APCO 3.110.1-2019

Cybersecurity Training for Public Safety Communications Personnel

TABLE OF CONTENTS

Copyright ©2019 APCO International | All Rights Reserved

Forward

APCO International is the world's largest organization of public safety communications professionals. It serves the needs of public safety communications practitioners worldwide, and the welfare of the public, by providing complete expertise, professional development, technical assistance, advocacy, and outreach.

The 2019-2020 APCO International Executive Board:

Tracey Hilburn, President

Margie Moulin, First Vice President

Jason Kern, Second Vice President

Holly Wayt, Immediate Past President

Derek Poarch, Ex-Officio

APCO International standards are developed by APCO committees, projects, task forces, writing groups, and collaborative efforts with other organizations coordinated through the APCO International Standards Development Committee (SDC). Members of the committees are not necessarily members of APCO. Members of the SDC are not required to be APCO members. All members of APCO's committees, projects, and task forces are subject matter experts who volunteer and are not compensated by APCO. APCO standards activities are supported by the Communications Center & 9-1-1 Services Department of APCO International.

For more information regarding APCO International and APCO standards please visit: www.apcointl.org

https://www.apcointl.org/standards.html

APCO American National Standards (ANS) are voluntary consensus standards. Use of any APCO standard is voluntary. All standards are subject to change. APCO ANS are required to be reviewed no later than every five years. The designation of an APCO standard should be reviewed to ensure you have the latest edition of an APCO standard, for example:

APCO ANS 3.101.1-2007 = 1- Operations, 2- Technical, 3-Training

APCO ANS 3.101.1-2007 = Unique number identifying the standard

APCO ANS 3.101.1-2007 = The edition of the standard, which will increase after each revision

APCO ANS 3.101.1-2007 = The year the standard was approved and published, which may change after each revision.

The latest edition of an APCO standard cancels and replaces older versions of the APCO standard. Comments regarding APCO standards are accepted any time and can be submitted to standards@apcointl.org, if the comment includes a recommended change, it is requested to accompany the change with supporting material. If you have a question regarding any portion of the standard, including interpretation, APCO will respond to your request following its policies and procedures. ANSI does not interpret APCO standards; they will forward the request to APCO.

APCO International adheres to ANSI's Patent Policy. Neither APCO nor ANSI is responsible for identifying patents for which a license may be required by an American National Standard or for conducting inquiries into the legal validity or scope of any patents brought to their attention.

No position is taken with respect to the existence or validity of any patent rights within this standard. APCO is the sole entity that may authorize the use of trademarks, certification marks, or other designations to indicate compliance with this standard.

Permission must be obtained to reproduce any portion of this standard and can be obtained by contacting APCO International's Communications Center & 9-1-1 Services Department. Requests for information, interpretations, and/or comments on any APCO standards should be submitted in writing addressed to:

APCO Standards Program Manager, Communications Center & 9-1-1 Services

APCO International

351 N. Williamson Blvd

Daytona Beach, FL 32114 USA

standards@apcointl.org

ISBN: 978-1-943877-33-1

Copyright ©2019

Executive Summary

On behalf of public safety communications professionals across the nation, the APCO Cybersecurity Awareness Training Working Group (Working Group) has created a standard to identify content for inclusion in an Emergency Communication Center (ECC) training program designed to mitigate the risk of Cybersecurity incidents. The Working Group consisted of industry experts in Cybersecurity and emergency communications and representatives from ECCs, bringing together a diverse set of perspectives on the topics and issues that a standard for Cybersecurity training should address.

The potential for Cyberattacks on ECCs is increasing as the ECCs become more reliant on IP-based technologies. ECCs have already experienced debilitating Denial of Service attacks and will become more vulnerable to Cyberattacks as they transition to FirstNet and Next Generation 9-1-1 networks. Public safety agencies and local governments experienced over 180 cyberattacks between March 2016 and March 2018.[1] Some examples include: Malicious Link in a Twitter message in October 2016 that caused iPhones using IOS 10 to continuously redial 9-1-1, flooding ECCs across many states; a Ransomware attack that crippled Atlanta, GA in March 2018; and a Ransomware attack on Baltimore's 911 system in which hackers shut down the Computer Aided Dispatch (CAD) system and demanded more than $51,000 in bitcoin to turn it back on.

The National Institute of Standards and Technology (NIST) identifies awareness training as a key component in building an effective information technology security program and notes that "a strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures and techniques."[2]

Cybersecurity awareness training educates individuals on how to recognize abnormal activity and actions they should take upon suspecting a Cybersecurity incident. It also increases awareness of "Cybersecurity Hygiene," a set of practices to reduce the risk of inadvertently opening the doors to a Cybersecurity attack. APCO Project 43 examined the implications of recent developments in broadband technology for the public safety. The ensuing report acknowledges the importance of Cybersecurity awareness and hygiene as an essential component of successful adoption of broadband technologies.[3]

Cybersecurity training should be viewed as an ongoing program rather than a one-time activity. The Federal Communications Commission Task Force on Optimal PSAP Architecture Report identifies best practices for a security awareness training program as containing refresher training augmented by reminders and tips.[4]

This Cybersecurity Training Standard addresses training for ECC staff, including Public Safety Telecommunicators (PSTs), Supervisors, ECC management and ECC administration. It also addresses training for personnel who are not in professional technical positions, but who are Privileged Users with administrative privileges allowing them to handle some technical tasks such as application installation,

---

[1] Zeiler, D. (2018). Three Critical Steps to Next-Gen 911 Security (Contributed). *Government Technology.*
[2] Wilson, M. and Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. National Institute of Standards and Technology, Special Publication 800-50 (p. ES-1).
[3] APCO (2017). Broadband Implications for the PSAP – A Project 43 Initiative.
[4] Federal Communications Commission Task Force on Optimal PSAP Architecture TFOPA (2015). Section 4.3.1.4

operating system updates, application administration, database management or system administration.

