NG9-1-1 Needs Cybersecurity (and E9-1-1 Does Too!)

Timothy Lorello – President & CEO
SecuLore Solutions
Tim.Lorello@SecuLore.com
SecuLore Solutions: Public Safety/Cyber Expertise

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
Why Should Public Safety Care About Cybersecurity?
Global Cyber Crime Continues to Skyrocket

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)

Cyber crime damage projections double to $6 trillion annually by 2021 (Herjavec Group 10/16/17)

US Employs 780K cyber professionals but needs 300K more (Cyberseek 2017)

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

Ransomware hitting Healthcare IT up 89% (Cyrptonite Jan 2018)
Cyber Crime Is A Daunting Public Safety Challenge

Montgomery County Alabama Suffers Massive Ransomware Attack
-- Montgomery County, AL (September, 2017)

It is much easier to fund gang efforts through cybercrime than it is to rob somebody or sell drugs on the street corner, because you are much less likely to get caught.
-- MN Chief Janeé Harteau

Hackers hit D.C. police closed-circuit camera network, city officials disclose
-- Washington, DC (January, 2017)

Cybercrimes essentially reduce the size of the world, so that someone across the globe can become part of your jurisdiction.
-- New York Capt. Michael Shugrue

Hackers Place ISIS Propaganda On Town Of Brookhaven Website
-- Suffolk County, NY (December, 2017)

...we have to be able to serve the citizens we’re sworn to protect, no matter where the perpetrators may be
-- Des Moines Maj. Stephen Waymire
Understanding Why PSAPs Are A Target

MISSION CRITICAL NATURE = HIGH VALUE

WE FACE A 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 2016 are believed to hit $1B (FBI)
- 132 incidents have affected public safety agencies in 40 states over the last 24 months
- Thanksgiving Day ransomware attack - hits SF & MD 911 Center
SecuLore Vision

Our focus is to protect the nation’s most important number: 9-1-1

Our desire is to help public safety prepare for and support NG9-1-1
  • NG9-1-1 is all based on internet protocols
  • Cybersecurity concerns should not impede NG9-1-1 progress

Our approach is to empower your staff to protect your network:
  • Provide a cybersecurity network appliance
  • Allows monitoring of all data into and out of the 911 PSAP
  • Provides visualization of the traffic, allowing anomalies to be found
Paladin™ - A New Layer of Cyber Defense

Your Network

• Works with existing cybersecurity
• No software installation
• Captures critical attack information

Monitor

The Internet

Visualize
• Incoming traffic
• Outgoing traffic
• Real time

Protect
• Affordable
• Built for Public Safety
• Customizable
SecuLore Solution – Monitor|Visualize|Protect

PALADIN™
Our patent-pending, network appliance monitors data between the firewall and external sources, visualizes the traffic, and provides sophisticated and dynamic protection of the network.

LEVELS OF PROTECTION

Watcher
Plug in the Paladin and go! Watcher Mode allows you direct access to self-monitor your traffic.

Overwatch
Need some expert monitoring? Overwatch mode includes weekly check in with a cybersecurity expert.

Guardian*
Need 24/7 protect? Guardian mode blocks known threats before they reach your firewall.

*COMING SOON*
SecuLore CyberBenchmark™

ELEVATE YOUR CYBER AWARENESS

The SecuLore CyberBenchmark is a cybersecurity evaluation and augmentation of your network. We conduct a risk assessment and guide you towards an in-depth cyberdefense strategy that provides constant monitoring and protection.

Incorporates best practice of public safety experts:

- **FCC** Task Force for Optimal PSAP Architecture (TFOPA)
- **DHS** Emergency Services Sector recommendations
- **NIST** Cybersecurity Framework
- **APCO** Cybersecurity Primer
Public Safety
Targeted Cyber Attacks
Can the Past Predict the Future?

