CDE #67613

ONLY YOU CAN PREVENT CYBER FIRES

Public safety telecommunicators must take responsibility for cybersecurity and the practices necessary to maintain it.

By The APCO Cybersecurity Committee

Let's be honest: Public safety communications sit at the front lines of emergency response. Society depends on the unseen operation of emergency communication centers (ECC), where public safety telecommunicators protect our way of life by managing the flow of information and directing resources. It's a difficult profession — more of a calling — chronically plagued by staffing crises. Technology has expanded the capacity of what a single person can accomplish in the modern ECC environment. Yet these same technological wonders that allow us to better protect our communities come with a new set of challenges.

CYBER IN THE SPOTLIGHT

It's all over the news today: *cyber*security, *cyber*attack, *cyber* this, *cyber* that. But what is cyber anyway? Beyond simply computers and printers typically associated with IT, cyber has a broader meaning and now describes anything with a digital system or a connection to a digital network. What began with computers and the internet now includes cell phones, home appliances, traffic lights, manufacturing systems, entire power plants and the list continues with no end in sight. Cyber is the foundation of our digital society.

A glance around the modern ECC confirms this reality. Computer aided dispatch (CAD) allows today's digital public safety telecommunicator to effortlessly manage units and calls for service, but it may as well be called *cyber* aided dispatch. Advanced phone systems enabling a telecommunicator to juggle between both 9-1-1 and non-emergency calls rely on computer servers either at the ECC

> **Regular training sessions can help ensure all staff members — from new hires to seasoned professionals — are up to date on the latest cyber threats and best practices for mitigating them. APCO recommends that ECCs provide four to eight hours of training annually on ECC cyber policies and procedures.**

or in the cloud. In smaller centers without such systems, the phone service itself is often provided through a digital network in the background. Even the radios are cyber now, as contemporary radio dispatch consoles are computer-based — trunked or simulcast — and radio systems are increasingly built upon or migrating to digital networks.

WHAT CONSTITUTES A CYBERATTACK

Armed with a grasp of cyber in the ECC environment, how then should we understand a cyberattack? Longtime computing giant IBM defines the term as "any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device."[1] Or in simple terms, a cyberattack is any incident that negatively affects the intended operation of a cyber asset. These attacks range from laughably simple to staggeringly complex, and they may be targeted toward a specific organization or opportunistic in nature.

These examples emphasize the importance of cybersecurity for critical infrastructure, including systems that support emergency response and management. While direct attacks on ECCs may not always be publicly disclosed, incidents affecting related systems or municipal services demonstrate the need for robust cybersecurity measures.

Imagine how a cyberattack might affect your agency, keeping in mind all the critical ECC systems are now cyber assets. Losing one of these major systems may be an inconvenience, but what if all of these critical systems were to disappear? In another scenario, an attacker might sneakily alter the CAD database to remove histories and officer cautions, rewrite call narratives or simply steal the database altogether. What could happen in the ECC environment?

- **Data breaches:** Unauthorized disclosures may expose sensitive information related to citizens, responders, emergency plans, resource allocations and coordination efforts.
- **Disruption of operations:** Cyberattacks, such as ransomware or distributed denial-of-service (DDoS) attacks, can hinder the timely and effective coordination of emergency response efforts by rendering systems or communication channels inaccessible.

- **False information and manipulation:** Cyber threats may involve the dissemination of false information through ECC communication channels or the manipulation of data. This can lead to confusion, misinformed decision-making and potentially impact public safety.
- **Compromised communication systems:** ECCs rely on communication systems to coordinate response and share critical information. Compromise of these systems can impede the ability to communicate with emergency responders, government agencies and the public.
- **Loss of public trust:** An attack involving an ECC can erode public trust in the government's ability to manage emergencies effectively. Confidence in the ECC's capabilities may diminish if citizens perceive their personal information is at risk or that help may not be available in an emergency.
- **Financial impact:** Incident response activities, such as restoring systems, conducting forensic investigations and implementing additional security measures, may incur significant costs.
- **Legal and regulatory consequences:** ECCs are often subject to privacy and data protection laws, such as the FBI Criminal Justice Information Services (CJIS) Security Policy.[2] A cybersecurity incident could result in legal actions, fines or other regulatory penalties.