The Working Group recognizes that myriad ECC configurations exist and roles may overlap or not exist in some ECCs. This standard should be used as a guide for the range of topics that should be covered in a Cybersecurity training program; individual agencies can adapt the standard to fit the division of responsibilities within their ECCs.

Before an ECC can develop a training program, it needs to establish policies and business practices aligned with sound cybersecurity practices and embrace a culture of cybersecurity awareness that permeates day-to-day ECC operations. The first chapter of this standard addresses these policies and business practices to help agencies set the groundwork for a Cybersecurity training program.

PSTs are heavy users of an ECC's systems and may be the first to notice something awry. The topics in Chapter 2 are designed to assist the ECC with developing a program to train PSTs on identifying the signs of a Cybersecurity Attack and knowing what to do if they suspect such an attack. Including the topics in a Cybersecurity Training Program will increase the likelihood that PSTs will be aware of agency policies addressing the use and securing of technology so that they do not unwittingly create vulnerabilities potentially leading to a Cybersecurity Attack. Including the topics will also increase their awareness of best practices for mitigating Cyberattacks through good Cybersecurity hygiene. The topics in this Chapter 2 also apply to administrative staff who access and use software and hardware to fulfill financial, human resource and other administrative functions.

Like PSTs, Supervisors are heavy users of the ECC's systems and may be among the first to notice something amiss. As such, they need to have the same training as PSTs. In their role of overseeing PSTs, they have additional responsibilities to ensure the enforcement and adherence to cybersecurity policies and safe cybersecurity practices. The topics Chapter 3 address these additional responsibilities.

Agency leadership sets the tone for the entire ECC. Support and acceptance of a Cybersecurity Training Program starts at the upper management level. Individuals holding positions in ECC management need to understand the importance of Cybersecurity awareness training and instill a culture of Cybersecurity awareness that permeates day-to-day ECC operations. To instill this culture and be a role model for supporting and accepting good Cybersecurity practices for the rest of the agency, Managers/Directors should have the same awareness of Cybersecurity risks and practice the same level of Cybersecurity hygiene as PSTs and Supervisors. As such, Chapter 4 for Managers/Directors includes topics identified for PSTs and Supervisors as well as topics that reflect the additional responsibility of instilling a culture of Cybersecurity awareness.

This standard also addresses training for Privileged Users whose access to accounts and systems creates additional responsibilities as well as an increased risk of exposing the ECC to a Cyberattack. The topics in Chapter 5 provide Privileged Users with the tools to accomplish the additional responsibility as well as with the awareness and knowledge to mitigate the potential risks. The topics in Chapter 5 may not apply to all Privileged Users and ECCs should tailor their Cybersecurity Training Program to cover only relevant topics.

Chapter One

Agency Responsibilities

1.1 Scope

This chapter outlines the ECC's responsibilities for providing Cybersecurity training to both new and veteran employees in accordance with this standard. All training programs should be developed in accordance with ECC policies.

1.2 ECC Training Program

Each ECC should adopt an in-service training practice which best serves the needs of the ECC and its members.

1.2.1 Training Hours

1.2.1.1 Depending on the size of the ECC and the scope of the ECC's Cybersecurity Policy, designated agency personnel should devote at least four to eight hours annually to educating members on the ECC's cybersecurity policy and the employees' role in maintaining security.

1.2.1.2 As Cyberattacks evolve and become more sophisticated, ECCs should consider providing some form of Cybersecurity training more than once per year to provide employees with up-to-date information about current Cybersecurity threats and to refresh employee commitment to Cybersecurity hygiene.

1.2.2 Instruction Methods

1.2.2.1 Methods of instruction may include instructor-led classroom training, internet-based learning modules, simulated cybersecurity attack exercises, policy review meetings, sharing current events regarding compromised ECCs or other public entities, periodic discussions during briefings and meetings, or any combination of delivery methods.

1.3 Agency Responsibilities

1.3.1 General Agency Responsibilities

1.3.1.1 The ECC should create and embrace a culture of Cybersecurity awareness.

1.3.1.2 The ECC shall provide adequate resources to ensure that all ECC personnel are adequately and routinely trained to identify cybersecurity attacks and maintain good cybersecurity hygiene.

1.3.1.3 The ECC should assign an individual to administer the ECC's Cybersecurity Training Program.

1.3.1.4 The ECC shall define acceptable use of ECC technology by role and level of authority.

1.3.1.5 The ECC shall provide ECC staff with regular Cybersecurity updates. Examples of updates may include new types of Cybersecurity attacks, improved security methods or examples of risks and recent attacks illustrating the importance of Cybersecurity

1.3.1.6 The ECC should assist in strengthening security across multiple offices and agencies by participating in regional or statewide forums to share information about Cybersecurity incidents.

1.3.1.7 The ECC should have a procedure defining what information regarding a Cybersecurity Incident is shared with external entities.

1.3.2 Use of Internet-Based Technology

1.3.2.1 The ECC shall have a policy that defines acceptable uses of the Internet, including websites and categories of websites that are explicitly forbidden by employees in different roles.

1.3.2.2 The ECC shall clearly identify websites that employees in different roles are authorized to access.

1.3.3 Use of Intranet-Based Technology

1.3.3.1 The ECC shall clearly identify web-based and applications that employees in different roles are authorized to access.

1.3.3.2 The ECC shall have a policy that defines acceptable uses of the Intranet.

1.3.4 Offsite Technology Usage

1.3.4.1 The ECC shall have a policy regarding what ECC devices employees are authorized to use outside of the ECC. The policy shall address storing, processing and accessing ECC data and applications.

1.3.4.2 The ECC shall have policies regarding Equipment Security for devices used offsite. Some guiding documents include the National Institute of Standards and Technology Framework for improving Critical Infrastructure, the U.S. Department of Justice FBI Criminal Justice Information Services Security Policy, and the Health Information Trust Alliance Common Security Framework, all of which are referenced in Chapter 6 (Resources).

1.3.5 Remote Access to ECC Technology

1.3.5.1 The ECC shall have a policy defining which ECC systems and applications can be accessed remotely by which employees.

