Cybersecurity & the PSAP

Protecting Against Malicious Cyber Activity

BY JAY ENGLISH

CDE #36485

Next Generation 9-1-1 (NG9-1-1) and coming national public safety broadband network being developed by FirstNet bring exciting new capabilities and possibilities to our PSAPs. As with any new technology, however, they also present new challenges. Principle among these challenges is the ability to secure our networks and systems from unwanted intrusions and attacks.

Merriam-Webster dictionary defines cybersecurity as: "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack."[1] The U.S. Department of Homeland Security (DHS) opens its discussion of cybersecurity with the following statement: "Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. We rely on this vast array of networks to communicate and travel, power our homes, run our economy, and provide government services. Yet cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy."[2]

SECURITY THREATS

Cybersecurity risks have the potential to affect everything from national security and public safety to our ability to use banking services or even power our homes or vehicles. Due in large part to the reliance of critical infrastructure such as banking, communications and energy transmission on cyber systems, cyber security touches virtually every aspect of modern life. In addition, as we have found in recent years, even the most sensitive and proprietary information is subject to intrusion and attack from malicious cyber entities, including "hactivists," criminal groups and even nation states.

As our technology changes, so do the threats we face. In order to ensure continuity of operations, and the safety

ALL PHOTOS AP

of the citizens we serve, it is essential that we learn to protect and secure our networks and systems in both the public and private sectors.

While we may be aware of the threats that exist, many do not understand just how vulnerable our public safety systems are to cyber attack. APCO has been working with DHS, the Federal Bureau of Investigation (FBI), the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), along with the major telecommunications providers and other key players, on a task force to investigate and develop strategies for recent Telephony Denial of Service (TDoS) attacks against public safety. To date, thousands of TDoS attacks have been identified, with nearly 800 of those attacks directed at public safety or public safety-related targets.

In the PSAP community, we've become accustomed to closed-loop systems. That is to say that our 9-1-1 networks have traditionally been secure, with limited access and substantial controls in place. Our computer-aided dispatch (CAD) software is typically designed and operated on closed, internal networks with little or no access to or from any system other than the 9-1-1 and radio systems maintained internal to the public safety entity. Even in this relatively secure environment, PSAPs, law enforcement agencies, fire-rescue organizations and even federal agencies have been successfully targeted and impacted by TDoS attacks.

SYSTEM VULNERABILITIES

The basic premise of cyber attacks against PSAPs is that the cyber criminals locate a pilot number for the target organization, and then begin a series of continuous phone calls to that number and all affiliated numbers. The ability of these cyber entities to automate dialing and propagate thousands of calls an hour against those numbers, tying up the phone lines and systems for hours at a time, can cripple telephony-based operations. As we know all too well, if we have no phone lines, we have no way of receiving requests for help, thus no way of sending that help. While the

actual 9-1-1 phone lines have not been as affected as other systems, there has been a definite degradation of operations at PSAPs and public safety communications facilities. These calls tie up not only administrative or 10-digit lines inbound to the PSAP (including alarm company numbers used to report fire, medical and law enforcement related alarms), but also the personnel that staff those lines. In addition, new concerns are emerging about the safety of the 9-1-1 closed-loop system, as we are discovering that the "loop" may not be quite as "closed" as we've always thought. Cyber actors are actively seeking back door access to 9-1-1 systems, and continue to look for ways to be more intrusive and disruptive, even with our legacy systems.

Given the vulnerability of our current systems, the need for education and emphasis on cybersecurity with emerging technologies takes on an even more important role. Unlike our current networks, next generation systems are based on the concept of emergency services Internet protocol networks (ESINets). An ESINet is a network of networks designed to facilitate interoperability and a rapid flow of information between the public, PSAPs and responders. NG9-1-1 systems rely on cyber capabilities and, as a result, are opportunistic targets for cyber attack. In addition to NG9-1-1 networks, we are beginning to see the advent of multiple apps intended to improve citizens' abilities to report activities, the PSAP's ability to receive and relay those reports, and responders' abilities to obtain much-needed, near real-time information directly from the scene. Our ability to secure our networks and critical data from cyber attack must be a primary consideration when designing and implementing any new solutions. Added to this, the exciting prospect of the first nationwide public safety broadband network, built and maintained under FirstNet, will allow fast and efficient flow of data via wireless networks, using a uniform technology and network design to further ensure interoperability. However, as with NG9-1-1, FirstNet is an IP-based network of networks, another ESINet, and will also be subject to cyber risk.

