

CYBERSECURITY ATTACKS THREATEN 9-1-1 RESPONSE

Timothy Lorello | President & CEO | SecuLore Solutions

Our public safety infrastructure is under cyber-attack! Like every other part of the internet-based economy, these systems are continuously exposed to attacks that have been increasing at an alarming rate.

Over 240 million 9-1-1 calls are made every year, with over 75% coming from wireless phones.^{1,2} Almost 6,000 public-safety answering points (PSAPs) field the calls and work in conjunction with approximately 70,000 police, fire, and emergency medical dispatch centers to send resources to those in need.^{3,4} All such centers across the country rely heavily on data systems to answer calls, manage resources, and maintain 24/7/365 operational status.

ATTACK VECTORS ON EMERGENCY SERVICES

For PSAPs and dispatch centers, two forms of cyber-attacks are particularly threatening. Telephony Denial of Service (TDoS) attacks are particularly challenging for systems like 9-1-1 networks, which accept telephone calls as a foundational part of their service. Internet-based telephony has allowed attackers to flood call centers with large numbers of internet-originated calls, inundating them with erroneous voice traffic that can prevent real emergencies from getting through. This can be done as a prank, or with an intent to extort a ransom.

The Department of Homeland Security (DHS) has reported that over 200 PSAPs across the country have been affected by TDoS threats, attempting to extort a \$5000 ransom.⁵ Failure to pay the ransom would result in a flood of calls with the intent of disrupting the PSAP's ability to provide emergency assistance to callers. TDoS attacks have also occurred with a number of hospitals across the country.⁶

The second type of attack, ransomware, is experiencing a meteoric rise across the country. It's begun to plague police and sheriff offices, which have had to face the embarrassment of paying cyber criminals to get their data back.

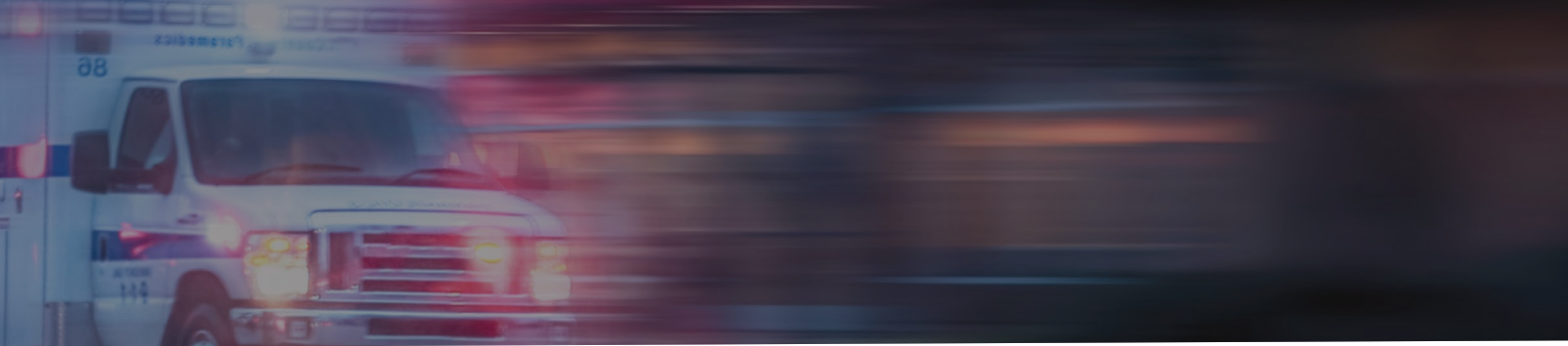
- The Internet Crime Complaint Center has seen almost 7,700 ransomware complaints since 2005, and cyber criminals have extorted over \$57.6M.⁷
- An April 2016 NBC news report revealed that police departments across seven states have been hit by ransomware attacks since 2013.⁸
- The March 2016 Beazley Breach Response Service tracked a 400% rise of ransomware since 2015.⁹

The vast majority of our public safety infrastructure is not equipped to deal with this onslaught. 80% of all PSAPs have fewer than five call-takers, lean budgets, and limited IT staff. And even if budgets were more robust, there are simply not enough cybersecurity experts available with the requisite skills to support their imminent needs.

9-1-1 EVOLUTION DEMANDS IP-BASED SOLUTIONS

In addition to the usual challenges, the public safety market is going through a major shift to next-generation, IP-based technologies, known as Next Generation 9-1-1 (NG9-1-1). Users of smartphones send massive amounts of texts, pictures, and videos, but these forms of data communication cannot be delivered from the scene of an emergency to a legacy PSAP. Because the vast majority of 9-1-1 calls come from these devices, PSAPs must upgrade to NG9-1-1 systems in order to accept these new forms of communication. However, this modernization exposes the PSAPs to Internet-based attacks, and therefore requires cybersecurity improvements concurrent with the system upgrades.