1.3.5.2 The ECC shall have a policy defining acceptable use of Remote Access. The policy should identify devices that are acceptable to use for Remote Access.

1.3.5.3 The ECC shall have a policy regarding employee accountability during Remote Access of ECC systems and applications.

1.3.5.4 The ECC should have a formal procedure for requesting Remote Access.

1.3.6 Ethics

1.3.6.1 The ECC shall create a Technology Code of Conduct for the use of ECC Technology Systems and Components.

1.3.6.2 The ECC shall have a policy regarding Personal Use and Gain of ECC Technology Systems and Components.

1.3.6.3 The ECC shall have a policy defining proper and improper use of ECC Technology Systems and Components, along with the consequences of improper use of the systems and components.

1.3.7 Passwords

1.3.7.1 The ECC shall provide password creation guidelines to all members with technology access.

1.3.7.2 The ECC shall provide users of ECC Technology and Systems with information on protocols for changing passwords.

1.3.8 Application Management

1.3.8.1 The ECC shall have a patch management policy.

1.3.8.2 The ECC patch management policy should include applying the latest patch to all impacted devices as soon as possible, and no longer than seven days, of being determined to be safe for full release in the ECC environment.

1.3.9 Data Management

1.3.9.1 The ECC should have a digital document/record retention policy.

1.3.10 Physical Security

1.3.10.1 The ECC shall have policies regarding who has access to different parts of ECC facilities (e.g., the building, the call taking and dispatching area, and the server room).

1.3.10.2 The ECC shall have formal procedures regarding how to access different parts of ECC facilities (e.g., the building, the call taking and dispatching area, and the server room).

1.3.10.3 The ECC shall have policies regarding which, if any, personal devices are allowed within the ECC.

1.3.10.4 The ECC shall have policies on where employees can use, attach, or plug in allowed personal devices and media such as phones, tablets, portable drives, and disks.

1.3.11 Workstation Security

1.3.11.1 The ECC shall have a policy regarding what workstations and ECC applications employees in different roles are authorized to access.

1.3.11.2 The ECC shall have a policy regarding what employee roles are authorized to install software on ECC hardware.

1.3.11.3 The ECC should have a policy regarding employee sharing of workstation access with other users.

1.3.11.4 The ECC should have policies defining which types of technology, such as workstation, CPE, phone systems, and radios, should be left on or off when a workspace is vacated either temporarily or permanently.

1.3.11.5 The ECC should have policies defining the types of technology, such as workstation, CPE, phone systems, and radios, on which employees should stay logged into or log out of when a workspace is vacated either temporarily or permanently.

1.3.11.6 The ECC shall have policies regarding the monitoring of employee activity on workstations.

1.3.12 Cybersecurity Attacks

1.3.12.1 The ECC shall update training curriculum addressing Cybersecurity Attacks as new types of Cybersecurity Attacks emerge.

1.3.12.2 The ECC shall have a policy regarding how to handle emails from unknown senders.

1.3.12.3 The ECC shall have a policy regarding who is authorized to check Malicious Links.

1.3.12.4 The ECC shall have a formal process regarding actions to take in the case of a suspected or actual Cybersecurity Attack, including who to advise, what information is required to report the issue and what immediate steps the employee discovering the suspected Cybersecurity Attack should take.

1.3.13 Cybersecurity Incident Response

1.3.13.1 The ECC should have formal mitigation strategies for the various types of Cybersecurity Incidents that could affect ECC operations.

1.3.13.2 The ECC should identify and make known the points of contact for the various types of Cybersecurity Incidents that could affect ECC operations.

1.3.13.3 The ECC should have and make known an escalation process if the primary point of contact for a Cybersecurity Incident is unavailable within a prescribed timeframe.

1.3.14 Violations of Cybersecurity Policies and Procedures

1.3.14.1 The ECC should have formal policies regarding corrective and/or disciplinary action taken for different types of violations of cybersecurity policies and procedures.

1.3.14.2 The ECC should have formal policies regarding how supervising and managing personnel will handle different types of violations of ECC cybersecurity policies and procedures.

Chapter Two

Public Safety Telecommunicators (PSTs)

2.1 Scope

This chapter identifies topics for inclusion in a Cybersecurity training curriculum for PSTs in an Emergency Communications Center (ECC). Training topics shall be developed consistent with agency policy. The topics in this chapter also apply to any ECC staff in administrative positions who use and access ECC technology.

2.2 Context for Training

PSTs should understand why security awareness training is important. PSTs are heavy users of an ECC's systems and may be the first to notice something awry. It is important that they can identify the signs of a Cybersecurity Attack and know what to do if they suspect such an attack. Additionally, PSTs should be aware of agency policies addressing the use and security of technology so that they do not unwittingly create vulnerabilities potentially leading to a successful Cybersecurity Attack against the ECC.

2.3 Use of Internet-Based Technology

2.3.1 Internet Usage

2.3.1.1 PSTs shall know the difference between the ECC Intranet and the Internet.

2.3.1.2 PSTs shall be trained on the acceptable uses of the Intranet and the Internet.

2.3.1.3 PSTs shall be informed of the risks involved in accessing the Internet from within the ECC.

2.3.1.4 PSTs shall be informed of the risks involved in accessing the Internet from computers on which CAD or other mission critical software is installed.

2.3.1.5 PSTs should be aware that their actions may be monitored and/or recorded while they are using the Internet.

2.3.1.6 PSTs shall be informed of what categories of external websites are authorized or forbidden.

2.3.2 Browser Plugins

2.3.2.1 PSTs should be informed on what Browser Plugins are, how they are used, and the potential risks of installing them.

2.3.3 Issues with Accessing the Internet

2.3.3.1 PSTs shall know whom to contact in the event an issue occurs with accessing a Web Application or a website.

2.4 Offsite Technology Usage

2.4.1 Offsite Device Usage

2.4.1.1 PSTs shall be trained on what devices they are authorized to use outside of the ECC for storing, processing and accessing ECC data and applications.

