PRESENTATION TO EENA: CISA AND CYBER THREATS TO USA 9-1-1

JAMES JARVIS, CISA EMERGENCY COMMUNICATIONS COORDINATOR
RICHARD TENNEY, SR. ADVISOR, CISA EMERGENCY COMMUNICATIONS DIVISION

Overview

- **Changes to technology**
- **Vulnerabilities**
- **What we are we doing about it**

Emergency Information Landscape

Governmental Agencies
(Federal, State, Local, Tribal, Territorial)

Incident Response and Coordination

Governmental Agencies
(Federal, State, Local, Tribal, Territorial)

Emergency Information Flow

Notifications, Alerts & Warnings

Reporting, & Requests for Assistance

Public, NGOs, Private Sector

Public Information Exchange

Public, NGOs, Private Sector

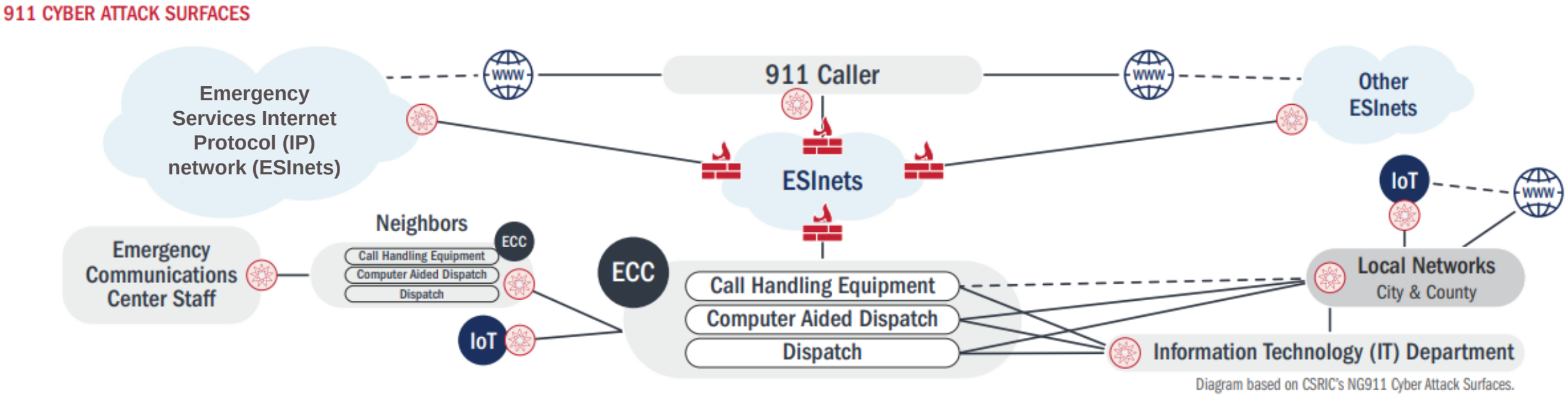
How PSAP Technology Has Changed

- Dispatch/PSAP technology used to be simple telephones and radios that presented almost no cybersecurity risk.
- Greater convergence towards IP based voice and data interoperability.

Risk Level Increases With the Next Generation

- **NG Architecture is different from traditional systems:**
  - Requires standardized identity management and credentialing across systems
  - Introduces new attack vectors
  - May provide for distributed attacks with reliance on IP protocols across geographic areas

NG Attack Surfaces



Risks to NG Systems Components

User and Devices	Network Infrastructure and Connections	Data, Applications and Services
▪ Data Breaches ▪ Insider Threats ▪ Malware ▪ Ransomware ▪ Spear-Phishing ▪ Spoofing	▪ Denial-of-Service Attack ▪ Man-in-the-Middle Attack ▪ Telephony-Denial-of-Service Attack ▪ Unauthorized Network Access	▪ Malicious Applications ▪ Swatting ▪ Unauthorized Data Access ▪ Ransomware Encryption ▪ Ransomware Exfiltration ▪ Denial-of-Service

Cyberattacks on USA 911 Functions

DIAMOND IT

IT Services Industries About DiamondIT Resource

911 Attacks on Cities Nationwide Bring the Ransomware Threat Home

CYBERSECURITY

DHS: 911 call centers vulnerable to cyberattack

BY ELISE VIEBECK - 05/08/15 11:24 AM ET

SHARE TWE

Emergency call centers around the country are vulnerable to cyberattacks, including denial-of-service assaults that could shut down 911 networks, a division of the Department of Homeland Security (DHS) warned.

