that any MDR provider you select offers comprehensive, ongoing training for their professionals. Ask if a provider follows the NIST Cybersecurity Workforce Framework, which is an important guide to cyber education and training efforts.

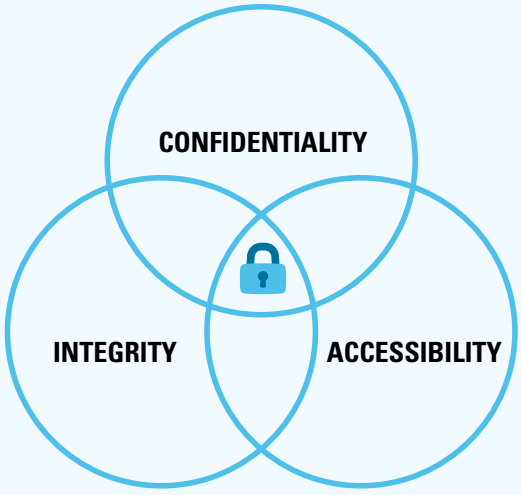
PROCESSES

Your MDR provider should offer a holistic set of services guided by the NIST Cybersecurity Framework, focusing on mitigation options, continuous 24/7 monitoring, diagnosis, and remediation to secure and protect systems and networks. They should prioritize three core objectives: confidentiality, integrity and availability. Data and information must be confined to people authorized to access it and not be disclosed to others. Data must be kept intact, complete and accurate, with IT systems operational and all information must be available to authorized users whenever needed.

Look for an MDR provider that is highly experienced monitoring and investigating attacks on PSAP workstations and servers. This applies to any workstations that are required to access critical applications, including CAD, records, and evidence access stations- both on-premises and cloud deployments.

In addition, if you've already deployed a next-generation EDR solution such as Defender ATP, CrowdStrike, or VMware Carbon Black to protect workstations and mobile devices, make sure you choose a provider that can seamlessly support them through API integrations. This will ease the burden on your internal team who may be struggling to keep up with the volume of alerts they generate or to otherwise manage them. If you haven't deployed these solutions, an experienced public safety focused MDR can advise on the best option for your organization, safely deploy it on your behalf, then continue to manage it.

CIA TRIAD



TECHNOLOGY

Cybersecurity moves fast. The methods and technologies threat actors use to carry out attacks are constantly shifting. Yet, staying current with the latest technology can be expensive and time consuming. To stay a step ahead, ensure any MDR provider you're evaluating is constantly becoming more predictive and proactive with investments in sophisticated tools such as network intrusion detection, vulnerability scanning, and perhaps most importantly, automation and analytics.

When properly applied, automation and analytics can lower operational costs, accelerate service response and augment predictive decision making by eliminating many of the time-consuming manual processes involved in managing threats.

In addition, using advanced analytics to examine threats and failure patterns across your system can eventually prevent security incidents more effectively by addressing their root causes before they can do harm.

But it's not enough to employ the latest cybersecurity technology. It's imperative that an MDR provider seamlessly integrate with a broad range of "traditional" IT infrastructure including endpoint, network, and cloud applications. This provides your agency with a single point of security visibility across core PSAP systems such as CAD, call taking, and record management platforms, but also the rest of your IT infrastructure for complete visibility.

REMEDIATION CHECKLIST

We've provided a checklist that focuses on Operational and Deployed Environment recommendations and guidance which we encourage you to follow in order to prepare for potential cyber attacks known to target environments like yours.

Patching and Updates

- [ ] Patch perimeter touch points: VPN servers, firewalls, routers, switches, and remote access applications (in that order of recommended priority)
- [ ] Patch known exploited vulnerabilities
- [ ] Complete regular operating system updates
- [ ] Complete application software updates as vendors make them available prioritizing security updates
- [ ] Consider updating aging software and hardware prior to their end-of-life dates to leverage next-generation security improvements

Logins / Credentials

- [ ] Require Multi-factor Authentication (MFA), prioritizing critical services and internet-accessible logins and applications (VPN for use and management accounts, accounts managing backups, and so on)
- [ ] Review strong password policies for service, administrative, and credential management privileged accounts and ensure they are being followed
- [ ] Maintain a policy of least privilege through reviewed and approved authorization policies and processes

Protected Backups

- [ ] Create offline (i.e., physically disconnected) data backups. Encrypt backup data at rest and require multi-factor authentication for access if network connected.
- [ ] Consider leveraging native cloud backup and data restoration services for cloud-based services your organization uses. Consider separating account roles to prevent an account that manages the backups from being used to deny or degrade the backs should the single backup account become compromised. Review all accounts for backup operations by reviewing access and actions logs.
- [ ] Develop business recovery plans that validate backups can be restored within your organization's designated recovery timelines, and ensure the integrity of the data backups meet your organization's needs during validation

