National Emergency Medical Services Advisory Council
DRAFT
Advisory and Recommendations

Title: **Cybersecurity – What to do when technology fails/ How to mediate in a pro-active way.**

As prepared by the Subcommittee on **Integration & Technology**

A. Executive Summary

Public safety is the first line of defense in protecting our nation. We are prepared to face any challenge thrown our way. Disasters are our specialty, and we have tools to manage them all. But what happens when our tools don't work. For years we have relied on paper records and some agencies still do. As agencies move into the digital age, we face a new potential disaster involving some of our most important tools. Those tools are our computers that we utilize for everything from taking 9-1-1 calls, dispatching calls, tracking units in the field, talking to units in an emergency, and documenting everything we did. According to the EMS Trend report, "Respondents to the annual EMS Trend Report acknowledge their organizations are poorly prepared for a cyberattack. More than half (56%) of 2021 respondents say their organization is "slightly prepared" or "not prepared at all."

EMS is in a unique position related to a cyber incident because they are in between dispatch and the hospital. If either of those entities are impacted by a cyber incident EMS will be impacted. On the dispatch side there would be the inability to receive 9-1-1 calls and respond in a timely fashion. If a hospital is impacted EMS will now be diverting patients to further destinations and if the incident is protracted and a hospital has to evacuate EMS will be involved in that as well.

Greg Friese, MS, NRP (Lexipol Editorial Director) stated, "All public safety leaders and personnel share the responsibility of understanding the risks of cyberattacks, educating themselves and taking action to protect their organizations, as well as their private information. "As these emerging threats arise, we need more than ever to make sure that our public safety agencies are prepared to deal with a technology failure in the midst of a crisis.

911.gov addresses the cybersecurity concerns for the PSAP (Public Safety Answering Point) by identifying vulnerable points associated with the technology such as Next Generation 9-1-1 (NG9-1-1) and Enhanced 9-1-1 systems. While the benefit of the communications technology is expansive, 911.gov addressed the concern with this statement, "With the increased use of IP-based platforms, comes the expanded risk of cybersecurity attacks and other cyber threats. PSAPs must be prepared to actively manage possible cybersecurity threats, such as hackers using auto-dialers to overwhelm PSAP phone lines or accessing or corrupting data."

B. Recommendations

The recommendation from this committee is for the Federal Interagency Committee for EMS (FICEMS) and Cybersecurity and Infrastructure Security Agency (CISA) to work together to create a specific document for EMS cybersecurity related issues, using these recommendations as guidance.

C. Scope and Definition

Every public safety agency that uses technology is susceptible to a cyber incident. In this document we will define the problem by discipline and certain areas of vulnerabilities specific to that discipline. In the last 24 months 93 public safety attacks (04/07/2022), according to (https://www.seculore.com/resources/cyber-attack-archive)

1. Types of cyber incidents
    a. Insider Threat – Internal employees purposefully disrupting technologies
    b. Loss of internet
    c. Malware - Software that compromises the operation of a system by performing an unauthorized function or process.
    d. Ransomware - form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
    e. Phishing - A digital form of social engineering to deceive individuals into providing sensitive information.
    f. Computer updates – Failure to test before implementation
    g. Infrastructure failure – Building collapse / fire / animals / cell networks
    h. Weather – Loss of power / flood
    i. Remote work platforms – Unauthorized intrusions during remote meetings

D. Analysis

1. EMS Telecommunicators
    a. E-mail –
        i. One of the most susceptible areas for cyberattacks. A simple click of a link can infect a variety of systems. When E-mail shares the same system as critical infrastructure, a click can take down a Computer Aided Dispatch (CAD) Records Management System (RMS)
    b. Network
        i. CAD – Cyberattacks specifically to CAD software will limit the Telecommunicator's ability to process and dispatch appropriate responses with timely update of information from a call taker and proper recording of associated times. A cyberattack can also compromise saved historical and hazard information in the database and any integrated or interfaced applications or programs within the system.
        ii. 9-1-1 calls – Inability to received incoming calls or make outgoing calls
    c. Radio – Inability to communicate with crews in the field
    d. Vehicle tracking – Inability to locate a unit in distress or dispatch closest unit
    e. Employees, vendors, contractors, or subcontractors – One or multiple persons who

could intentionally or unintentionally improperly safeguard data, make a data resource unavailable when performing maintenance or upgrade operations, not follow physical or cyber protection procedures, or enter a typing mistake that could result in loss of data integrity.

