Chapter 7

Security Considerations

The implementation of NG9-1-1 technology provides ECCs with the opportunity to take a holistic approach to cybersecurity protections. As APCO has previously stated, cybersecurity should be baked in, not bolted on.[23] This means cybersecurity protections should be incorporated by design into planning, implementation, and operation models from the onset. Viewing cybersecurity in this manner will reduce the need for costly, after-the-fact solutions that may not meet the level of security protections required by emergency communications. ECCs will need to ensure that their technical and operational cybersecurity protocols are sufficient for both an NG9-1-1 and a legacy environment.

New Threat Vectors for NG9-1-1

With the current E9-1-1 environment, there are challenges and threats that will continue to evolve and, without proper mitigation techniques, pose threats to ECCs. These challenges include spoofing, swatting, and hacking known vulnerabilities in systems, networks, and infrastructure. With the implementation of NG9-1-1, some of these challenges will be mitigated. However, new threats will arise as bad actors identify new tactics, techniques, and procedures (TTPs) to exploit emergency communications equipment. As ECCs transition to IP-based technologies, 9-1-1 systems will transition from operating on networks with limited access to sharing networks with other ECCs, agencies, and vendors. This open environment will create new ways to access emergency communications networks, thus further increasing the risk of a cyberattack.

Due to the critical nature of the work performed, ECCs will continue to be a high-value target for multiple categories of hackers. Despite the substantial risk of cyberattacks, many ECCs have inadequate protective infrastructure and lack appropriate and industry-specific cybersecurity training.

ECCs will need to ensure that their technical and operational cybersecurity protocols are sufficient for both an NG9-1-1 and a legacy environment.

Hardware and Software Vulnerabilities

NG9-1-1 implementation will require significant hardware and software upgrades to any ECC. From a cybersecurity perspective, some factors to consider for hardware cybersecurity are EOL support, maintenance, zero-day vulnerabilities, known threats, and flash updates.

EOL support can be critical as the emergency communications industry transitions from E9-1-1 to NG9-1-1. EOL support refers to the assistance a company offers after it decides to discontinue a product or service. For example, after Microsoft discontinued support for Windows 7 the company provided users an iterative path to upgrade their operating system before support would no longer be provided.

ECC stakeholders should understand how their hardware solutions will handle zero-day vulnerabilities, known threats, and flash updates. A zero-day vulnerability is a security flaw that has been disclosed and identified, but a mitigation patch has not been developed. Once a vulnerability is known, it is incorporated into the Known Exploited Vulnerabilities Catalog along with any known mitigation techniques.[24] Any cybersecurity plan should include a strategy to update and protect ECCs from zero-day and known vulnerabilities, such as through flash updates, regular security updates, or other mitigation strategies determined by local resources.

ECCs should examine any new pieces of hardware and software that will be installed on local networks. IT professionals should review the new pieces of equipment in a virtually secure and segmented environment where they can determine if a device has any known vulnerabilities already installed (known as a pre-hacked device). An IT Department should sanitize all hardware and software that will be incorporated into the ECC network to ensure it is safe.

Before selecting an NG9-1-1 solution vendor, ECCs should verify the following information:

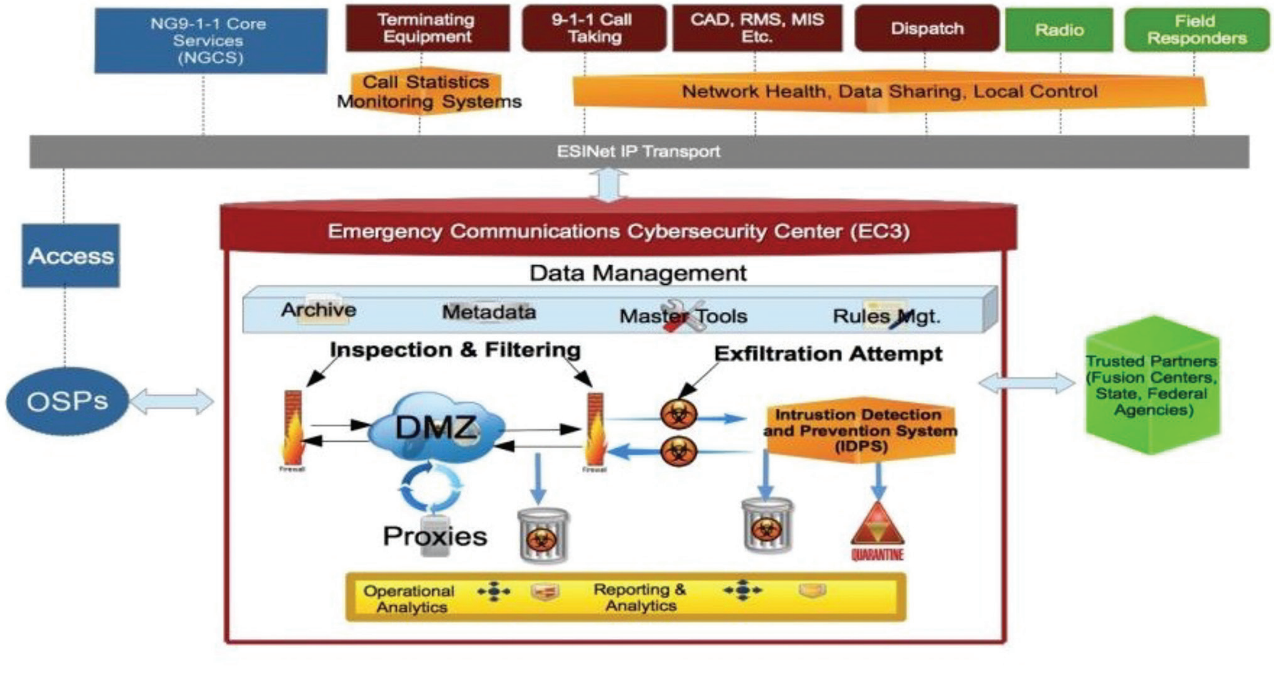
- How are security patches provided to the ECC? ECCs should work with software vendors to ensure that these security patches adhere to local policies and procedures and do not interrupt ongoing services.
- For regularly scheduled updates, how will the vendor work with local IT support to implement security patches? ECCs must be prepared for any system change and coordinate with IT staff.
- What is the EOL support plan? When a vendor stops support for a software program, local jurisdictions should understand what the EOL support plan will be.
- If there is a need for a version update, will there be any costs for the ECC and will the vendor outline the known cybersecurity vulnerabilities? Software evergreen is essential to address emerging cyber threats and to improve or add functionality to the ECC.

NG9-1-1 Cybersecurity Architecture Centralized

The FCC's Task Force on Optimal PSAP Architecture (TFOPA) reports outlined a cybersecurity defense mechanism called the Emergency Communications Cybersecurity Center (EC3) (see Figure 2).[25] The EC3 concept encourages a holistic approach to emergency communications by allowing public safety entities to build one core cybersecurity infrastructure that serves several agencies. This approach allows local authorities to share costs and benefit from comprehensive services and capabilities that might otherwise be cost-prohibitive. According to the FCC TFOPA final report:[26]

> *The TFOPA has determined that an additional layer should be introduced into the recommended future architecture. The intent of the logical architecture proposed in the form of the EC3 is to create a*

Figure 2: Emergency Communications Cybersecurity Center (EC3)



> *centralized function for securing NG networks and systems. By centralizing certain features, including cybersecurity in general and Intrusion Detection and Prevention Services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices that may already be in place or at a minimum readily available for deployment and use.*

As illustrated in Figure 2, the potential flow of this system would begin with the originating service provider and NG9-1-1 core services elements, encompass the transport networks between ECCs, 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.

