Why NG911 Might Actually Be MORE Cyber Secure Than Legacy E911 Networks
Tim Lorello - CEO

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

We provide Cybersecurity solutions:
- CyberBenchmark (assessment)
- Monitoring solutions
- Training Services
- Free Webinars (2pm; 2nd Wednesdays)
- SecuLore Alerts

Cyber-Protecting Our Nation’s Most Important Number: 9-1-1
Global ransomware damage costs $11.5B+ in 2019; $5B+ in 2017; up from $325 million in 2015
(Cybersecurity Ventures 11/14/17)

Carbon Black highlights a 2,502% growth in the ransomware Dark Web economy
(Bleeping Computer 10/11/17)

The largest data breaches in history:
River City Media: 393M
Deep Root Analytics: 198M
Blue Cross/Blue Shield/Anthem: 80M
Verizon: 14M
Equifax: 143M
Yahoo!: 3B

US Employs 780K cyber professionals but needs 300K more
(Cyberseek 2017)
Public Safety Infrastructure Faces Cyber Threats

**FIRST LINE OF DEFENSE 24X7 = HIGH VALUE**

~6000 PSAPs & Dispatch Centers

**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)
- 221 incidents have affected public safety agencies in 49 states over the last 24 months
- SecuLore helped local MD county with recovery from Thanksgiving Day ransomware attack
SecuLore recorded a total of **221 Public Safety incidents in 49 states** in the last 24 months!
A Growing List Of Cyber Attacks on Public Safety

- TX: Eight years' worth of Cockrell Hill Police evidence wiped out - Ransomware (01/25/2017)
- DC: Police hit by ransomware - The threat of IoT - Public Safety paying ransoms with Bitcoin (1/30/2017)
- ID: Repeated attacks from hacker obfuscation - Eternal Blue (1/30/2017)
- MO: Warren County sheriff's office leaked police informants/victims audio after ransomware attack (3/16/2017)
- TN: Ransomware hits Murfreesboro emergency services (7/5/2017)
- NY: Schuyler County 911 system crippled by hacking - unable to dispatch deputies (9/7/2017)
- NY: Brookhaven is one of 76 government sites hacked by ISIS (06/26/2017)
- TN: Ransomware attacks City of Spring Hills impacting 911 dispatchers - hackers retaliate after not being paid (11/8/2017)
- NC: Ransomware shuts down county servers - hackers refuse to release data until being paid (12/4/2017)
- TX: Virus attacks City of Dallas - limits access to city services, CAD included (2/5/2018)
- CO: CDOT employees dealing with yet another SamSam ransomware attack (3/1/2018)
- GA: City of Atlanta shut down for 6 days due to SamSam ransomware (3/22/2018)
- MD: Baltimore City CAD Hacked - down for 17 hours (3/27/2018)
Categories of Public Safety Cyber Attacks

- **Phishing**: An email attack, intended to make the victim take an action that installs malware on the victim’s machine.

- **Web site drive by**: A technique that lures a victim to an infected web site, thereby installing malware on the victim’s machine.

- **Ransomware**: Malware which, once activated on a victim’s machine, encrypts data that can only be unlocked by paying a ransom.

- **Persistent threat**: Malware that hides on a system and which either slowly leaks information to the attacker or awaits activation.

- **Hacking**: A brute-force attack method by which an attacker identifies a system vulnerability and then directly exploits that weakness.
So Isn’t This Bad for NG9-1-1: an All-IP Network?

Sounds Logical

- Cyber attacks occur on IP networks
- NG9-1-1 is an IP network
- Therefore cyber attacks will occur on NG9-1-1 networks!

But let’s analyze why these attacks succeeded
Analysis of the 221 Cyber Incidents

Phishing ➔ Most preferred vehicle

Web site drive by ➔ In fastest decline

Ransomware ➔ Largest

Persistent threat ➔ Most undocumented

Hack ➔ Fastest growing
Analysis of Types of Attacks - Phishing

Phishing

NH, AL, ME, MA, IA, PA, MD, SC, TX

Both a vehicle (for ransomware) and an attack (data breaches)
Email Alert – Reading Techniques

Identify

- Examine subject line (urgent = warning)
- Examine sender (don’t recognize = warning)
- Did you expect the email (unexpected = warning)
- Does sender ask for personal information (info request = warning)
- Does sender have links in email (links = warning)

Mitigate

- Save email – do not discard

Report

- Send to IT security team for analysis

Exception: 9-1-1 “calls”!
Cyber Hygiene – Protection Against Phishing

The Hidden Hoodwink

Your package could not be delivered by our courier because no person was present at your address. Your signature is required to successfully deliver the parcel.

Shipping service: Next Day Air
Box size: Large
Date: Feb 21th 2017

A new delivery can be scheduled, by calling the number on the delivery notice we left at your address. You need to including the address and tracking number, which can be found on the notice.