2. EMS
    a. E-mail - One of the most susceptible areas for cyberattacks. A simple click of a link can bring down a system.
    b. Patient records – HIPAA risks, if the patient care record system is compromised. This can not only result in unanticipated release of private information, it can result in financial impact to the agency.
    c. Mobile data terminals – Inability to get data enroute
    d. Scheduling – Inability to appropriately staff vehicles (recent attack on Telestaff (Chicago Fire)
    e. Payroll – Inability to pay staff (recent Kronos attack)
    f. Preplans – Access to layouts of buildings or clinical protocols.
    g. Hospitals - A recent study (Dameff et al) showed that, "There was a statistically significant higher EMS census during the cyberattack when compared to the four (4) weeks prior, with most days experiencing double the normal volume."
    h. Any data-linked vendor connected to the agency.
    i. Bodycam - Accidental compromise of video that could be during clinical care can be a large problem.
3. Hospitals Based EMS
    a. Security in place for the hospital system does not have the requirement for extension to EMS, either incoming or outgoing
    b. Reliance is on the provider of transport for security and back-up plan if cyber failure occurs.
    c. Standards - JACHO (US) has not yet issued any standards for the hospital to EMS space. International JACHO standards are lacking in cybersecurity requirements.
    d. Down time - Hospitals may or may not have the ability to accept patients if down time occurs.
    e. Disaster Planning - Multi-agency cyberattack drills may not be a consideration for the hospital disaster planning program.
    f. Back-up Systems - Although hospitals may have backup systems for both previous and current patient, they are dependent on transport providers to have a secure plan in place
    g. Patient records – Hospitals may or may not have the ability to retrieve old records or to recreated those delivered by EMS practitioners.
    h. HIPAA – Risks include lack of consistency for the securing of incoming patient documentation delivered by EMS practitioners, compiled with inconsistent and unsecured delivery methods (i.e. written, electronic, etc.)

E. Recommendations

a. FICEMS and CISA work to create a specific document for EMS cybersecurity related issues using these recommendations as guidance.
b. Best practices (taken from https://www.cisa.gov/emergency-services-sector-cybersecurity-initiative
    1. **Identify**: Develop an organizational understanding to manage the cybersecurity risks to systems, people, assets, data, and capabilities.
    2. **Protect**: Develop and implement appropriate safeguards to ensure delivery of critical services;
        a. Use of strong passwords (maximum characters allowed for the password and should include the following:
            i. Upper case
            ii. Lower case
            iii. Numbers
            iv. Special characters (avoid using an "!" at the end)
        b. Balancing security and functionality
            i. Cloud account versus contracted account- ensure that the proper security measures are in place regardless of the method of data storage.
            ii. Recognize VPN is prone to data leaks.
        c. Address the risks of rushed technology adoption prior to adopting
        d. Provide practitioner education, most security relies on the individual vs technical
        e. Implement Two-Factor Authentication
        f. Physical security
            i. Never leave laptop unattended
            ii. Use of locking mounts
            iii. Place unsecured laptops in trunk if necessary to leave in vehicle
            iv. Lock computers
            v. Encryption – bitlocker on Windows 10
        g. Cybersecurity insurance
            Consider obtaining cybersecurity insurance added to the current organization policy.
    3. **Detect**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity incident.
        a. Conducting multi-agencies tabletop exercises that include a cybersecurity event.
        b. Identify known and potential unknown threats, internal and external
        c. Conduct risk analysis of technology itself
        d. Use a cost-benefit analysis and other factors
    4. **Respond**: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
        a. Mitigation measures
        b. Determine how to stop an active cyber attack

5. **Recover**: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
    a. **Report attacks and ransom payments to Federal Government** https://www.cisa.gov/reporting-cyber-incidents

F. Strategic Goals

1. How to Prepare for a 9-1-1 Outage (https://private.infragard.org/Application/Member/NewsItems?c=1)
    a. Before there is an emergency, contact your local emergency services authorities for information on how to request service in the event of a 9-1-1 outage. Find out if text-to-9-1-1 is available in your area.
    b. Have non-emergency contact numbers for fire, rescue, and law enforcement readily available in the event of a 9-1-1 outage.
    c. Sign up for automated notifications from your locality if available to be informed of emergency situations in your area via text, phone call, or email.
    d. Identify websites and follow social media for emergency responders in your area for awareness of emergency situations.
    e. Set up social media accounts that could be used to make public notifications about an outage.
    f. Sign up for automated notifications from your locality if available to be informed of emergency situations in your area via text, phone call, or email.
    g. Annually review and update cybersecurity plans coupled with annual training for all staff

