CYBERSECURITY

INTRODUCTION

Cybersecurity presents one of the most complex set of challenges for PSAPs in a broadband environment. Not only must each PSAP manage cybersecurity for its own networks and equipment, the networks and systems that interconnect with each PSAP must likewise be secured from intrusion and interference. PSAPs must account for the cybersecurity needs of other related networks and databases including criminal justice, investigative, and medical data for responding agencies, personnel, and the public. It is essential that cybersecurity is considered at the onset, and not treated as an afterthought, when adopting new technologies. In other words, cybersecurity must be "baked in," not "bolted on."

> *It is essential that cybersecurity is considered at the onset, and not treated as an afterthought, when adopting new technologies. In other words, cybersecurity must be "baked in," not "bolted on."*

THE CYBERSECURITY ROLE

Cybersecurity risks have the potential to affect everything from national security to public safety communications networks and other critical elements such as financial institutions, electric power distribution, and even intrusions into vehicles. Even the most sensitive and proprietary information is subject to intrusion and attack from malicious cyber actors, criminal groups, and nation states. With public safety communications systems becoming ever more reliant on IP-based technologies, including in a legacy environment, the threat is real and potentially very consequential.

For these reasons, cybersecurity practices and policies must be established and applied to PSAP personnel and technology vendors. Key concepts include the need to identify vulnerabilities, detect anomalous behavior, respond to incidents, mitigate the damage, and recover from the event. A new culture of cybersecurity awareness must be fostered and integrated with technical and operational considerations to defend both legacy and next generation systems.

The Existing Threat

To date, thousands of Telephony Denial of Service (TDoS) attacks have been identified nationally, with an alarming amount of those attacks directed at public safety or related targets. 9-1-1 networks have traditionally been secure, with limited access and effective controls in place. CAD systems are typically designed and operated on closed, internal networks with little or no access to or from any system other than the 9-1-1 and radio systems maintained internal to the public safety entity. Despite this relatively secure environment, PSAPs and other law enforcement, fire/rescue, and even federal agencies have been successfully targeted and impacted by TDoS, Distributed Denial of Service (DDoS), and ransomware attacks.[63] These attacks can render PSAPs unable to receive, process, and respond to calls for service, and public safety data and records can become inaccessible or corrupted (including potentially without actual knowledge that records have been changed).

The scale and sophistication of cyber-attacks vary. For example, one DDoS incident in October 2016 resulted in widespread disruptions to some of the most used sites on the Internet.[64] This attack against Dyn, one of the companies that run the Internet's domain name servers, represented a successful manipulation of multiple Internet of Things (IoT) devices on a global scale to effect damage on a specific target. The Dyn attack represents a coordinated and complex approach with global impact.

In a separate incident, also in October 2016, a single actor perpetrated a multi-state TDoS attack against numerous PSAPs in twelve states in the United States.[65] The perpetrator was an 18 year old who developed a simple JavaScript (programming language) code that was spread through a popular web link and infected mobile phones, causing them to repeatedly dial 9-1-1 without the knowledge of the user. This actor did not require specialized knowledge of 9-1-1, but was nonetheless able to create a signficant disruption to 9-1-1 through an exploit that was extremely difficult for PSAPs to mitigate.

