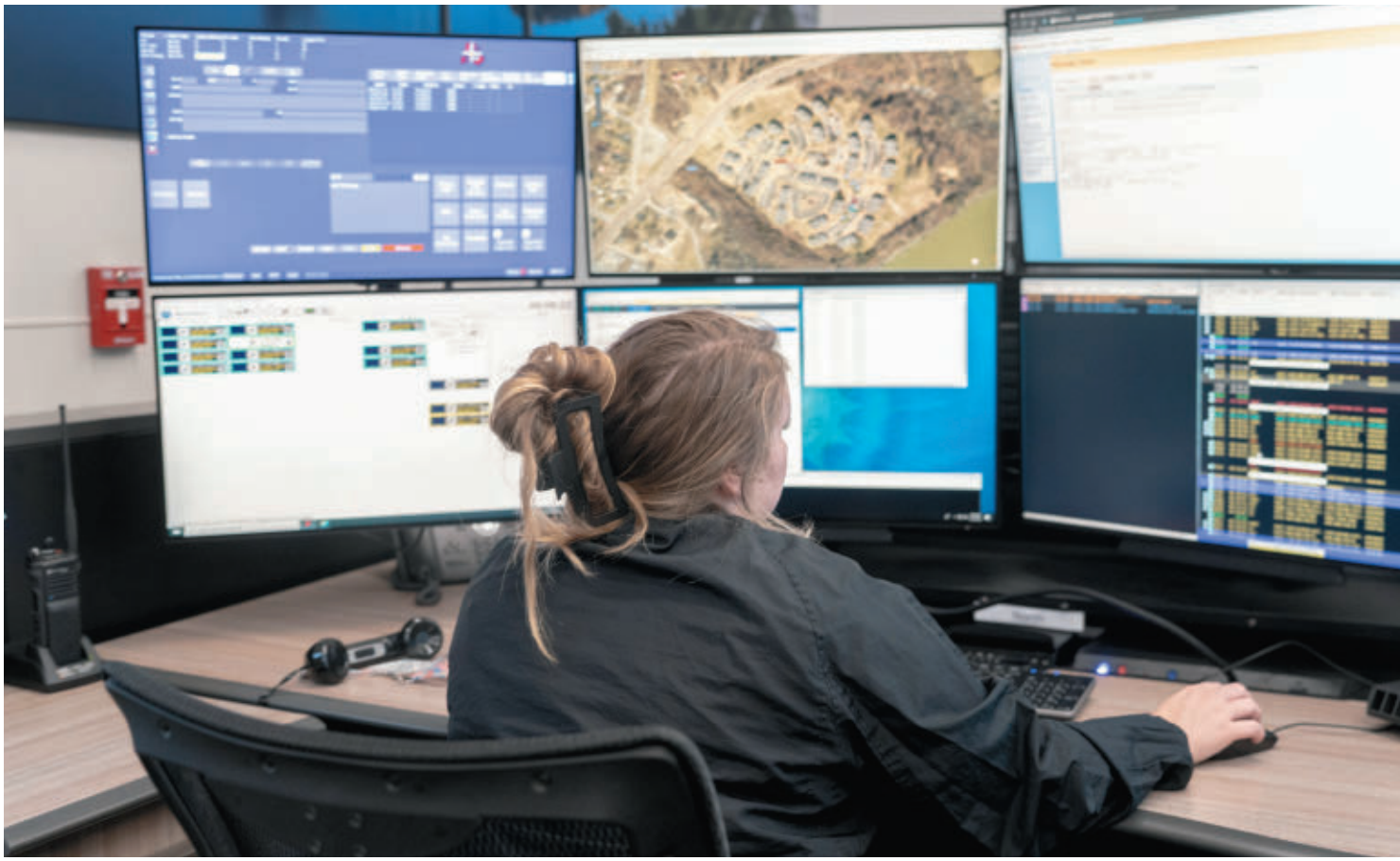
WHEN TECHNOLOGY BECOMES THE EMERGENCY

As cyber threats grow more frequent and disruptive, ECCs must treat incident response planning as an essential part of operational preparedness.

By Megan Bixler and Riley Cunningham



Cyberattacks against critical infrastructure and public safety agencies are becoming more frequent, sophisticated and disruptive. For emergency communications centers (ECCs), the stakes are especially high. A successful cyberattack can interrupt call handling, disrupt dispatch operations, impact radio communications and delay emergency response when communities need help most.