The threat is an increasing source of concern for 911 operators, law enforcement officials and their representatives in Washington.

{mosads}Virtually no enterprise is safe from hackers, but the idea that online vandals could tamper with emergency call systems is worrying as a matter of basic public safety, officials said.

"News reports of successful government website hacks appeared frequently over the past year, with several activist groups openly targeting cities and local government for political reasons," an alert from the U.S. Fire Administration said Thursday.

× Close Ad

NEWS Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?

U.S. NEWS

Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?

America's emergency-response networks remain dangerously vulnerable to criminals bent on crippling the country's critical infrastructure.

A dispatch call center in Washington, D.C. on January 12, 2016. Marvin Joseph / The Washington Post/Getty Images file

SAVE Create your free profile or log in to save this article

3, 2018, 8:38 AM EDT / Updated April 3, 2018, 8:38 AM EDT

n Schuppe

Sponsored Stories by Taboola

Public Safety Attacks in USA

Twin Falls County, ID
August 11, 2021*

Curry County, OR
April 26, 2023

Grass Valley, NV
June 29, 2021

Sebastopol, CA
July 14, 2021

Clearfield, UT
July 11, 2021

Northern District of TX
March 2019 – August 2021

Quincy, IL
May 7, 2022

Tulsa, OK
May 11, 2021*

Clark County, OH
May 26, 2021*

Dallas, TX
