APCO International Emerging Technology Forum

The Seven Cybersecurity Challenges of ESInet

APCO International
Leaders in Public Safety Communications®

Timothy James Lorello
President & CEO

SECULORE™ SOLUTIONS
Cyber-Protecting Our Nation's Most Important Number: 9-1-1

Thursday, 11/01, 9:45am

SecuLore Solutions: Public Safety/Cyber Expertise

AT&T Bell Laboratories

TCS TeleCommunication Systems
Enabling Convergent Technologies®

Tim Lorello - CEO

- Public Safety NG9-1-1 expert
- Guidance to FCC
- Former CMO (TCS)
- 1+ years public safety
- 7+ years cybersecurity
- 30+ years telecomm
- BA Physics, MSEE
- 20 patents

SECULORE™ SOLUTIONS

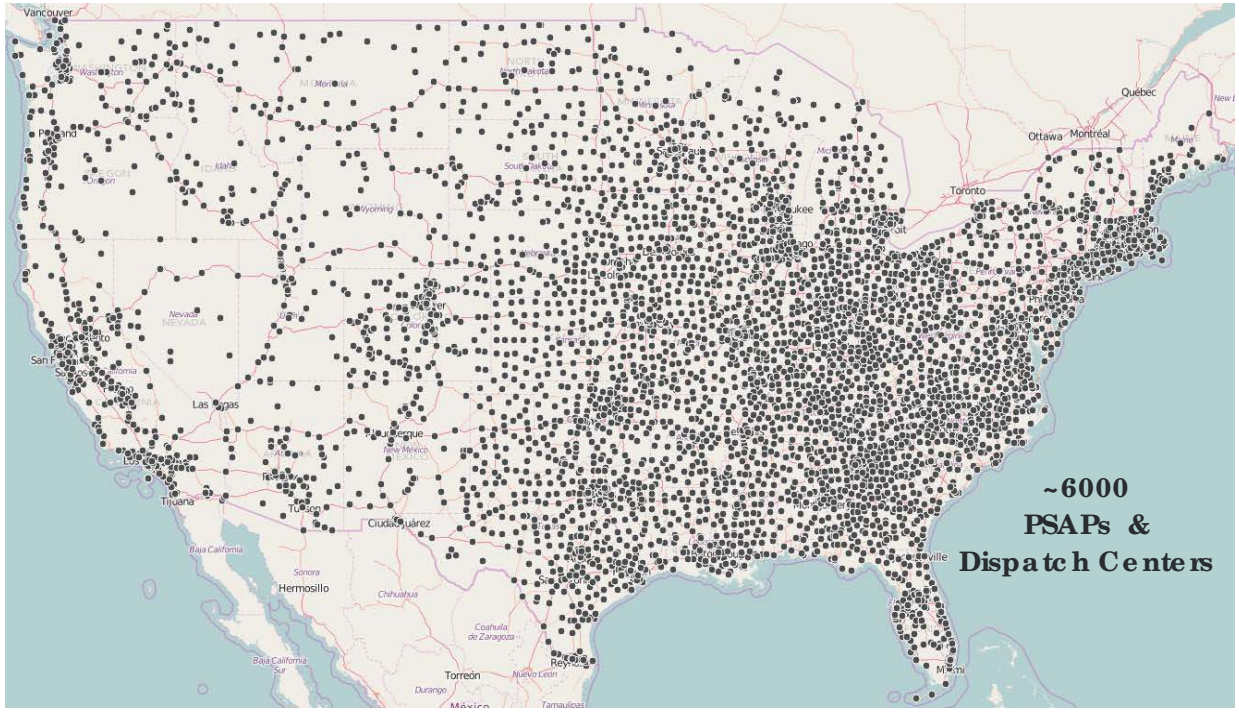
Cyber-Protecting Our Nation's Most Important Number: 9-1-1

We provide Cybersecurity solutions:

- CyberBenchmark (assessment)
- Monitoring solutions
- Training Services
- Free Webinars (2pm; 2nd Wednesdays)
- SecuLore Alerts
- Web CyberArchive

Public Safety Infrastructure Faces Cyber Threats

FIRST LINE OF DEFENSE 24X7 = HIGH VALUE



HIGH RISK OF 9-1-1 DISRUPTION

HIGH VULNERABILITY

- **80%** are small centers
- Many PSAPs have **inadequate cyber infrastructure**
- Most public safety personnel are **not cyber trained**

HIGH THREAT

- Ransomware payments for 2017 have doubled to **$2B** (Bitdefender)
- **286** incidents have affected **public safety** agencies in **50 states + DC** over the last 24 months
- **SecuLore** helped local **MD** county with recovery from **Thanksgiving Day** ransomware attack

Public Safety Is Being Targeted

SecuLore recorded a total of

286 Public Safety incidents

in 50 states + DC

in the last 24 months!

Public Safety Cyber Attack Every Month of 2018

Jan) NM: City of Farmington recovering after SamSam ransomware attack (01/05/2018)

Feb) NC: Davidson County computers shut down by ransomware (02/16/2018)

Mar) GA: Cyber Attack Hits Atlanta Computers (03/22/2018)

Mar) MD: Baltimore 911 dispatch system hacked, investigation underway (03/27/2018)

Apr) NH: City of Portsmouth hit by Emotet - Police computers taken offline (04/24/2018)

May) MS: Virus shuts down Lauderdale County's computer network (05/29/2018)

Jun) MO: Kansas City PD experiences department-wide computer outage (06/01/2018)

Jul) CT: City of Derby police computers hacked by ransomware (07/10/2008)

Aug) CA: Malware brings San Benito County Sheriff's office taken offline (08/29/2018)

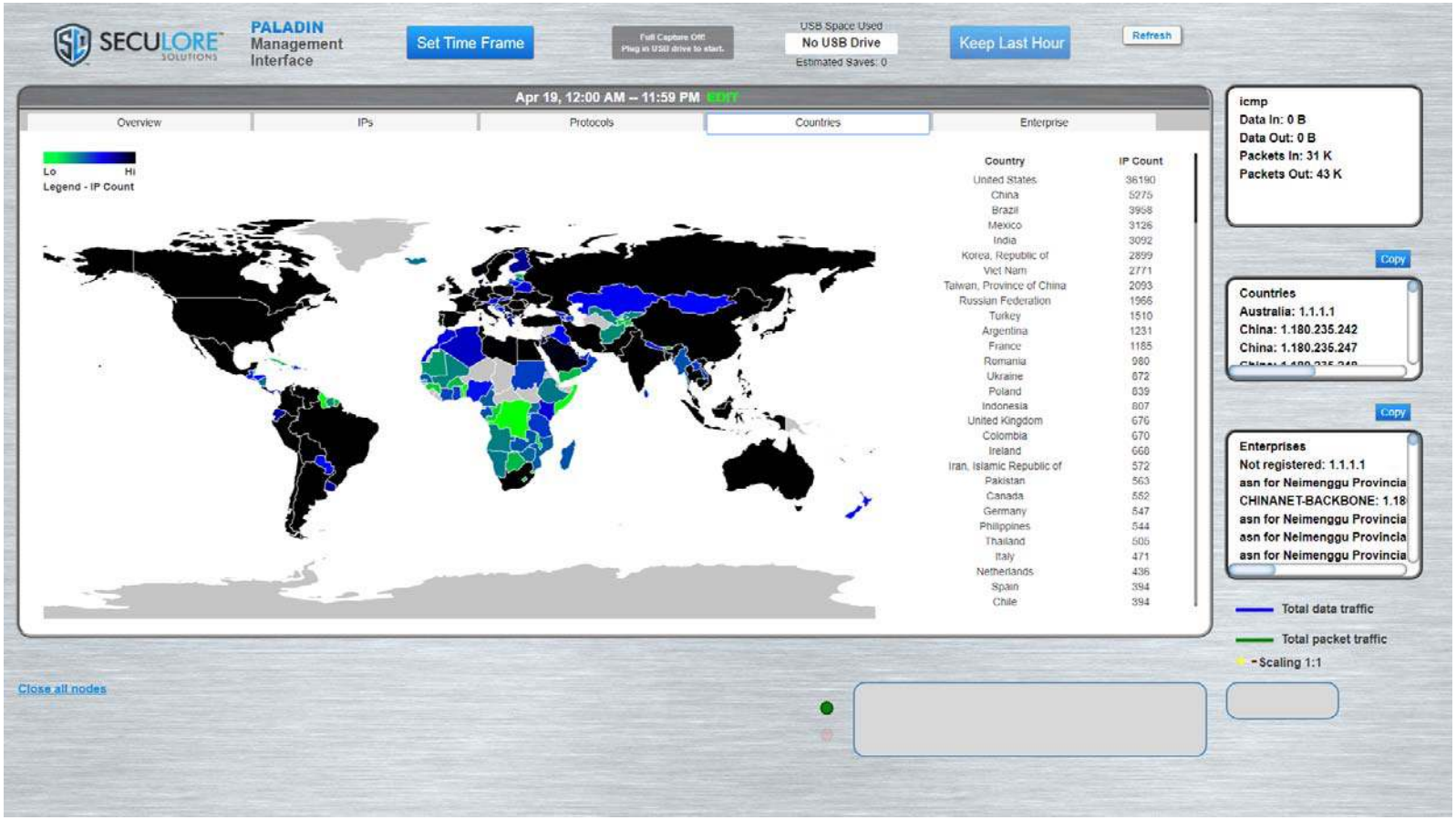
Sep) NE: Virus hits City of Beatrice services - PD, Fire & Rescue phones down (09/26/2018)

Oct) NY: Ostego County servers were hacked by crypto miners (10/10/2018)

Legacy Networks: The Illusion of Cyber Safety

Why are there so many successful attacks on our Public Safety infrastructure?

