APCO International

Leaders in Public Safety Communications®

APCO International

Emerging Technology Forum

Securing Emergency Communications Networks

Cybersecurity Assessment and Planning

Jay English
Chief Technology Officer
APCO International

APCO International
Emerging Technology Forum

Topics

- Overview – Cybersecurity Risk
  - Threat Landscape
  - Sector Specific Risk Briefings
- Cybersecurity Options for Consideration
  - The Future
  - The EC3
- What you can do now to improve your cyber posture
  - Training
  - Password and Physical Security
  - Vendor Management and cooperation (hint – it's a two way street…)

Overview

- As we transition to IP-based architectures across government, we will face increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy environment.
- Existing work including the NIST Cybersecurity Framework, the ongoing work of CSRIC and the FCC, the FCC TFOPA reports, along with other foundational documents, can assist in cyber risk management strategies for the ecosystem as a whole
- Cyber risk management strategies must be implemented at multiple levels from core services to the local level.

What is Cybersecurity?

- The protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
- Safeguarding computer systems, as well as the data contained within, and maintaining:
  - Confidentiality
  - Integrity
  - Availability

Key Definitions

- Computer Network Exploitation: Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks. ***SOURCE: CNSSI-4009*** [1]
- Cyber Attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. ***SOURCE: CNSSI-4009*** [1]
- Risk Assessment: In this presentation, defined as a qualitative judgment of risk based on an analyst's synthesis and interpretation of limited information.

1 - Committee for National Security Systems Instruction 4009 (CNSSI-4009)

The Threat

- Advanced technologies are becoming more integrated into government communications networks
- New and emerging cyber risks are an increasing concern
- Many initiatives to mitigate and combat these risks are underway in both the public and private sectors to keep these systems safe and secure

The Threat

- **Destruction:** Physical destruction of information or communications systems rendering them unusable
- **Corruption:** The changing of information such that it is no longer accurate or useful
- **Removal:** The removing of information so that it cannot be accessed, but is not destroyed
- **Disclosure:** Unauthorized release of confidential or sensitive information to the detriment of owner of said data
- **Interruption:** Interfering with communications such that legitimate users cannot send or receive messages

Cyber Threat Sources

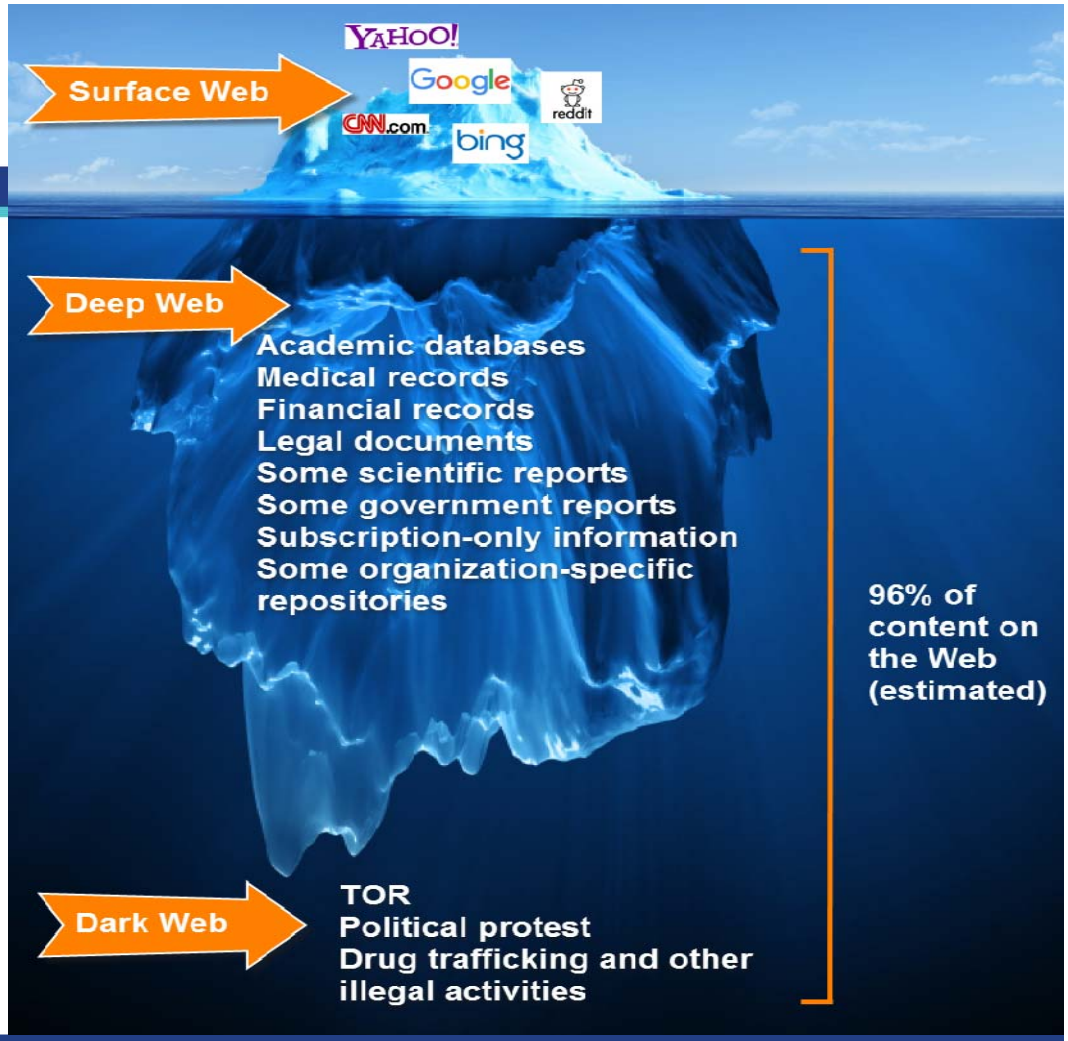
- Various factors can compromise the confidentiality, integrity, or availability of systems or data:
  - Natural disasters
  - Environmental issues
  - Technical or mechanical failure
  - Human error
  - Malicious actors

Cyber Threat Landscape

- **Cyber Threat Actors**
  - State Sponsored
  - Terrorist/Violent Extremists
  - Insider Threat
  - Hackers
  - Hacktivists
  - Criminals / Organized Crime

2018 This Is What Happens In An Internet Minute

The Deep Web & Dark Web



The Deep Web & Dark Web

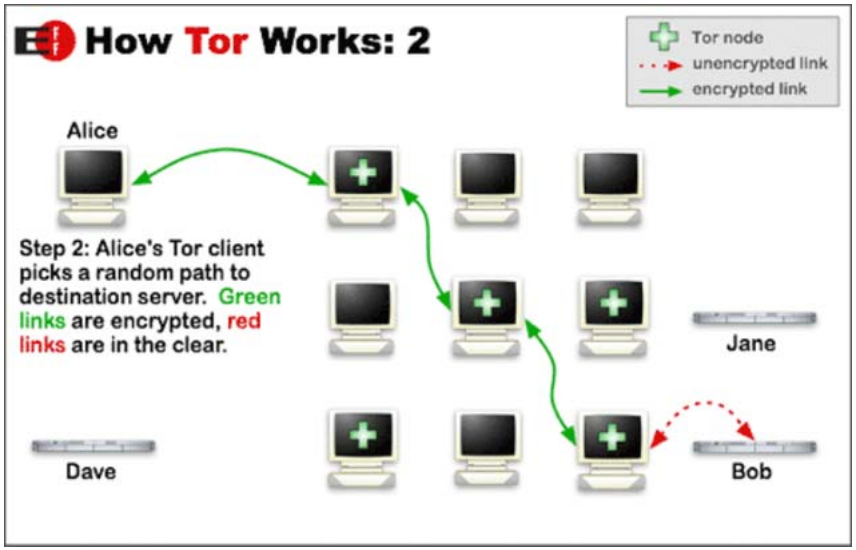
- The dark web is the World Wide Web content that exists on darknets, overlay networks which use the Internet but require specific software, configurations or authorization to access.
- The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web.
- The darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Tor, Freenet, and I2P, operated by public organizations and individuals.
- Users of the dark web refer to the regular web as Clearnet due to its unencrypted nature.
- The Tor dark web may be referred to as onionland, a reference to the network's top-level domain suffix .onion and the traffic anonymization technique of onion routing. [2]

2 https://en.wikipedia.org/wiki/Dark_web

The Onion Router

Tor is short for "The Onion Router." This refers both to the software that you install on your computer to run Tor and the network of computers that manages Tor connections.