May 1, 2023

Presque Isle, ME
April 28, 2022

Berkeley, MO
April 13, 2021

New Bedford, MA
January 27, 2022

Quincy, MA
February 8, 2022

Lowell, MA
April 25, 2023

Plainfield, CT
March 2022

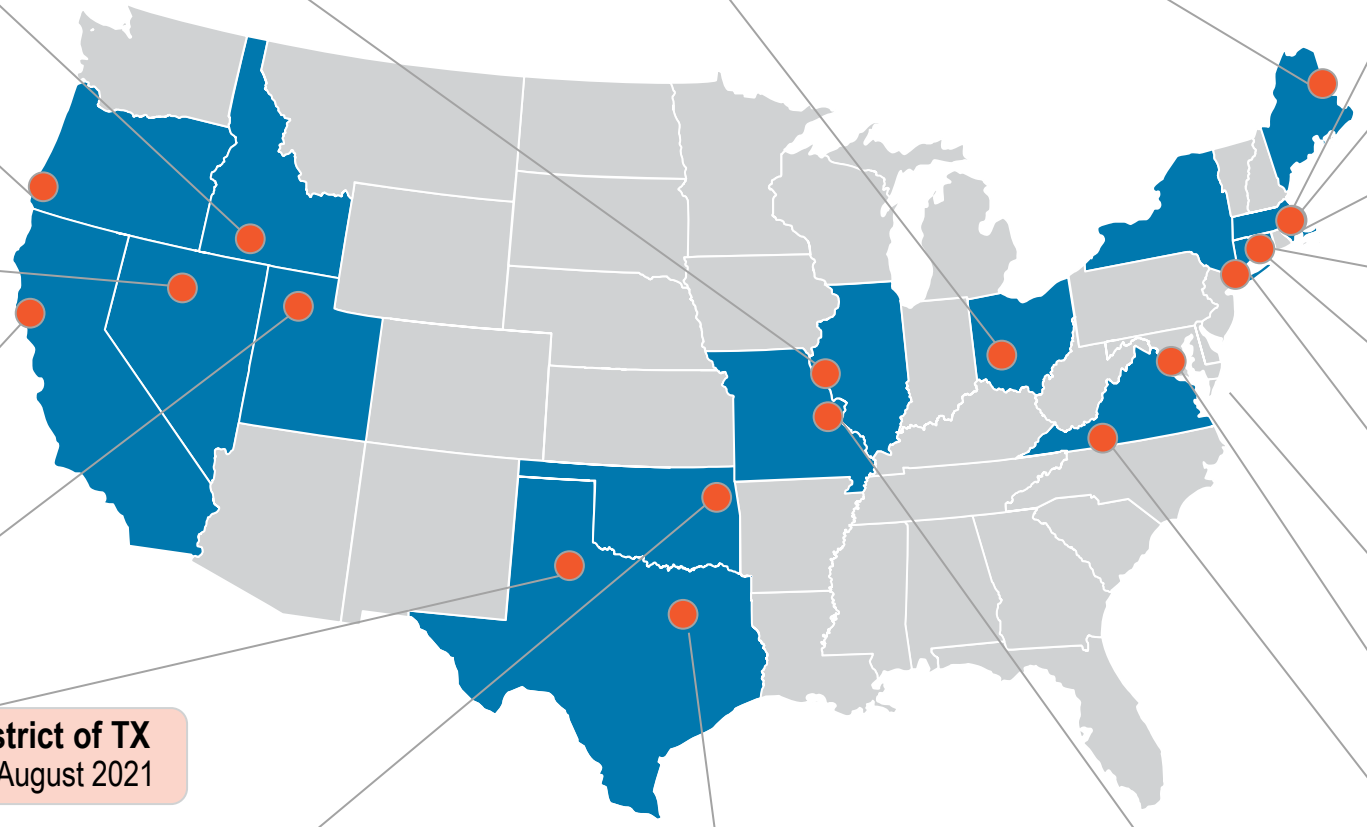
Clearfield, CT
July 20, 2021

Suffolk County, NY
September 8, 2022

New York, NY
June 2021

Washington DC
April 2021

Bristol County, VA
July 27, 2021



*Open source information; Managed service provider attack

Attackers' Motives

Disruption

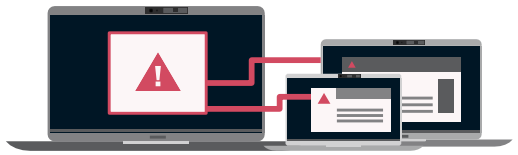
Cyberattacks may shut down public access to PSAPs, leading to public confusion and disrupting the dispatch of First Responders

Ransom

As the networks, data and services are vital to public safety, PSAPs are more likely to pay a Bitcoin ransom in order to restore service

Lack of Defenses

PSAPs, municipalities, may not have a strong cyber defense system – especially when compared to other targets



Collateral Damage

Victim of Lateral Attack (IT Services Providers)

Lessons Learned from Attacks

People

- Educate staff on cyber threats and how to prevent them
- Identify staff with knowledge of system and network architecture
- Collaborate with neighboring jurisdictions to provide back-up call capabilities
- Coordinate with service providers when developing cyber response plans

Process

- Ensure operating systems and data are backed up regularly
- Review policies and procedures
- Keep a detailed record of attacks for incident reporting