To facilitate cybersecurity protections, the EC3 concept utilizes intrusion detection and prevention services (IDPS). This means the EC3 architecture has the capabilities to identify possible incidents, log information about them, attempt to stop them, and report them to security administrators.[27]

Inherent in the IDPS nature of the EC3 concept is the continuous monitoring of both voice and data networks to ensure a timely and efficient cybersecurity response. Several free resources assist ECCs in this effort through DHS CISA. Some of these free resources include:[28]

- Vulnerability scanning
- Web application scanning
- Phishing campaign assessment

In addition to outlining the EC3, the TFOPA reports also provide the following cybersecurity specific resources for ECCs to implement:

- Checklists to assist ECCs in assessing current cybersecurity posture.
- A roadmap of the cybersecurity lifecycle and assistance to achieve a more cyber secure posture.
- Cybersecurity use cases that are specific to emergency communications.
- Additional authoritative cybersecurity resources.

Developing a Response Plan to Cyberattack

Although ECCs can enhance cybersecurity awareness, it is essential that ECCs create a cyber incident response plan to guide employees in responding to an attack. In the instance that computers are unavailable, a printed copy should be provided to all staff. There are several resources that ECCs can rely on to create this document, including:

- National Institute of Science and Technology (NIST) Special Publication 800-61,[29] which outlines the four phases of an incident response lifecycle: preparation; detection and analysis; containment, eradication, and recovery, and post-incident activity (See Figure 3), and provides guidance on categorizing functional impacts, information impacts, and recoverability efforts.[30]
- The TFOPA reports, which include a generic template (complete with dependencies) to create a thoughtful approach to a cyber incident response plan based on the incident response lifecycle.[31]
- NIST Special Publication 800-61R2 that outlines 11 Crisis Handling Steps.[32]

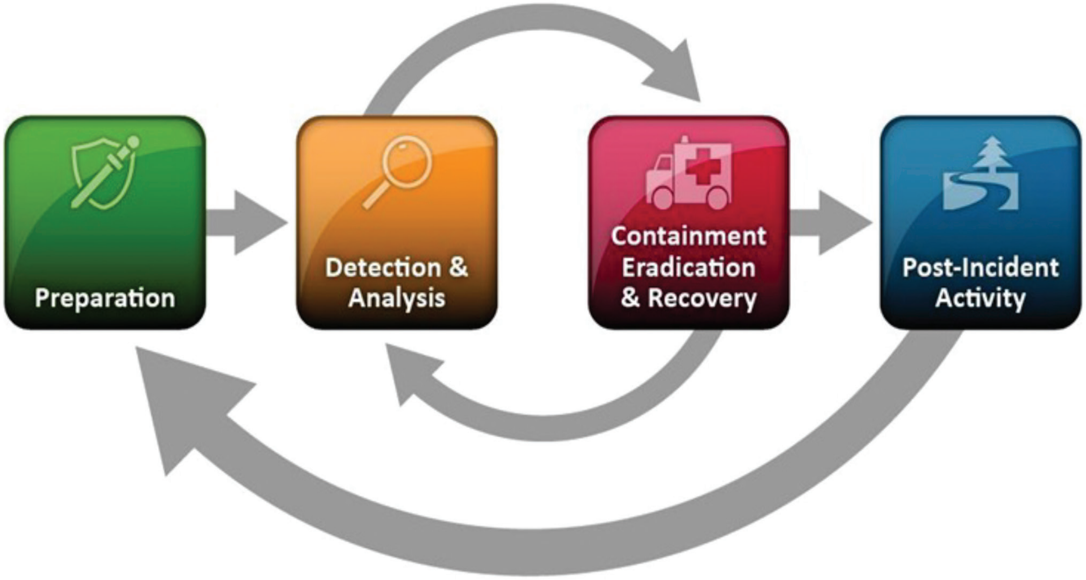
Cyber incident response plans may take several months to develop properly and should be created and maintained with the support of all jurisdictional stakeholders.

Once complete, ECCs should distribute the plan to all employees and conduct training to ensure that employees understand how to protect operations properly. Employees should maintain a printed copy of this plan in case networks are unavailable.

