State 9-1-1 Program Updates

Oregon APCO/NENA Statewide Quarterly Meeting

September 14, 2021

Agenda

- **Opening Remarks**
  - **OEM Organizational Updates**
- **9-1-1 Program Updates**
  - **Staff Recruitments**
  - **Subaccount Funding Eligibility**
  - **Update - 988 Planning & Implementation**
  - **Jurisdiction Plan Update Requirements**
    - *Cyber Security Considerations*
  - **CPE Lifecycle Replacements**

9-1-1 Program Staff Recruitments

- New GIS Data Analyst
- Statewide 9-1-1 GIS Coordinator
- Project Portfolio/Project Manager

Questions?

Subaccount Funding Eligibility

- Funding eligibility now includes coverage for ‘make busy’ services
- Includes both one-time instillation and monthly recurring costs
- Enables faster rerouting of calls to alternate PSAP or designated backup locations in the event of a business interruption or disaster
- Contact 9-1-1 Program – Janine Mayer Janine.mayer@state.or.us
- OEM will direct pay for services
- Will not require submission of program Payment Authorization Form

Subaccount Funding Eligibility

Eligibility Guidance List for 9-1-1 Subaccount Expenditures

COST TYPE:	COST CATEGORY	ELIGIBLE USE:	EXAMPLES INELIGIBLE USE: *
(Continued) NETWORK / INFRASTRUCTURE CONNECTIVITY	Additional Data Repository (ADR) connectivity Make Busy Switch	A one-time fixed funding allocation of $2,500 reimbursement or direct vendor pay, for network configuration and access services for PSAPs wishing to access RapidSOS supplemental location data repository for a wireless 9-1-1 call. If a condition at a PSAP requires call takers to stop taking calls, the PSAP activates the "make busy" switch which diverts calls to an alternate PSAP or back-up center.	
TEXT-TO-9-1-1	Text-to-9-1-1	Cost to support a stand-a-lone text-to-9-1-1 solution	Integrated

https://www.oregon.gov/oem/Documents/Subaccount_Eligibility_Guidance_List_v4.pdf

Questions?

988 Planning & Implementation Update


Jan – Feb 2021
Draft legislation
Convene 988 Governor's workgroup
Draft amendments to legislation to establish minimum standards
Identify consultant to help with 988 implementation planning
Consumer engagement
Feb-April 2021
Complete analysis of current state of crisis response infrastructure to support 988
Finalize whether Telecom tax should go into current legislation
Finalize legislation with amendments
April-Aug 2021
Pass legislation (HB2417)
Finalize minimum standards and implementation plan for Mobile Crisis and 988 call Centers driven by consumer input
Identify funding for 988 Call Centers and mobile crisis services
Identify OAR and
Aug-Nov 2021
Finalize minimum standards for crisis stabilization centers
Draft RFP
Draft plan for Telecom tax strategy in short session
Consumer guidance
We are HERE
Nov-Dec 2021
Final 988 Implementation Plan to ensure 988 is ready to go live on July 16, 2022.
Final implementation plan
Consumer engagement
Complete technology needs study and evaluation plan
988 goes live nationwide on July 16, 2022

988 Planning & Implementation Contact

Oregon Health Authority

Rusha Grinstead, BH Crisis System & 988 Lead

Rusha.Grinstead@dhsoha.state.or.us

503-602-9214

Questions?

Jurisdiction Plan Update Requirements

- 403.130 9-1-1 jurisdiction plan; requirements review; revised plans:
  - (5) Each 9-1-1 jurisdiction shall submit to OEM in writing within 30 days any change to a PSAP that alters the approved jurisdiction plan. Changes may include, but are not limited to:
    - (e) The method used to direct an emergency call once received by the primary PSAP
  - (6) If an established 9-1-1 jurisdiction proposes to move a PSAP to another location or…

Jurisdiction Plan Update Requirements

- Examples of changes requiring OEM notification and/or plan updates:
  - Rerouting of calls to an alternate location *(for the purposes of a situation not defined within your current DR plan or temporary facility relocation)*
  - Any change to the CPE environment *(relocation of CPE, addition of call taking positions, modification of the CPE network to support functionality/capability beyond initial installation/configuration)*
- If unsure your situation requires jurisdiction plan or disaster recovery plan updates, please contact Janine Mayer – Janine.mayer@state.or.us
- *Communicate, Communicate, Communicate – We are all in it together to ensure a secure and reliable emergency communication system!*

Cyber Security Considerations

Cyber Threats And Cyber Hygiene & Best Practices

Theresa A. Masse
Cybersecurity Advisor – Region 10 (Oregon)
Cybersecurity and Infrastructure Security Agency

September 14, 2021

CISA
CYBER+INFRASTRUCTURE

THREAT OVERVIEW

Threats to Critical Infrastructure

- America remains at risk from a variety of threats including:
  - Acts of Terrorism
  - Cyber Attacks
  - Extreme Weather
  - Pandemics
  - Accidents or Technical Failures

CISA
CYBER+INFRASTRUCTURE

Threat Actors – Who Are They?

Nation States –usual suspects:

- China
- Russia
- North Korea
- Iran

Bad Actors - Everywhere:

- Typically, in it for money (Ransomware!)
- And, don't forget - - Insiders!

CISA
CYBER+INFRASTRUCTURE

Cyber Threat Alerts

- Joint FBI-CISA Public Service Announcements
- DHS Intelligence Enterprise Reference Guides
- CISA Alerts

CISA
CYBER+INFRASTRUCTURE

5

Threat Actors Are Sophisticated…

CISA
CYBER+INFRASTRUCTURE

But They Don't Always Need To Be

CSO FROM IDG

Home > Information Security

ANALYSIS

Zero-days aren't the problem -- patches are

Everyone fears the zero-day exploit. But old, unpatched vulnerabilities still provide the means for malicious hackers to carry out the vast majority of hacks

> . . . Most hackers follow the path created by a very few smart ones -- and zero days make up a very small percentage of attacks. It turns out that patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

CISA CYBER+INFRASTRUCTURE

But They Don't Always Need To Be

DARKReading

91% Of Cyberattacks Start With A Phishing Email

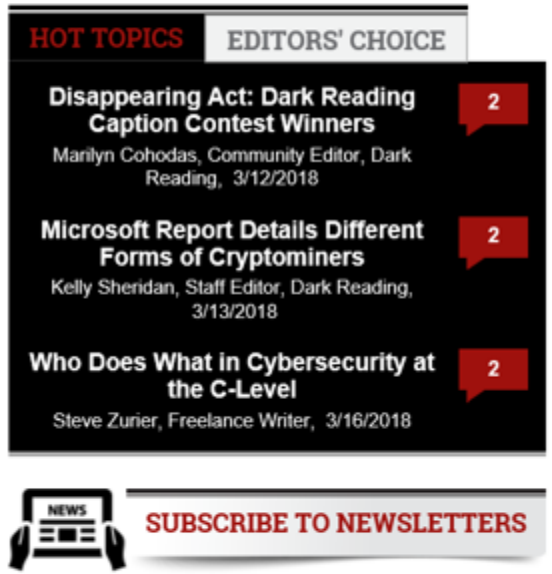
Phishing remains the number one attack vector, according to a new study that analyzes why users fall for these lures.

The majority of cyberattacks begin with a user clicking on a phishing email. Ever wondor why users continue to fall for phishing emails?

According to a new report from PhishMe that found that 91% of cyberattacks start with a phish, the top reasons people are duped by phishing emails are curiosity (13.7%), fear (13.4%), and urgency (13.2%), followed by reward/recognition, social, entertainment, and opportunity.

"Fear and urgency are a normal part of every day work for many users," says Aaron Higbee, co-founder and CTO of PhishMe. "Most employees are conscientious about losing their jobs due to poor performance and are often driven by deadlines, which leads them to be more susceptible to phishing."

Higbee says PhishMe based the study on more than 40 million simulation emails by about 1,000 of its customers around the world. The study took place over an 18-month span from January 2015 through July 2016.



CISA
CYBER+INFRASTRUCTURE

PHISHING IS THE MAIN ATTACK VECTOR FOR RANSOMWARE!

What is Ransomware?

- Ransomware is malware that is designed to deny access to a computer system or data until a ransom is paid.
- It is spread by phishing emails or clicking on an infected website.
- The goal of ransomware is for cybercriminals to obtain valuable data from an individual or an organization.
- A user is typically notified with a message on the screen that tells them they've been infected.
- Anyone with data stored on their computer is at risk.

CISA
CYBER+INFRASTRUCTURE

How Can Ransomware Affect You?

- Cybercriminals may be able to gain your personal, sensitive information stored on your device including saved passwords, important documents, photos, financial information, etc.
- You may be blocked from using your computer, network and files.
- Your data is at risk of being destroyed.
- CISA does not recommend paying a ransom since there is no guarantee you will ever get your data back.

CISA
CYBER+INFRASTRUCTURE

How Can Ransomware Affect Your Organization?

- The organization could temporarily or permanently lose corporate data.
- You may be blocked from using your computer, network and file access.
  - This results in interference of your organization's operations.
- The organization may face financial loss and may also experience severe legal penalties if protected information is stolen.
- The organization faces a damaged reputation.

CISA
CYBER+INFRASTRUCTURE

How to Respond If You've Been Affected

- **Report it** immediately:
  - If you're a part of an organization, be sure to report the issue to the proper Points of Contact.
  - Contact the FBI, MS-ISAC – and me!
- Prevent the spread of the infection by isolating the infected computers and systems.
- Try to identify the type of ransomware to help understand what you are working with.
- Work with cybersecurity professionals who are trained in resolving these issues.
- Recover your data from your backups **after** you test the backups to ensure the data on the backups is safe to restore.

CISA
CYBER+INFRASTRUCTURE

CYBER HYGIENE AND BEST PRACTICES

Cyber Hygiene & Best Practices

- Review Cybersecurity Frameworks & Controls – NIST, CIS Controls, etc.
- Develop and implement Information Security Policies
- Develop an Information Security Strategic Plan and Architecture
- Inventory Assets -identify what is critical and protect accordingly
- Implement multi-factor authentication
- Segment critical data

CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene & Best Practices

- Conduct Security Awareness training on a regular basis for all staff & management
- Conduct Phishing exercises on a regular basis -review metrics*
- Create an incident response plan and exercise it regularly*
- Do due diligence on third parties & vendors and regularly review access
- Review/control admin. privileges
- Evaluate cyber security insurance
- * CISA service

CISA
CYBER+INFRASTRUCTURE

For Your Remote Users

- Do not use public Wi-Fi
- Utilize VPN (virtual private network)
- Cover the camera on laptops and tablets
- Segregate personal and work information

CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene & Best Practices

- Keep software and operating systems up to date
- Implement patches as soon as possible
- Install software to scan for viruses/malware/vulnerabilities
- Schedule regular assessments*
- (scans, pen tests, etc.)
- Install a tracker to locate lost devices
- * CISA service

CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene & Best Practices

- Install a program/app that can remotely lock or wipe lost devices
- Implement encryption - servers, backups, devices, documents, etc.
- Ensure backup is not connected to your system and maintain backup files in a secure offsite location

- Click to add text

CISA
CYBER+INFRASTRUCTURE

Additional Information Sharing Opportunities

- Multi-State Information Sharing and Analysis Center
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

- ISACs and ISAOs
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

CISA
CYBER+INFRASTRUCTURE

Contact Information

CSA Contact Information

Theresa A. Masse

Cyber Security Advisor, Region 10 (Oregon)
Cybersecurity Infrastructure Security Agency
U.S. Department of Homeland Security

Email: theresa.masse@cisa.dhs.gov
Mobile: (503) 930-5671

CISA
CYBER+INFRASTRUCTURE

Questions?

CPE Replacement List 2021 Target List

Issued NTE Draft for CPE Replacement – Astoria / Seaside, Umatilla, Warm Springs, Douglas County, Milton-Freewater, Lincoln City/ Toledo

Waiting for first quote draft – Columbia, Grant County, Josephine County

CPE Replacement List 2022 Target List

Issued NTE Draft for CPE Replacement – Tillamook, Morrow County, Brookings Police, METCOM, Coos County, Coos Bay, Union County, Wallowa County, Burns Police, Wasco County, Curry County, Hood River, Deschutes, YCOM

Questions?

Additional Information:

OEM, State 9-1-1 Program Contact:

Frank Kuchta, State 9-1-1 Program Manager
frank.kuchta@state.or.us
503-378-4620