ENTER CYBERSECURITY

Ignoring the risk of cyberattack is an invitation for disaster. The sensitive nature of

JANEWS/SHUTTERSTOCK.COM

the data ECCs handle and the critical role they play in emergency response make them attractive targets. This is where cybersecurity, the art of protecting cyber assets, takes the stage. Cybersecurity refers to protecting computer systems, networks, programs and data from digital attacks, unauthorized access, damage or theft.[3] It encompasses a broad range of technologies, processes and practices designed to safeguard digital infrastructure. Key aspects of cybersecurity include:

- **Confidentiality:** Ensuring that only authorized individuals or systems have access to sensitive information.
- **Integrity:** Safeguarding the accuracy and completeness of data, ensuring that it is not altered or tampered with in an unauthorized manner.
- **Availability:** Ensuring that systems and data are accessible and operational when needed, minimizing downtime and disruptions.
- **Authentication:** Verifying the identity of users, devices or systems to ensure that access is granted only to authorized entities.
- **Authorization:** Determining the level of access and permissions granted to authenticated users based on their roles and responsibilities.
- **Network security:** Protecting the integrity and confidentiality of data as it is transmitted across networks, including the internet.
- **Endpoint security:** Securing individual devices (endpoints) such as computers, smartphones and tablets from cyber threats.
- **Incident response:** Developing plans and procedures to respond effectively to cybersecurity incidents, such as breaches or attacks.
- **Security awareness and training:** Educating users and employees about potential cybersecurity threats and best practices to mitigate risks.
- **Vulnerability management:** Identifying, assessing and mitigating vulnerabilities in software, hardware and processes to reduce the risk of exploitation.

STARTING A CYBERSECURITY PROGRAM FOR ECCS

The first step toward a robust cybersecurity program is well-defined policies and response plans. Does your organization have policies or response plans for things

such as suspicious email or digital compromise? If so, how old are they? Are they regularly reviewed and updated to address the evolving threat landscape? A comprehensive cybersecurity policy should cover areas such as access control, data protection, incident response and disaster recovery to name a few. It should also be reviewed and updated regularly to ensure its relevance and effectiveness. In addition to cybersecurity policies, your organization should have a disaster recovery plan. This plan outlines steps to be taken in the event of a major incident, such as a cyberattack, to ensure continuity of operations.

Training is the second crucial component of a cybersecurity program. It's not enough for the policies to simply exist; staff members need to understand and follow them. Does the onboarding process address training on cyber concepts? Do existing employees receive ongoing training? Regular training sessions can help ensure all staff members — from new hires to seasoned professionals — are up to date on the latest cyber threats and best practices for mitigating them. APCO recommends that ECCs provide four to eight hours of training annually on ECC cyber policies and procedures.[4]

The ultimate test of your training program is its effectiveness. Do personnel know how to operate during instances of downtime or disaster? Regular drills and simulations can help assess this. These exercises can also identify areas where more training is needed.

According to Microsoft, embracing the basics of a cybersecurity program, also known as cyber hygiene, can prevent 99% of cyberattacks.[5] A well implemented program will offer significantly greater protection and allow faster recovery from an incident when one eventually occurs. However, one of the greatest obstacles to launching and maintaining a successful program is convincing employees that it's worth the trouble.

BUSTING THE MYTH OF CYBERSECURITY

A commonly held misconception is all things cyber are solely the responsibility of dedicated technology staff — whether an in-house team or a contracted service provider. But the reality is cybersecurity isn't simply *their* problem; it's also *your* problem.

When it comes to cybersecurity, everyone is responsible. From the newest telecommunicator trainee to upper management, each has a role to play in protecting the vital operations of their ECC. This means that not one person is excluded, regardless of how much or how little training they've had or how aware they are of current cyber trends. Organizations cannot rely solely on IT staff due to increased demands in other areas of the organization, and some agencies may not have any technology staff.

Additionally, traditional technical countermeasures like firewalls and anti-virus software aren't sufficient by themselves to protect an organization. Research indicates as much as 91% of all cyberattacks begin through email,[6] an approach that targets the person using the computer rather than the computer itself. Critical ECC systems must be secured, but educating the people interacting with these systems about their security responsibilities is equally important.

NOW IT'S PERSONAL

Encourage your team to take ownership of their actions online. Simple habits like regularly updating passwords, being cautious of suspicious emails and only using secure networks can go a long way in preventing cyberattacks. Remember, a chain is only as strong as its weakest link. By fostering a culture of personal responsibility, you can ensure that every link in your chain is strong. Other ways to encourage employee involvement in a cyber program include:

- **Incentives:** Rewarding employees for getting involved in cybersecurity is effective. The cost of recovering from an incident is outrageously high compared to an ice cream social or gift card.[7]
- **Gamification:** Game-like mechanics like avatars, badges or leaderboards can make cybersecurity more fun and interactive.[8]
- **Cybersecurity champions:** Selecting knowledgeable individuals to actively promote cyber awareness will ensure greater success with program adoption.

