CDE #58175

LEAN INTO LEARNING: CYBERSECURITY

Resources abound to aid the quest for cybersecure ECCs.

By Stephen Martini, ENP, RPL and Michael Bateman

Cyber hacking: It's at the forefront of everyone's mind in almost every profession.

In May 2021, hackers shut down the flow of gasoline and jet fuel throughout the Southeast and disrupted beef plants and slaughtering operations across the United States, Australia and Canada.

Hackers are disrupting the delivery of goods and services by targeting supply chains, which is why public safety communications centers (ECCs) need to be more vigilant than ever to mitigate these threats.

ISTOCK.COM/EVGENIYSHKOLENKO

From the first call in 1968 to the first text message sent to 9-1-1 in 2009, technology has been the backbone of public safety communications. Through the past two decades, enhanced 9-1-1 arrived, making way for Next Generation 9-1-1 solutions, dramatically increasing dependence on technology inside the ECC. With those demands came new challenges and threats. ECCs are not immune, and it seems the target on their back is only getting larger.

According to APCO International Chief Technology Officer Jay English, the primary goals of cyberattackers are to destroy, corrupt, remove or disclose data or interrupt services.[1]

Shrinking the size of your target requires implementing some cybersecurity measures.

But where should you start? Education. A variety of resources are available to increase your understanding and help you develop a cybersecurity checklist.

First, the National Institute of Standards and Technology (NIST) Cybersecurity Framework developed in 2014 and revised in 2018, focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of an ECC's risk management process.[2] It applies to all phases of a cybersecurity plan, including planning, design, build and acquisition, deployment, operation, and decommission.

Not all checklists cover the same topics, but a good cybersecurity checklist will help determine if you need an audit. If you think you don't need an audit, chances are you do.

Another great resource is the Task Force for Optimum PSAP Architecture (TFOPA) checklist, available as Appendix 2 in the 2015 report,[3] which serves as a roadmap to securing your networks.

Both resources should take you through critical steps to address personnel security, physical security of your network, account and password management, confidentiality of sensitive data, disaster recovery, training and education, policy and compliance. Cybersecurity checklists help eliminate gaps, identify inefficiencies, provide metrics and serve as a knowledgebase for ECC technical support.

Not all checklists cover the same topics, but a good cybersecurity checklist will help determine if you need an audit. If you think you don't need an audit, chances are you do.

In his article "Lessons from Cyber Attacks on Local Governments – Are You Protected," Keith Melancon stated, "Ransomware attacks on federal and state entities, healthcare providers and educational institutions cost an estimated $7.5 billion in 2019."[4] The average cost of a cyberattack during 2018-2019 was an estimated $1.1 million.[5] PurpleSec, a veteran-led offensive and defensive cybersecurity company, estimates cybercrime is up 600% due to the COVID-19 pandemic. They also predict a new organization will fall victim to a ransomware attack every 11 seconds.[6] SecuLore, a company specializing in ECC cybersecurity solutions, estimated that in the last 24 months there have been 125 attacks on public safety agencies.[7]

All of this points to the importance of an audit to understand your cybersecurity vulnerabilities. An audit will assure that you are taking all appropriate actions to avoid disruption to center operations due to network failures as a result of a cyberattack. These assessments should be thorough,

ISTOCK.COM/ALEXSL

testing all networks connected inside the ECC, including call processing equipment, computer aided dispatch, records management systems, radio dispatch consoles, virtual or physical desktops, and any interfaces.

When considering an audit of your system, establishing relationships with partners is critical. Local agency, government and industry partners need to work together to assess network connections and identify weak areas that hackers could manipulate to facilitate an attack. Ego and overconfidence are deterrents to taking an objective look at your system – and those connecting to it – to truly identify and rectify areas for improvement.

Coordinating with a cybersecurity consultant to conduct an audit is part of a concerted effort to respond to, remediate against, restore and resolve concerns. But the audit results are simply a snapshot in time, good to resolve and restore threats found at that moment. We know networks remain active, constantly communicating and coordinating with other networks to send and receive data and potentially new threats. Identifying a trusted solution to continue monitoring your networks for potential threats and to initiate quick response and remediation is key to long-term success.

A more recent consideration for the ECC is cybersecurity insurance.

Advisorsmith Solutions, a company specializing in different types of business insurance, found that cyber liability policies in 2019 averaged around $1,500 per year for $1 million in coverage with a $10,000 deductible.[8]

Cybersecurity insurance should not be considered your only safety net, however, as it may or may not cover all costs associated with a cyberattack. Coverage depends on the policy's terms. Even if you pay a ransom in response to a ransomware attack, the key that the hackers provide to unlock your data may or may not work, and you will still have to rebuild affected systems. Your mindset should be that the hackers remain in your system and aren't leaving just because you paid the ransom.

Resources abound to begin your quest for cybersecurity. The APCO Institute's comprehensive course, "Cybersecurity Fundamentals for the ECC," contributes to the growing knowledge among public safety communications professionals. Your state APCO chapter may have additional resources dedicated to cybersecurity or even a cybersecurity checklist focused on your area or a network design similar to that of your ECC. Subscribe to newsletters and keep up with the cybersecurity world. MS-ISAC and EMR-ISAC are resources with monthly bulletins. Attend a regional or national conference to identify industry partners specializing in cybersecurity and physical security of ECC environments. Often, these partners provide whitepapers, webinars, statistics, alerts and other resources for you to increase your knowledge about securing your ECC.

Cyberattacks are not fading away. If anything, they seem to be increasing. Take the time to locate a checklist, conduct an audit and partner with an industry partner

working to help ECCs build a strong cybersecurity plan. ●

Michael Bateman *is an IT professional with the Metro Nashville Department of Emergency Communications. He has 27 years of experience in information technology.*

Stephen Martini, ENP, RPL, *is Director at Metro Nashville Emergency Communications Center.*

REFERENCES

1. "Securing Public Safety Networks: The APCO Perspective." APCO International. https://techforum.apcointl.org/wp-content/uploads/2J_English_Cybersecurity.pdf
2. "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology. 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
3. "Task Force on Optimal PSAP Architecture." Federal Communications Commission. 2015. https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf
4. "Lessons from Cyber Attacks on Local Governments." Delta Risk. 2020. https://deltarisk.com/blog/lessons-from-cyber-attacks-on-local-governments-are-you-protected/
5. "The Price of Security: How Much Does a Cybersecurity Attack Actually Cost?" DynaSis. https://dynasis.com/2019/03/price-security-how-much-cybersecurity-attack-actually-cost/
6. "2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends." PurpleSec. https://purplesec.us/resources/cyber-security-statistics/
7. www.seculore.com
8. "How Much Does Cyber Insurance Cost?" https://www.embroker.com/blog/cyber-insurance-cost/

CDE EXAM #58175

QUIZ

1) Cyberattacks in 2021 appear to be focused on disrupting distribution of goods and services.
   a. True
   b. False

2) The introduction of enhanced and Next Generation 9-1-1 increased cybersecurity threats to the ECC.
   a. True
   b. False

3) Which of the following is not addressed by The National Institute of Standards and Technology (NIST) Cybersecurity Framework checklist?
   a. Planning
   b. Design
   c. Renovation
   d. Decommission

4) What are the primary goals of a cyberattacker?
   a. Destroy, connect, resolve, dissect or inject
   b. Destroy, corrupt, remove, disclose or interrupt
   c. Destruct, coordinate, renovate, disclose or interrupt
   d. Destroy, corrupt, restrict, dismember or illicit

5) Cybersecurity checklists help eliminate gaps, identify inefficiencies, provide metrics and serve as a knowledgebase for your ECC's technical support.
   a. True
   b. False

6) All ECCs should never conduct an audit of their cybersecurity vulnerabilities.
   a. True
   b. False

7) When identifying cybersecurity threats in the ECC, which resource does not need to be considered?
   a. APCO Institute courses
   b. State APCO Chapters
   c. Industry partners
   d. Social media posts

8) An audit is part of a concerted effort to:
   a. Respond, remediate, restore and resolve
   b. Redact, respond, refer and resolve
   c. Respond, remediate, refer and redact
   d. Resort, reduce, refinish and resolve

9) Which of the following is not a resource for ECCs to use when building a cybersecurity plan?
   a. Monthly bulletins
   b. Regional or national conferences
   c. Industry partners
   d. Gut feelings and good intentions

10) Industry partners often provide whitepapers, webinars and other alerts regarding cybersecurity threats and mitigation efforts.
   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 http://apco.remote-learner.net/login/index.php to create your username and password. Enter CDE in the search box, and click on the "2021 Public Safety Communications Magazine Article Exams," then click on "enroll me" and choose "Cybersecurity for the ECC **(58175)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.