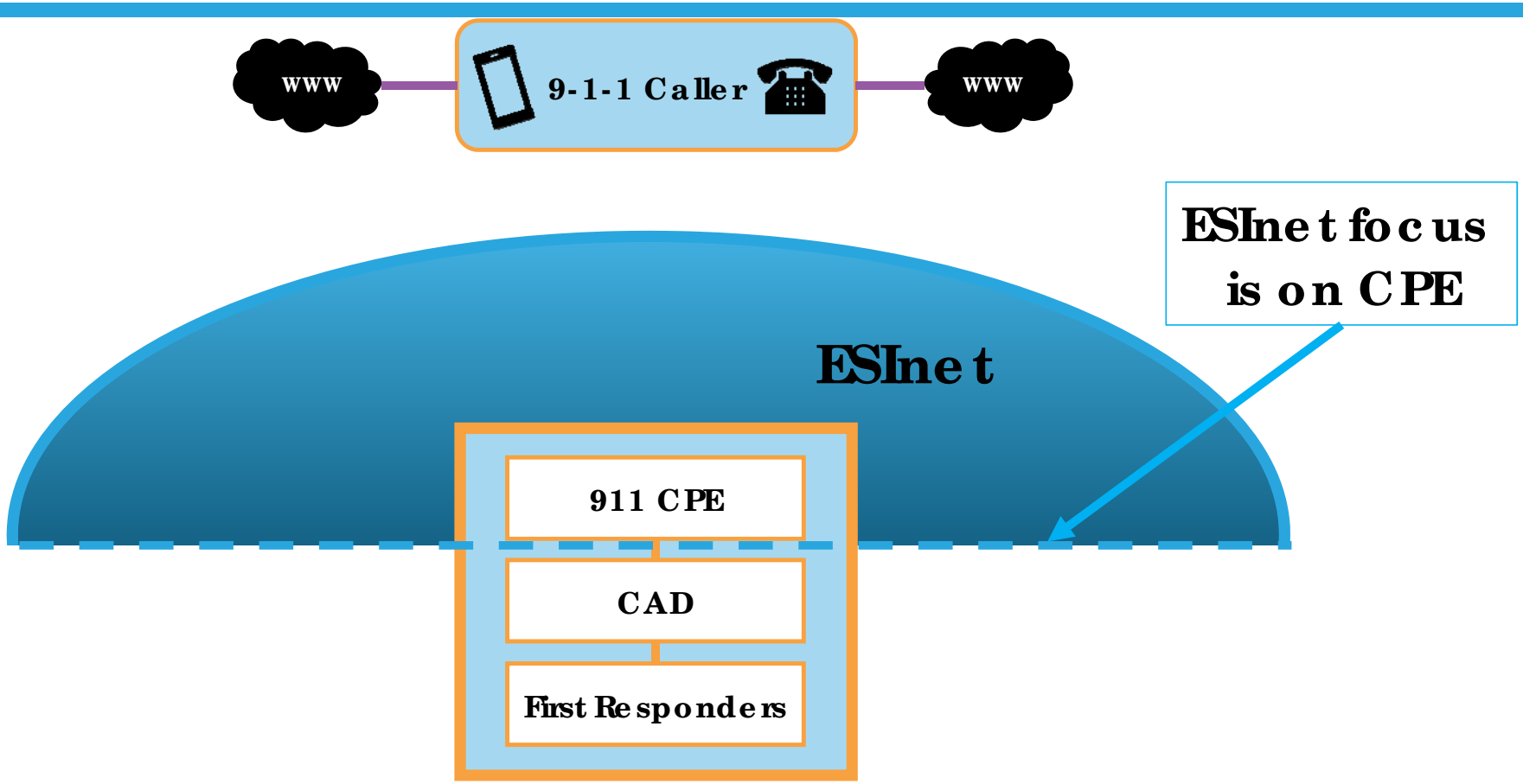
Hint: City/County Cyber Threats Can Affect You



Typical county internet traffic

Darker color indicates greater amount of traffic

ESInets will have similar challenges



Known

Possible

The Seven Cyber Challenges of ESInet

Smartphones Have Been Compromised

All Android Phones Vulnerable to "Cloak and Dagger" Full Device Takeover Attack
May 2017 – The Hacker News

Android Malware 'Judy' Hits as Many as 36.5 Million Phones
May 2017 – Fortune

41 percent of Android phones are vulnerable to 'devastating' Wi-Fi attack
October 2017 – The Verge

Hacked Android APKs Using CoinHive's Script to Mine Monero on Compromised Phones
January 2018 – Cryptovest

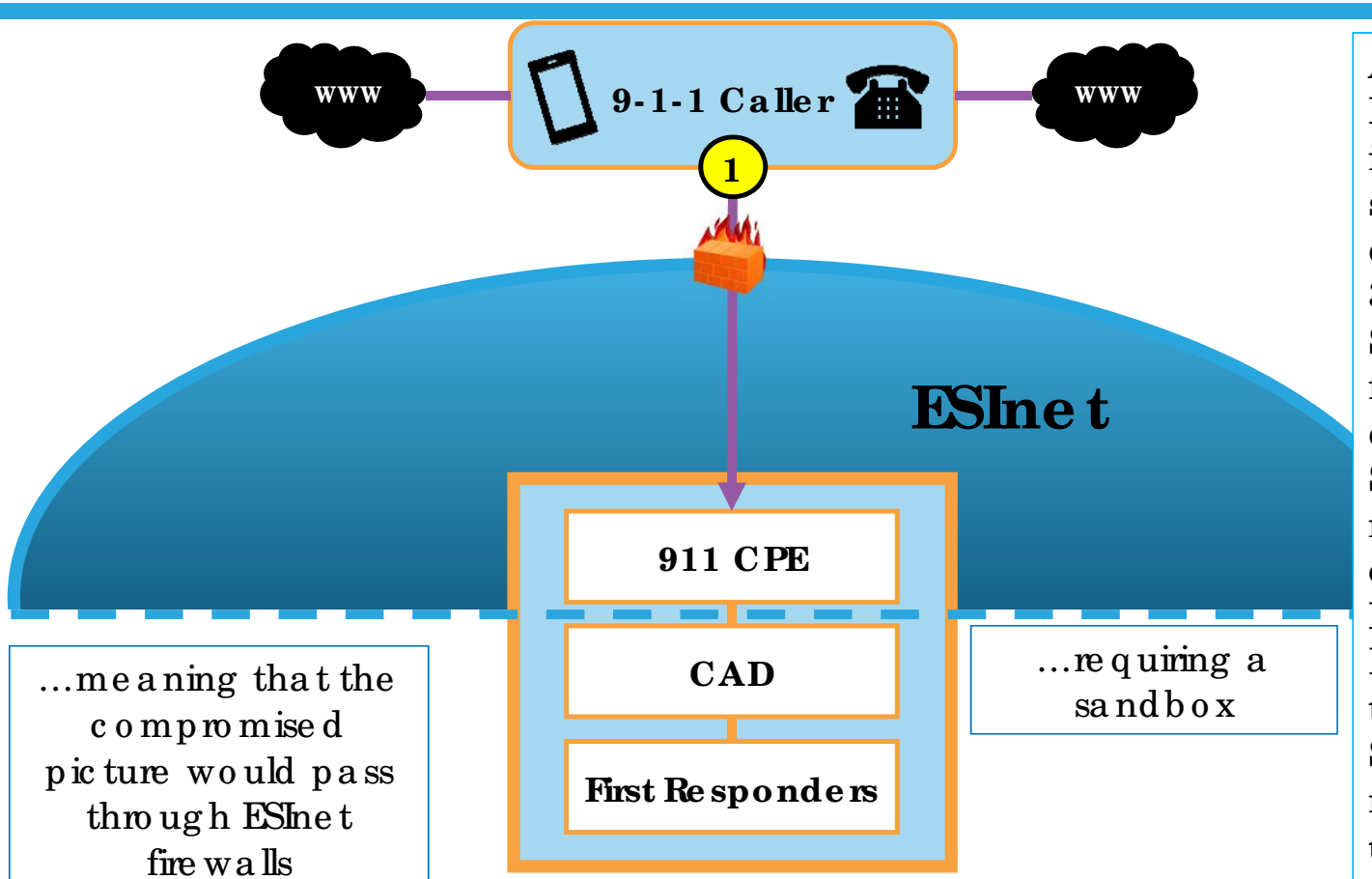
iPhone hack that threatened emergency 911 system lands teen in jail
October 2016 – Ars Technica

John Kelly's personal cellphone was compromised, White House believes
October 2017 – Politico

iPhone 7 Compromised Several Times at Hacking Event
November 2017 – Softpedia News

Apple confirms iPhone, Mac affected by Meltdown, Spectre flaws
January 2018 – ZDnet

The Seven Cyber Challenges of ESInet



All endpoints in an ESInet must implement media security with SRTP as defined in RFC 3711 and SDP Security Descriptions for Media Streams as defined in RFC 4568. SRTP Security must be requested in all calls originated within an ESInet.
If a call is presented to the ESInet with SRTP, SRTP must be maintained **through the ESInet.**

…meaning that the compromised picture would pass through ESInet firewalls

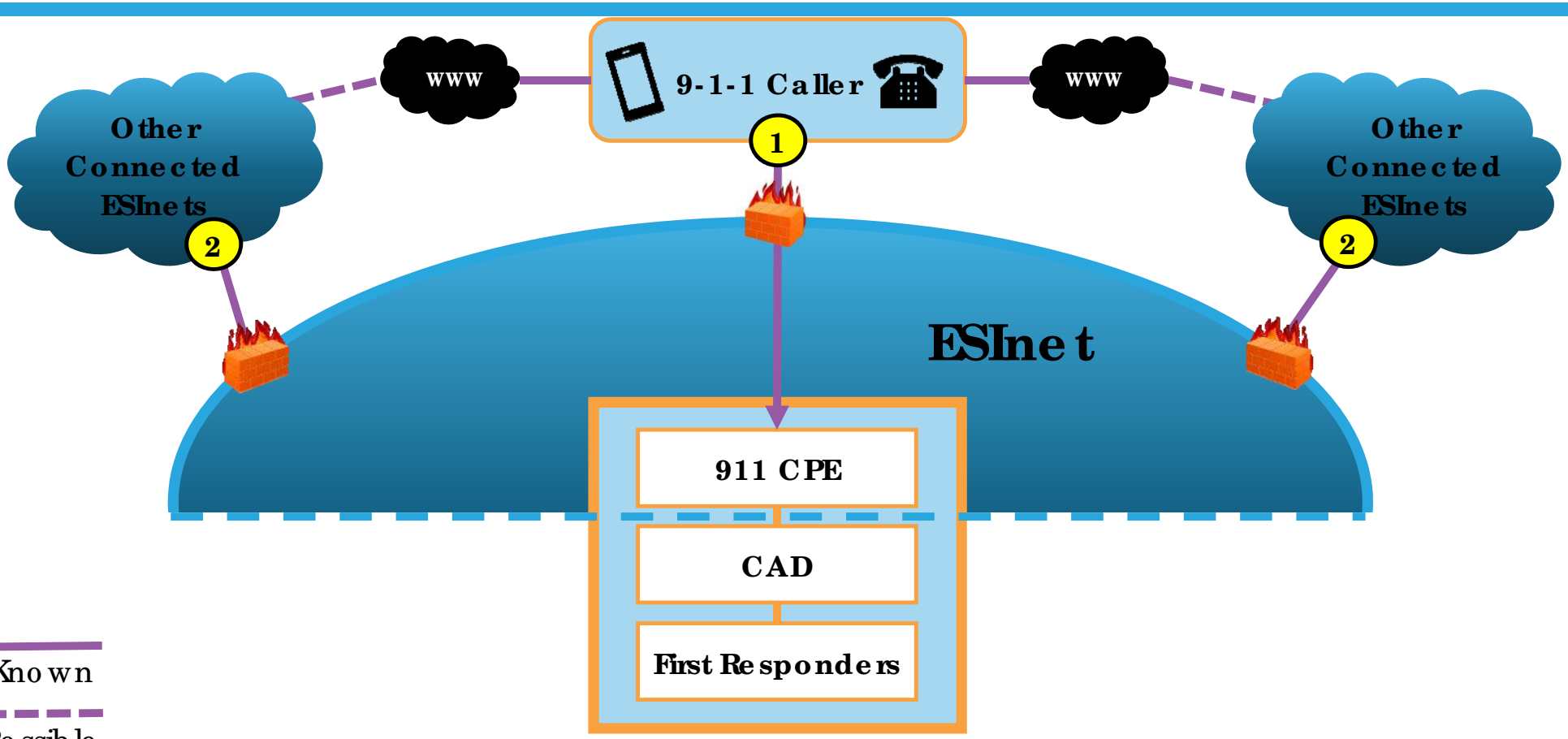
…requiring a sandbox

Known

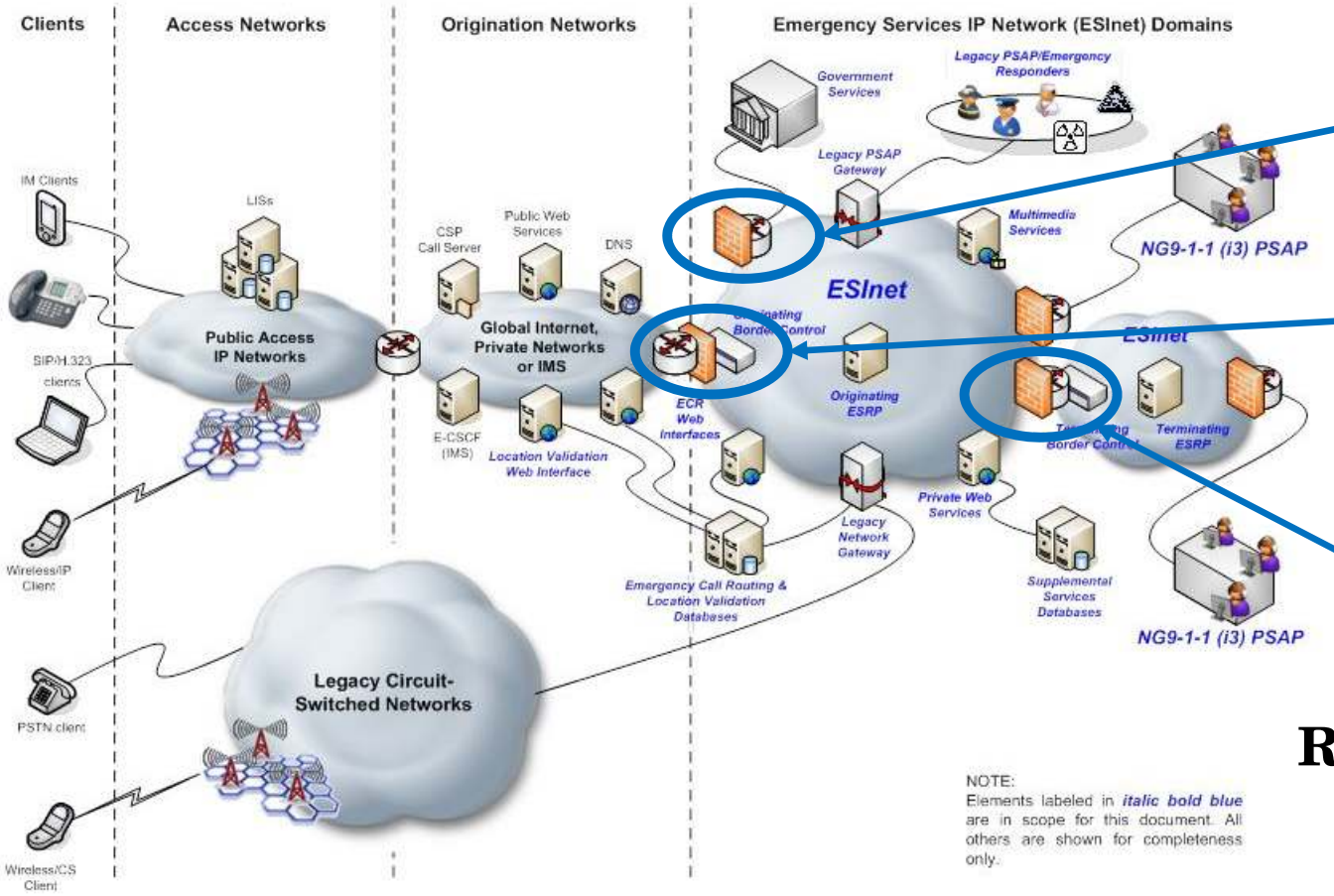
Possible

Talk to your vendor!!