2.4.1.2 PSTs shall be trained on ECC policies regarding Equipment Security for

devices used offsite.

2.4.1.3 PSTs shall be trained in how to use equipment containing sensitive data, such as Personally Identifiable Information, and/or processing sensitive data offsite.

2.4.2 Remote Access to ECC Technology

2.4.2.1 PSTs authorized to access ECC technology remotely shall be trained on the risks to the ECC of accessing ECC technology from remote locations.

2.4.2.2 PSTs authorized for remote access shall be trained on what ECC systems and applications they have permission to access remotely.

2.4.2.3 PSTs authorized for remote access shall be trained on what devices and connections they may use for remote access.

2.4.2.4 PSTs authorized for remote access shall be trained on the proper way to remotely access ECC systems and applications for which they are authorized.

2.4.2.5 PSTs authorized FOR remote access shall be trained on the proper procedures for securing and protecting remote access credentials.

2.4.2.6 PSTs authorized for remote access shall be informed as to whom they shall report any suspected or known disclosure of access credentials.

2.4.3 Personally-Owned Devices

2.4.3.1 PSTs authorized to connect personally-owned devices to ECC technology shall be trained on the ECC's policies regarding connecting personally-owned devices to ECC systems.

2.4.3.2 PSTs authorized to connect personally-owned devices to ECC technology shall be trained on the risks of connecting personally-owned devices to ECC systems.

2.4.3.3 PSTs authorized to connect personally-owned devices to ECC technology shall be trained on any settings they must make on their devices prior to connection.

2.4.4 Emergency Operations

2.4.4.1 PSTs shall be trained on additional cybersecurity procedures and precautions to take when moving operations to a temporary, emergency or backup location.

2.5 Ethics

2.5.1 Policy

2.5.1.1 PSTs shall be trained on the ECC's code of conduct for using ECC Technology Systems and Components.

2.5.2 Personal Use and Gain

2.5.2.1 PSTs shall be trained on the ECC's policies regarding Personal Use and Gain of ECC Technology Systems and Components.

2.5.3 Individual Accountability

2.5.3.1 PSTs shall be trained on the potential consequences of violating ECC policies regarding the use of ECC technology.

2.6 Passwords

2.6.1 Password Creation

2.6.1.1 PSTs shall be trained on how to create passwords in accordance with ECC policy.

2.6.2 Password Changes

2.6.2.1 PSTs shall be trained on how to change passwords in accordance with ECC policy.

2.6.3 Password Management

2.6.3.1 PSTs shall be trained on the importance of using different passwords for different accounts.

2.6.3.2 PSTs shall be trained on the importance of not using ECC passwords for personal accounts and vice versa.

2.6.3.3 PSTs shall be trained on why passwords should not be shared with others.

2.6.3.4 PSTs shall be trained on the danger of saving passwords in browser applications.

2.6.4 Password Accountability

2.6.4.1 PSTs shall be trained to identify the signs of a compromised password.

2.6.4.2 PSTs shall be trained on what to do if they suspect one of their passwords has been compromised, including how to report the incident and how to change the compromised password.

2.7 Physical Security

2.7.1 ECC Access

2.7.1.1 PSTs shall be trained on the importance of physical security.

2.7.1.2 PSTs shall be trained on policy and procedures for accessing ECC facilities.

2.7.2 ECC Portable Electronics and Media

2.7.2.1 PSTs shall be trained on how to secure Portable Devices when leaving the devices unattended.

2.7.2.2 PSTs shall be trained on how to secure Portable Media when leaving the media unattended.

2.7.2.3 PSTs shall be trained on how to secure or dispose of Portable Media when the media is no longer needed.

2.7.3 Personal Devices and Media

2.7.3.1 PSTs shall be informed about the dangers of plugging phones, tablets and other personal equipment into the ECC's systems.

2.7.3.2 PSTs shall be informed of what, if any, personal devices are allowed within the ECC.

2.7.3.3 PSTs shall be trained on where they may and may not use, attach, or plug in allowed personal devices and media such as phones, tablets, portable drives, and disks.

2.8 Workstation Security

2.8.1 Workstation Access

2.8.1.1 PSTs should be informed of what workstations they are authorized to access.

2.8.1.2 PSTs should be aware of which individuals are authorized to install software on ECC equipment.

2.8.1.3 PSTs should be informed of what applications they are authorized to access

on their workstations.

2.8.1.4 PSTs shall be informed of the risks involved in using software installed on the same computers and networks on which CAD or other mission critical software is installed.

2.8.1.5 PSTs shall be trained to identify indicators of attempted or actual unauthorized workstation access.

2.8.1.6 PSTs shall be trained on whom to contact in the event they suspect an attempted or actual unauthorized workstation access.

2.8.1.7 PSTs should be trained on ECC policies regarding sharing workstation access with other users.

2.8.1.8 PSTs shall be trained on the risks of allowing other users to use their logon credentials.

2.8.2 ECC Workspace Equipment

2.8.2.1 PSTs shall be trained on how to secure their workspace equipment.

2.8.2.2 PSTs shall be trained on how to leave their workspace when leaving temporarily and at the end of their shift.

2.8.2.3 PSTs shall know what material needs to be secured or disposed of securely and how to properly secure or dispose of the material.

2.8.2.4 PSTs shall be trained on what types of technology should be left on and what types of technology they should turn off upon leaving the workstation.

2.8.2.5 PSTs shall know which technology they may remain logged into and which technology they must log out of upon leaving the workstation.

2.8.3 Workstation Environmental Protection

2.8.3.1 PSTs should be informed of the types of environmental hazards from which workstations need to be protected. Some examples of environmental hazards are obstructions to the intake and exhaust vents and open liquid containers.

2.8.3.2 PSTs shall be trained on how to protect their workstations from environmental hazards.

2.8.4 Workstation Endpoint Protection

2.8.4.1 PSTs should be informed of what Endpoint Protection has been provided on workstations to which they have access, along with responsibilities they may have with that Endpoint Protection.