2. How the PSAP can assist in preparing EMS practitioners for a PSAP Outage

A PSAP outage can include an outage in 9-1-1, network outage for any reason, or other outages that effect the receipt and delivery of emergency calls for service.

a. Schedule nightly backup of essential data
b. Plan contingencies for outages to address 9-1-1 call receipt, dispatching, and staffing
c. Provide scenario-based training and education for PSAP staff semi-annually, or annually, including EMS practitioners.
d. Enforce appropriate security measures
e. Communicate closely with providers regarding planned or unplanned outages
f. Identify websites and follow social media for emergency responders in your area for awareness of emergency situations.
g. Publicize non-emergency contact numbers for EMS practitioners to have readily available in the event of a 9-1-1 outage.
h. Educate the public on what to do during an outage.

220

G. References

911.gov. (2018, April 12). *Cyber Risks to Next Generation 911*. Retrieved February 26, 2022, from https://911.gov/pdf/OEC_NG911_Cybersecurity_Primer

Careless, J. (2020, January 1). *Protecting EMS From Cyberthreats*. EMS World. Retrieved January 25, 2022, from https://www.hmpgloballearningnetwork.com/site/emsworld/article/1223681/protecting-ems-cyberthreats

CISA. (n.d.). *Emergency Services Sector Cybersecurity Initiative*. Cisa.Gov. Retrieved March 3, 2022, from https://www.cisa.gov/emergency-services-sector-cybersecurity-initiative

CISA. (2019, November 1). *Cyber Risks to Next Generation 9–1-1*. Cisa.Gov. Retrieved March 3, 2022, from https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf

CISA. (2020, September 1). *Ransomware Guide*. CISA.GOV. Retrieved September 15, 2021, from https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

CPA Academy. (n.d.). *Cybersecurity*. CPAAcademy.Org. Retrieved January 16, 2022, from https://www.cpaacademy.org/cybersecurity

Dameff, C., Farah, J., Dotson, M., Killeen, J., & Chan, T. (2021, September 15). *Cybersecurity*. Annals of Emergency Medicine. Retrieved March 21, 2022, from https://www.annemergmed.com/article/S0196-0644(21)00856-8/fulltext

Friese, G. (2021, June 14). *Cyberattackers are coming for Public Safety; prepare now*. EMS1. Retrieved January 13, 2022, from https://www.ems1.com/cybersecurity/articles/cyberattackers-are-coming-for-public-safety-prepare-now-75YuF5gNYhEYqBME/

JACHO. (n.d.-a). *Joint Commission International Accreditation Standards for Medical Transport Organizations*. Joint Commission International. Retrieved March 20, 2022, from https://www.jointcommissioninternational.org/accreditation/accreditation-programs/medical-transport-organization/

JACHO. (n.d.-b). *Joint Commission International Survey Process Guide for Medical Transport Organizations*. Joint Commission International. Retrieved March 20, 2022, from https://www.jointcommission.org/standards/

Joint Commission International. (n.d.). *Joint Commission International Accreditation Standards for Medical Transport Organizations*. JACHO. Retrieved March 20, 2022, from https://www.jointcommissioninternational.org/accreditation/accreditation-programs/medical-transport-organization/

National Initiative for Cybersecurity Careers and Studies. (n.d.). *Workforce Framework for Cybersecurity*. Niccs.Cisa.Gov. Retrieved March 6, 2022, from https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

Quinn, S., Ivy, N., Barrett, M., Witte, G., & Gardner, R. (2022, February 1). *Prioritizing Cybersecurity Risk for Enterprise Risk Management*. Csrc.Nist.Gov. Retrieved March 5, 2022, from https://csrc.nist.gov/publications/detail/nistir/8286b/final

Texas A&M Engineering. (n.d.). *Cybersecurity for Everyone*. TEEX. Retrieved March 8, 2022, from https://teex.org/class/AWR397/

TLP: WHITE. (2021, November 1). *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*. Cisa.Gov. Retrieved February 3, 2022, from https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

United States Secret Service. (n.d.). *Preparing for a Cyber Incident*. Retrieved March 19, 2022, from https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident