WAUKESHA COUNTY DEPENDS ON PATCH MANAGEMENT TO MINIMIZE CYBER THREATS

For the first time ever, first responders and dispatchers in Waukesha and Milwaukee Counties have the ability to easily communicate across county lines, municipalities and agencies using the new OASIS (Organization of Affiliated Secure Interoperable RF Subsystems) public safety radio system. The radio system makes interoperability easy for the first responder in the field, improving the way they communicate with each other and the 9-1-1 centers.

READY FOR A NEW RADIO SYSTEM

It was time for a new public safety communication system in Waukesha County Wisconsin; the analog system they had relied on for years was at the end of its useful life. So discussions began between Milwaukee County and Waukesha County to build an interoperable state-of-the-art communications system they could both share. They purchased a new, IP based P25 radio system; the Motorola Solutions ASTRO 25 simulcast 800MHz. The system called OASIS has a single shared core with two sub-systems and multiple public safety answering points (PSAPS) for 9-1-1.

The goals of the new system are to improve radio coverage, provide direct communication between users of different agencies, increase system reliability and security, and increase capacity. The go-live date for the system was March 15, 2017 when 9-1-1 calls started being dispatched.[1] "When we looked at public safety coordination, we really focused on the idea that there are no boundaries," said Gary Bell, director of emergency preparedness. "The IP environment allows for that to occur relatively effectively so we can share infrastructure and assets, and provide better outcomes for the responders."

WAUKESHA COUNTY, WISCONSIN

- Population: 390,000
- Third most populated county in Wisconsin
- Milwaukee Metro area resides within its borders
- Adjacent County is Milwaukee County to the East

RADIO COMMUNICATIONS

ASTRO® 25 800MHz Simulcast System

Shared system with Milwaukee County

One shared core and two subsystems

In addition to Police and Fire/EMS the system also serves:

- 19 municipalities
- 13 county agencies
- 8 mutual aid partners
- Twelve 9-1-1 dispatch centers

MULTIPLE COUNTY INTEROPERABILITY ACHIEVED

In the past there were siloed radio systems serving different departments across the county. This caused problems when multiple agencies or departments responded to incidents. Chris Petterson, manager of the Waukesha County Radio Services, extols the benefits of the new IP-based radio system, "Now, everyone in Waukesha County has 100% ability to communicate with anyone else countywide. Now we have two-county interoperability. And with the advent of ISSI (Inter RF-Subsystem Interface), we interface with the City of Milwaukee, which is nearby, and, in fact, the State of Wisconsin. So now we've expanded interoperability to everyone in the county, in both counties."

FIRST RESPONDERS RELY ON THE RADIOS AS A LIFELINE

The new IP mission critical radio system is about serving the needs of the dispatchers and the first responders in the field. In addition to making sure the network is available Waukesha county radio service specialist, Steven Milner, talked about the benefits of servicing the mobile and portable radios to make sure they are optimized, providing a lifeline for first responders. "We make sure that our equipment meets all the latest standards, they are up-to-date on firmware so there is nothing that is going to affect our users in the field, (such as) somebody hacking into the system or getting a hold of a radio and reprogramming it or cloning the radio on the system. We really take a lot of care in how we program the radios. We use link-layer authentication. We use radio management. And we just make sure that everything is up-to-date. We're very careful about how we do it. We keep the system very secure, keep tight control on passwords."

RESILIENCY – BOTH PHYSICAL AND CYBER

Because the system is used by law enforcement and fire service personnel, when the system was being designed and built a lot of thought went into making sure the radio system was resilient, minimizing physical and cyber security risks. Redundancy is built into the system and precautions have been taken to a make sure the physical site and core equipment is always available. Towers were built to class 3 tower specifications for critical infrastructure; every site has standby generators, redundant uninterruptible power. There are fire suppression, intrusion alarms and video surveillance at every site.

The second part of the system resiliency is cyber security, protecting against potential cyber threats such as Malware, Botnets, denial of services and whatever potential threats lurk in the future. As Petterson explains, "We have taken every precaution we can think of to protect against fairly static events like power failures, and storms, things that are semi-predictable. Something like cyber attacks are new, they're evolving, and they're dynamic. The fact that we have Motorola and the engineers who designed this system actually actively evaluating everything, and looking at threats actively, and making those changes without our active intervention is really important."