2.8.5 Workstation Monitoring

2.8.5.1 PSTs should be informed that their workstation activity may be monitored in accordance with ECC policies.

2.9 Wireless Communication within the ECC

2.9.1 Wireless Connections

2.9.1.1 PSTs should be trained on ECC policy regarding wireless connections.

2.9.1.2 PSTs shall be trained in vulnerabilities associated with wireless connections to include, but not limited to, Wi-Fi, Bluetooth, Infrared, and near field.

2.9.1.3 PSTs should be trained on how to disconnect from wireless connections when they are no longer needed.

2.9.2 Wi-Fi Security

2.9.2.1 PSTs should have a high-level awareness of the vulnerabilities associated with both private, public, and guest Wi-Fi.

2.9.2.2 PSTs should how to protect ECC equipment and data when connecting to authorized public and private Wi-Fi.

2.9.3 Cellular Devices

2.9.3.1 PSTs shall know the ECC policy on authorized use of cellular devices within the ECC.

2.10 Encryption

2.10.1.1 PSTs should be trained on how to properly use any encryption tools utilized by the ECC.

2.10.1.2 PSTs should be trained on the purposes and reasons behind encrypting data in motion and at rest to protect their agency from Cybersecurity Attacks.

2.11 Cybersecurity Attacks

2.11.1 General Cybersecurity Attacks

2.11.1.1 PSTs shall be trained on the types of Cybersecurity Attack they may encounter.

2.11.1.2 PSTs should be aware of the methods used to initiate a Cybersecurity Attack.

2.11.2 Messaging Attacks

2.11.2.1 PSTs shall be informed about the different types of Messaging Attacks that can be executed through email and text. Topics should be relevant to the current threat landscape and should include, at a minimum, Technical Support Scams, Phishing, Spear Phishing, Whaling, SMiShing, Ransomware, Malicious Links and Malicious Attachments.

2.11.2.2 PSTs shall be trained on how to identify the various types of Messaging Attacks.

2.11.2.3 PSTs shall be trained in how to check Malicious Links through anti-virus or other scanning process, according to ECC policy.

2.11.2.4 PSTs shall be informed in how to handle emails from unknown senders.

2.11.2.5 PSTs should be trained in how to set and adjust their Spam filters for their email client.

2.11.2.6 PSTs shall be informed on who to advise in the case of a suspected or actual Messaging Attack, along with how to provide the information required to report the issue and what immediate steps they should take.

2.11.3 Denial of Service (DoS) Attacks

2.11.3.1 PSTs should understand the impacts of different types of DoS attacks.

2.11.3.2 PSTs should know the signs of a DoS attack on ECC technology, Intranet, telephone system or radio system.

2.11.3.3 PSTs shall be trained on what steps to take if they suspect or are experiencing a DoS attack, what information is required to report the issue and what immediate steps they should take.

2.11.4 Malware Attacks

2.11.4.1 PSTs shall be aware of the potential ways that Malware can infect ECC Technology Systems and Components.

2.11.4.2 PSTs should be aware of the signs of a Malware infection.

2.11.4.3 PSTs shall be trained on what steps to take if they suspect or are experiencing a Malware Attack, what information is required to report the issue and what immediate steps they should take.

2.11.5 Man-in-the-Middle Attacks

2.11.5.1 PSTs should have an understanding of Man-in-the Middle Attacks.

2.12 Cybersecurity Incident Response

2.12.1 Cybersecurity Incidents

2.12.1.1 PSTs shall be trained on what is considered a Cybersecurity Incident.

2.12.1.2 PSTs shall be trained on how to identify and report suspected or actual Cybersecurity Incidents.

2.12.1.3 PSTs shall be trained on what actions to take for various types of Cybersecurity Incidents.

2.12.2 Mitigation

2.12.2.1 PSTs shall be trained on the immediate steps they should take to mitigate a Cybersecurity Incident.

2.12.2.2 PSTs should be trained on the different mitigation strategies for the different types of Cybersecurity Incidents that could affect ECC operations.

2.12.2.3 PSTs should be informed that their mitigation steps are only the first measure of response and that additional actions may be required by other staff.

2.12.3 Points of Contact

2.12.3.1 PSTs shall be trained on the points of contact for the different types of Cybersecurity Incidents that could affect ECC operations.

2.12.3.2 PSTs should know the escalation process if the primary point of contact is unavailable within an ECC-defined timeframe.

Chapter Three

Supervisors

3.1 Scope

This chapter identifies the topics that should be covered in a Cybersecurity training curriculum for a Supervisor in an ECC. A Supervisor shall be proficient in all the topics for PSTs (Chapter 2) as well as in the additional topics identified in this chapter. Training topics shall be developed consistent with agency policy.

3.2 Context for Training

Like PSTs, Supervisors are heavy users of ECC systems and may be among the first to notice something awry. As such, they need to have the same training as PSTs. In their role of overseeing PSTs, they have additional responsibilities to ensure adherence to Cybersecurity policies and safe Cybersecurity practices.

3.3 Supervisor Cybersecurity Training Program

The Supervisor Cybersecurity Training Curriculum shall address the following topics, as well as all the topics in the Telecommunicator Cybersecurity Training Program.

3.3.1 Violations of Cybersecurity Policies

3.3.1.1 Supervisors shall be trained on how to handle anticipated types of violations of ECC Cybersecurity policies and procedures.

3.3.2 Passwords

3.3.2.1 Supervisors shall know the ECC procedure for handling an account lockout.

3.3.2.2 Supervisors shall know the ECC procedure for handling a forgotten password.

3.3.3 Emergency Operations

3.3.3.1 Supervisors shall be trained on additional Cybersecurity procedures and precautions to take when hosting another agency that has been relocated to the ECC.

3.3.3.2 Supervisors shall be trained on additional Cybersecurity precautions to take when the ECC gives non-ECC entities access to its systems or facilities.