The Seven Cyber Challenges of ESInet



ESInets Should Be Thoroughly Firewalled



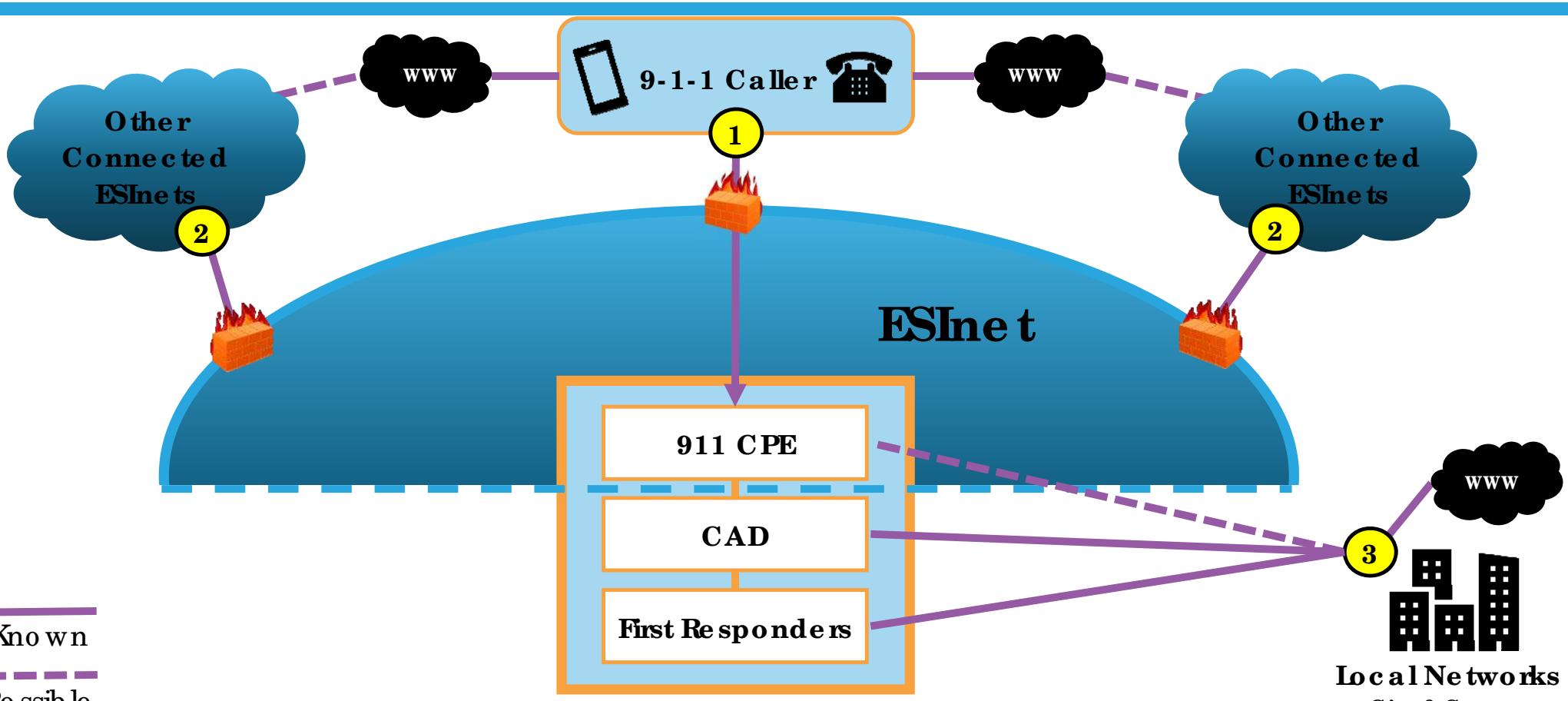
Firewalls between services

Firewalls between networks

Firewalls between ESInets

Recommended architectures address this

The Seven Cyber Challenges of ESInet



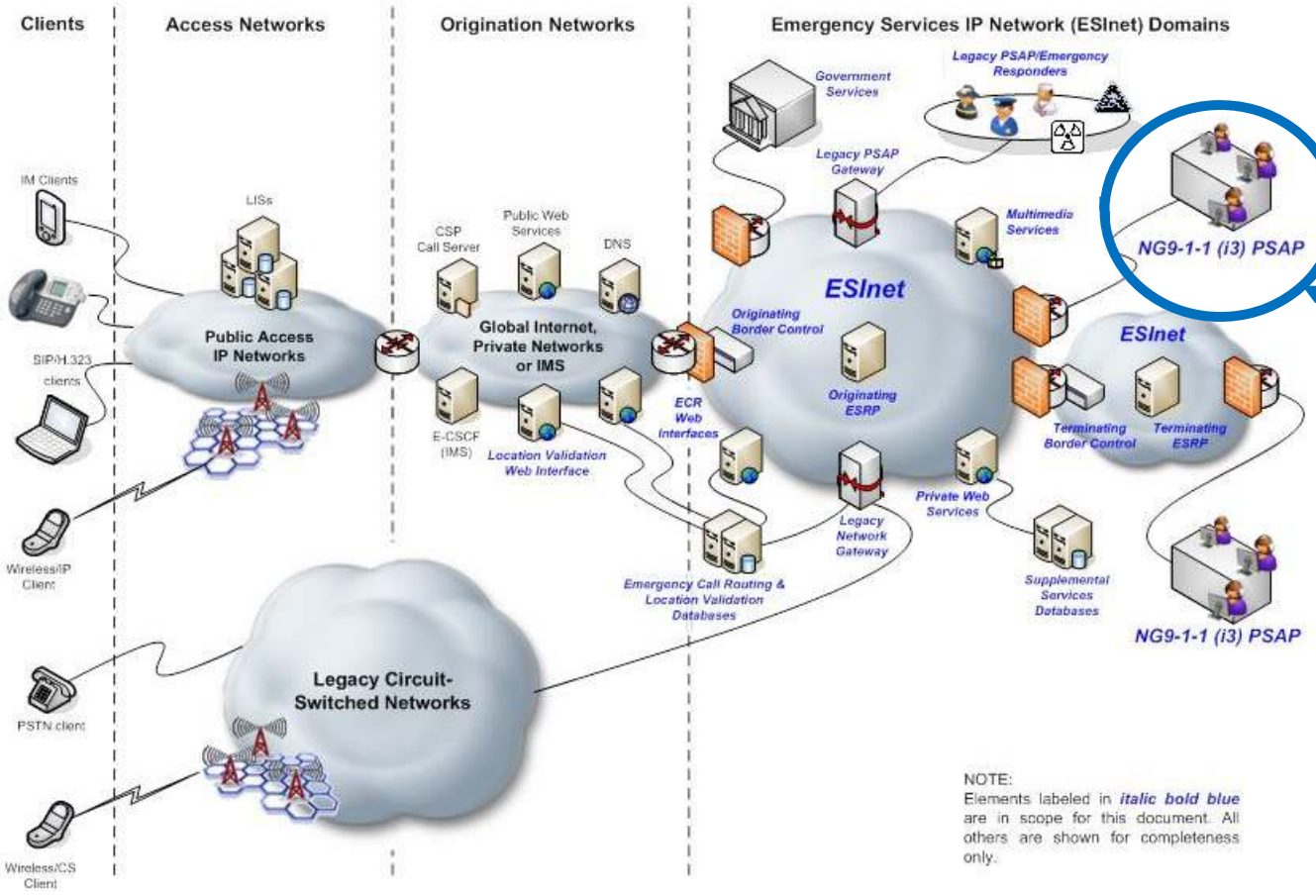
CyberBenchmark Discovered ESInet Vulnerabilty

Expected only US traffic

Instead, saw two-way traffic to 23 non-US destinations

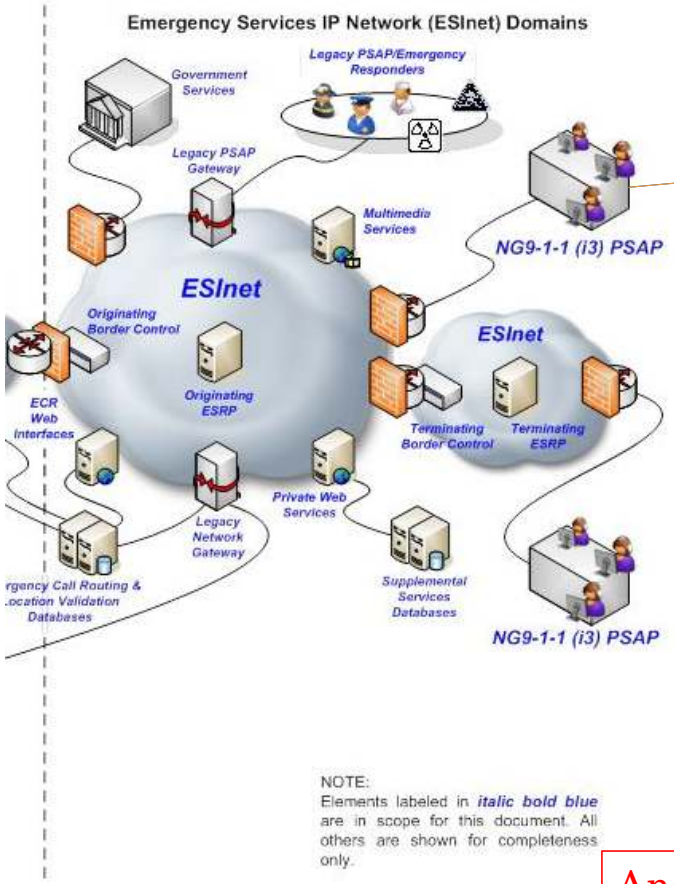
How could this happen?

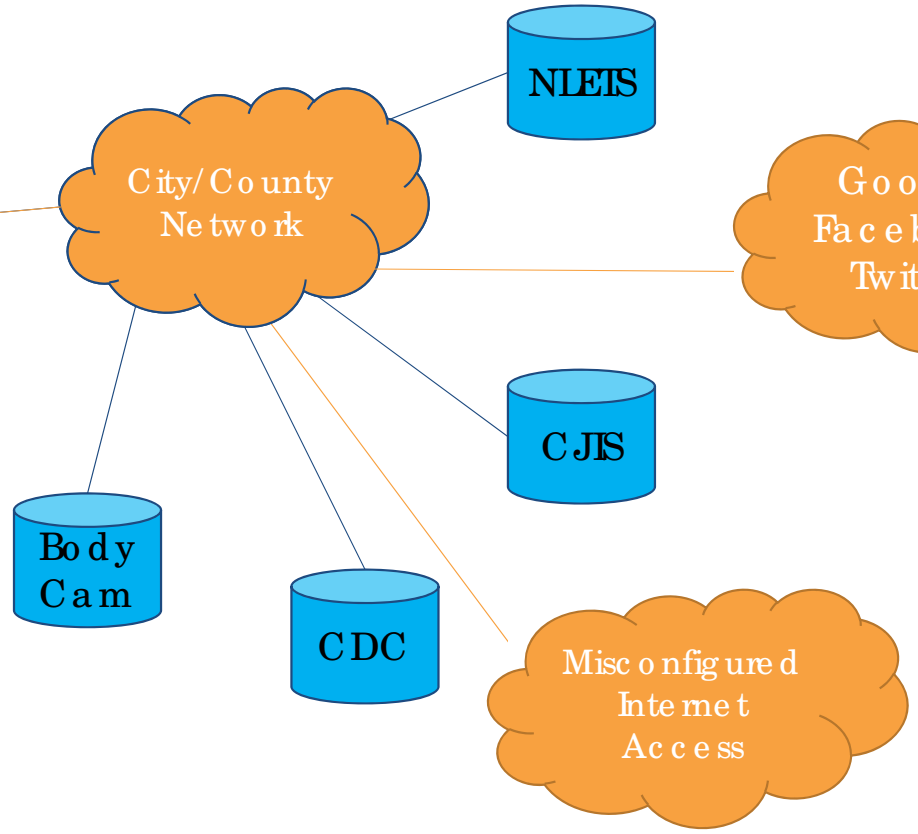
ESInet Focuses on Citizen-Originated Data



ESInet addresses data/calls from citizen – it might not address data from other sources

But Modern PSAPs Access Many Data Types

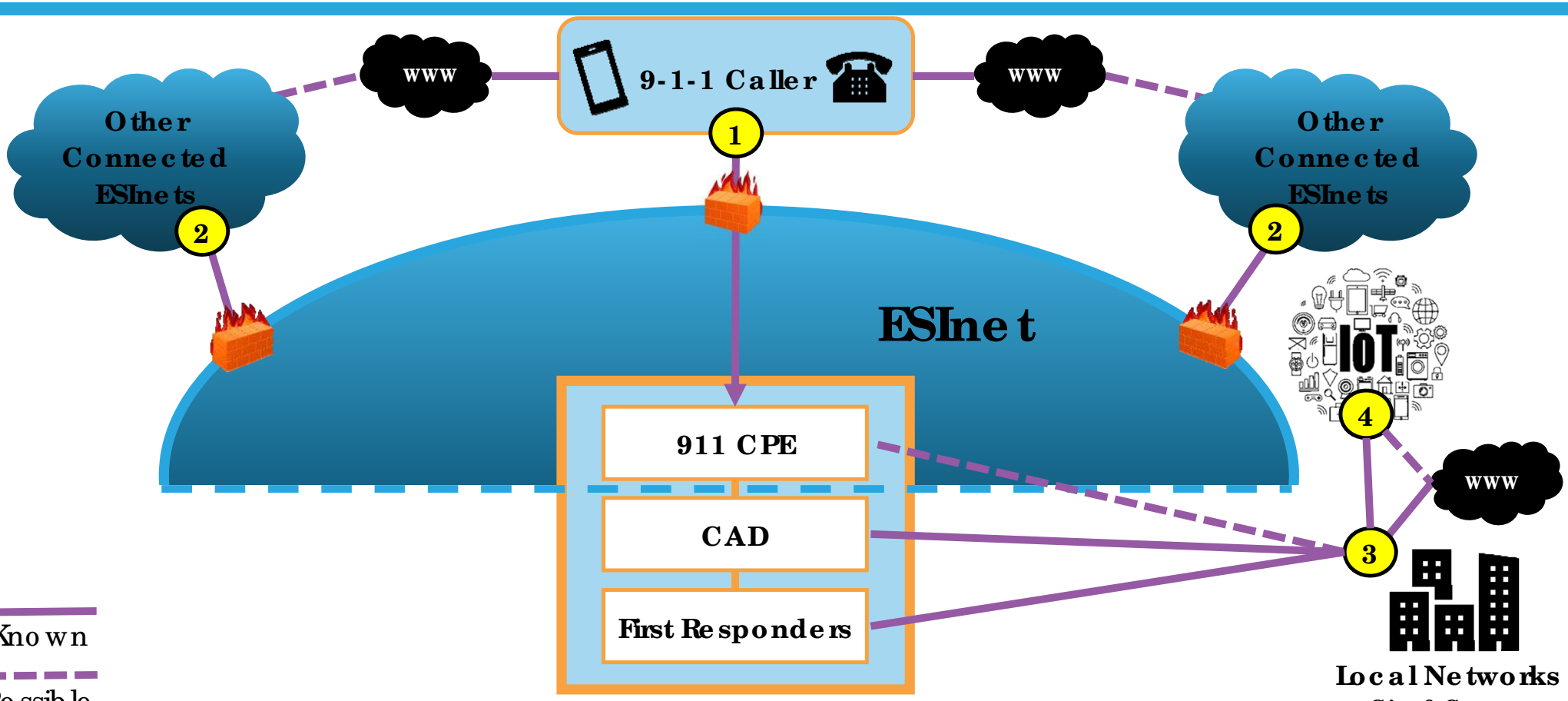




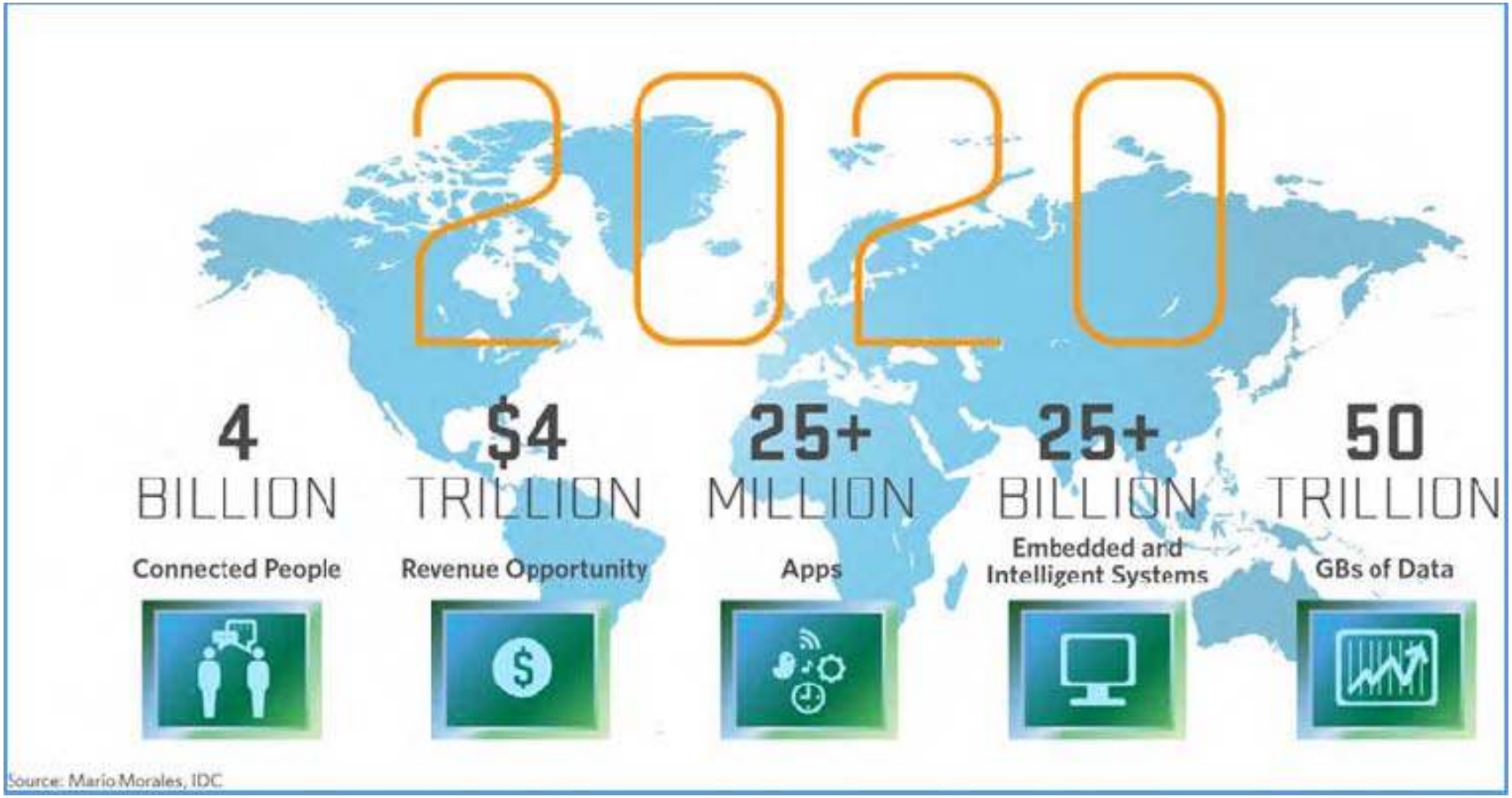
ESInet addresses data/calls from citizen – it might not address data from other sources

And some of those sources could be compromised

The Seven Cyber Challenges of ESInet



The Internet of Things – It's BIG!



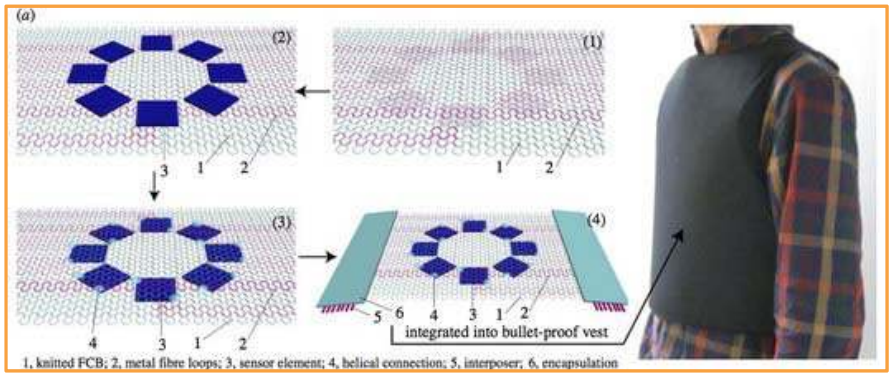
Benefit: Find a Person in Trouble in Difficult Environments

Someone in need of help…

…when finding her can be a challenge

Benefit: Find a First Responder in Trouble

An officer is down…



…and his body armor alerts you

Benefit: Monitor a First Responder's Health Stats

As the firefighter enters the fray…

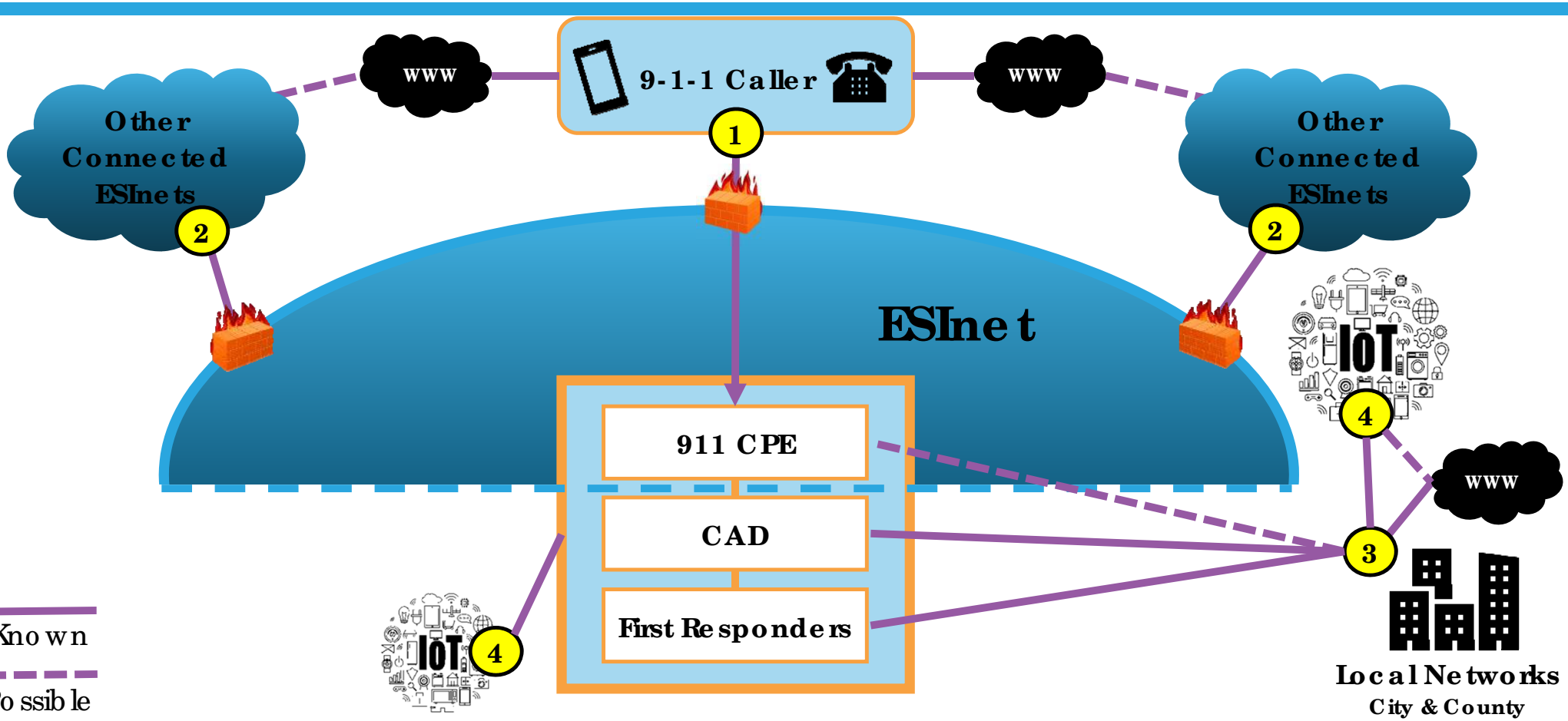
…monitor his stats along the way

Public Safety IoT Being Directly Targeted

Hackers use ransomware to hit [District of Columbia] police closed-circuit camera network (01/27/2017)

