Three Critical Steps to Next-Gen 911 Security (Contributed)

Dan Zeiler | October 3, 2018

Next-Generation 911 (NG911) services are the future for emergency call centers. Unfortunately, so are cyberattacks. Over the past two years, there have been more than 180 cyberattacks on public safety agencies and local governments. About 20 percent of them impacted 911 call centers.

As we move from a legacy, landline network environment for Public Safety Answering Points (PSAP) to an open Internet protocol-based solution, we can more accurately pinpoint the exact location and nature of emergencies and help save many more lives. But a more open system is a more vulnerable system. This is the dilemma that NG911's advancements have created: if you can communicate, you're vulnerable. If you can't communicate, you're irrelevant.

Emergency call center managers must accept the reality that any NG911 solution that can interface with other applications and platforms (GIS technologies, remote sensor data, shot detection, remote camera access) is subject to compromise.

The good news? The risk cyberattacks pose can be mitigated by strong defenses. In fact, there are proven steps PSAP managers can take to maximize NG911 while

minimizing the risk and impact of cyberattacks, and that starts with understanding the new environment at play.

Walled Garden vs. Cyber Garden

There is no more walled garden, the safe and secure place where dedicated lines and data flows were isolated and unimpeded by outside interference. Today, there is a new ecology called the “ cyber garden.”

The walled garden model assumed the wall itself was impenetrable. The cyber garden model assumes it’s not. PSAPs must adopt the attitude that the perimeter of the garden is constantly under threat; it must be patrolled vigilantly and reinforced with additional safeguards to thwart attackers who breach the perimeter.

To do this, PSAP managers must change the way they tend the garden. They need to replace lax practices with diligence and discipline. Use proven knowhow and experience, and implement meticulous short- and long-term cybersecurity plans that envision every contingency.

Here are the top three critical steps to keep PSAP centers secure.

Step One: Patch

In virtually all cyberattacks studied in 2016 and 2017, failure to patch — or update — systems regularly was the primary reason hackers were successful.

That’s why patching is the single most important way for PSAPs to limit the threat of cyberattacks. The key to successful patching is partnering with external and internal experts that possess the following qualities:

- Proven and broad technological expertise.
- Proactive experience developing and adhering to an aggressive schedule for updates and testing them to ensure proper installation and effectiveness.
- Confident worriers — confident in their abilities and strategies, worried about when the next attack is coming and prepared to deliver the bad news.

The obvious question is, “If patching works so well, why doesn’t everyone patch?” The answer: patching causes operational pain, and too few so-called experts possess the qualities enumerated above. Therefore, two additional patching strategies should be employed along with strong personnel:

- Develop a Patch Plan — written operational strategies and tactics so that patching isn’t delayed because of time off by critical personnel.
- Embrace an architecture that allows for automatic patching without impact. It won’t negate the need for human oversight, but it will help institute discipline painlessly.

As your Patch Plan evolves, it becomes harder to patch the most vulnerable older systems. The more frequently systems need patching, the costlier they become until, like an old car, repair costs outstrip replacement costs. Be wise about replacing older systems that are exposing you to risk. Track the costs, and use the savings and risk control to justify the capital costs of replacement.

Step Two: Assess Risk

Even if you have a new system, a solid Patch Plan and the right team to execute it, test it. Run a risk assessment before your NG911 system goes live.

Components of an effective risk assessment include:

- Expect and demand transparency and honesty. Whoever is conducting the assessment should be able to explain the results in detail and in terms you can understand. Risk is not a technical concern. It is a straightforward life safety concern.
- Start with: “What are we protecting?” If you don’t know what you’re trying to accomplish, false starts will multiply, and you’l l spend all your resources protecting something that might not be that critical.
- Develop a Risk Registry with four key components:
- Threats — List eight to 10 possible threats and threat scenarios.
- Vulnerability — Determine how vulnerable you are to each threat. Could it happen often, or is it a more unlikely scenario?
- Impact — Fully understand how both threats and vulnerabilities will affect your constituents.
- Risk Assessment — Understanding impact allows you to assess risk. Determine the potential fallout from each threat, and how to handle and prioritize scenarios.
- Communicate your Risk Registry to your funding sources! Get their buy-in. It’s amazing how much this simple act builds trust and changes outcomes.
- Reassess. Risks change, and deployments change. Re-examine your threats and vulnerabilities and update the Risk Registry annually or with any large-scale change.

Step Three: Plan

Always assume criminals will get into your cyber garden and wreak havoc in myriad ways. Plan accordingly. That means developing extensive strategies and tactics — with help from cybersecurity experts — for addressing as many scenarios as possible.

Components of an effective cybersecurity plan include:

- Know your normal: Set benchmarks, take inventory, know how everything is supposed to function.
- Check your backups: Practice restoring a few. Make sure you understand the timelines and impacts.
- Turn off unnecessary equipment: From unused switch ports and USB connections to services and old equipment, off is safer all-around.
- Create an environment of visibility: All devices should give alerts as their status changes. If a solution is in distress, it should alert operators that this is a new status. This ensures earlier and more effective alerting and provides the monitoring opportunity to detect failures before they happen. Check in regularly: Ask your teams, “If X breaks, how will that affect you, and what would you do?” Ask these types of questions once a quarter, and make sure your team members understand that there are no wrong answers.

- Develop an Incident Response protocol: when X breaks, how do you handle the situation? Who gets what calls? How do you control the fallout and get back to normal? How do you communicate with stakeholders?

Summary

In the end, risk is always present. By originating and maintaining a dedicated Patch Plan, you can control and reduce risks. Once that plan is in place, evaluate where your risks are and what you're trying to solve. Start with the basic question, "Who/what is going to get hurt, and what does that look like?" Next, conduct threat modeling and assess vulnerabilities by creating a Risk Registry. Finally, share the registry and explain it to decision-makers in non-technical terms. Come to agreement with them about tolerating those risks or providing funding to remediate them.

After that, it's a matter of never getting comfortable in the new cyber garden. Plan for the worst. Plan for things to break or be impacted. It will make all the difference.

http://www.govtech.com/security/Three-Critical-Steps-to-Next-Gen-911-Security-Contributed.html