APCO International
Emerging Technology Forum

Securing Public Safety Networks

Cybersecurity Assessment and Planning for Emergency Communications

Gerald “Jay” English, ENP
Public Safety Program Manager
US Dept. of Homeland Security
National Cybersecurity & Communications Integration Center
National Coordinating Center for Communications

Topics

- Overview
- Threat Landscape
- The Path Forward

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 recently concluded 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

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

- Emergency communications increasingly rely on broadband systems and cyber technologies, and this reliance will grow significantly with the emergence of the Nationwide Public Safety Broadband Network (NPSBN).
- From the FCC Whitepaper titled – Cybersecurity Risk Reduction (18 JAN 17):
  - "The digitized and interconnected nature of communications now makes the nation's communications backbone susceptible to new and proliferating global threats and hazards. A focused attack, cyber or physical, on core communications infrastructure could prevent the conveyance of the nation's most critical and time sensitive communications." [1]

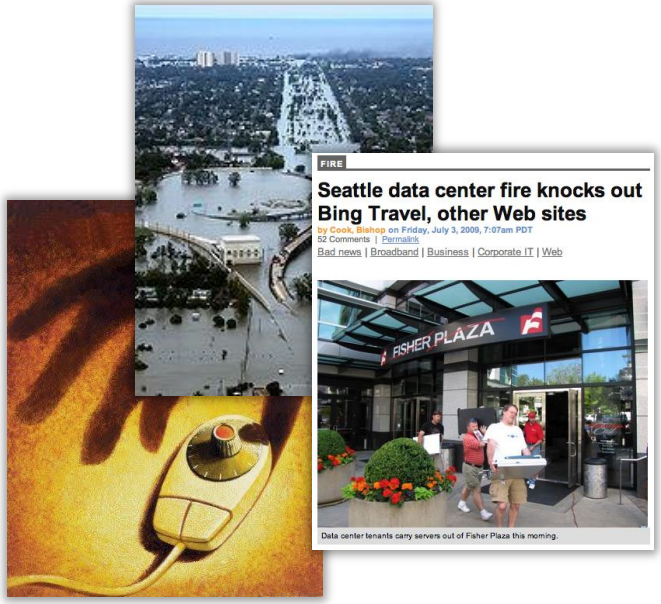
•1- http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0118/DOC-343096A1.pdf

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



The Human Threat

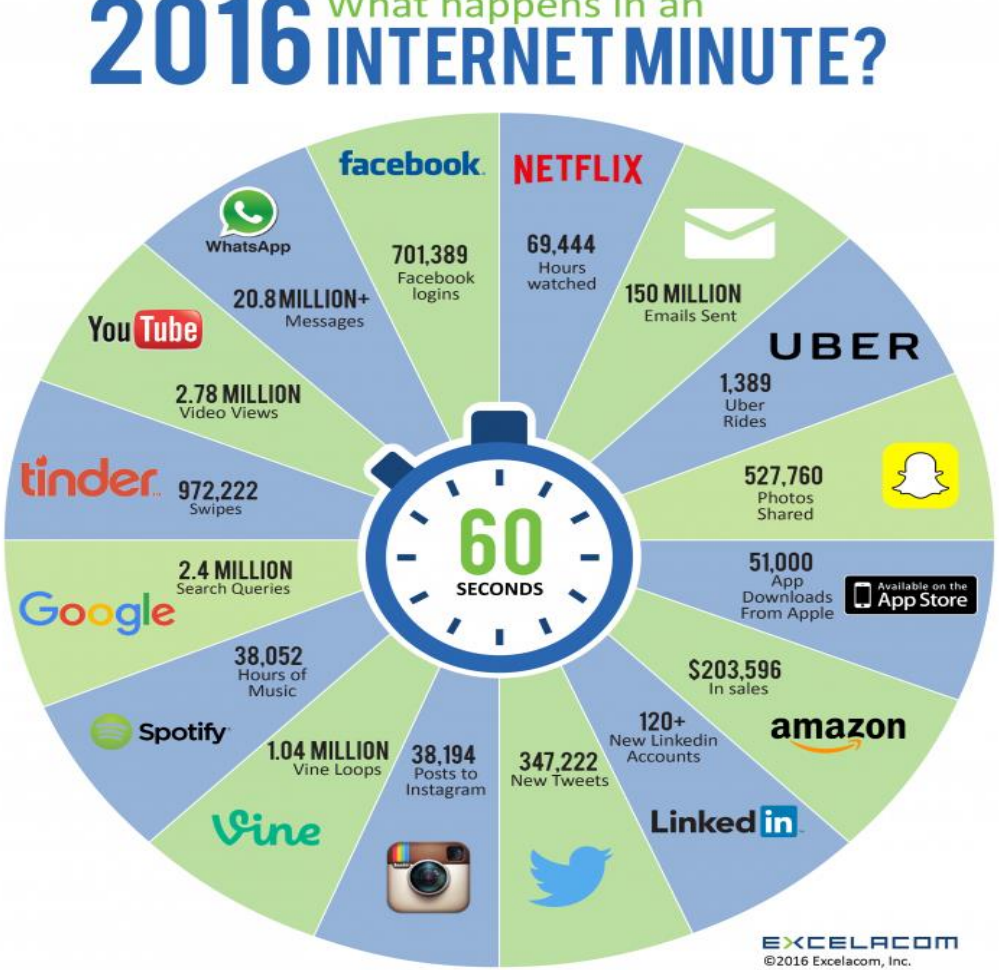
- Threat Actors
  - Criminals
  - Nation-states
  - Hacktivists
- Insider Threat
  - Unintentional
  - Malicious

Source: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

Cyber Threat Landscape

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

I only looked away for a minute....



Cyber Threat Trends

- **ENORMOUS** increase in Cyber Attacks/Crime both in numbers and sophistication.
  - State sponsored attacks likely to increase. (Cyber Warfare is real now.)
  - CYBER CRIME as a SERVICE
  - Cyber-weapon toolkits

Cyber Threat Trends

Nation-States That Have Declared Offensive Cyber Capability

- Iran
- India
- UK
- China
- Russia
- U.S.A.
- Australia
- Italy
- France
- Syria
- Germany
- Israel

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

Threat actors are using multiple techniques:

- (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

Well-Known Cyber Incidents

OPM Data Breach

- At first OPM thought that over 4 million people were affected by the breach, but further investigation suggested a much larger number
- OPM has concluded that over 22 million people had their personal information stolen from security clearance applications
- The Data Breach is a major concern for U.S national security

Insider Trading via Hacking

- Dozens of stock traders in the U.S would send overseas hackers a list of corporate news releases they wanted the hackers to obtain before the information went public
- 32 traders and hackers profited over $100 million from illegal insider trading
- For example a former hedge fund manger and Morgan Stanley employee in Philadelphia made an illegal $17 million
- 9 people were charged with insider trading

Anthem Data Breach

- On January 29, 2015, Anthem, Inc. Discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Anthem's IT system and obtained personal information
- Up to 80 million customer records were compromised
- Hackers exploited known vulnerabilities in the target's system
- Anthem believes that the breach occurred over the course of several weeks

Cyber Incidents

Attacks, and more attacks

"Research shows that there were at least 2,928 publicly disclosed attacks in 2016 involving greater than **2.2 billion records** in total.

Sometimes, you know that you're a victim of a data breach…however, as with the recent data breach at Modern Business Solutions (MBS), you may not even be aware that the company exists…" [2]

2- http://www.digitaltrends.com/computing/modern-business-solutions-data-breach/

Cyber Incidents

MBS Attack – October, 2016

"MBS is a company specializing in providing in-house data management and monetization services to other companies. If you're an MBS customer, then you probably don't even know it, and the 58 million stolen database records could belong to just about anyone

At this point, there's some confusion as to the actual number of records that were released. While it's ***at least 58 million*****, it *could be as many as 258*** million based on an analysis of the database involved. While research is ongoing, it's entirely possible that we'll never know exactly how much data was released and who was affected." [3]

3-http://www.digitaltrends.com/computing/modern-business-solutions-data-breach/

Cyber Incidents – Public Safety

- Ransomware (within last 90 days)
  - Maine, Arkansas, Tennessee Law Enforcement agencies
  - California Health Care
  - OH PSAP / County
  - DC CCTV
- 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
- Jamming / Interference
  - Known incidents Nationwide
  - COTS products
  - Impact expanding

Cyber Risk 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

Cybersecurity : Planning for the Future

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.

Cyber Strategy

- NIST Cybersecurity Framework (NCF)
- Identity Credentialing Access Management (ICAM)
- DHS recommendations and resources
- NICE Workforce Framework
- CSRIC Best Practices Related to Public Safety\
- TFOPA Reports

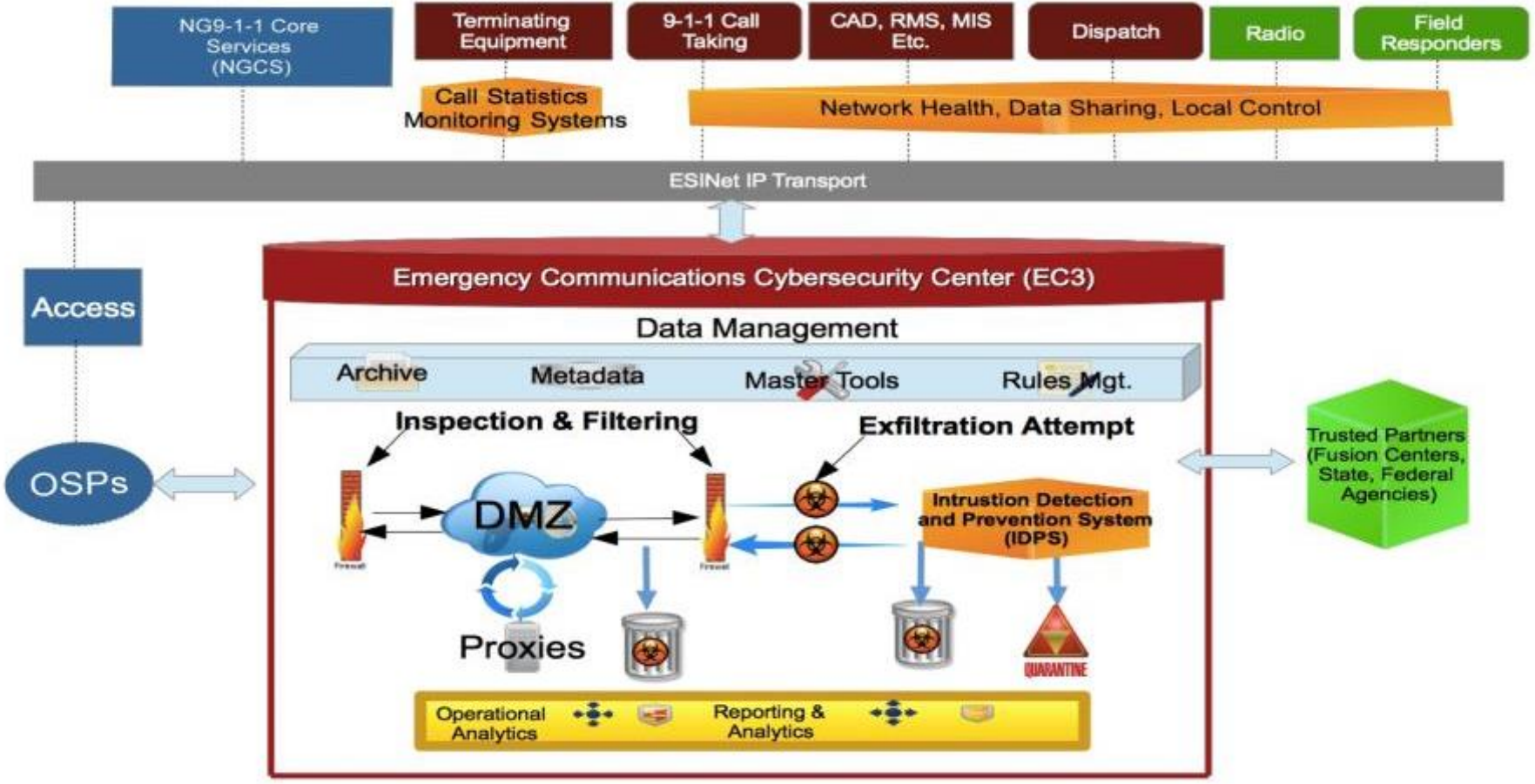
Cybersecurity Resources

- 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



The Approach

- 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.
- 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).

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.

Cybersecurity is a Risk

The security “DNA” of our networks will define our success

QUESTIONS?

Gerald "Jay" English, ENP
Public Safety Program Manager
US Dept. of Homeland Security
National Cybersecurity & Communications Integration Center
National Coordinating Center for Communications

Gerald.English@hq.dhs.gov

703-235-5107

Homeland Security