Hackers took 70% of CCTVs offline using ransomware

The Seven Cyber Challenges of ESInet



IoT Is Already Here – Printers

Printers are commonly targeted

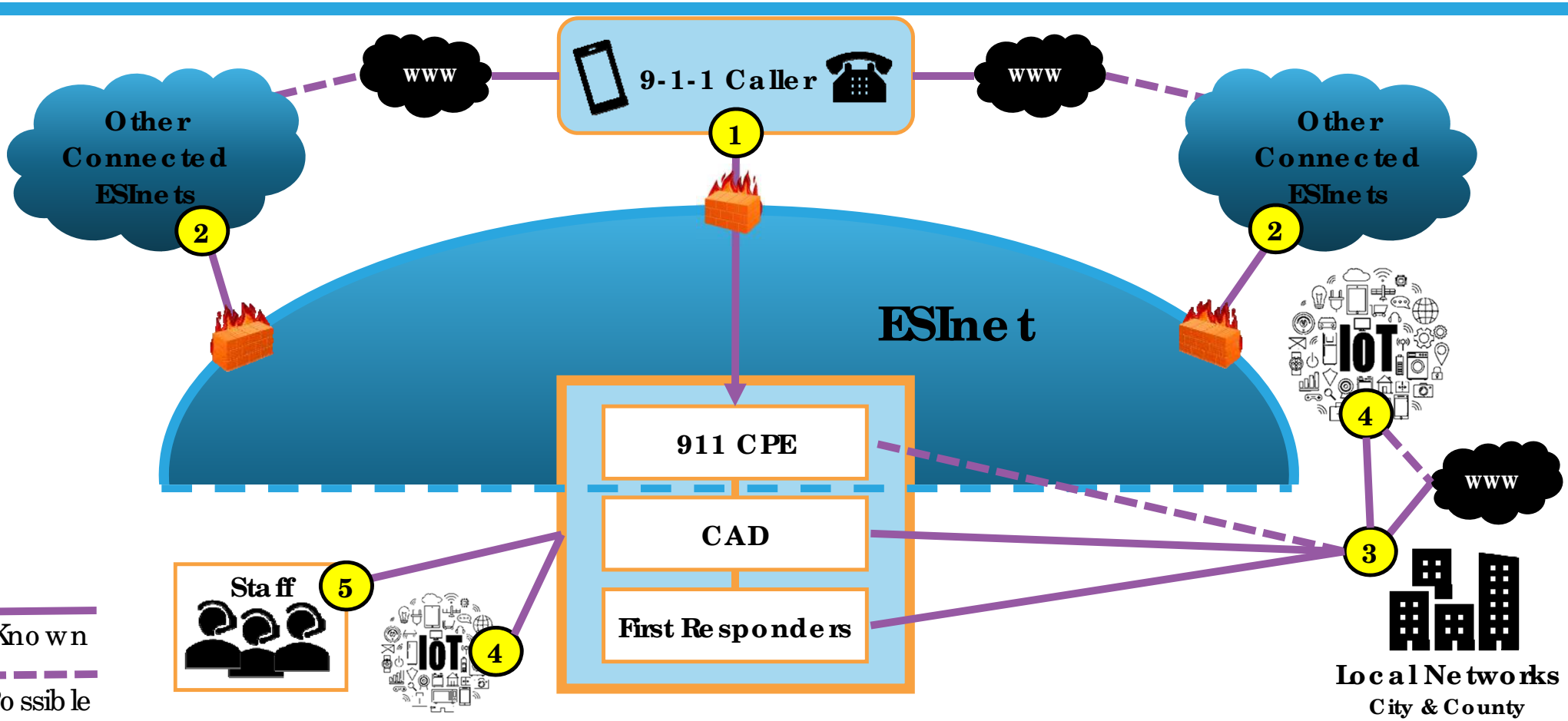
And printer manufacturers are responding

IoT Is Already Here – VoIP Devices

This is NOT an analog device (anymore)!

IoT Is Already Here - Detectors

The Seven Cyber Challenges of ESInet



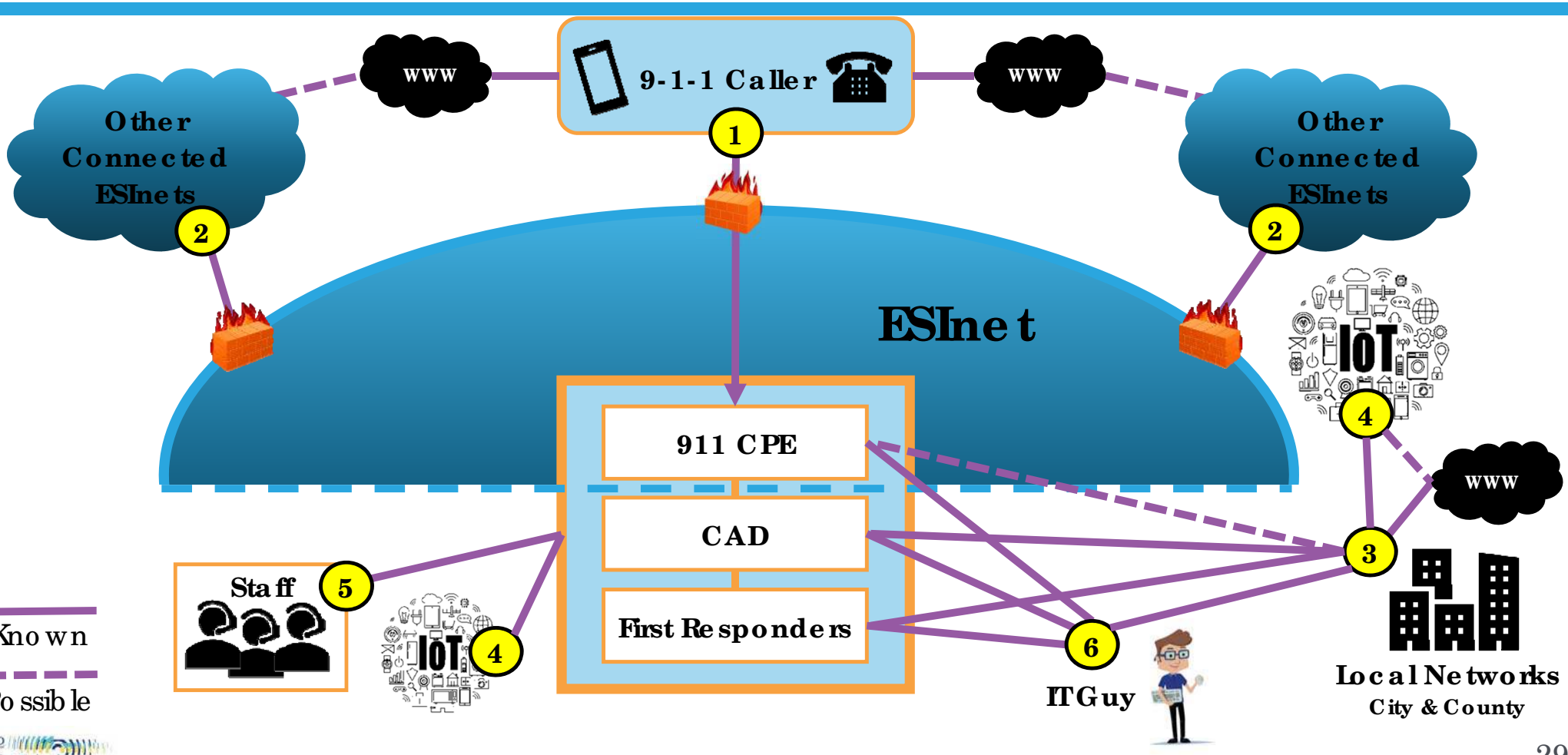
Staff Members Will Make Mistakes

Half of people plug in USB drives they find in the parking lot
April 2016 – The 'A' Register

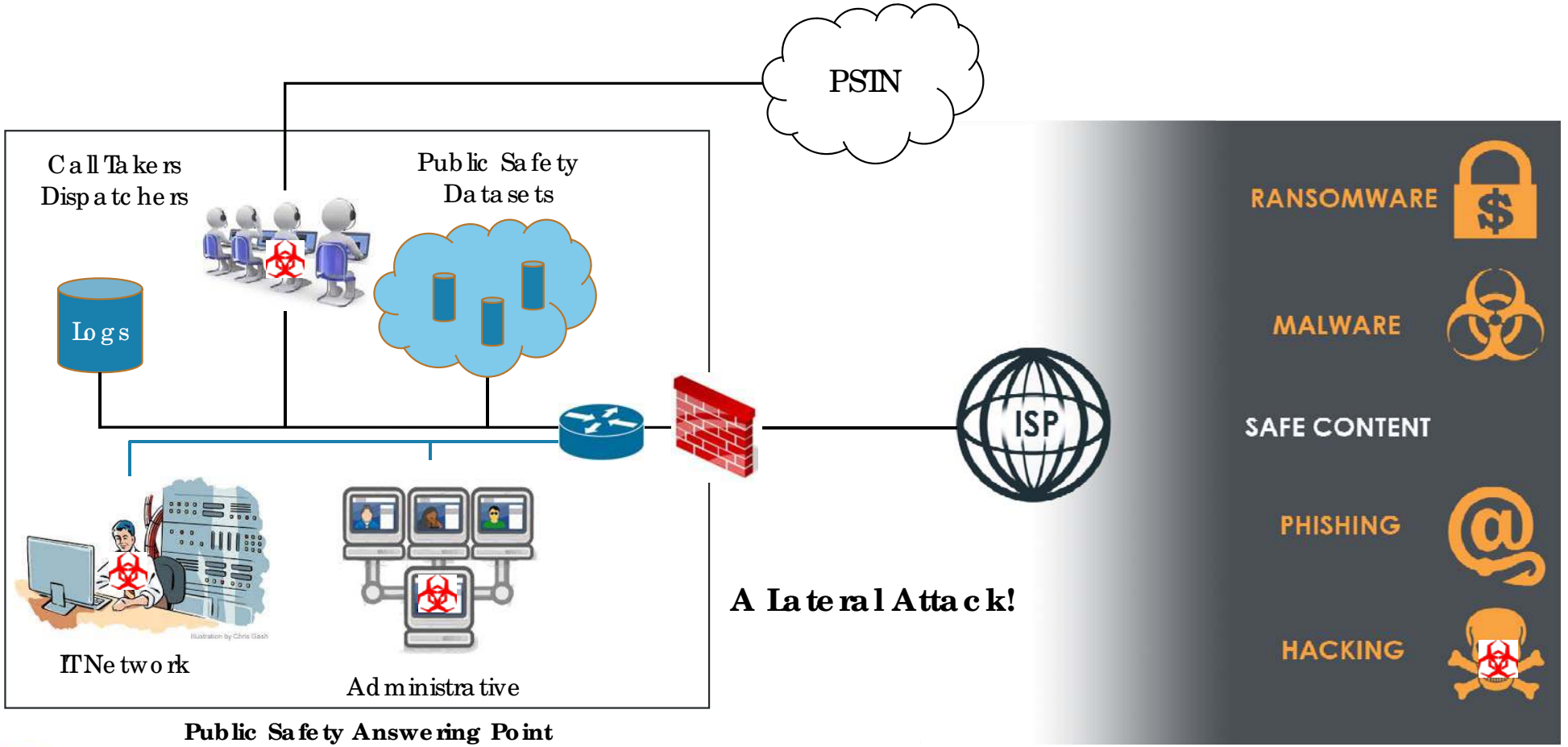
BYOD

Using personal devices on Center network
Using Center devices on personal network