The Future Threat

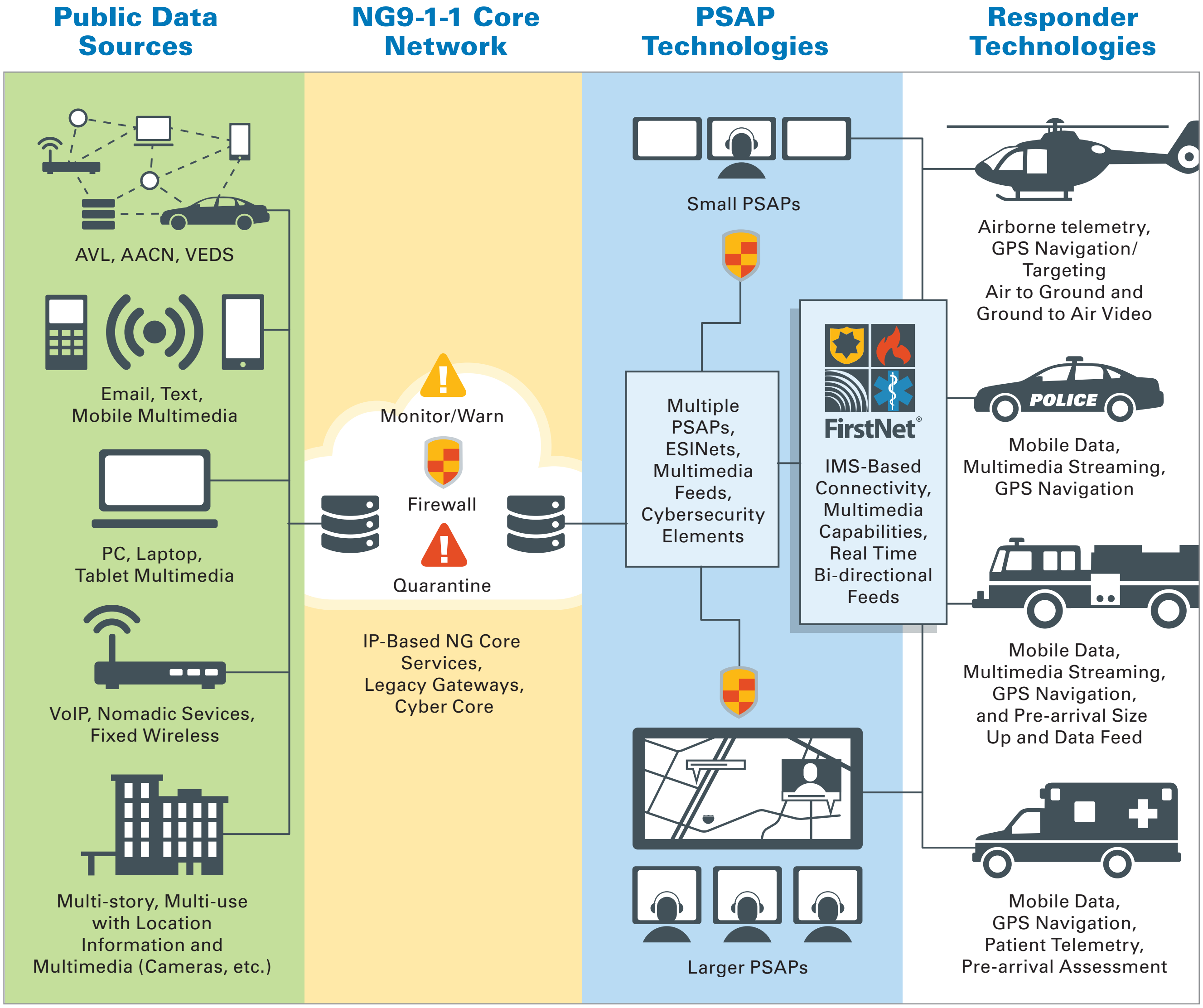
As public safety communications transition to IP-based technologies, PSAPs will experience more cyber-attacks. Broadband-based systems such as NG9-1-1, IoT, smart cities, intelligent highways, mobile apps in use by the public and responders, and next generation alerting platforms that may benefit PSAP operations also create new vulnerabilities. With the introduction of various new ways to access public safety communications networks, most of them in the relatively open Internet environment, the ability to secure networks and critical data from cyber-attack must be a primary consideration when designing and implementing any new solutions.

As public safety communications transition to IP-based technologies, PSAPs will experience more cyber-attacks.

Added to this, the implementation of the NPSBN, managed by FirstNet, will provide first responders with wireless broadband communications using a uniform technology and network design to ensure interoperability. Like NG9-1-1, the NPSBN will be an IP-based network of networks that will be subject to cyber risk. Given that NG9-1-1 and FirstNet networks will enable significant exchange of data, all stakeholders should pay close attention to the prospect of bad actors seeking to exploit one or both of these significant pillars of the future emergency response ecosystem. Figure 1 illustrates the flow of information and a number of the touch points of these two networks. See Appendix 1 for a detailed list of potential vulnerability points resulting from the interconnection of NG9-1-1 with the NPSBN.

The threat of cyber-attack cannot deter the progression into what may well be the most significant advancement in emergency communications since the advent of two-way radio or basic 9-1-1 services. Public safety must commit to deploying these new technologies in such a way that cybersecurity is incorporated by design into planning, implementation, and operations models at the onset. The resolve to combat cyber-criminals and cyber-activists on every front must be unwavering. Education and training, proper planning and design, and a unified approach centered on information sharing and collaboration will help to ensure success.