For all of these reasons, now is the time to begin educating ourselves on cyber security. We need to understand not only the risk, but what we can to do mitigate that risk. Waiting until the networks are built is too late. While we strive to combat the current cyber attacks, cyber criminals are already designing the next vector for attack, and they are constantly adapting. As public safety professionals, we are accustomed to adapting quickly to changing conditions. We need to use this experience and our capabilities as communications experts to plan for and prevent cyber attacks.

MITIGATING RISK

So, we know the threat exists, we know it is expanding, and we know we have to plan. What is the next step? Unfortunately, there is no "silver bullet" that kills cyber crime. There are, however, a number of proactive steps we can take. Here are a few suggestions:

1. Have a pre-plan. Recent TDoS attacks resulted in activation of a task force to provide best practices and much-needed cooperation among multiple parties. Those best practices can be found at http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service/.

2. Study NG9-1-1. Our ability to defend our networks and systems is directly related to our understanding of those systems. There are a number of resources available to provide education on NG9-1-1 and emerging technologies. Some good places to start are www.apcointl.org/resources/next-generation-communications-systems.html and www.ng911institute.org. Look into available security options for networks, all the way down to the PSAP equipment level. Consider what solutions your records systems integrate with, your CAD and mobile requirements, recording and retention requirements, and integration of any outside network into your "closed" PSAP or jurisdictional systems.

3. Research FirstNet and emerging apps. FirstNet is developing exciting technology that will bring some tremendous capabilities to the public safety community. APCO encourages all members of the public safety community to begin researching and understanding the networks and systems that will make up the national public safety broadband network here: www.ntia.doc.gov/category/firstnet. Once you have a fundamental understanding of the concepts here, look into the security and priority sections of the FirstNet Statement of Requirements, found at www.npstc.org/statementOfRequirements.jsp. This research into security requirements provides a toolbox of information and questions as well as some design considerations for your own systems.

LOOK AHEAD

In addition to the actual FirstNet system, applications will play a key role in public safety. Today, apps are fun and convenient ways to send messages, retrieve information about a selected topic or even find the closest place to eat when you're traveling. In the future, apps will provide lifesaving services and links to public safety in near real-time. Understanding the makeup of emerging apps is critical to understanding how the networks of tomorrow will work. APCO has established a website specifically designed to provide public safety professionals with a one stop source of information on public safety related apps. The site can be found at www.appcomm.org.

Once you've done some research, prepare a list of related questions for your vendor partners as you consider what systems you plan to implement in the future. Don't underestimate the importance of security and don't be afraid to ask tough questions. If your concern is opening up your network to any outside transport system (such as the Internet) explain that concern and don't take "don't worry, we've got it covered" for an answer. Your understanding of these emerging technologies, the networks and systems that comprise them, and the security risks and potential solutions available, will provide you with the ability to ask direct, technical questions and will allow your vendor partners to provide direct and focused responses, as well as design solutions that will both meet your needs and provide for the safety and security of your PSAP.

Even the most sensitive & proprietary information is subject to intrusion.

Cybersecurity is a concern for all of us. Understanding our vulnerabilities and planning for ways to protect against them is the best defense we can take. If the worst happens and your system is hit by a cyber attack, having a plan available for immediate implementation and mitigation, and establishing critical partnerships with technology partners and government resources, will lessen the impact to your organization and increase the ability of enforcement agencies to locate and prosecute the perpetrators responsible.

These are exciting times in public safety technology. We cannot for one minute allow the threat of cyber attack to deter us from progressing into what may well be the most significant advancement in emergency communications since the advent of two-way radio or 9-1-1 services. That said, our resolve to deploy these new technologies must be matched by our resolve to combat cyber criminals on every front. Education, planning and a unified approach will ensure that we can do just that. ||PSC||

JAY ENGLISH is APCO International's director of communications center and 9-1-1 services. He has served in public safety and emergency communications for more than 25 years. He also has a background in electronic warfare and intelligence with the U.S. Air Force and served as a cyber crimes investigator during his law enforcement career.

REFERENCES

1. http://www.merriam-webster.com/dictionary/cybersecurity
2. http://www.dhs.gov/topic/cybersecurity