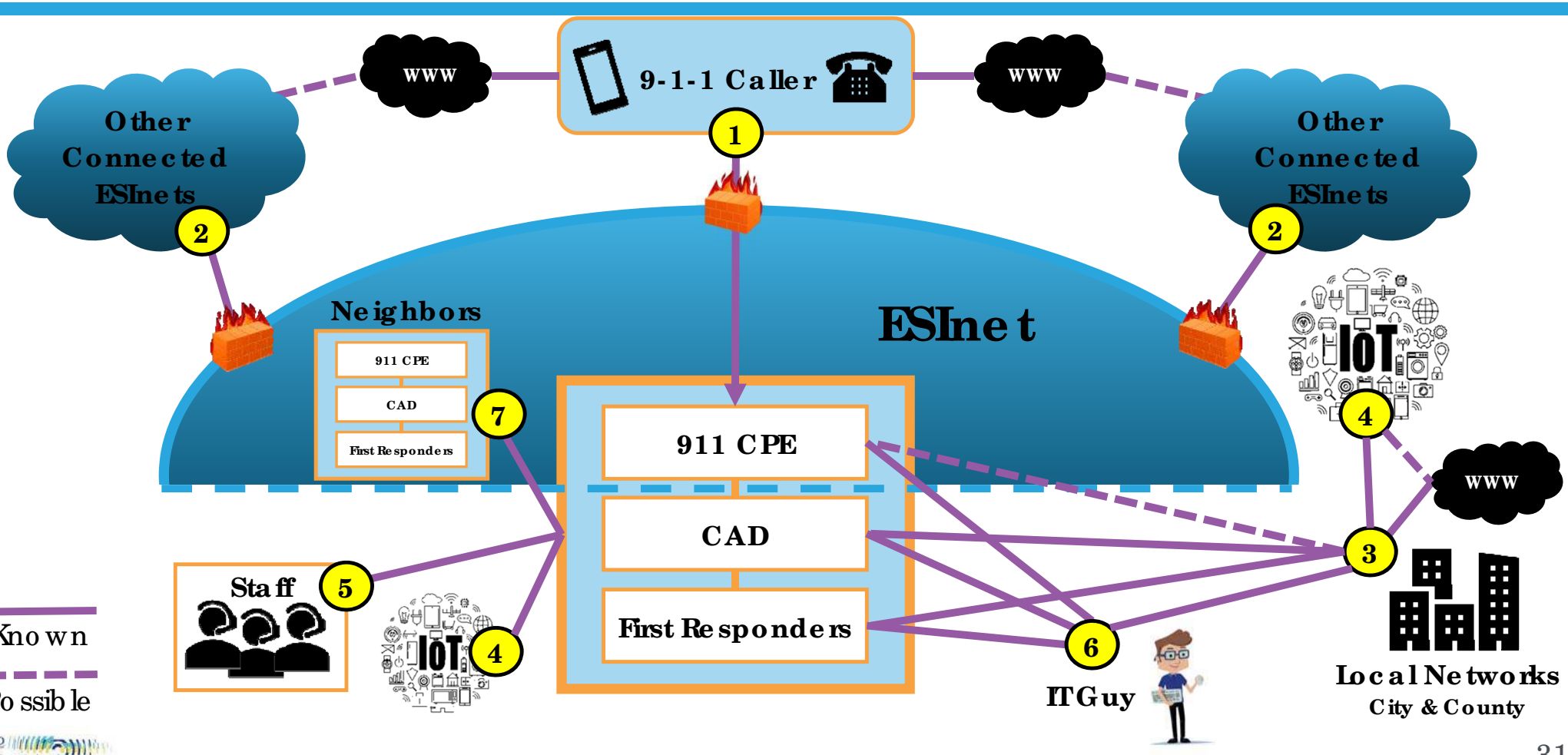
The Seven Cyber Challenges of ESInet



Hackers Used the IT Network to Bring Down 9-1-1

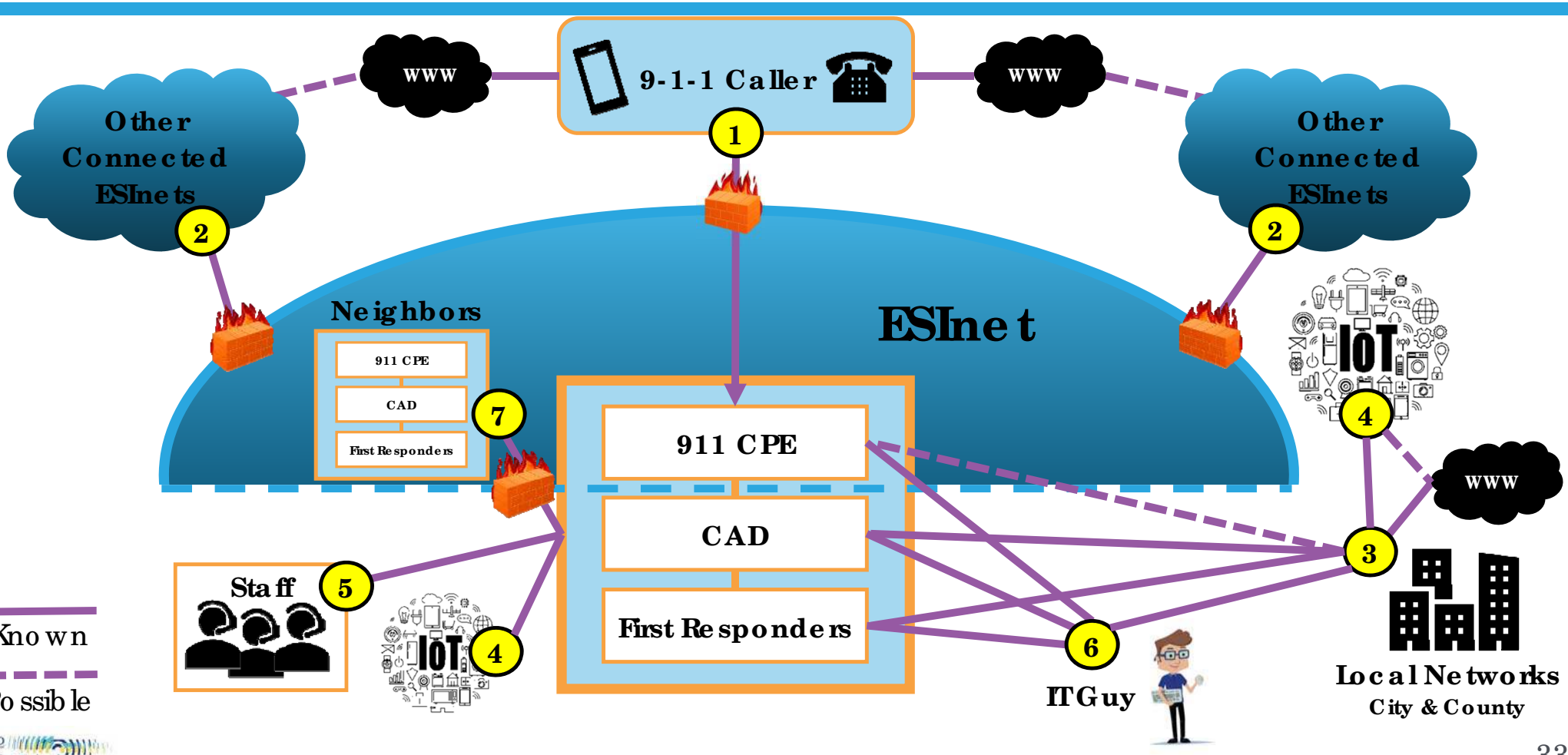


The Seven Cyber Challenges of ESInet

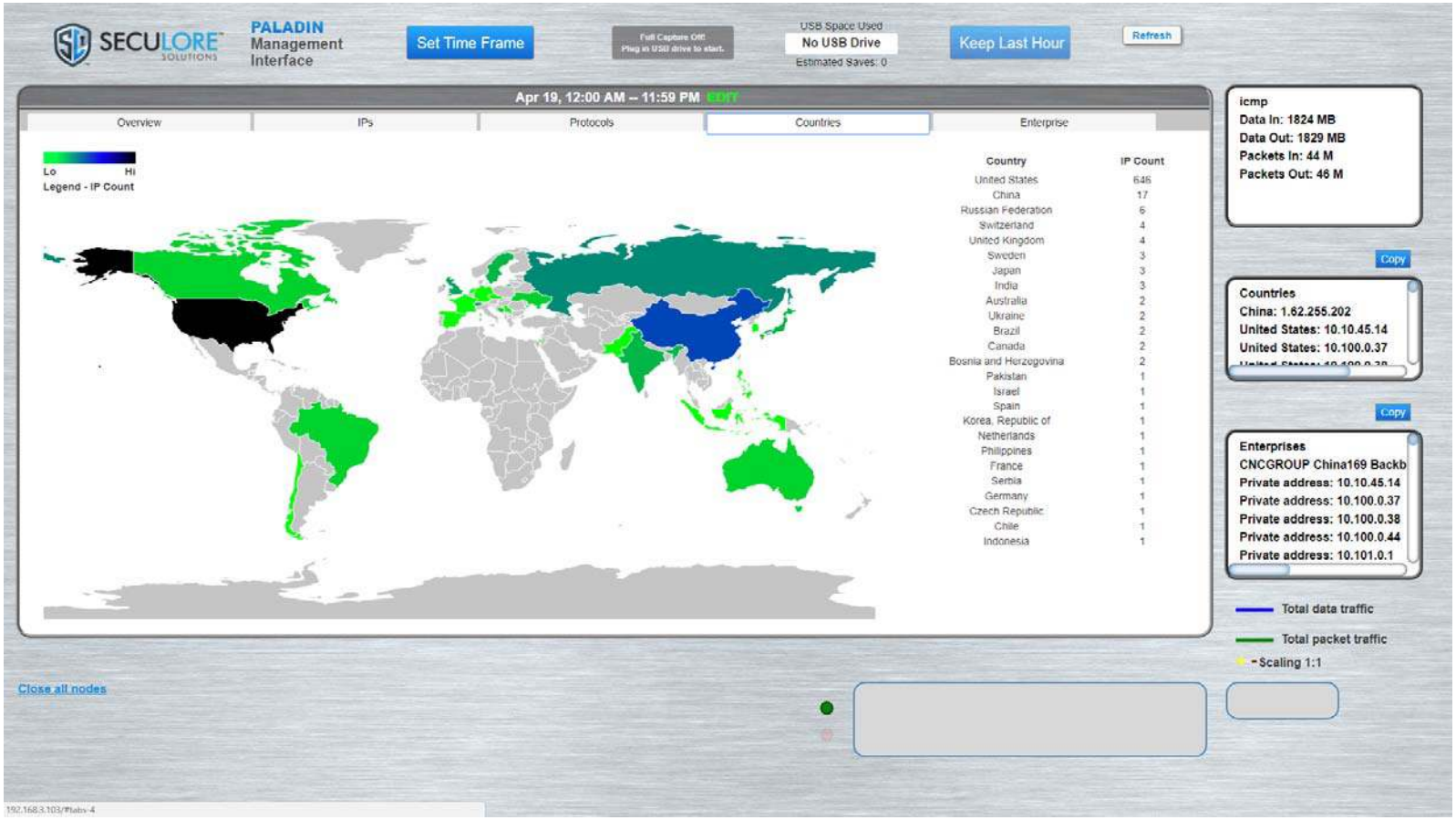


You Are Only As Strong As the Weakest Link

The Seven Cyber Challenges of ESInet



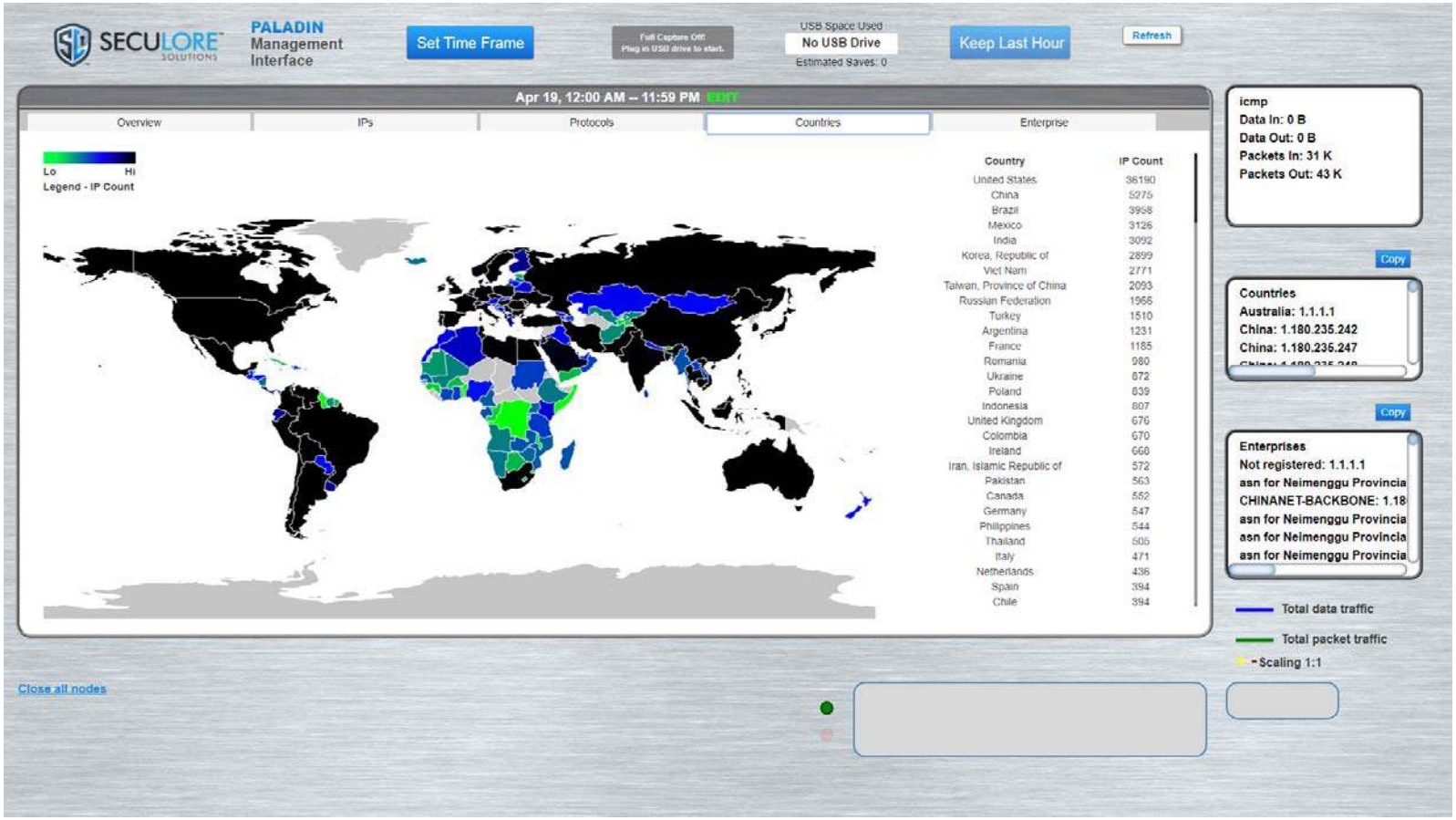
ESInet – A More Cyber-Secure Environment



By paying closer attention to cyber issues, NG9-1-1 can be safer

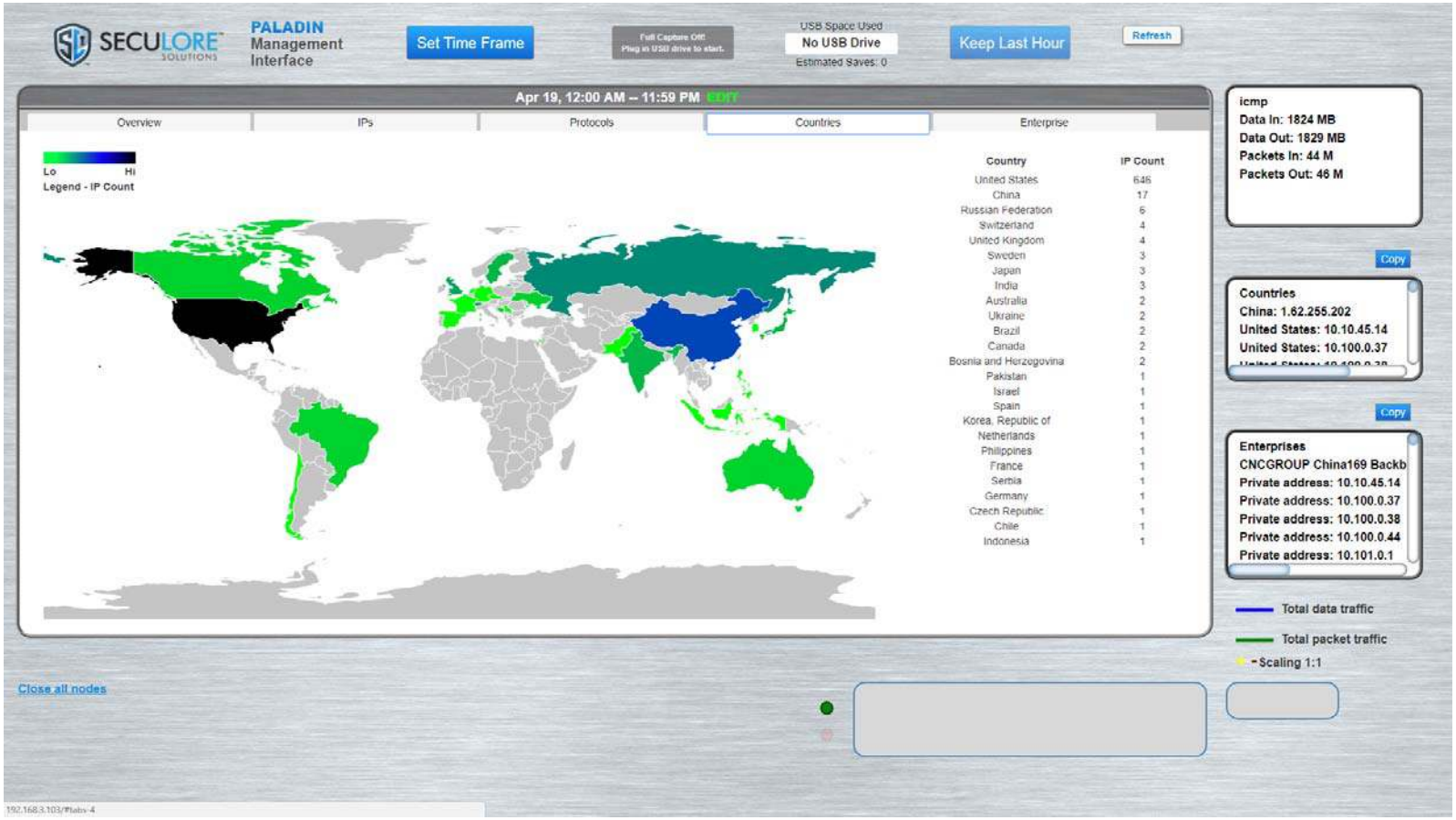
The threats can be reduced, but the risks are higher: a successful cyber-attack would cripple 9-1-1 response

Compare!!



Which Network is easier to protect?

Compare!!



Which Network is easier to protect?

Seven ESInet Cyber Challenge Summary

Two are unique to NG911 – Five impact Legacy E911

Malware from citizens needs vendor attention

PSAPs will get data via methods beyond ESInets

Internet of Things will bring internal attack vectors

Hackers know how to exploit staff and IT network

Continuous Monitoring Can Catch Bad Traffic

Monitor – Visualize - Protect

Questions?

Timothy James Lorello
President & CEO

Email: Tim.Lorello@SecuLore.com
Phone: (410) 703-3523
Web: www.SecuLore.com

Thank you for participating!

Email me for PDF!

The Seven Cybersecurity Challenges of ESInet