The Federal Communications Commission (FCC), which oversees wireless carriers and their efforts to support 9-1-1, has been fiercely driving an agenda to promote NG9-1-1. Recognizing that NG9-1-1 will expand the cyber-



attack surface of PSAPs, the FCC Chairman has pressed Congress to provide funding that would support their cyber protection.¹⁰ The current FCC Chief of the Public Safety and Homeland Security Bureau has frequently stated that cybersecurity tops his list of major public safety concerns.¹¹


PROPER LEVELS OF CYBERSECURITY CAN BE ACHIEVED

With the use of appropriate tools and processes, cyber-attacks such as the following can be detected:

- Exploits that have breached a PSAP or dispatch center's firewall and are trying to exfiltrate data or communicate with an external server for further instructions
- Intentional or unintentional visits to dangerous web sites by insiders
- Digital attachments with embedded malware sent to PSAP email addresses

To properly protect their internal data and data flow, PSAPs and dispatch centers must learn how cyber attackers operate. First, they must understand their current state of cybersecurity strengths and vulnerabilities. This includes following guidelines provided by the FCC and DHS. Then, through the use of proper practices and tools, they should monitor their data flow and visualize their traffic patterns. It is now possible to interrupt cyber-attacks before they start, or detect those that have had initial success and prevent them from doing serious harm. It is wise to assume that cyber attackers will eventually penetrate the PSAP or dispatch center's defenses, so it is important to have defensive detection methods in place and backup procedures that will enable rapid restoration of a center's function should a breach occur.

To accomplish all of these steps, we must recognize that these cybersecurity solutions will be used by public safety IT managers with a wide range of expertise, from inexperienced to advanced. A combination of sophisticated data protection systems coupled with refined, intuitive data visualization techniques will create PSAP cyber situational awareness and readiness.

Only a handful of cybersecurity companies have extensive knowledge of 9-1-1 systems and the necessary expertise to address this emerging marketplace and the problems they face. To address the scope of these concerns, cybersecurity firms must work in collaboration to serve the public safety market, building the capabilities required for continuous protection. 

About the Author:



Timothy Lorello is President and CEO of SecuLore Solutions, a cybersecurity company focused on solutions for the public safety market. Mr. Lorello has been presenting technology solutions to public safety audiences for over fifteen years, has provided frequent guidance to the FCC, and has testified before Congress on matters related to the nation's public safety infrastructure. He holds a BS Honors in Physics from University of Chicago and an MSEE from Northwestern University. Mr. Lorello has been awarded 20 patents.



Sources

1. National Emergency Number Association. (n.d.). 9-1-1 statistics. Retrieved September 22, 2016, from <http://www.nena.org/?page=911Statistics>
2. 2015 National 911 Progress Report (Rep.). (2016, February). Retrieved <http://www.911.gov/pdf/National-911-Program-2015-ProfileDatabaseProgressReport-021716.pdf>
3. National Emergency Number Association. (n.d.). 9-1-1 statistics. Retrieved September 22, 2016, from <http://www.nena.org/?page=911Statistics>
4. Reaves, B. A., Ph.D. (2011, July). Census of state and local law enforcement agencies, 2008 (Rep. No. NCJ 233982). Retrieved <http://www.bjs.gov/content/pub/pdf/cslea08.pdf>
5. Department of Homeland Security (DHS); Intelligence Assessment: Cyber Targeting of the US ESS; 09/2015; p.3
6. Finkle, J. (2014, April 23). Exclusive: FBI warns healthcare sector vulnerable to cyber attacks. Retrieved from <http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423>
7. Department of Justice report to the Senate, 03/04/16
8. Francescani, C. (2016, April 26). Ransomware hackers hold U.S. police departments hostage. Retrieved from <http://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746>
9. Beazley Group. (2016, March). Beazley Breach Insights 2016 (Rep.). Retrieved https://www.beazley.com/Documents/TMB/BBR/BeazleyBreachInsights_March2016.pdf
10. Chairman Tom Wheeler. Hearing before the House Subcommittee on Communications & Technology, 07/12/16
11. Martini, S. (2016, March 16). FCC Chief of Public Safety and Homeland Security Bureau: "9-1-1 must remain tailored to serve communities". Retrieved from <http://psc.apointl.org/2016/03/16/fcc-chief-of-public-safety-and-homeland-security-bureau-9-1-1-must-remain-tailored-to-serve-communities/>