Put simply, Tor enables you to route web traffic through several other computers in the Tor network so that the party on the other end of the connection can't trace the traffic back to you. That way, the more Tor users there are, the more protected your info. As the name implies, it creates a number of layers that conceal your identity from the rest of the world. [3]



3 https://gizmodo.com/tor-the-anonymous-internet-and-if-its-right-for-you-1222400823

Cyber Threat Trends

- Threats are increasing:
  - Hacking tools are more readily available and simpler to use
  - The potential impact of cyber attacks continues to grow
- Hacker motivation is changing:
  - No longer egocentric, hobbyist hackers seeking entertainment and internet status
  - Shift to professional cyber criminals motivated by money whose success relies on remaining undetected
- Certain factors are enabling threat actor success:
  - Economy of organized cybercrime
  - Inter-connected systems
  - Widespread organizational failure to implement cyber hygiene

Top 5 Threat Attack Vectors

- (Spear)Phishing
  - Work and personal email
- Web Browsers
  - Vulnerability exploitation
  - Unpatched browsers
- Web Servers
  - Unpatched systems and applications
- Remote Access
  - Single factor (password-based)
- Point-of-Sale
  - Exploited credit card machines

Cyber Incidents – Public Safety

- Ransomware Maine, Arkansas, Tennessee Law Enforcement agencies
  - Multiple Health Care facilities worldwide
  - OH PSAP / County
  - DC CCTV
  - Law Enforcement and Medical are prime targets to due nature of records
- TDoS
  - 300+ TDoS vs Public Safety (9-1-1, Law Enforcement, Fire, EMS, Emergency Management)
  - 12 State TDoS event
- Swatting
  - Known incidents Nationwide
  - COTS products
  - Impact expanding – Recent fatal shooting is example of risk
- Jamming / Interference
  - Known incidents Nationwide
  - COTS products
  - Impact can be minor to severe (TX, OK, HI)

APCO International
Emerging Technology Forum

Sector Specific Risks & Consequences

APCO International
Emerging Technology Forum

Sector Specific Risk

- Health Care
- Energy
- Public Safety

APCO International
Emerging Technology Forum

Healthcare and Public Health

System considerations

- The expansion of connected medical devices over the next three to four years will result in an expanded attack surface for malicious cyber attacks
- Cybersecurity challenges include continued use of legacy systems, retention and recruitment of cybersecurity professionals, information sharing among public and private entities, and lack of cybersecurity within medical devices
- Criminal and nation-state actors use malware to exfiltrate personally identifiable information (PII), protected health information, and intellectual property data from healthcare companies for illicit financial gain, stock manipulation, or industrial espionage

Potential Consequences

- Electronic Health Records (EHRs) attain a high value on the black market, often 10 to 20 times more than the price of a stolen credit card. This value will encourage future attacks. EHR data can be used to create false identities that criminals can use to open credit card accounts and file false medical claims.
- Cyber actors are increasingly using malicious software known as ransomware to prevent victims from accessing their data. These cyber actors achieve this by encrypting victim information, providing the decryption key only until after the ransom is paid, typically in Bitcoin.

Risk Assessment: Healthcare and Public Health Sector has a moderate to high risk of attacks by a variety of cyber actors (criminal, non-state, and state actors), primarily for criminal financial gain and industrial espionage (theft or alteration of sensitive proprietary data).

Electric Power

System considerations

- The U.S. electrical grids' protection and coordination systems are complex, heterogeneous, and robust, making a successful cyber attack, leading to catastrophic damage across the grid, extremely unlikely
- A cyber attack aimed at causing widespread failure of one or multiple interconnections of the U.S. electrical grid would be a complicated, expensive, and resource-intensive undertaking

Potential Consequences

- Idaho National Labs, conducted a computer simulation of cyber attacks on tap changers within transmission substation components which indicated:
  - Transmission lines experiencing amperage increases in excess of their rated limits when transformer voltages were increased and decreased in parallel
  - Increase in amperage through the lines, coupled with the rating limits of the lines, suggests that maintaining tap changes for extended periods could damage the lines and transformers
  - Unmanned configuration of transmission substations combined with a remote cyber attack designed to perform the tap changes as well as send erroneous substation information to grid operators could result in substation equipment damage; however physical safeguards are in place on most substations.