Chapter Four

Managers/Directors

4.1 Scope

This chapter identifies the topics that should be covered in a Cybersecurity training curriculum for staff at the Manager or Director level in an Emergency Communications Center (ECC). Managers and Directors need to be proficient in the training topics for PSTs as identified in Chapter 2, for Supervisors as identified in Chapter 3, and the additional topics identified in this chapter. Training topics shall be developed consistent with agency policy.

4.2 Context of Training

Agency leadership sets the tone for the entire ECC. Support and acceptance of a cybersecurity awareness training program starts at the upper management level. Individuals holding positions in ECC management need to understand the importance of Cybersecurity Awareness training and instill a culture of cybersecurity awareness that permeates day-to-day ECC operations.

4.3 Manager/Director Cybersecurity Training Program

4.3.1.1 Managers/Directors shall be trained on internal and external resources available to keep them apprised of potential Cybersecurity incidents.

4.3.1.2 Managers/Directors shall be trained on what internal and external resources are available to handle different types of cybersecurity incidents.

4.3.1.3 Managers/Directors shall be familiar with any governing laws, policies and regulations for ECC actions and responses during a Cybersecurity incident.

4.3.1.4 Managers/Directors shall be trained on the circumstances for which Cybersecurity Incidents require immediate attention, even if after regular business hours, and those for which can be addressed on the next business day.

4.3.1.5 Managers/Directors shall be trained on what information about Cybersecurity Incidents should be shared with ECC personnel and other internal entities and/or external entities, such as neighboring ECCs or affiliated vendors.

4.3.1.6 Managers/Directors shall be trained on how to share information about Cybersecurity Incidents with ECC personnel and other internal entities and/or external entities, such as neighboring ECCs or affiliated vendors.

Chapter Five

Privileged Users

5.1 Scope

This chapter identifies additional topics on which Privileged Users should receive training. The topics in this chapter address training for personnel who may not be in professional technical positions, but who are Privileged Users with administrative privileges allowing them to handle some technical tasks such as application installation, application administration, database management or system administration. Privileged Users shall be proficient in all the topics for PSTs, Supervisors and Managers/Directors, as identified in Chapters 2 through 4, as well as in the additional topics identified in this chapter.

5.2 Context for Training

Privileged Users have access to accounts and systems that allow them to perform a range of tasks including application installation, operating system updates, application administration, database management or system administration (such as performing backups). With this access comes additional responsibility and risk of exposing the ECC to a Cyberattack. The topics in this chapter are designed to provide Privileged Users with the tools to fulfill that additional responsibility as well as the awareness and knowledge to mitigate the risks. These topics may not apply to all Privileged Users and the ECC should tailor the Training Program to cover only relevant topics.

5.3 Account Management and Access

5.3.1 Account Privileges

5.3.1.1 Privileged Users shall be trained in the concept of least privilege, how to discern between levels of privilege, and how to grant account privileges.

5.3.1.2 Privileged Users shall be provided training on the importance of factoring cybersecurity into providing account privileges.

5.3.2 Account Access

5.3.2.1 Privileged Users shall be trained on ECC policy regarding who can create what type of accounts.

5.3.2.2 Privileged Users shall be trained on ECC policy regarding who can unlock what types of accounts.

5.3.2.3 Privileged Users shall be trained on how to secure privileged accounts, establish multi-factor authentication, and manage encryption keys.

5.3.2.4 Privileged users shall be trained on how to address suspected or actual misuse of user accounts.

5.3.2.5 Privileged Users shall be trained on the importance of and process for prompt removal of stale, old, and unused accounts.

5.4 Remote Access

5.4.1.1 Privileged Users shall be trained on ECC remote access policies.

5.4.1.2 Privileged Users shall be trained on the necessity of securing points of entry to ECC systems.

5.4.1.3 Privileged Users shall be trained in different types of authentication for entry from remote devices.

5.4.1.4 Privileged Users shall be trained in the importance of multi-factor authentication for remote access to ECC systems.

5.4.1.5 Privileged Users shall be trained in how to achieve multi-factor authentication.

5.5 System Management

5.5.1 Log Files

5.5.1.1 Privileged Users shall be trained in what normal log files look like and ways to identify abnormalities that may indicate a Cybersecurity incident.

5.5.1.2 Privileged Users shall be trained in how to protect ECC system log files from unauthorized access.

5.5.1.3 Privileged Users shall be trained in how to keep the log files from being tampered with or destroyed.

5.5.1.4 Privileged Users should be trained in ECC retention policies for log files

5.5.2 Patch Management

5.5.2.1 Privileged Users shall receive training on the role of patch management in preventing the exploitation of ECC equipment.

5.5.2.2 Privileged Users shall receive training on the ECC patch management policy.

5.5.3 Software Installation

5.5.3.1 Privileged Users shall receive training in what constitutes a trusted source for software acquisition and installation.

5.5.3.2 Privileged Users shall be trained on how to validate installation files to make sure they have not been tampered with.

5.5.3.3 Privileged Users should be trained in how to protect and manage digital certificates for the ECC.

5.5.4 Backups

5.5.4.1 Privileged Users should be trained on how to properly backup ECC systems in accordance with ECC policy.

5.5.4.2 Privileged Users should be trained on how to properly secure and store system backups to avoid unauthorized access or tampering

5.5.4.3 Privileged Users should be trained on how to use backups to restore systems in the event of a Cybersecurity incident.

5.6 ECC Equipment Management

5.6.1 ECC Equipment Disposal and Reassignment

5.6.1.1 Privileged Users shall be trained on how to correctly clean hardware so that it is free of sensitive data before disposal or reassignment

5.6.1.2 Privileged Users shall be trained in ECC retention policies to avoid deleting data that should be retained.

5.6.1.3 Privileged Users shall be trained in ECC policies and procedures regarding the disposal or reassignment of hardware and software.

Resources

Association of Public Safety Communications Officials. (2018). *Cybersecurity Attacks: Detection and Mitigation – A Guide for PSAPS*. https://www.apcointl.org/download/introduction-to-cyber-security-a-guide-for-psaps/. Retrieved 3 September 2019.