As ECCs continue adopting interconnected and interoperable technologies, cloud-based systems and Next Generation 9-1-1 (NG9-1-1) capabilities, cybersecurity preparedness has become an operational necessity rather than simply an information technology (IT) concern. A well-developed and regularly practiced cyber incident response plan is a critical part of that preparedness, providing agencies with a structured framework to quickly identify, respond to and recover from cyber incidents while maintaining continuity of operations during a crisis.

While many ECCs have developed cyber incident response plans, having a plan on paper is only part of the equation. The effectiveness of any response plan ultimately depends on whether personnel understand it, practice it and can execute it under pressure. In emergency communications, where seconds matter and stress levels are high, regularly exercising a cyber incident response plan is critical to maintaining continuity of operations during a cyber event.

BUILDING AN EFFECTIVE CYBER INCIDENT RESPONSE PLAN

According to National Institute of Standards and Technology's (NIST's) Computer Security Incident Handling Guide (SP 800-61), preparation is one of the most important phases of incident response.[1] NIST emphasizes that organizations should establish clear procedures, define roles and responsibilities, and conduct training and exercises before an incident occurs. Proper preparation allows organizations to respond more efficiently, minimize operational disruption and restore critical services following a cyberattack.

For ECCs, preparation is particularly important because cyber incidents can quickly become operational emergencies. A ransomware attack affecting a computer-aided dispatch (CAD) system, for example, could force personnel to revert to manual processes or backup systems with little warning for several months. Phishing attacks targeting employees could compromise credentials or disrupt access to critical applications. Distributed denial-of-service (DDoS) attacks can interfere with network availability and communication systems. In each of these scenarios, confusion and delayed decision-making can worsen the impact of the incident.

A cyber incident response plan provides structure during these high-pressure situations. Effective plans typically identify who is responsible for technical response efforts, internal communications, coordination with vendors and external notifications. They also establish procedures for containment, recovery and continuity of operations. However, plans that are never exercised often reveal weaknesses once a real incident occurs. Staff may be unfamiliar with their responsibilities, communication procedures may break down and operational gaps may emerge under stress. This is why practicing the plan is just as important as developing it.

WHY PRACTICING THE PLAN MATTERS

The Cybersecurity and Infrastructure Security Agency (CISA) strongly encourages organizations to conduct regular cybersecurity exercises, including tabletop exercises and operational simulations, to evaluate preparedness and improve coordination.[2] CISA notes that exercises help organizations identify vulnerabilities, test communication pathways and clarify decision-making responsibilities before a real-world event occurs.

Tabletop exercises are one of the most practical ways ECCs can evaluate their preparedness. These discussion-based exercises walk participants through a simulated cyber incident and require leadership, supervisors, IT personnel and operational staff to discuss how they would respond at each stage of the event. These exercises can reveal gaps in communication procedures, uncertainties in escalation protocols and dependencies on systems or vendors that may not have been fully considered previously.

More advanced functional exercises or simulated cyberattack drills can help agencies evaluate operational continuity in real time. These exercises may involve testing backup communications methods, manual dispatch procedures or system restoration capabilities. While these exercises require more coordination, they help build confidence and familiarity among personnel who may need to respond during an actual cyber incident.

ADAPTING TO A GROWING CYBER THREAT ENVIRONMENT

Just as important as the exercise itself are the lessons learned afterward. After-action reviews (AARs) allow agencies to identify what worked well, where confusion occurred and what procedures should be updated. Cyber threats and technologies evolve constantly, and incident response plans should evolve alongside them. A plan that was effective several years ago may no longer adequately address today's operational environments, making it essential for agencies to continually evaluate and update their cyber incident response plans to ensure they remain effective.[3]

Cybersecurity preparedness also requires organizational culture and leadership support. Cybersecurity cannot be viewed solely as the responsibility of IT personnel. Every employee plays a role in identifying suspicious activity, following security procedures and supporting operational resilience. Leadership must prioritize ongoing training, encourage reporting of potential threats and invest in preparedness efforts that strengthen the agency's ability to respond under pressure.