1a) TX: Eight years’ worth of Cockrell Hill Police evidence wiped out in ransomware attack (01/25/2017)

1b) KS: Ransomware attack hits Butler County network - 911 GIS unavailable (09/12/2017)

2) TN: Ransomware attacks City of Spring Hills impacting 911 dispatchers computer systems (11/08/2017)

3) ID: 911 Dispatchers Affected by County-Wide Ransomware Attack (02/01/17)

4) DC: Police hit by ransomware lose 70% of CCTVs before Trump inauguration (01/30/17)

5) NY: Schulyer County [NY] 911 system crippled by hacking – unable to dispatch deputies (09/07/2017)

6) OH: Licking County takes a licking - 911 down for the count (02/17/17)

7) MO: Warren County sheriff’s office leaked police informants/victims audio after ransomware attack (03/16/2017)

8) TN: Wannacy ransomware hits Murfreesboro emergency services (07/05/2017)

9) NC: Ransomware shuts down county servers – hackers retaliate after not being paid (12/04/2017)

10) NY: Brookhaven is one of 76 government sites hacked by ISIS (06/26/2017)
SecuLore recorded a total of **132 Public Safety incidents** in **40 states** over the last 2 years!
## Cyber Attack Profiles

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phishing</strong></td>
<td>An email attack, intended to make the victim take an action that installs malware on the victim’s machine.</td>
</tr>
<tr>
<td><strong>Web site drive by</strong></td>
<td>A technique that lures a victim to an infected web site, thereby installing malware on the victim’s machine.</td>
</tr>
<tr>
<td><strong>Ransomware</strong></td>
<td>Malware which, once activated on a victim’s machine, encrypts data that can only be unlocked by paying a ransom.</td>
</tr>
<tr>
<td><strong>Persistent threat</strong></td>
<td>Malware that hides on a system and which either slowly leaks information to the attacker or awaits activation.</td>
</tr>
<tr>
<td><strong>Hacking</strong></td>
<td>A brute-force attack method by which an attacker identifies a system vulnerability and then directly exploits that weakness.</td>
</tr>
</tbody>
</table>
Cyber Attack Profiles

Which Attack Category Is:
- Fastest growing
- In fastest decline
- Largest
- Most preferred vehicle
- Most undocumented

Phishing
Web site drive by
Ransomware
Persistent threat
Hacking
Types Of Cyber Attacks

- **Phishing**: Most preferred vehicle
- **Web site drive by**: In fastest decline
- **Ransomware**: Largest
- **Persistent threat**: Most undocumented
- **Hacking**: Fastest growing
Cyber Attacks Breakdown: Phishing

Phishing

NH, AL, ME, NC, MA, IA, PA, MD, SC, TX, FL, TN
Hackers Love To Phish

- Phishing
- Phishing + Social Engineering = Spear Phishing
- Spear Phishing + Top Dogs = Whaling
Continuous Monitoring Helps with Phishing

Hacker in Thanksgiving PSAP Attack used a phishing attack as a cover-up

Allows for repeating an attack

Came from many countries - but most from US!
Cyber Attacks Breakdown: Bad Web Sites

**Phishing**
NH, AL, ME, NC, MA, IA, PA, MD, SC, TX, FL, TN

**Website drive by**
WY, HI, IN
Four Types - Website Drive By

1. Website with similar name

2. Website embedded with Ransomware

3. Link in email

4. Attachment in email
Continuously Monitor for Bad Web Addresses

Look for non-US destinations

TOR
JAR
North Korea
Cyber Attacks Breakdown: Ransomware

Phishing
NH, AL, ME, NC, MA, IA, PA, MD, SC, TX, FL, TN

Website drive by
WY, HI, IA

Ransomware
NH, AL, ME, NC, MA, WY, FL, IA, TX, HI, MN, CA, PA, MD, IN, AR, SC, DC, OH, IL, ID, MO, GA, TN, LA, KS, CO
WannaCry - Laterally Attacking Ransomware

Once behind the firewall, a hacker acts like IT personnel

Even a “segmented” 911 center can be attacked/infected in this way

Initial Attacker Unknown?
MalwareTech: As of May 19th, 416,689 unique IPs have been infected 150 countries - over $86K in bitcoin ransom collected

“Kill switch” found by UK cyber researcher

First infection: 7:24am UTC

Kill switch active: ~12:30 UTC

New variants!!!