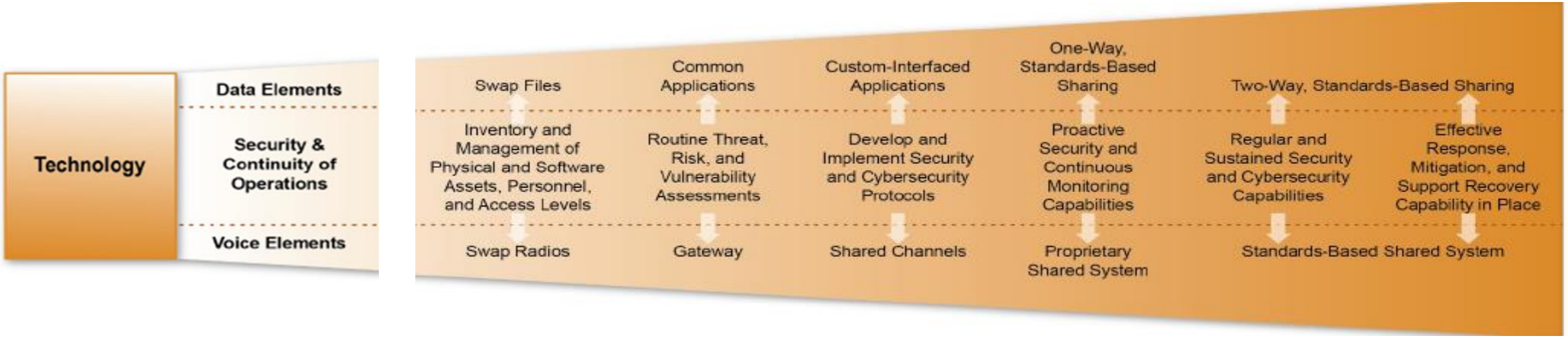
Technology

- Ensure networks are separated and critical operations are on a closed network
- Implement strong passwords and two-factor authentication
- Disable use of universal serial bus (USB) ports
- Include ten-digit lines when implementing security capabilities
- Implement call authentication and threat detection tools

NG Cybersecurity Defense

- **PSAP cybersecurity requires defending attack surfaces:**
  - Emergency Call Handling
  - Computer Aided Dispatch (CAD)
  - Radio
  - Records
  - Critical Systems – Audio/Video

Interoperability Continuum



- Inventory and Management of Physical and Software Assets, Personnel, and Access Levels
- Routine Threat, Risk, and Vulnerability Assessments
- Develop and Implement Security and Cybersecurity Protocols
- Proactive Security and Continuous Monitoring Capabilities
- Regular and Sustained Security and Cybersecurity Capabilities
- Effective Response, Mitigation, and Support Recovery Capability in

Practical Defensive Considerations

- Consider tabletop and functional exercises
- Education and awareness of staff
- Know key points of contact – law enforcement, and threat assessment centers
- Consider who has the authority to “turn off” 911
- Maintain audit logs
- Perform third-party cybersecurity evaluations

Other Considerations:

- What vulnerabilities exist in my network?
- Is my organization protected from evolving cyber threats?
- Am I meeting the basic requirements for compliance?
- Do my employees have the know-how to identify and mitigate threats?

Continuity of Operations (COOP) Plan

COOP plans can help ensure the continuity of critical services during a cyber disruption event.

CONSIDERATIONS FOR ESTABLISHING/UPDATING COOP PLANS

- Collaborate with personnel, information technology, stakeholders, and partners to identify alternate emergency communications centers
- Establish protocols for maintaining data
- Engage with partners and stakeholders
- Address cybersecurity risks to NG systems
- Establish a COOP planning cycle

Best Practices – Your Vendor and Remote Access

- Zero Trust – concept of trust, but verify
- Vendors typically “require” remote access to your call handling and other ECC systems, but is that really just for their convenience?
- Perform audits of logs which has/had access to your system
- Insist network users have unique logins
- Vendors’ handling accounts and credentials upon employee transition event (termination, resignation, promotion, etc.)
- Network segmentation

Cybersecurity Resources for Public Safety

Find additional cybersecurity resources specifically for public safety at: cisa.gov/public-safety-cybersecurity

- *Two Things Every 911 Center Should Do to Improve Cybersecurity*
- *Cyber Risks to 911: Telephony Denial of Service*
- *Guide to Getting Started with a Cybersecurity Risk Assessment*
- *"First 48": What to Expect When a Cyber Incident Occurs*
- *Interoperable Communications Technical Assistance Program Service Offerings Guide*
- *Considerations for Cyber Disruption in an Evolving 911 Environment*

Questions

For more information:
www.cisa.gov

Questions?

Email: James.Jarvis@cisa.dhs.gov
Richard.Tenney@cisa.dhs.gov

Phone: +1 202-834-0631
+1 202-422-2668

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Back up Slides

SAFECOM Interoperability Continuum 2.0

A Tool For Improving Emergency Response Communications and Interoperability