Cyberattacks are not slowing down; they are becoming more frequent, sophisticated and disruptive. Cyber incidents affecting critical infrastructure organizations nationwide continue to rise, with the Federal Bureau of Investigation's (FBI's) annual Internet Crime Report documenting increasing ransomware and cybercrime activity targeting government entities and critical infrastructure sectors.[4] Organizations of all sizes remain vulnerable to cyberattacks, and the resulting operational disruptions can carry significant financial and public safety consequences. As emergency communications technology continues to evolve and become more interconnected, ECCs must treat cybersecurity

preparedness as an operational priority rather than simply an IT responsibility.

Real-world incidents within public safety and emergency communications environments have demonstrated how disruptive cyberattacks can become. In 2024, a cyberattack impacted the CAD system in Bucks County, Pennsylvania, forcing public safety telecommunicators to temporarily rely on manual processes while officials worked to restore systems.[5] Similarly, the 2023 ransomware attack on Dallas disrupted several city operations, including police dispatch systems, requiring some emergency response functions to revert to backup radio communications.[6] These incidents demonstrate how quickly cyberattacks can affect day-to-day emergency operations and reinforce the need for agencies to regularly exercise and refine their cyber incident response procedures.

HELPFUL TIPS FOR DEVELOPING A CYBER INCIDENT RESPONSE PLAN

For ECCs, developing a cyber incident response plan requires a structured, collaborative approach grounded in both NIST and CISA guidance. NIST emphasizes that an effective plan should establish clear roles, responsibilities and communication pathways across technical staff, leadership, legal and external partners so teams can act quickly and cohesively during an incident. Building on that, ECCs should define a repeatable process aligned to the incident response lifecycle (i.e., preparation, detection, response and recovery) while integrating it into broader risk management activities to improve overall resilience and reduce operational impact.

CISA reinforces the importance of preparation by recommending agencies train staff, develop stakeholder contact lists, coordinate with law enforcement and regional partners and pre-establish communication strategies, especially since primary systems (e.g., call-handling systems, CAD, etc.) may be unavailable during an incident. These cyber incident response plans should prioritize continuity of operations, ensuring backup systems, redundancy and clear escalation paths are in place to protect mission-critical services. In addition to CISA's training recommendation, APCO suggests that ECCs conduct four to eight hours of cybersecurity training annually.[7] This training should include how all ECC staff should respond to cyber incidents.

It is critical to maintain both printed and electronic copies of a cyber incident response plan, because cyber incidents often disrupt the very systems needed to access digital resources. CISA specifically advises organizations to print their plans and contact lists, noting that email, chat and document storage platforms may be unavailable or compromised during an incident, making offline access essential for coordination and decision-making.[8]

> **ECCs routinely train for natural disasters, mass casualty incidents and large-scale emergencies because personnel understand that preparation improves performance under pressure. Cyber incidents should be treated with the same level of urgency.**

Having a physical copy ensures telecommunicators can quickly mitigate impacts of a cyberattack even in a worst-case scenario where networks, CAD systems or authentication tools are down. Although a printed copy of a cyber incident response plan is important, maintaining electronic copies remain important for accessibility, version control and ease of updates, supporting NIST's emphasis on maintaining clear, current procedures that improve the efficiency and effectiveness of response and recovery activities. Together, maintaining both formats enhances resilience by ensuring continuity of operations and reliable access to critical information, regardless of whether systems are operational, degraded or completely offline during a cyber event.

When developing a cyber incident response plan, ECCs should establish reporting needs and requirements. Upon the realization of a cyber incident, ECCs should report the incident to local law enforcement agencies. In addition, these federal resources can be contacted to assist in recovery efforts:

- The FBI. The Internet Crime Complaint Center (IC3) is a reporting mechanism to assist ECCs in reporting a cyber incident to the FBI. ECCs should add keywords (e.g., Public Safety, Emergency Communications, ECC, etc.) in the subject line.
- CISA, a component of the Department of Homeland Security (DHS). Contact 1-844-SAY-CISA (1-844-729-2472) or central@cisa.dhs.gov.

CYBER PREPAREDNESS MUST BE ONGOING

As emergency communications technology continues to evolve, ECCs must ensure cybersecurity preparedness evolves with it. Cyber incident response plans should not remain static documents stored away until an emergency occurs. They should be living operational tools that are reviewed, practiced and refined regularly.

In public safety communications, preparation has always been essential. ECCs routinely train for natural disasters, mass casualty incidents and large-scale emergencies because personnel understand that preparation improves performance under pressure. Cyber incidents should be treated with the same level of urgency. Consistently practicing a cyber incident response plan before an attack occurs can reduce confusion, strengthen coordination and help agencies maintain critical services when communities rely on them most.