Final count: over 2M sites

Largest attack ever seen
Wannacry looked for open 445 ports and spread via a vulnerability in versions of that protocol.

Hundreds of thousands of machines infected in
Net BIOS Server Session (or NBSS) protocol uses ports 445 and 139 - the Wannacry exploit doorways
## Cyber Attacks Breakdown: Persistent Threat

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>States/Provinces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>NH, AL, ME, NC, MA, IA, PA, MD, SC, TX, FL, TN</td>
</tr>
<tr>
<td>Website drive by</td>
<td>WY, HI, IA</td>
</tr>
<tr>
<td>Ransomware</td>
<td>NH, AL, ME, NC, MA, WY, FL, IA, TX, HI, MN, CA, PA, MD, IN, AR, SC, DC, OH, IL, ID, MO, GA, TN, LA, KS, CO</td>
</tr>
<tr>
<td>Persistent threat</td>
<td>Unknown?</td>
</tr>
</tbody>
</table>
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.
Note heavy traffic within the US
Persistent Threats From Russia - Hidden Sources

Note use of benign US corporations
Cyber Attacks Breakdown: Hacking

- **Phishing**: NH, AL, ME, NC, MA, IA, PA, MD, SC, TX, FL, TN
- **Website drive by**: WY, HI, IA
- **Ransomware**: NH, AL, ME, NC, MA, WY, FL, IA, TX, HI, MN, CA, PA, MD, IN, AR, SC, DC, OH, IL, ID, MO, GA, TN, LA, KS, CO
- **Persistent threat**: Unknown?
- **Hacking**: RI, NJ, FL, CO, NY, MD, AR, WI, DC, OH, CT, ID, MO, GA, TN, IN, IL
Thanksgiving PSAP Attack began with a scan two days before ransomware execution.

This Hacker loved to scan from Iran.
Thanksgiving PSAP Attack: Strikes a Web Server

Monitor inside traffic Alerts sent to SOC

4 Layers of Protection
- Web reputation
- Firewall
- Email antispam
- Workstation antivirus

Monitor outside traffic Full data capture

4 Layers of Protection
- Web reputation
- Firewall
- Email antispam
- Workstation antivirus
Hacktivism And Terrorism

Anonymous:

- Published Baltimore Police officials emails and passwords after Freddie Gray death
  - City faced cyberattacks amid chaos and unrest on the streets

- Released Cincinnati PD officers’ data
  - Jeopardized safety

ISIS & ISIS-Linked Groups:

- Website defacing & recruitment videos

- Stemms County, MN website redirected to a page that stated "this is not an attack we are just testing some tricks."
  - This is just the beginning…

TOO MUCH TRAFFIC!

Darker color indicates greater amount of traffic.

Legacy PSAP, as part of local infrastructure, is exposed to typical traffic patterns.
Implement/Enforce Rules Unique to Public Safety

- 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
Unwanted traffic can still occur because of malware on internal systems (IoT?)

Comparatively Quieter Activity
2018 Brings New Threats - Meltdown/Spectre

**Meltdown:**
- Easy to exploit, but much easier to patch
- Most vendors have software patches available
- Exploits Javascript - used frequently in browsers

**Spectre**
- Harder to exploit – may need hardware patch
- Allows access to memory on machine

Contact your vendors!
- Make sure that they are aware of these vulnerabilities
- Ask them about their plans to protect your systems

Do not save passwords in your browsers - clear any so stored
Only go to trusted sites
Cyber-Protecting Our Nation’s Most Important Number:  9-1-1

NG9-1-1 Needs Cybersecurity  (and E9-1-1 Does Too!)

Timothy Lorello – President & CEO
SecuLore Solutions
Tim.Lorello@SecuLore.com