Figure 1. **Interconnected NG9-1-1 and FirstNet Networks**


Public Data Sources
NG9-1-1 Core Network
PSAP Technologies
Responder Technologies
AVL, AACN, VEDS
Email, Text, Mobile Multimedia
PC, Laptop, Tablet Multimedia
VoIP, Nomadic Sevices, Fixed Wireless
Multi-story, Multi-use with Location Information and Multimedia (Cameras, etc.)
Monitor/Warn
Firewall
Quarantine
IP-Based NG Core Services, Legacy Gateways, Cyber Core
Small PSAPs
Multiple PSAPs, ESINets, Multimedia Feeds, Cybersecurity Elements
FirstNet
IMS-Based Connectivity, Multimedia Capabilities, Real Time Bi-directional Feeds
Larger PSAPs
Airborne telemetry, GPS Navigation/ Targeting Air to Ground and Ground to Air Video
POLICE
Mobile Data, Multimedia Streaming, GPS Navigation
Mobile Data, Multimedia Streaming, GPS Navigation, and Pre-arrival Size Up and Data Feed
Mobile Data, GPS Navigation, Patient Telemetry, Pre-arrival Assessment

Cybersecurity Concepts

While the purpose of this report is not to provide comprehensive educational material on cybersecurity, a brief overview of several important topics is essential for a discussion of the implications to PSAPs.

Identity, Credential, and Access Management (ICAM)

ICAM refers to the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources such as electronic files, computer systems, or physical resources such as server rooms and buildings.

Firewalls

Firewalls contribute to security by controlling the flow of information into and out of network entry points. By using a set of user-defined configuration rules, a firewall determines which traffic will be allowed to pass through and onto the network. Traffic that doesn't satisfy the configured rules is rejected. For more guidance on the use of firewalls to control access, see Appendix 2.

User Access

Secure user access is achieved through the use of authentication and authorization. Authentication is the means by which a user's identity is confirmed. Once authenticated, a user is authorized to perform certain functions as defined by his or her role within the organization. User access can be restricted in various ways, such as by using solutions commonly deployed by IT departments, establishing authorization requirements for individual devices (e.g., routers, servers, embedded controllers, workstations), and by stronger authentication methods for critical host devices such as smart cards or USB tokens, biometric authentication, and two-factor authentication.

Remote Access

Providing access to remote users presents a unique set of security challenges. Addressing these challenges may require building additional protections into the network infrastructure, such as using secure connections and data transfer protocols, multi-factor authentication, and placing strict limits on who may remotely access the network.

Vendor Access

Virtually all organizations have networks, systems, and facilities that rely on outside vendors for service. Those vendors might require physical access, dedicated remote network access, network cloud access, or any combination of the three. When using a vendor, a level of risk is inherent in the relationship.

Vendor staff should meet the agency's security and background check requirements. The due diligence and negotiation processes should include a thorough vetting of the vendor's in-house cybersecurity practices, as well as the specific protections designed into its offering. It's important to inquire of employee continuity, both to limit those having access to PSAP systems, and to ensure continuity of support. The vendor company must be stable and financially sound. These factors should be addressed in vendor contracts.

PSAPs need to balance the risk to networks with the level of access needed for vendors to service their equipment. For example, remote access by vendors to the network can be accomplished through either a Secure Shell (SSH) Tunnel, Virtual Private Network (VPN), or dedicated communication link. Regardless of the access mechanism, security patches should always be kept up to date.

When a vendor accesses the agency network a strong password policy must be required. For example, single-use passwords for vendors are an effective means of minimizing the risk of vendor access.

Passwords

User passwords for public safety networks must balance security needs with burdens on the user. Unrealistic password policies can actually undermine cybersecurity if users develop workarounds (such as keeping a written list of passwords at a workstation). Password protection policies should apply to user-level, system-level, network equipment, web, email, and public safety application accounts, and include routine changing of passwords, careful storage of passwords, avoiding repetitive use of similar passwords, separate passwords for separate systems, and review of the password policy with employees. These measures can help ensure the public safety network remains secure and that all users (including employees, contractors, consultants, temporary workers, etc.) adhere to the password policy. See Appendix 3 for recommended guidelines and practices for password creation and protection.