Hardening

- [ ] Review the need for remote services like Microsoft Windows Remote Desktop Protocol (RDP) — disable at the perimeter OR place behind VPN authenticated access to enable its use. Consider adding multi-factor authentication for remote services which are deemed business-necessary.
- [ ] Review the need for Microsoft Windows Server Message Block (SMB) which enables Windows file sharing, printer sharing, and other like services within the network
- [ ] Review the need for network communication ports and protocols that are not being used for a business purpose throughout the network
- [ ] Implement a user training program and email phishing exercises to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links in emails and elsewhere, and opening suspicious downloaded documents or email attachments. Reinforce appropriate user response to phishing and spear phishing email attacks.
- [ ] Implement end-to-end encryption in web sites and your IT network, as well as within the call handling and communications systems. Discuss with third-party vendors how they've implemented end-to-end encryption or how to enable it for your deployments of their products and services
- [ ] Document all external remote connections through an authorization approval process and regularly audit and review for remote access throughout your organization. Investigate any unauthorized remote access solution installed on servers or workstations immediately.

Monitoring

- [ ] Establish continuous monitoring by leveraging a managed Security Operations Center service for 24/7 monitoring or enabling a team which can continuously review important alerts
- [ ] Monitor traffic flows between segmented networks, looking for abnormal activity
- [ ] Monitor incoming traffic for abnormal activity, prioritizing remote services and VPNs
- [ ] Monitor accounts for abnormal activity and consider adding multi-factor authentication for accounts to limit the threat of compromised credentials
- [ ] Monitor telemetry from your organization's cloud environments and ensure the managed Security Operations Center service has visibility to network, storage, and access telemetry from the cloud instance(s)

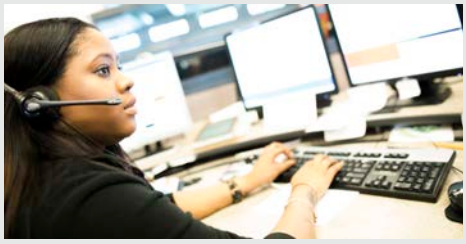
MOTOROLA SOLUTIONS:

ONE SERVICE PARTNER FOR ALL YOUR CYBERSECURITY NEEDS

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the 'one service provider' for your cybersecurity needs.

With the best-in-class people, processes and technology, we bring scalable operations that can help agencies manage cyber risk awareness, detection, response, and recovery. Our cutting-edge Security Orchestration, Automation and Response (SOAR) platform, ActiveEye, delivers deep insights on security management, system performance and service delivery, enabling a co-managed approach.

Motorola Solutions' Managed Detection and Response (MDR) service provides a complete managed security solution to surface risks, identify imminent threats and provide a quick response to mitigate cybersecurity attacks around the clock. The service includes a technology platform enriched with public safety threat intelligence and third-party threat intelligence sources, along with 24/7 support from our SOC cybersecurity experts to investigate threats and initiate a response.

