

'Holistic' approach needed for cybersecurity threats in age of FirstNet, next-gen 911

Urgent Communications By Jill Nolin

September 4, 2014

When hackers ramp up efforts to attack next-generation systems such as [next-generation 911](#) networks and the nationwide public-safety broadband network, public-safety professionals must be ready to stay a step ahead of them, say cyber security experts.

“We can’t be complacent about this threat, nor can we take the path that we have for many years of setting up a security perimeter, installing the anti-virus software on our machines, putting intrusion detection in place in the networks and then letting that be enough to try to protect our networks and our data,” Stephen Ashurkoff, a next-gen 911 systems integrator for General Dynamics IT, said during a session at the recent [APCO](#) conference in New Orleans.

“As the threats evolve and as the hackers become more sophisticated, we also have to evolve the way we address those concerns and threats.”

Ashurkoff said he has noticed a “deep misunderstanding” in the public-safety community about the threat. It’s difficult for people to see the danger when it comes to networks like next-generation 911, because there is no apparent benefit to the attacker for targeting a [public-safety answering point](#) (PSAP) and even a hacker can see the obvious harm to the community.

“What people don’t realize is that, as we’ve added all these capabilities to our communications systems, we’ve become part of a larger web of networks, and there are parts of those networks that are going to be attacked for logical reasons, because there is a way to make money or there is a way to steal something that they think is important,” Ashurkoff said.

“And, as we move into the world of NG-911 and [FirstNet](#), we’re accessing data that also has a monetary value,” he said. “As we’re looking forward into the future of being to access health records or have easy access to criminal databases or license plate views, etc. etc.—that information is attractive to the threat community, the ones who want to turn that into a financial or military gain.

“So, our attractiveness is growing and our vulnerability—as a result of taking advantage of these new technologies and the networks that are available to us—is also growing.”

There have also been reported cases where hackers have tried to tie up the phone lines at 911 call centers and threatened to continue to overload the system until a sum of money was paid.

Although there will be weaknesses in a network and someone looking for those weaknesses, the public-safety community can take measures to defend itself from attacks, said Ashurkoff and Jeremy Willingham, director for advanced cyber training for TeleCommunication Systems (TCS).

Constant communication among public-safety agencies is an essential part of counteracting these ever-evolving threats, because hackers are swapping information. Also, if one agency is experiencing a particular vulnerability, other agencies probably are, too.

“There is a threat to public safety. We need to be very cognizant of that fact and that it’s growing,” Ashurkoff said. “In defending against it, we have to take a holistic approach. We can’t rely on one tool or one service provider to give us that protection. We need to take charge of our security.

“Finally, I can’t emphasize enough: collaboration, collaboration, collaboration. We need to share. We need to stay ahead of those who are attacking us.”

Continuous training is also important, as strategies change and new threats are ever surfacing. Employees also represent a vulnerability. All it takes is something as simple as an employee clicking on a bogus link to “give away access to the system,” Willingham said.

Willingham said it’s also important for [PSAP](#) managers to embrace their role in cybersecurity. That means understanding the details of their system and what the weaknesses are, as well as identifying what controls need to be implemented and what aspects of the network need to be

monitored.

“One of the questions that we’ll ask is, ‘What is the normal data flow on your network for an average day, an average week, an average month?’ And the number of people who can actually answer that question is very small,” Willingham said.

“How does your network normally function? How does it normally look? What users normally access given resources? These are things that leaders and managers need to understand, so they can start to identify what is abnormal. If your secretary never accesses the file server and, all of a sudden, she’s accessed that file server 53 times in the last two days, that is abnormal.”

[Link to Article](#)

[Link to Urgent Communications News Articles](#)