CDE #65182

CYBER THREAT PREP

Cybersecurity in the ECC requires educating personnel about the risks.

By Megan Bixler

In 1966, the Defense Advanced Research Projects Agency (DARPA) accepted the concept that became the prototype for the internet. This concept was called Advanced Research Projects Agency Network (ARPANET). Its design was the beginning of the internet that we know today, with commercialization of this technology occurring in 1985. During this time, there was little to no discussion about cybersecurity, using this technology for public safety purposes (and addressing those unique needs) and/or incorporation of the internet of things (IoT).

Almost 60 years after DARPA accepted ARPANET, we have the conveniences of the modern-day internet. In 2023, the internet is used for activities like banking, driving directions and staying connected with people.

IoT devices are also becoming increasingly common in U.S. households. According to the National Institute for Standards and Technology (NIST), IoT devices are "devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world."[1] Examples of these devices can be Wi-Fi enabled refrigerators, alarm systems or thermostats. IoT is becoming so ubiquitous that there will be 27 billion connected IoT devices by 2025.[2]

There is no argument that in the 60 years since the internet's inception we've become increasingly reliant on the internet. The incorporation of the internet has also welcomed people that want to exploit these capabilities — and our reliance on them — for their gain. Threat actors and hackers. A cyber threat actor is an individual or group posing a threat,[3] and a hacker is an unauthorized user who attempts to or gains access to an information system.[4]

A cyber threat actor or hacker has tactics, techniques and procedures (TTPs) that constantly evolve. There have been hundreds of cyberattacks directed at public safety communications. These cyberattacks range from ransomware to data exfiltration to advanced persistent threats. ECCs have reported that during a cyberattack, their backups have been compromised and deemed unusable. As APCO's P43 report states, "It isn't if you are attacked. It is when."

PREVENTING CYBERATTACKS

Public safety has access to tools and guidance that will assist with preventing a cyberattack. NIST has published guidance in Special Publication 800-61 revision 2: Computer Security Incident Handling Guide (nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf). In Section 3 of this special publication, the incident response lifecycle is detailed.[5] The stages of the incident response lifecycle are: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

GORODENKOFF/SHUTTERSTOCK.COM

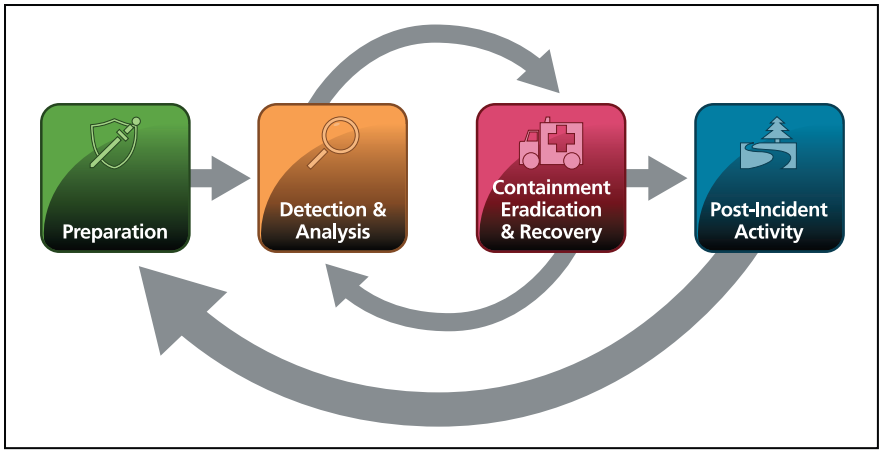

Figure 1: The incident response lifecycle from NIST Special Publication 800-61, revision 2.

Although prevention efforts are not categorized the same as preparation efforts, NIST SP 800-61 R2 outlines five areas on which ECCs can focus to prevent a cyberattack. They are:

- **Risk assessments**. ECCs should conduct risk assessments on systems and networks to discover any vulnerabilities that would allow a hacker to gain unauthorized access. After each risk is identified, it should be prioritized and mitigated.
- **Host security.** All devices on an ECC network should be included in the ECC patch management plan, properly configured according to the principles of leave privilege and auditing enabled to log security events.
- **Network security**. ECC networks should be properly configured to deny unauthorized activity. This includes securing connection perimeter connection points and connection points to other organizations.
- **Malware prevention**. Software should be deployed throughout the ECC network to detect and stop malware.
- **User awareness and training**. ECCs should educate all employees on current cyber-related policies and procedures, current cyber threat trends, and cyber incident response plans.

REASONS TO CONDUCT CYBERSECURITY-SPECIFIC TRAINING

It isn't if your ECC experiences a cyberattack, it is when. Since the first 9-1-1 call in 1968, there have been a lot of technological advances in the way we take and process calls for service. To date, all 50 states and Washington, D.C., have been affected by a cyberattack. Additionally, we must prepare for Next Generation 9-1-1 (NG9-1-1). According to APCO International's Definitive Guide to NG9-1-1,[6] NG9-1-1 will be an interoperable, secure, IP-based system that:

A. Employs commonly accepted standards;
B. Enables ECCs to receive, process and analyze all types of 9-1-1 requests for emergency assistance;
C. Acquires and integrates additional information useful to handling 9-1-1 requests for emergency assistance; and
D. Supports sharing information related to 9-1-1 requests for emergency assistance among ECCs and emergency response providers.

One of the best defense mechanisms for ECCs to protect against cyberattacks is providing cybersecurity education specific to public safety. Below are three reasons why cybersecurity education is beneficial to both ECC employees and the ECC's cybersecurity program by fostering a culture of cybersecurity awareness.

- **Protection of personal information**. ECCs are trusted by citizens and fellow responders with sensitive information. With that trust, there is a great responsibility to ensure that information is safeguarded. Daily, ECCs handle a great deal of personal identifiable information (PII). NIST defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."[7] PII is vital for maintaining privacy, preventing identity theft, complying with regulations and building trust. Cyber threat actors gaining access to citizen PII data could put them at risk for identity theft and an increased risk of social engineering and cause a loss of confidence in public safety. If fellow responder data is gained, you add the threat of compromised responder safety. ECCs have an ethical obligation to protect the personal information they are entrusted with. Respecting an individual's rights to privacy and taking appropriate measures to secure PII is a fundamental aspect of ethical data handling.
- **Defending against cyber threats**. Cyber threats constantly evolve, and cyber threat actors continually modify threat vectors, TTPs and explore new cyber threat vectors. Cybersecurity education provides ECC employees with knowledge about evolving cyber threats, types of cyber activity that impact public safety and common cyber hygiene techniques. This will reduce the likelihood of a successful cyberattack by enabling ECC employees to identify these types of threats including critically examining inbound emails and appropriately identifying phishing scams. The likelihood of clicking on a nefarious link dramatically decreased when ECC employees were provided with tips about what to look for.
- **Empower employees.** Cybersecurity education empowers employees to contribute to a secure environment. By promoting cybersecurity practices, ECC employees commit to a safe online ecosystem for themselves, fellow responders and citizens. This could include reporting suspicious activities to their IT department, adhering to ECC cybersecurity policies and procedures, and fostering a culture of cyber awareness.

The APCO Institute offers two cybersecurity courses that are specifically designed for public safety.

- **Cybersecurity Fundamentals for the ECC**. This course provides ECC professionals with a foundational knowledge of cyberattacks, including the anatomy of a cyberattack, signs of an ongoing cyberattack and mitigation techniques. This includes preparing for cyberattacks, response to those attacks and the type of data to protect for post-attack forensics.

- **Intermediate Cybersecurity Principals for the ECC.** This course is designed for public safety IT personnel, IT leadership personnel who work on critical networks within ECCs and ECC supervisory staff charged with IT and cybersecurity responsibilities. This course provides an understanding of a hacker's perspective, motives and weaknesses. It includes additional information on the incident response by looking at the conditions contributing to a network's vulnerability and dissecting the step-by-step process of a cyberattack.

AMERICAN NATIONAL STANDARD

In 2019, APCO published an ANSI-accredited American National Standard (ANS) titled "APCO ANS 3.110.1-2019 Cybersecurity Training for Public Safety Communications Personnel." This standard states that ECCs should devote four to eight hours annually toward educating ECC employees on ECC cybersecurity policies and reviewing an employee's role in maintaining a good cybersecurity posture. It also states that public safety telecommunicators should understand why cybersecurity awareness training is important, be able to identify signs of a cyberattack and provide any actions that should be taken. This standard is free for download and can be found on the APCO standards page. (www.apcointl.org/services/standards/find-standards)

CYBER INCIDENT RESPONSE PLANS

Since its inception in 1966, the internet has become part of everyday lives. We have computers that assist in making daily life more accessible and convenient, including Wi-Fi enabled home thermostats that you can monitor and adjust remotely. There have also been massive improvements to 9-1-1 in that time. No longer do public safety telecommunicators need to manually keep track of incidents with pen and paper. Computer aided dispatch (CAD) helps ECCs to organize and streamline resources.

Cyber threat actors have learned to exploit this connected and convenient world. ECCs are a high-value, high-threat and high-vulnerability target.

ECCs can strengthen cybersecurity programs by developing a cyber incident response plan. These plans should take a holistic approach to planning for when a cyberattack occurs. NIST Special Publication 800-61 R2 Computer Security Incident Handling Guide (referenced above) describes the elements that each cyber incident response plan should have. Those elements are:

- A mission.
- Strategies and goals.
- Senior management approval.
- Organizational approach to incident response.
- How the incident response team will communicate with the rest of the organization and with other organizations.
- Metrics for measuring the incident response capability and its effectiveness.
- Roadmap for maturing the incident response capability.
- How the program fits into the overall organization.

Part of any cybersecurity training program should include educating ECC employees on the specifics of their cyber incident response plan. Additionally, this plan should be available via electronic and physical means as a reference. If a computer system is unavailable, telecommunicators should still be able to access the plan. ●

***Megan Bixler, RPL**, is the Technical Program Manager for Communications Center and 9-1-1 Services for APCO International.*

REFERENCES

1 NIST. Information Technology Laboratory. Computer Security Resource Center. "IoT device." https://csrc.nist.gov/glossary/term/iot_device.

2 IOT Analytics. "State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally." https://iot-analytics.com/number-connected-iot-devices/.

3 NIST. Information Technology Laboratory. Computer Security Resource Center. "threat actor." https://csrc.nist.gov/glossary/term/threat_actor

4 https://csrc.nist.gov/glossary/term/hacker

5 NIST, U.S. Department of Commerce. "Computer Security Incident Handling Guide." Paul Cichonski, et. al. August 2012. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

6 APCO International. "APCO's International's Definitive Guide to Next Generation 9-1-1." 2022. https://www.apcointl.org/ext/pages/APCOng911Guide/APCO_NG911_Report_Final.pdf

7 NIST. Information Technology Laboratory. Computer Security Resource Center. "PII." https://csrc.nist.gov/glossary/term/PII

CDE EXAM #65182

1. According to NIST 800-61 R2, all of the following are elements of a cyber incident response plan except:
   a. Mission
   b. Schedules
   c. Effectiveness metrics
   d. Strategies and goals

2. IoT stands for:
   a. Intermediate obvious threat
   b. Irony of telecommunicating
   c. Isometric oddity training
   d. Internet of things

3. A cyber threat actor is:
   a. Someone who received a theater degree on the internet.
   b. An individual or group posing a threat.
   c. A reporting party that works in the tech industry.
   d. The new supporting role on Tik Tok videos.

4. Stages of the incident response life cycle include:
   a. Preparation, detection and analysis, containment eradication and recovery, and post-incident activity.
   b. Posing as a hacker, analyzing the content, cryptocurrency and ECC preparedness.
   c. Hosting a website, securing the scene, clearing cache and cookies, and powering off your computer.
   d. Awareness, education, prevention and eradication.

5. PII (personal identifying information) doesn't include:
   a. Name
   b. Mother's maiden name
   c. Biometrics
   d. Your waist size

6. It isn't if you experience a cyberattack, it's when.
   a. True
   b. False

7. ECCs are:
   a. A high value, high threat and high vulnerability target
   b. A low value, low threat and low vulnerability target
   c. A high value, low threat and high vulnerability target
   d. A low-value, medium-threat and never-vulnerable target

8. Not included among the reasons cyber education is beneficial to ECC employees and to cybersecurity is:
   a. It keeps personnel busy
   b. It fosters a culture of cybersecurity
   c. ECCs are trusted by citizens and fellow responders with sensitive information
   d. Cyber threat actors continually modify threat vectors

9. APCO ANS 3.110.1-2019 Cybersecurity Training for Public Safety Communications Personnel states that ECCs should devote _____ hours annually toward educating ECC employees on ECC cybersecurity policies and review an employee's role in maintaining a good cybersecurity posture.
   a. 12-24
   b. 6-10
   c. 4-8
   d. 1-5

10. U.S. Advanced Research Projects Agency Network (ARPANET) was:
    a. A hacker's entry-level job.
    b. The first prototype of the internet.
    c. A way to make easy money in college.
    d. The first malware installed on a computer.

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.

2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).

3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online! To receive a complimentary certificate of completion, you may take the CDE exam online. Go to http://apco.remote-learner.net/login/index.php to create your username and password. Enter CDE in the search box, and click on the "Cyber Threat Prep," then click on "enroll me" and choose **"Cyber Threat Prep (65182)"** to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.