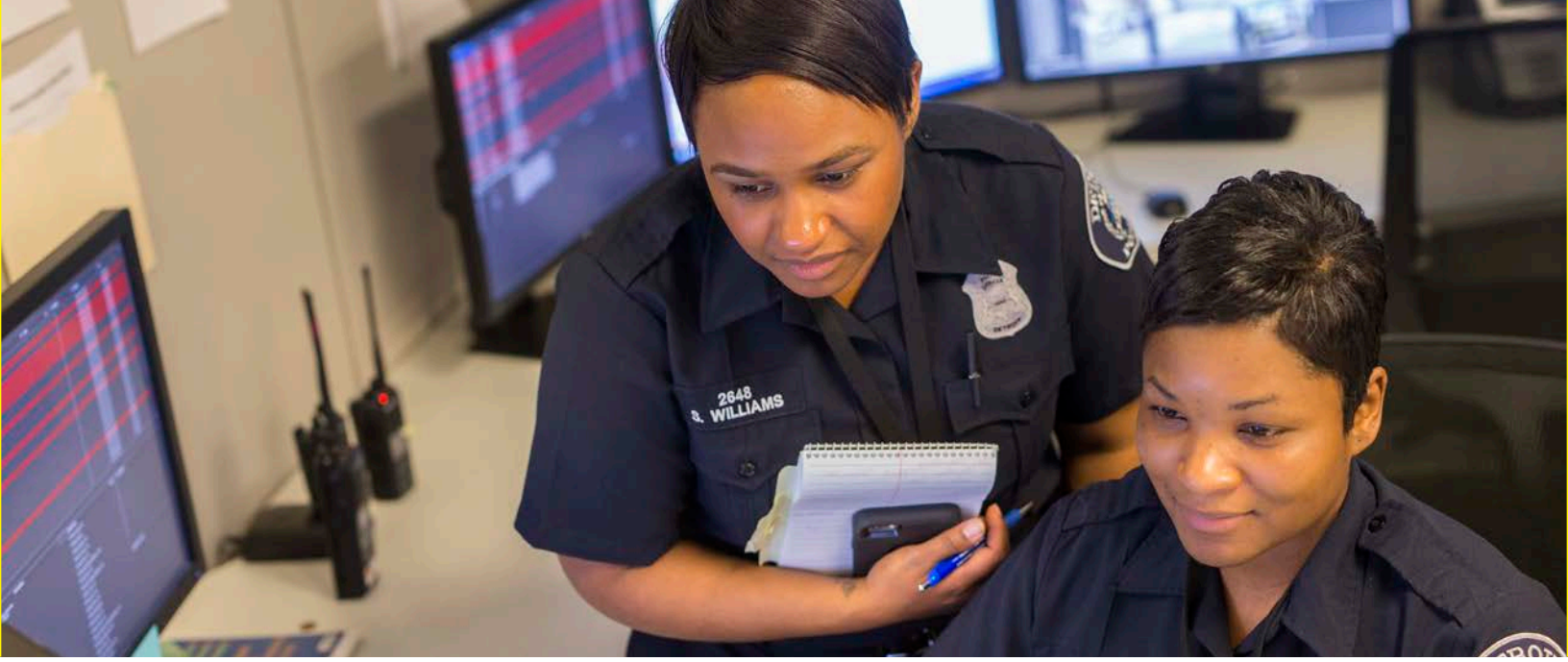


ActiveEye Platform: The core of our ActiveEye security management platform is an analytics and automation engine that learns which cyber events require action and surfaces these to security analysts. Using advanced analytics machine learning and automation, ActiveEye can pinpoint substantiated threats and alleviate false positives and omissions. Both our customers and our SOC team use ActiveEye to get complete visibility into what's happening in their environment.

24/7 SOC: Our SOCs are staffed 24/7 with cybersecurity experts who have a broad set of skills and platform knowledge. These experienced, highly trained and certified security professionals are dedicated to monitoring the secure state of your mission-critical system. They are well-versed in a broad range of attack scenarios and will investigate and initiate a response when necessary. The team is continuously responding to attacks on public safety such as ransomware and has the skills to begin remediation immediately.

Endpoint Detection and Response: Our Endpoint Security Services provide protection against known and unknown threats, quickly identify anomalies and enable investigation if there's a suspected incident. We deploy endpoint security agents to monitor for attacks on all types of PSAP workstations and servers required to access critical applications, including CAD, Records Management Systems and evidence access stations, both on-premises and hosted in the cloud. If your agency has already deployed a next-generation EDR solution to protect workstations and mobile devices, but is struggling to manage it, we can provide 24/7 managed security services to support you via our API integrations.

Managed Detection and Response is just one component of Motorola Solutions Cybersecurity Services. Our portfolio also includes Advisory services such as Cyber Exercises, Risk Assessments and Penetration Testing, as well as services such as Incident Response readiness planning and System Recovery.



THE FIRST STEP TO ROBUST PSAP SECURITY

Today, it's no longer a matter of if, but when and how your PSAP will become a target for cyber intrusion. As agency budgets continue to be stretched thin, cybersecurity hiring continues to be constrained, and PSAPs remain low risk yet highly profitable targets for threat actors, these risks will only increase.

The good news is that no matter where your agency is on its cybersecurity journey, help is available. Managed Detection and Response services can play a critical role in helping you secure your organization and ensure the continuity of your mission. By asking the right questions, then finding the right MDR service provider that can answer them based on your specific agency's needs, you can confidently take the first step on the road to robust PSAP security. When lives are the line, your community deserves nothing less.

For more information about Motorola Solutions cybersecurity services for public safety, visit: **motorolasolutions.com/cybersecurity**

Sources

1 https://www.wkrn.com/special-reports/how-the-lawrence-co-911-center-hit-by-a-ransomware-attack-amid-the-covid-pandemic-handled-the-threat/

MOTOROLA SOLUTIONS

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