Involving new hires from the beginning is also a good way to help solidify a cybersecurity program. The onboarding process is an opportunity to educate them on the importance of protecting critical ECC equipment, as well as how to recognize and report abnormalities.

REMEMBER SMOKEY BEAR

Without a doubt, cybersecurity is paramount to ensuring that an ECC continues to fulfill the ever-present need for coordinating emergency response. As public safety professionals, urge each other to add cybersecurity near the top of the seemingly unending list of "other duties as assigned." Ask how to get involved with the organization's cyber program or review the cyber plans during a spare moment. If an ECC lacks cyber policies or a fully fledged cyber program, there's no better time to start building them than today.

Smokey Bear said it best, "Remember ... Only YOU Can Prevent Wildfires." Smokey was calling upon the American people to reduce the occurrence of forest fire tragedies, but the spirit of his message applies just the same. *You*, right now, can do your part to prevent your home agency from becoming the next cyber calamity, thereby protecting responders our communities and, ultimately, society at large. ●

Contributors to this article are members of the APCO Cybersecurity Committee: ***Mike Wurst****, Springfield-Greene County (Missouri) 911;* ***Josh Clegg****, Athens County (Ohio) 911 Emergency Communications;* ***Jordan Dlask****, Flathead (Montana) Emergency Communications Center;* ***Paresh Patel****, Carbyne (New York);* ***Steven Zitney****, WSI Technologies (Indiana);*

and ***Kimberly Burdick****, Chouteau County (Montana) Sheriff's Office.*

REFERENCES

1 "What is a cyberattack?" IBM. https://www.ibm.com/topics/cyber-attack.

2 FBI. Criminal Justice Information Services (CJIS) Security Policy. June 1, 2020. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view.

3 "What is cybersecurity?" Quora.

4 "Cyber Threat Prep" by Megan Bixler. *PSC*. APCO International. September/October 2023. https://www.apcointl.org/~documents/article/cde-65182-cyber-threat-prep.

5 Microsoft. "Microsoft Digital Defense Report 2023." https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

6 Deloitte. "91% of all cyber attacks begin with a phishing email to an unexpected victim." January 9, 2020. https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html.

7 Indusface. "Why is Cybersecurity in the Workplace Everyone's Responsibility?" May 6, 2022. https://www.indusface.com/blog/why-is-cybersecurity-in-the-workplace-everyones-responsibility.

8 Fortra | Terranova Security. "5 Reasons Why You Need Gamification In Your Cyber Security Awareness Program." June 3, 2024. https://terranovasecurity.com/blog/reasons-you-need-gamification-in-security-awareness.

CDE EXAM #67613

1. According to Microsoft, embracing what cybersecurity concept can help prevent cyberattacks?
   a. Training
   b. Response plan
   c. Cybersecurity budget
   d. Cyber hygiene

2. What should a comprehensive cybersecurity policy cover?
   a. Access control, data protection, incident response and disaster recovery
   b. Only access control and data protection
   c. Only incident response and disaster recovery
   d. None of the above

3. Who is responsible for cybersecurity in the ECC?
   a. Only the dedicated IT staff
   b. Only upper management
   c. Only new telecommunicators
   d. Everyone from the newest telecommunicator to upper management

4. Which of the following are cyber assets?
   a. CAD systems
   b. Phone systems
   c. Radio systems
   d. All of the above

5. Using mechanics such as avatars, badges or leaderboards are an example of?
   a. Gentrification
   b. Gamification
   c. Germination
   d. Genuineness

6. What is the first step toward a robust cybersecurity program for ECCs?
   a. Regular drills and simulations
   b. Having a set of well-defined policies and response plans
   c. Training the staff
   d. Convincing the employees that it's worth the trouble.

7. According to APCO, how many hours of training should ECCs provide annually to maintain personnel currency on ECC cyber policies and procedures?
   a. 2-4 hours
   b. 4-8 hours
   c. 8-12 hours
   d. 12-16 hours

8. What is the second crucial component of a cybersecurity program?
   a. Regular drills and simulations
   b. Having a set of well-defined policies and response plans
   c. Training the staff
   d. Convincing employees that it's worth the trouble

9. What is a common misbelief about Cybersecurity?
   a. Cybersecurity is everyone's problem
   b. Cybersecurity is solely the responsibility of dedicated IT staff
   c. Cybersecurity is not important
   d. Cybersecurity is easy to handle

10. Which of the following is not a key aspect of cybersecurity?
    a. Integrity
    b. Security awareness and training
    c. Endpoint security
    d. EMD

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 "Cybersecurity," then click on "enroll me" and choose **"Cybersecurity (67613)"** to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.