Physical Security

Because a single point of intrusion such as a work station or server room can expose an entire system to cyber-attack, physical security is an essential component for mitigating cybersecurity risks. Physical security prevents unauthorized access to devices, networks, and information. Without it, intruders have the means to circumvent all of these otherwise restricted vulnerabilities. Physical security policies should address building security, workstation and individual program authorizations, visitor access, and other measures (such as security cameras). Regularly scheduled audits of physical security measures should also be conducted.

Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction, or malfunction of equipment. In order to minimize these risks, data must be stored in an appropriately secure and safe environment, and frequently backed up.

Removable media should not be the only place where data obtained for agency purposes is held. Copies of any data stored on removable media must remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

The Human Element

The people who interact regularly with an agency's network play a critical role in maintaining overall system security. Cybersecurity protections can easily be undermined, either knowingly or unknowingly, by a single individual. Policies and procedures must outline what is considered acceptable use of the agency's networks, proper email usage, and approved use of removable media.

Social engineering and phishing are two types of hacking techniques that are considered "low tech" methods of intrusion into a facility or network. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Phishing is an example of a social engineering attack, typically carried out by email, that is the favored method used by cyber-criminals. A phishing email might appear to come from a colleague or friend, using personal information for the appearance of authenticity, to deliver malware and ultimately gain access to secure systems.

Removable Media and Access Ports

Removable media is a well-known source of malware infections and has been directly tied to loss of sensitive information in many organizations. Open and unsecured network access ports on switches, routers, firewalls, etc. pose a similar threat as individuals can connect removable media to gain physical presence on the agency network.

Removable media include, but are not limited to:

- USB Memory Sticks (also known as pen drives or flash drives)
- CDs
- DVDs
- Optical Disks
- External Hard Drives
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and answering machines)

Removable media are helpful for processes such as backing up data, updating software, and transferring files without a network connection. However, removable media have historically been a source of spreading malware and viruses. A well-documented and closely followed removable media and access port policy helps ensure the integrity of the network, data, and computer systems of the agency. See Appendix 4 for guidance on removable media security and access port policy.

FINDINGS

Existing Educational Materials

Many organizations have developed resources that the public safety community can use to improve cybersecurity. This report need not attempt to replicate the work done in these documents, but the following may be of interest to public safety communications professionals seeking to learn more about cybersecurity issues:

- APCO's Cybersecurity Committee report, "An Introduction to Cybersecurity: A guide for PSAPs"[66]
  - This document can serve as a starting point to educate PSAP supervisors on identifying, preventing, and minimizing exposure to cybersecurity risks and vulnerabilities.

- The FCC Task Force for Optimal PSAP Architecture (TFOPA) report[67]
  - The TFOPA report includes a section entitled "Optimal Approach to Cybersecurity for PSAPs" with recommendations and a toolkit for use by PSAPs that includes a guide for evaluating cybersecurity capabilities and risks, a roadmap for creation of a cybersecurity strategy, and a list of potential resources for PSAPs and 9-1-1 authorities.

- The 2012 DHS "Emergency Services Sector (ESS) Cyber Risk Assessment"[68]
  - This document is intended to provide a risk profile that ESS partners can use to enhance the security and resilience of the ESS disciplines by increasing the awareness of risks across the public and private sector domains.

- The 2014 DHS primer on "Cyber Risks to Next Generation 9-1-1"[69]
  - The primer is an introduction to improving the cybersecurity posture of NG9-1-1 systems nationwide and provides an overview of the cyber risks that will be faced by NG9-1-1 systems. It is intended to serve only as an informational tool for system administrators to better understand the full scope and range of potential risks, as well as to recommend mitigations to these risks.

- The NIST Framework for Improving Critical Infrastructure Cybersecurity[70]
  - The NIST Framework is designed to help organizations manage cybersecurity risk, and a next version is under development.

- Industry best practices relevant to TDoS attacks[71]
  - As a result of a cooperative effort between federal authorities, public safety representatives, and commercial service providers, a checklist was developed to assist in the development of a continuity of operations plan for TDoS attacks.

The Key Role of Personnel

Training PSAP personnel about the role each person plays in maintaining security within an organization is critical. From basic cyber hygiene to more advanced network security training and programs (such as to recognize risks or actual attacks in progress), security begins and ends with the people who operate the systems and services that support the public safety mission.

Opportunities for Resource-Sharing

FirstNet and NG9-1-1

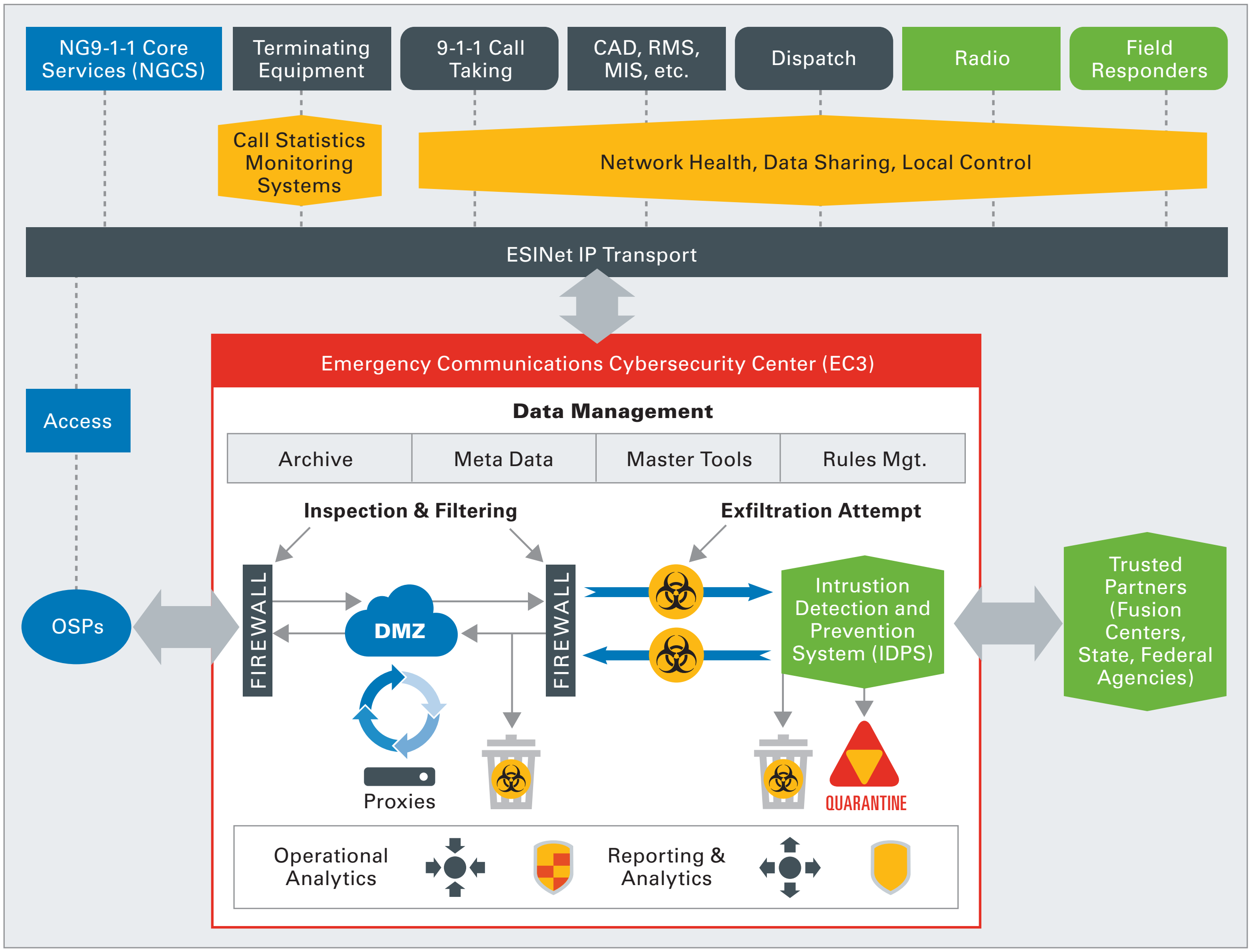
FirstNet and NG9-1-1 networks are both designed with IP technologies and therefore are susceptible to cybersecurity risks. They will constitute the twin pillars of the future emergency response ecosystem, frequently exchanging data and information and sharing a mutual, strong interest in protecting the integrity of public safety communications networks and data. As FirstNet implements its cybersecurity strategies, and approaches are being considered to protect NG9-1-1 networks, there could be benefits to a cooperative approach.

The Emergency Communications Cybersecurity Center

Intrusion Detection and Prevention Systems (IDPS) are network security/threat prevention technologies that examine network traffic flows to detect and prevent vulnerability exploits. By centralizing services such as IDPS, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place. The FCC's TFOPA developed a concept known as the Emergency Communications Cybersecurity Center (EC3), which would centralize IDPS for next generation public safety networks.

In the proposed architecture, the EC3 takes on the role of providing IDPS services to PSAPs and

Figure 2. **The Emergency Communications Cybersecurity Center**

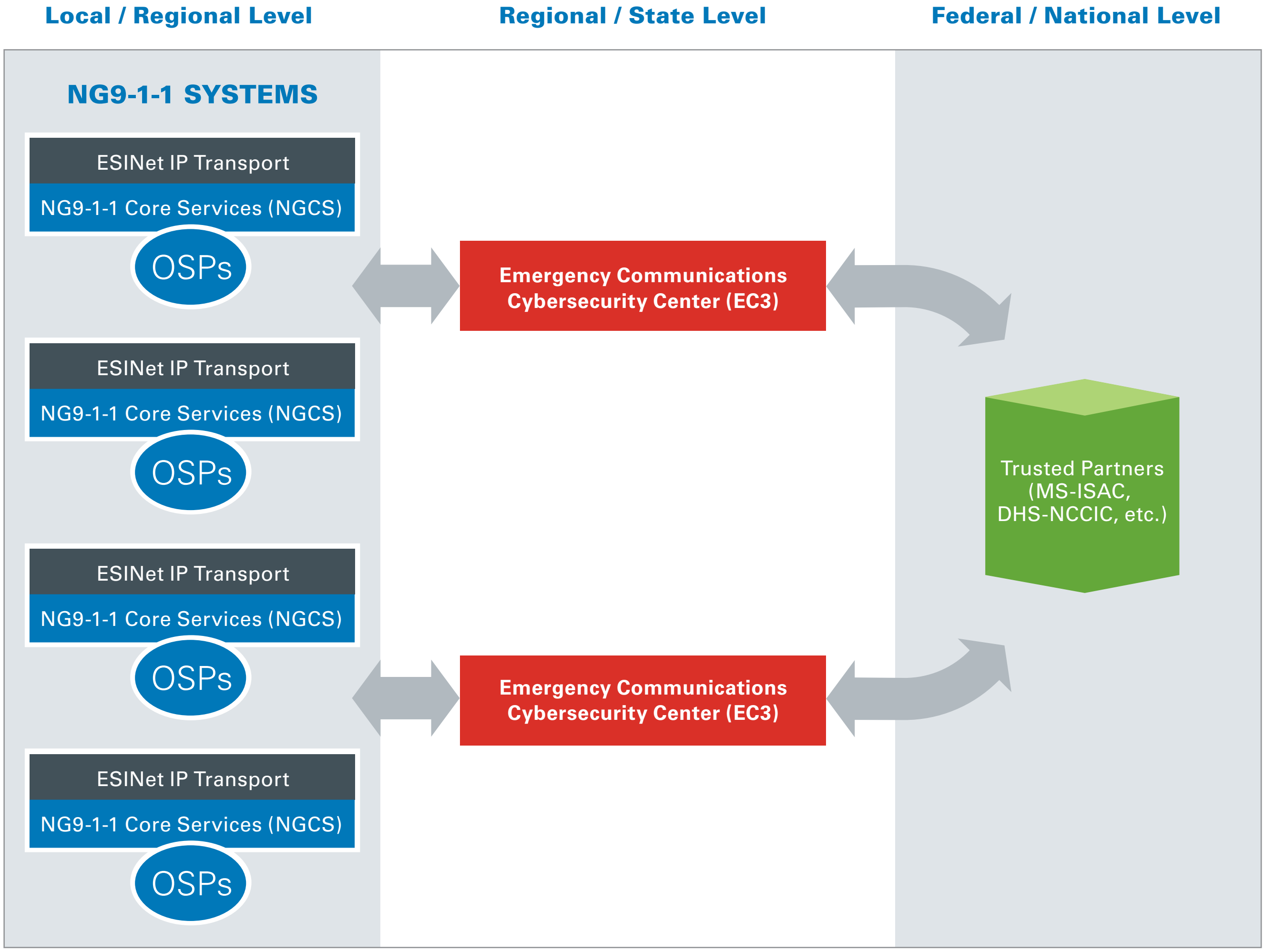


any other emergency communications service or system that would consider utilizing the centralized core services architecture proposed. For example, emergency operations centers could also connect to the EC3 service. This approach would allow public safety entities to build one infrastructure that serves many clients. EC3s could be designed to interconnect with other IDPS throughout the United States, for example if a large public safety entity wanted to manage its own EC3 but benefit from the analysis made possible from the larger ecosystem. This flexibility provides significant economies of scale, puts multiple resources into the same protection scheme, and allows for sharing of data, mitigation strategies, and recovery efforts across the public safety ecosystem.

As illustrated in Figures 2 and 3, the potential flow of this system would begin with the originating service provider (OSP) and NG9-1-1 core services elements, encompass the ESInet transport network between disparate PSAPs, and provide for monitoring of call statistics, system health, anomaly detection, data sharing, mitigation, and recovery, while still allowing local agencies to maintain control of day-to-day operations.

Rather than requiring PSAPs to build and staff such facilities, the EC3 concept allows for PSAPs across all jurisdictions to interconnect to the core cybersecurity system and benefit from its capabilities. While not specified, the interconnect requirements would include cyber hygiene elements at the PSAP, single user sign-on and multi-factor authentication at the local level, and

Figure 3. **The EC3 Deployed**


Local / Regional Level
Regional / State Level
Federal / National Level
NG9-1-1 SYSTEMS
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
ESINet IP Transport
NG9-1-1 Core Services (NGCS)
OSPs
Emergency Communications Cybersecurity Center (EC3)
Emergency Communications Cybersecurity Center (EC3)
Trusted Partners (MS-ISAC, DHS-NCCIC, etc.)

some form of agreed upon, trusted connection (and relationship) from the local levels to the state or regional level EC3.

This architecture is intended to represent a scalable and customizable approach. This means for localities with larger than average emergency communications systems (such as major metropolitan areas) there is ample opportunity to construct a single EC3 to serve this individual customer. However, any EC3 should be designed and constructed in such a way that it will interconnect with other EC3s throughout the United States with the same functions and requirements. From the regional or state level, the information should flow to a centralized, trusted, federal repository with adequate service capabilities to support multiple clients and incidents in real time.

Increased Complexity and Risk from Interconnection

Individual networks are expected to maintain a heightened level of cybersecurity posture to protect from exposure to other networks that may have been compromised. It is reasonable to expect that each network will interconnect to its peers through a series of firewalls, intrusion detection systems, and border control mechanisms.

Following the FCC’s TFOPA cybersecurity recommendations, an overall IDPS is needed to protect public safety networks as an enterprise, and individual networks should have specific security requirements to interconnect via IDPS to other networks. Security is needed at each end point, meaning at each user-termination node, such as a

PST workstation or CAD terminal. Stronger security protections should be in place at touch points with connections to non-secure networks and devices such as the citizen caller, external databases, web-based traffic, and other data connections to systems beyond the operational ownership of the modernized public safety network. Even interconnection points between internal public safety networks, such as between ESInets, legacy PSAPs, and next generation core services, and between FirstNet systems and NG9-1-1 systems, should have a certain level of cybersecurity rather than assuming that these networks are safe.

Land Mobile Radio (LMR)

When addressing security surrounding communications systems and infrastructure, it's easy to overlook traditional LMR. Today's radio system infrastructure no longer simply consists of a transmitter in an equipment shed with an outside antenna that may be considered immune to cyber-attack. Rather, LMR bears a closer resemblance to a traditional data center than that of the old "radio room." There are servers, routers, and firewalls as well as other IP-connected devices that need to be secured.

CAD, CPE, and GIS

The variety in approaches for implementing CAD, CPE, and GIS, including the concept of hosted solutions, adds to the complexity of addressing related cybersecurity challenges. It is important to keep in mind that all of these systems represent a method of accessing the PSAP and may be shared among several PSAPs, introducing a greater vulnerability and level of potential impact. Common cybersecurity approaches should include limiting access to these systems by other systems and software applications, and use of strong passwords.