Improving Physical Security

For existing and future NG9-1-1 ECCs, strong cybersecurity practices should also include strong physical security practices. Developing a physical protection policy and procedures to safeguard hardware, software, media, and data from unauthorized access and use is essential. A systematic approach to physical security begins with performing an inventory of assets within the ECC, identifying potential vulnerabilities to the assets, identifying the potential threats,

Figure 3: Incident Response Lifecycle



understanding expected losses, and establishing a cyber incident response plan to prevent unauthorized access. Perimeter fencing, secured doors, locks, security cameras, and alarm systems assist in limiting access to secure areas of the ECC.

Secure and non-secured areas within the ECC should be prominently posted and separated by physical controls so that ECC personnel may verify individuals before allowing access. Risk is minimized when the ECC has an active list of authorized and credentialed personnel or deploy escorted access within the facility. Access should be limited to work areas minimally necessary to persons within the ECC, and devices that display PII or CJI must be positioned in a manner to prevent viewing by unauthorized persons.[33] Additionally, access to any physical components connected to the network and any unsecured workstation or external media control-removable hardware presents a significant risk of a cybersecurity attack, including when allowing bring your own device (BYOD) on the ECC system.

Cyber Training

The training of personnel to fully understand cybersecurity risks is a continual process that requires the fundamental recognition that networks, software, applications, and the devices and processes used within the ECC are significant targets for cyberattacks.[34]

A common phrase within cybersecurity circles is, “a system can be technologically the most secure system in the world, but there will always be a vulnerability – the people using the system.” APCO has an ANSI-accredited standard titled “Cybersecurity Training for Public Safety Communications Personnel.”[35] This standard recommends specific training for ECC personnel based on their role and the development of local policies and procedures, including on the topics addressed above. This standard recommends that designated ECC personnel devote at least four to eight hours annually to educating employees on policies and the employees’ role in maintaining a security posture.

Developing and Implementing NG9-1-1 Policies and Procedures

Although the TFOPA report provides a framework for NG9-1-1 cybersecurity, ECCs must create policies and procedures to help guide employees toward a secure NG9-1-1 ecosystem. When creating these policies and procedures, it is essential to gather the perspective of jurisdictional stakeholders, including IT staff, ECC leadership, and any local personnel that maintain systems and networks. Some examples of useful policies and procedures for cybersecurity include:

- Acceptable use policy
- Social media use
- Authentication procedures
- Password creation
- Email
- Remote access
- Endpoint protection

Chapter 7

KEY TAKEAWAYS

- The TFOPA report provides multiple resources specific to **enhancing cybersecurity for emergency communications**, including the EC3 concept, checklists for evaluating an ECC's cybersecurity posture, a roadmap of the cybersecurity lifecycle, and cybersecurity use cases.
- When implementing new hardware and software into the ECC, **local jurisdictions should work with vendors** to ensure that security updates will be provided.
- Jurisdictions should **create and maintain policies and procedures** to ensure an enhanced cybersecurity posture.
- ECCs are a high-value target for cybercriminals. **ECCs should create a cyber incident response plan** to guide employees through a response to a cyberattack.

[23] *Project 43: Broadband Implications for the PSAP*, APCO International, at 37 (2017).

[24] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[25] Task Force on Optimal PSAP Architecture, Federal Communications Commission (2016) *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-16- 179A2.pdf.

[26] transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf

[27] csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf

[28] https://www.cisa.gov/cyber-hygiene-services

[29] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[30] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[31] Task Force on Optimal PSAP Architecture, Federal Communications Commission (2016) *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-16- 179A2.pdf.

[32] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[33] FBI, (2020). CJIS Security Policy (5.9). https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf

[34] Bixler, M. & English, J. (2020). *Fundamentals of cybersecurity for the ECC*. APCO International: Alexandria, VA.

[35] https://www.apcointl.org/~documents/standard/31101-2019-cybersecurity/?layout=default