Association of Public Safety Communications Officials. (2016). *An Introduction to Cybersecurity: A Guide for PSAPs* (Version 1.0). https://www.apcointl.org/download/introduction-to-cyber-security-a-guide-for-psaps/. Retrieved 3 September 2019.

Association of Public Safety Communications Officials. (2018). *APCO Updated Cybersecurity Guidance.* https://www.apcointl.org/download/apco-cybersecurity-guidance/. Retrieved 3 September 2019.

Federal Trade Commission Consumer Information. Computer Security. https://www.consumer.ftc.gov/articles/0009-computer-security. Retrieved 3 September 2019.

Federal Trade Commission Consumer Information. *Tips for Using Public Wi-Fi Network.* https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks. Retrieved 3 September 2019.

Federal Communications Commission. (2019). *Task Force on Optimal PSAP Architecture (TFOPA), Final Report.* https://www.fcc.gov/about-fcc/advisory-committees/general/task-force-optimal-public-safety-answering-point. Retrieved 3 September 2019.

Franklin, J., et al. (2019). *Mobile Device Security: Cloud and Hybrid Builds.* National Institute of Standards and Technology, National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid. Retrieved 3 September 2019.

Hicks, A. and Cline, B. (2014). *Managing Cybersecurity Risk in a HIPAA-Compliant World.* Health Information Trust Alliance. https://hitrustalliance.net/content/uploads/2016/01/Coalfire_HITRUST_Managing_Cybersecurity_Risk_in_HIPAA_Compliant_World.pdf. Retrieved 3 September 2019.

McCabe, J. (2019). *FBI Tech Tuesday: Protecting Against PII Theft.* FBI Phoenix. https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-protecting-against-pii-theft. Retrieved 3 September 2019.

Scarfone, K. (2009). *Security for Enterprise Telework and Remote Access Solutions.* National Institute of Standards and Technology, Information Technology Laboratory Bulletin. https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=903007. Retrieved 3 September 2019.

National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Retrieved 3 September 2019.

United States Department of Homeland Security CISA. *National Cyber Awareness System – Tips.* https://www.us-cert.gov/ncas/tips. Retrieved 3 September 2019.

United States Department of Justice Federal Bureau of Investigation Criminal Justice Information Services Division. (2019). *Criminal Justice Information Services (CJIS) Security Policy* (CJISD-ITS-DOC-08140-5.8). https://www.fbi.gov/file-repository/cjis-security-policy_v5-8_20190601.pdf/view. Retrieved 3 September 2019.

Acronyms

ANS	APCO American National Standards
CAD	Computer Aided Dispatch
DDoS	Data Denial of Service
DoS	Denial of Service
ECC	Emergency Communications Center
FTP	File Transfer Protocol
MITM	Man-in-the-Middle
NIST	National Institute of Standards and Technology
PST	Public Safety Telecommunicator
SDC	APCO International Standards Development Committee
PSAP	Public Safety Answering Point
TDoS	Telephony Denial of Service
URL	Uniform Resource Locators

Definitions

This chapter contains definitions of terms used throughout this document.

Acceptable Use of Technology: The appropriate and approved ways that ECC technology can be accessed and used. Acceptable use of ECC technology may vary from one ECC to another and the training should be tailored to reflect the Agency's stated policies.

Browser Plugin: A piece of software that provides additional functionality to a browser.

Cybersecurity: Technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity may also be referred to as information technology security.

Cybersecurity Attack: Any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an of computer information systems, infrastructures, computer networks, or personal computer devices for the purpose of gaining private, technical, institutional information, or other intellectual assets for the purpose of vandalism, interference in service delivery or monetary gain.

Cybersecurity Incident: Any event that threatens the security, confidentiality, integrity, or availability of ECC electronic information assets, information systems, and/or the networks that deliver the information. Any violation of security policies, acceptable use policies or standard computer security practices is an incident. Incidents may include: unauthorized entry; security breach or potential security breach; unauthorized scan or probe; Denial of Service; malicious code or virus; violations of the ECC IT Policies and Standards; widespread networking system failure; and widespread application or database failure.

Cybersecurity Training Program: A training program tailored to the needs of an ECC and designed to equip ECC staff with the knowledge of how to prevent Cybersecurity Incidents and Attacks, what qualifies as an Incident or Attack, who to notify in an actual or suspected incident and how to remedy the Incident or Attack.

Cybersecurity Policies: ECC specific directives designed to protect the ECC from Cybersecurity Incidents and Attacks.

Denial of Service (DoS): Attacks that affect the functionality of one or more devices on the ECC network. A DoS attack in the form of a flood of unwanted, malicious inbound calls is called a Telephony Denial of Service (TDoS). A TDoS attack is the type of Cybersecurity Attack that an ECC's phone system is most likely to experience. A DoS attack in the form of a flood of data to a system or website, rendering the system or website unusable is called a Data Denial of Service (DDoS). A final type of DoS attack PSTs might encounter is interference with radio channels through the intentional jamming, saturation, or overtaking of control elements or base stations.

Emergency Communications Center (ECC): The organization that is providing communications services to the public and/or first responders. The organization can be a stand-alone agency, a department or unit within a larger agency, a consortium of several agencies, or other configurations.

Equipment Security: Securing equipment includes both physical security (e.g., a cable lock or pelican

case) and procedural security (e.g., shutting down and locking screen or preventing others from viewing the screen).

Endpoint Protection: Software, such as anti-virus software, intrusion detection software and host-based firewalls, that assists in the protection of workstations from Cybersecurity attacks.

Internet: The global, public network of billions of servers, computers, and other hardware devices. Devices with a valid IP address can connect with any other device. The Internet provides the platform for email, File Transfer Protocol (FTP), instant messaging services, and the information sharing system known as the Web.

Intranet: A private network that operates like the World Wide Web, but that can be accessed only by authorized users.