Internet Access and Mobile Apps

PSAPs increasingly provide Internet access at PST work stations. This can be a useful tool for obtaining information such as real-time weather and news reports, but even when the connection is separated from CAD and other important systems, Internet access presents a cybersecurity threat. For example, a PST might receive a call over the PSAP's ten-digit line that was initiated through a mobile app advertised for use by the public during emergencies. The caller could be a representative working at the app's third party call center, claiming that an app user in the PSAP's jurisdiction reported an emergency and that further information is available through a website. With the cybersecurity vulnerabilities of mobile apps and the Internet, the information ultimately being received and recorded by the PST could be misleading or even malicious. To counteract this threat, some PSAPs limit access to only pre-approved ("whitelist") websites. Other PSAPs have established criteria for blocking sites that are not related to their positional duties or pose a potential security threat. As described in the Technology section of this report, APCO is continuing efforts to ensure public safety apps are as safe and effective as possible.

Other IP-Based Systems

Many systems within PSAPs are IP-based. It is imperative that centers consider all of the various systems which could be threatened by a cyber-attack. Some of these systems are:

- Power (uninterrupted power supply (UPS), climate controls, building monitoring systems, battery chargers, remote monitoring systems)
- Security cameras
- Fuel pump systems
- Any device with an assigned IP-address ■

RECOMMENDATIONS: CYBERSECURITY

There are a number of proactive steps that public safety agencies can take to plan and properly defend networks and systems. The following section represents some high level recommendations to help agencies begin this critical process.

Education and Training

APCO encourages agencies of all sizes, and personnel at all levels, to get engaged in the cybersecurity conversation, get educated about the threat, and become proactive in the defense of the public safety communications ecosystem.

> *APCO encourages agencies of all sizes, and personnel at all levels, to get engaged in the cybersecurity conversation, get educated about the threat, and become proactive in the defense of the public safety communications ecosystem.*

The ability to defend networks and systems is directly related to the understanding of those systems. Even basic knowledge of the networks and systems, and the security risks and potential solutions available, will empower public safety leaders to ask relevant questions of their vendors who, in turn, can provide focused responses and design solutions for the safety and security of the PSAP.

Security training works best if participation is mandated and monitored for effectiveness, and made part of quality assurance/quality improvement programs. APCO will develop and offer a cybersecurity hygiene course for public safety communications professionals to assist with these challenges.

Sharing Cybersecurity Resources

APCO supports the concept of an EC3 as described by the FCC's TFOPA cybersecurity report.[72] APCO recommends becoming familiar with the EC3 concept and proposed architecture, as well as considering requirements for full IDPS capabilities in any forthcoming RFPs related to next generation systems and services.

> *APCO supports the concept of an EC3 as described by the FCC's TFOPA cybersecurity report.*

Develop a Cyber Strategy

PSAPs should develop strategies for preventing and mitigating cyber-attacks. Individual approaches may vary. For example, strategies may entail conducting audits of cyber hygiene and unauthorized access on a monthly basis, or setting more stringent protection measures for systems based on cost and perceived need. Universally, however, these strategies should be comprehensive, recognizing that cybersecurity needs to be a group effort, with everyone made to feel they are part of the solution.

If a system is hit by a cyber-attack, having a plan available for immediate implementation and mitigation is essential. Establishing critical partnerships with technology partners and government resources will lessen the impact to the organization and increase the ability of enforcement agencies to locate and prosecute the actors. APCO currently participates in federally-coordinated response efforts by working with the DHS National Coordinating Center for Communications (NCC) to distribute information about potential cyber-attacks affecting PSAPs.

Report Suspicious Activity, Threat, or Attack

PSAP personnel having reason for concern of a cybersecurity issue should report the event as soon as practical after attending to any operational priorities. This helps situational awareness particularly if the attack is widespread. Complaints can be filed with the Internet Crime Complaint Center, www.IC3.gov, which is co-sponsored by the Federal Bureau of Investigation and the National White Collar Crime Center.

> *PSAP personnel having reason for concern of a cybersecurity issue should report the event as soon as practical.*

Notes

63 "In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software."
Incidents of Ransomware on the Rise - Protect Yourself and Your Organization, Federal Bureau of Investigation, at https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.

64 https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service.

65 http://securityaffairs.co/wordpress/52895/cyber-crime/911-service-attacks.html.

66 https://www.apcointl.org/resources/cybersecurity/cyber-security-guide-for-psaps/file.html.

67 https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf.

68 https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-508.pdf.

69 https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20FINAL%20508C%20(003).pdf.

70 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. For the NIST Framework and documents related to an updated version, see https://www.nist.gov/cyberframework/draft-version-11.

71 http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service/.

72 https://apps.fcc.gov/edocs_public/attachmatch/DA-16-179A2.pdf.