An electronic copy of the delivery notice can be viewed online on the USPS website: [https://tools.usps.com/web/pages/view_invoice?id=10548203&dest=tim.lorello@seculore.com](https://tools.usps.com/web/pages/view_invoice?id=10548203&dest=tim.lorello@seculore.com)

No info request

STOP
Urgent?

Expected?

Unknown contact?

Odd Source?

Click on something?

“hover” mouse over link
Analysis of Types of Attacks – Web Site Drive By

Web site drive by WY, HI, IA

Browser manufacturers are combatting these techniques
Four Types - Website Drive By

1. Website with similar name

2. Website embedded with Ransomware

3. Link in email

4. Attachment in email
Analysis of Types of Attacks - Ransomware

Ransomware: NH, AL, ME, NC, MA, WY, FL, IA, TX, HI, MN, CA, PA, MD, IN, AR, SC, DC, TX, OH, IL, ID, MO, GA, TN

A mult-billion-dollar business!
Step 1: Identification

Attacker may:
1) Probe the network
2) Send continuous interrogations
3) Send continuous phishing attacks

Hacker rents an exploit kit

“Command and Control” server
Step 2: Exploitation

Success!! The exploit succeeds in being installed on the victim’s machine.
Anatomy of a Ransomware Attack (3/6)

Exploit communicates with “HQ”: Asks for malware (ransomware in this case)

Step 3: Retrieve Ransomware

Ransomware to deposit
Anatomy of a Ransomware Attack (4/6)

Step 4: Key exchange

Hacker delivers encryption key

Network Provider
Anatomy of a Ransomware Attack (5/6)

Step 5: Encryption

Encrypt files/system using encryption key from hacker
**Anatomy of a Ransomware Attack (6/6)**

**Step 6: Extortion**

- **Victim pays the ransom**
- **Does the victim get the key?**
- **Hacker gets his cut**
- **Extortion with a smile!**
Advanced Persistent Threat MD, Unknown?

148 days, on average to detect a data breach
A Joint Analysis Report identified 876 IP addresses likely associated with Russian cyber hacking.

13 of these IP addresses were seen talking to a public safety agency.

Note heavy use of encrypted traffic.
Advanced Persistent Threats from Russia

Note heavy traffic within the US
Advanced Persistent Threats – Hidden Sources

Note use of benign US corporations
Surprising growth of hacking – notable increase in 2016
Thanksgiving PSAP Attack: Vulnerability Scan

Step One
The Scan

This Hacker loved to scan from Iran
Thanksgiving PSAP Attack: The Phishing Fake

Step Two
The Fake Phishing emails

Came from many countries – but most from US!
The Strike: Web Permit Server Takes Out 9-1-1

PSAP Network

Web Server

Monitor inside traffic
Alerts sent to SOC

Web Rep

Firewall

ISP for Web

ISP for Network

4 Layers of Protection
Web reputation
Firewall
Email antispam
Workstation antivirus

Monitor outside traffic
Full data capture

Employee

Email

Web

AV

AV

AV

AV

AV

Web Rep

Email Antispam
Hackers Used the IT Network to Spread

A Lateral Attack!
Cyber Incidents Associated with Computers

- Phishing
- Web site drive by
- Ransomware
- Persistent threat
- Hack

Nothing unique to NG9-1-1!

Behavioral

Business driven

Agendas....

Brute force
Three Ways NG9-1-1 Will Be More Secure

1. Rules specific to Public Safety
Implement/Enforce Specific Public Safety Rules

- Block non-US data traffic
- Reduce or focus social media usage
- Easier network segmentation
- Sandbox data coming from citizens
- Gather data specific to public safety
Three Ways NG9-1-1 Will Be More Secure

1. Rules specific to Public Safety
2. Focused Protection
Your Agencies Share County/City Cyber Threats

Typical county internet traffic

Darker color indicates greater amount of traffic
ESInet can be broadly protected, blocking unwanted traffic.

Unwanted traffic can still occur because of malware on internal systems (IoT?)
Three Ways NG9-1-1 Will Be More Secure

1. Rules specific to Public Safety
2. Focused Protection
3. TDoS protection
TDoS Threats: NG9-1-1 Can Help!

TDoS attacks more easily addressed with an all-IP path to the calls

- VoIP ISP
- VoIP
- VoIP
- Legacy
  - Must convert data
- NG9-1-1
  - All IP – no conversion
- TDM
- SR
- PSAP
- NG911 PSAP
- Traceback!

VoIP

ESInet
Summary of Our Analysis

Cyber threats to Public Safety are real and growing

Primary problems are tied to using computers in systems

NG9-1-1 offers unique cybersecurity protections

Concluding:

Don’t let cybersecurity concerns delay NG9-1-1
Why NG911 Might Actually Be MORE Cyber Secure Than Legacy E911 Networks

Wednesday, 5/2, 10:45am – 11:15am