Risk Assessment: The overall risk to the Electric Power Sub-Sector from computer network attack is low, but high for exploitation/reconnaissance. A successful cyber attack leading to catastrophic damage across the U.S. electrical grid is extremely unlikely. A cyber attack aimed at causing widespread failure of one or multiple interconnections of the U.S. electrical grid would be a complicated, expensive, and resource-intensive undertaking. Changes in Geopolitical climate may increase or reduce risk.

APCO International
Emerging Technology Forum

Public Safety Communications

System considerations

- The introduction of IP based, Next Generation 9-1-1 (NG911) will result in an expansion of connected devices capable of contacting 9-1-1, creating an expanded attack surface for cyber attacks
- Cybersecurity challenges include continued use of legacy systems, retention and recruitment of cybersecurity professionals, information sharing among public and private entities, and lack of cybersecurity within multiple network elements and devices
- Criminal and nation-state actors use malware to exfiltrate information of a law enforcement sensitive nature, including ongoing investigations and details about criminal enterprises and live response data

Potential Consequences

- CJIS and HIPAA sensitive data could be compromised and used for nefarious purposes. This data can be used to compromise investigations, mislead public safety agencies during responses, and identify public safety personnel. Additionally, compromise may occur at multiple levels (Law Enforcement, Fire/Rescue and Medical) impacting multiple stakeholders simultaneously
- Cyber actors are increasingly using malicious software known as ransomware to prevent victims from accessing their data. These cyber actors achieve this by encrypting victim information, providing the decryption key only until after the ransom is paid, typically in Bitcoin. Attacks of this nature have occurred against public safety

Risk Assessment: Public Safety Communications has a moderate to high risk of attacks by a variety of cyber actors (criminal, non-state, and state actors), with a variety of motivations from financial gain to compromise of emergency response during a major event

APCO International
Emerging Technology Forum

Cybersecurity : Options and Actions

Cyber Strategy

- The reduction of any cybersecurity framework to practice is rooted in the ability to identify assets, owners of these assets, threats/risks to these assets, and methods to mitigate the threats/risks.

APCO International
Emerging Technology Forum

Cyber Strategy

Best Practices

- NIST Cybersecurity Framework (NCF)
- Identity Credentialing Access Management (ICAM)
- DHS recommendations and resources
- NICE Workforce Framework
- TFOPA Reports
- P43 Report

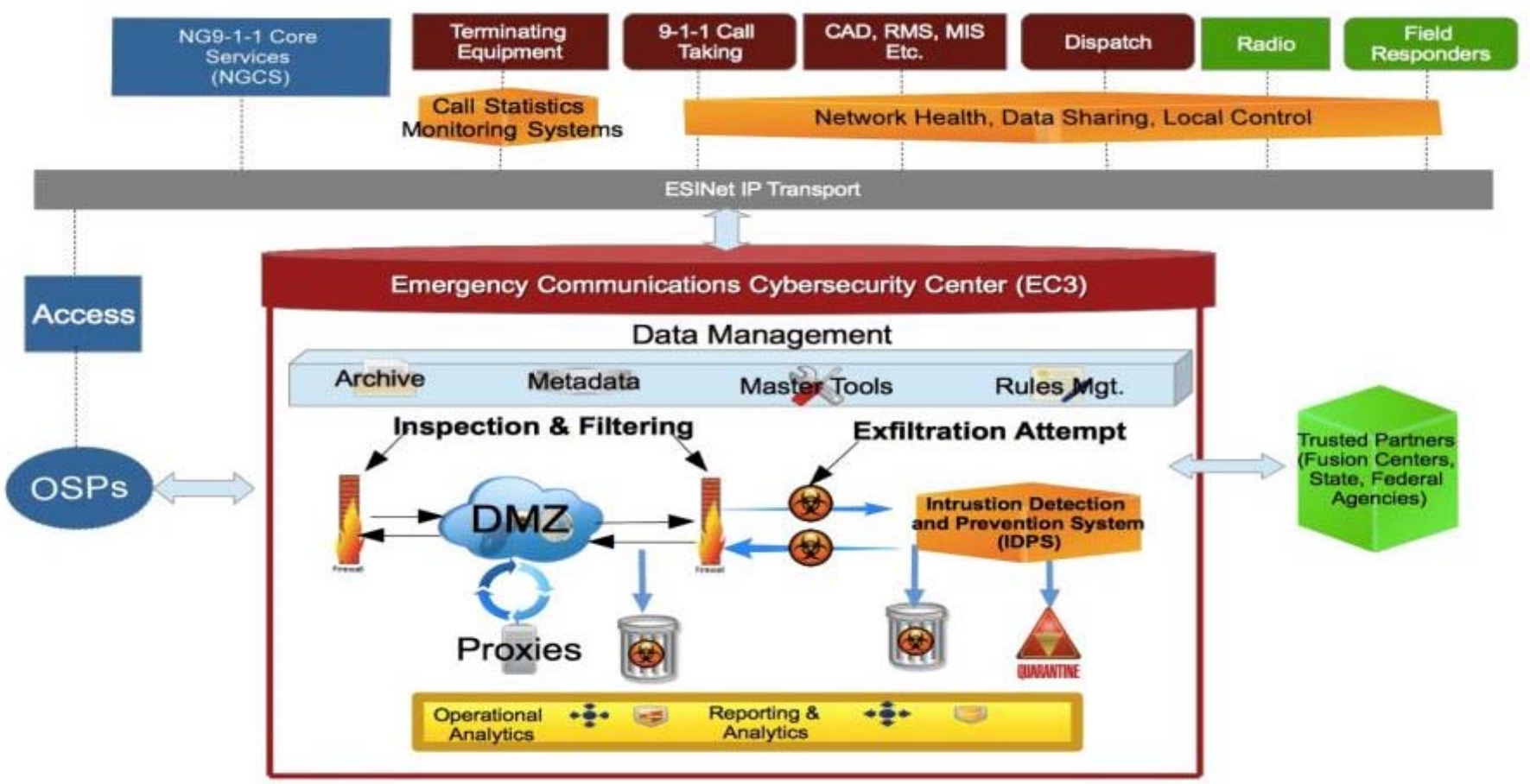
Cybersecurity Resources

- U.S. Department of Commerce
  - NIST: Cybersecurity Framework
  - NIST: Cyber Physical Systems- Public Work Group Report
    - Relationship To PSAPs: Identify, Protect, Detect, Respond, Recover
  - NICE Workforce Framework
    - Relationship of occupational specialties to PSAPs
    - Define any new/missing occupational specialties
    - Consider Cyber Professional Best Practices for PSAP workforce

Cybersecurity Resources

- Department of Homeland Security
  - Critical Infrastructure Cyber Community Voluntary Program (C3VP)
  - Critical Infrastructure Cyber Information Sharing and Collaboration Program (CISCP)
  - Cyber Reports & Recommendations
  - Cybersecurity Products & Solutions:
  - National Cybersecurity and Communications Integration Center (NCCIC)
    - NCCIC/National Coordinating Center for Communications (NCC)
    - NCCIC/United States Computer Emergency Readiness Team (US-CERT)

Emergency Communications Cybersecurity Center



APCO International
Emerging Technology Forum

Cybersecurity : What you can do now

APCO International
Emerging Technology Forum

The Approach

APCO International
Emerging Technology Forum

The Approach

The Approach

- ***Aviate***
- ***Navigate***
- ***Communicate***
- ***Mitigate***

Fly the Aircraft First

- NTSB accident data suggest that pilots, while distracted by less essential taskings, have lost control of their aircraft and crashed.
- In light of this pilots are reminded to maintain aircraft control at all times. This may mean a delay in responding to ATC communications and passenger requests, or not responding at all unless positive aircraft control can be maintained throughout.
- In other words, ***Fly the Aircraft First!***
- From the earliest days of flight training, pilots are taught an important set of priorities that should follow them through their entire flying career: Aviate, Navigate, and Communicate. The top priority — always — is to aviate. That means fly the airplane first!
- ***Cybersecurity is very similar for Public Safety***