Malicious Attachments: Attachments in any format, such as, but not limited to, Word, PDF, and RTF, that contain malicious code designed to launch when opened and cause harm to data and/or systems.

Malicious Links: Links that connect to a site or location that performs a malicious action. These can be masked to look like a legitimate Uniform Resource Locators (URL) or hidden through a URL shortening service.

Malware: Any software designed to damage or interfere with data, hardware or network systems and that may take the form of executable code, scripts, active content or other software.

Man-in-the-Middle (MITM): Attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

Messaging Attacks: Cybersecurity Attacks propagated through a digital conveyance like email, text, and instant messaging. Messaging Attacks use manipulative techniques to get the attention of the recipient and typically express a sense of urgency hoping to induce the recipient to perform an action that would result in access to otherwise secure information. Examples of actions include scanning with an antivirus program, validating the sender/request/link/attachment through an independent source, opening in a secured environment on a specific computer or device, or possibly having a designated individual who is trained and has the required equipment handle all such traffic.

Personally Identifiable Information: Personally identifiable information is personal information, which includes names, biometric records, social security numbers, dates of birth, and financial information. This information may be used in conjunction with other personal information, such as mother's birth name or one's place of birth.

Personal Use and Gain: The use of one's position or ability to access technology for the personal profit of any money, property, special favors or anything else of value that solely benefits the person and not the agency.

Phishing: A type of Messaging Attack in the form of emails that appear to be from a reputable company and induce an individual to reveal personal information, such as passwords. Phishing emails are sent out in mass and are not targeted to a specific person or group.

Portable Device: An electronic device that can be carried from one location to another. Examples include laptops, tablets, cell phones and wearable devices.

Portable Media: An electronic device capable of storing and playing digital media. Examples include thumb drives, external drives, and storage disks.

Pretexting: A type of Messaging Attack in the form of an email in which the sender masquerades as someone else to get an individual to divulge information or take an action.

Privileged Account: An administrative account with more privileges than a normal user account. Additional privileges include activities such as modifying an operating system, domain, or application, installing and removing software or drivers, running scripts, and changing user permissions.

Privileged User: A person with a Privileged Account who may or may not be in a professional technical position, but handles some technical tasks such as application installation, application administration, database management or system administration.

Public Safety Telecommunicator (PST): An individual employed by a public safety agency as the first of the first responders whose primary responsibility is to receive, process, transmit, and/or dispatch emergency and non-emergency calls for service for law enforcement, fire, emergency medical, and other public safety services via telephone, radio, and other communication devices.

Ransomware: A type of Cybersecurity Attack that infects a system or database and prevents access until a ransom is paid. Ransomware exploits vulnerabilities in software and is delivered most commonly through phishing emails.

Remote Access: Connecting to the work environment applications from a known secure device or location or a public device or location. Work environment applications could be a scheduling, email, CAD database, RMS and other database type applications use.

SMiShing: A Phishing attack performed through text or SMS messaging.

Spam: Spam emails and text messages are usually just an inconvenience. They take time to go through and can fill up an inbox.

Spear Phishing: Phishing attacks customized for a target individual or organization.

Technical Support Scam: An offering of services to repair a system, device, program or network under the false pretense that it is not working properly or has a virus. A Technical Support Scam is usually used for monetary gain or malicious activity.

Technology Code of Conduct: A set of rules outlining responsibilities of and proper practices for the use of technology.

Web (also known as the World Wide Web): a network of online content in an information space where documents and other web resources are identified URLs, interlinked by hypertext links, and accessible via the Internet.

Web or Web-Based Application: An application program that is stored on a remote server and delivered over the Internet through a browser interface.

Whaling: Phishing attacks targeted to a specific individual of prominence, such as a member of the ECC executive team.

Wi-Fi: Network infrastructure component allowing desktop computers and Portable Devices to wirelessly connect to the internet or communicate with each other.

Acknowledgements

Special recognition goes to Cybersecurity Training Working Group members that provided their expertise in successfully creating the standard. The Cybersecurity Training Working Group included the following membership, whose work was overseen by the Standards Development Committee:

Dr. Monica Lynn, Chair
Manager
DELTAWRX
Woodland Hills, California

Aerica Ramos
Regional Communications Center Manager
Florida Highway Patrol
Lake Worth, Florida

Timothy Lorello
President and CEO
SecuLore Solutions
Odenton, Maryland

Tim Hannah
Assistant Director - Technical Services
South Sound 9-1-1
Tacoma, Washington

Phil Rotheram
Atos
Folsom, California

Megan Bixler
Technical Program Manager
APCO International

Tony Pasquale, CCS/CTO-I
Rochester Police Department
Rochester, Minnesota

Steve Walsh, CISSP
State 9-1-1 Cyber Security Manager
Washington State 9-1-1 Coordination Office

Stacy Banker, RPL, ENP
Standards Program/ACS Manager
APCO International

APCO Standards Development Committee

Daniel Morelos
Tucson Airport Authority
Arizona

Karen Allen
SRP Security Services
Phoenix, Arizona

Sherry Taylor
Indianapolis Fire Department
Communications Division,
Indiana

Bradford S. Smith
Framingham Fire Department
Massachusetts

Judith Weshinskey-Price
Pinellas County Regional 9-1-1
Largo, Florida

Bud Hicks, ENP
Grundy County 911
Morris, Illinois

Rick Thomas, RPL
Apex, North Carolina

Jackie Pace
Redwood City, California

James Leyerle, ENP
OnStar, Retired

Kim Ostin
Sterling Heights Police Dept.
(Ret)
Sterling Heights, MI

Nathan McClure, ENP
Past APCO International
President
AECOM, Retired

Nicola Tidey, RPL, ENP
Mission Critical Partners
College Station, Pennsylvania

Stephen Ashurkoff, ENP
Safety & Security Technologies
Comtech Telecomunications
Corp.
Westwood, Massachusetts

Stephen Devine
FirstNet

Stacy Banker, RPL, ENP
Standards Program/ACS
Manager
APCO International