INVOLVING ALL STAKEHOLDERS

Developing an effective cyber incident response plan requires actively involving all stakeholders, including IT professionals and ECC operational staff. Involvement of a diverse group of stakeholders ensures that the plan reflects real operational needs and technological considerations and can be executed under pressure. IT staff bring critical expertise in identifying, analyzing and mitigating technical threats. ECC operational personnel provide essential insight into maintaining continuity of mission-critical services, where even brief disruptions can have life-safety consequences.

By involving both IT and ECC staff in planning and exercises, organizations can identify operational gaps, align technical response actions with real-world workflows and strengthen coordination across disciplines. Ultimately, this inclusive approach ensures that the incident response plan is not just technically sound, but also practical, actionable and capable of preserving critical public safety operations during a cyber event. ●

***Megan Bixler, RPL, CPE**, is APCO Director of Technology; Riley Cunningham is Executive Office Administrator, both for APCO International.*

REFERENCES:

[1] National Institute of Standards and Technology. SP 800-61 Rev. 3. "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile." April 2025. https://csrc.nist.gov/pubs/sp/800/61/r3/final

[2] Cybersecurity and Infrastructure Security Agency. CISA Tabletop Exercise Packages (CTEP). U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2023-02/ctep_fact_sheet_v._11_16_2021_final.pdf

[3] Cybersecurity and Infrastructure Security Agency. Cross-Sector Cybersecurity Performance Goals. U.S. Department of Homeland Security. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[4] Federal Bureau of Investigation (2025). Internet Crime Report 2024. Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[5] Fox-Sowell, Sophia. (Jan. 24, 2024). "Cyberattack Downs Emergency Dispatch System in Bucks County, Pennsylvania." https://statescoop.com/cyberattack-bucks-county-pennsylvania-dispatch-emergency/

[6] Sabin, Sam.(May 9, 2023). "Inside Royal's Ransomware Spree Against U.S. Cities." https://www.axios.com/2023/05/09/royal-ransomware-us-cities-cybersecurity-hacking

[7] APCO International. (2019). APCO ANS 3.110.1-2019: Cybersecurity training for public safety communications personnel. https://www.apcointl.org/~documents/standard/31101-2019-cybersecurity/?layout=file

[8] Cybersecurity and Infrastructure Security Agency. (n.d.). Incident response plan (IRP) basics. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

CDE EXAM #77098

1. Having a physical copy of your ECC's cyber incident response plan is not needed and is not helpful during a cyberattack
   a. True
   b. False

2. According to National Institute of Standards and Technology's Computer Security Incident Handling Guide (NIST SP 800-61), _____ is one of the most important phases of incident response.
   a. Preparation
   b. Cyber incident response plan
   c. Training
   d. MFA

3. What does IC3 stand for?
   a. Intelligence Community Common Clearance
   b. Internet Crime Community Center
   c. Internet Crime Complaint Center
   d. Information Technology Community Complaints

4. Both IT professionals and ECC operational staff should be involved in developing the Cyber Incident Response Plan.
   a. True
   b. False

5. APCO states that ECCs should conduct cybersecurity specific training between four and _____ hours annually.
   a. 24
   b. 10
   c. 9
   d. 8

6. ECCs should contact local law enforcement to report a cyber incident.
   a. True
   b. False

7. Consistently _____ a cyber incident response plan before an attack occurs can reduce confusion, strengthen coordination and help agencies maintain critical services when communities rely on them most.
   a. Practicing
   b. Educating
   c. Connecting
   d. Iterating

8. According to the FBI, ransomware and cybercrime activity is targeting government entities and critical infrastructure sectors less often.
   a. True
   b. False

9. What does CISA note that conducting cyber incident response plan exercises will help with?
   a. Additional stakeholders
   b. Identifying vulnerabilities, testing communication pathways and clarifying decision-making responsibilities before a real-world event occurs
   c. Adherence to NIST SP 800-61
   d. Meeting APCO cybersecurity standards

10. An inclusive approach to developing a cyber incident response plan assists with ensuring that the plan is technically sound, but also practical, actionable, and capable of preserving critical public safety operations during a cyber event.
    a. True
    b. False

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 https://www.training-apcointl.org/ to create your username and password. Enter CDE in the search box, and click on the "**Technology Emergency**," then click on "enroll me" and choose "**Technology Emergency (77098)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.