The Approach

The 4R's

- In addition to discussions that identify the threats already known, and available mitigation strategies, focus should be placed on procedures to ***Respond, Remediate, Restore and Resolve ("the 4R's).***
- A realistic self assessment for government entities and agencies to evaluate their current cybersecurity capabilities and risks.
- A roadmap for the creation and implementation of a successful Cybersecurity strategy that applies to local public safety levels of government, up to and including State level government.
- Cyber risk mitigation strategies for interconnectivity with potential federal level resources and capabilities.

The Approach

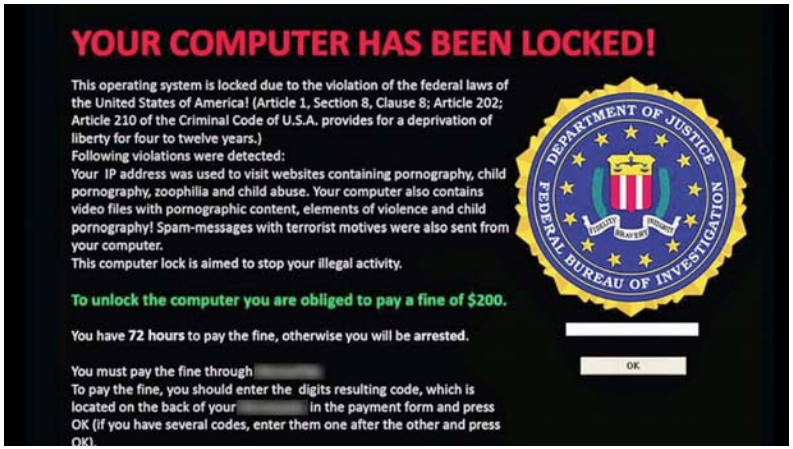
- "123456" is NOT a password, neither is "BobsComputer"….just saying….
  - A password shared is access gained
- Encryption….know it, use it, love it….but back everything up just in case…

The Approach

- The door is locked, but is the network?
  - I know I put that thumb drive somewhere…..
  - There's an app for that…..
  - But I only went to that website once…..

The Approach

Well we don't use the "Internet" ....



Neither did they .....

The Approach

- Not only the physical elements of cybersecurity should be addressed. As noted in much of the work already done by NIST and DHS, the human factor is vital when preparing for and defending against cyber threats.

- Personnel security including cyber hygiene, training, and other mitigation steps related directly to the personnel involved with day to day operations and maintenance of any public safety system is key.

Next Steps

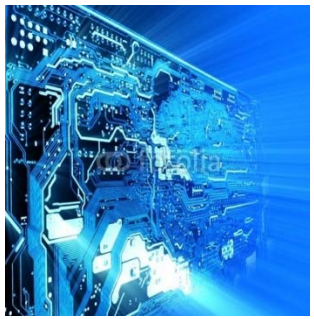
- Forward looking issues must be examined to expand the context of the threat to the public safety communications as a result of the expansion of the public safety ecosystem
- This must include additional information sources and new “players” such as FirstNet, Health care providers, public safety “Apps”, and other entities that reflect the emergence of new technologies.
- Self assessment of current capabilities, initiation of training, and incorporation of cybersecurity into all new architectures is critical to success.

Next Steps

- Establish a structured response tree with your vendors in the event of any cyber incident
- “We’ve got you covered” is not an adequate answer. You have a right to know what that means. Ask.
- Communication must be a two way street. They will ask for a lot of information about your networks and systems. You should ask for the same about theirs.
- Build a good relationship with service providers, know who to call, don’t be afraid to be proactive. When you get a cyber bulletin, be sure they get it to, and follow up to ensure your networks, and systems, are protected.

APCO International
Emerging Technology Forum

Cybersecurity is a threat – but it's a threat we can mitigate.



***Be Prepared *Be Proactive *Be Engaged**

QUESTIONS?