CYBER ATTACKS ARE ON THE RISE

No IP-based system is immune to outside attacks including mission-critical IP communication systems. According to a 2017 survey by Ponemon, 98% of companies surveyed consider malware to be at the top of the list of threats with ransomware breaches on the rise, increasing from 13% in 2016 to 27% in 2017.[2]

Bell explains the potential threats to the mission critical network, "Every time you stand up a system almost immediately as soon as the system is on a network you're getting injects and attempts to get into that system. Black hats are out there trying to do damage or hold you accountable to get back at your data to pay them Bitcoin or some other cyber currency. What we try to do is make it more difficult for those people that are wearing black hats to get into our system to impact the functionality."

85% OF ALL TARGETED ATTACKS CAN BE PREVENTED BY APPLYING A SECURITY PATCH.[3]

PATCHING IS EXTREMELY VITAL

According to Homeland Security's Cyber Emergency Unit[3], as many as 85 percent of all targeted attacks can be prevented by applying security patches. Keeping a system patched with as many access points and infrastructure sites as an interoperable multi-county mission critical radio system has been a real challenge. In fact, 80% of data breaches are the results of poor patch management.[4]

"Software update and patching is extremely vital for any IP-based system," highlights Bell. He then goes on to explain the potential risks with doing the patching in house. "The OASIS regional radio system has multiple agencies with different IT professionals that would be responsible for making those updates. So, you just need one person who is on vacation or doesn't update the system and it can expose the entire system to a downtime event. Anything that is not touched or if you have different and disparate people doing that work, that's really 75% of injects where those vectors that come in and impact your systems. So, having the right software update service allows one individual to touch all those inputs into our system."

MANAGED SECURITY PATCHING

To address potential cyber security threats and provide a consistent professional process for updating security patches, Waukesha County chose to use a Security Update Service. Experts from Motorola Solutions monitor security updates for antivirus and related operating system patches as new threats and vulnerabilities are discovered. In dedicated test labs, teams of experts test and certify the updates are essential and critical and will not adversely impact the communication operations. When everything is validated and it is safe for the systems, the software is automatically updated. A status report is then provided, keeping the team informed.

The benefits to us are simple, explains Waukesha county radio service specialist, Steven Milner. "The patching is transparent to us. We have a subscription service, where they (Motorola Solutions) do the patching. We are not really aware of anything that happens in the background. It does not cause us any problems. And they advise us when they're doing patches or anything that we may see; they make sure that we're aware of it ahead of time."

From a management standpoint, Bell went on to highlight why they choose to do security patches through a service. "It's not something that I have to attribute to my staff in trying to make sure that they're subject matter experts on the systems because there are many systems. As we know, one little gap or one little opening from a patch update can cause significant issues. So we rely upon our industry partners, Motorola Solutions, in this case, to follow their protocol, to make those updates remotely into the system through the firewall."

> **"The reason why we chose the SUS (Security Upgrade Service) was really to prevent against ransomware attacks. What we try to do is make it more difficult for those people that are wearing black hats to get into our system to impact the functionality."**
>
> –Gary Bell , Director of Emergency Preparedness

TEAMWORK HELPS MANAGE THE COMPLEXITY

"Teamwork in system security, that's where we look at all relationships with our industry partners." Bell went on to talk about the value to his organization knowing that all of the updates, whether it's Windows® patches or McAfee® protection, are being pre-vetted before they are sent to the real world. The results are exactly what he wants. "No field partner (radio user) or any person behind the headset (9-1-1 operators) are seeing any kind of impact."

Bell continues, "Just knowing that there's individuals out there that are dedicated to watching the system, have a baseline for what normal traffic is, and can see when the spikes occur to take action definitely allows me as an administrator of the system to relax a little bit and focus on the things I need to focus on."

PEACE OF MIND

There is something very calming about knowing that we are doing everything we can to minimize vulnerabilities, protect against cyber attacks and provide law enforcement and fire personnel within Waukesha and Milwaukee Counties the best public safety communication system. As an administrator, Bell notes, "I want to be focused on my people rather than the technology. So, having individuals that are supportive behind the scenes, monitoring the system, making sure they (field and dispatch personnel) have the tools to do their jobs is vital."

For more information, please visit us at motorolasolutions.com/services

[1] OASIS Annual Report http://county.milwaukee.gov/ImageLibrary/Groups/cntyOEM/Gov-Board/2017OASISAnnualReportFINALsigned.pdf
[2] https://www.motorolasolutions.com/content/dam/msi/docs/services/support-services/cyber-security-professional-services/cyber-resilience-whitepaper.pdf
[3] https://www.us-cert.gov/ncas/alerts/TA15-119A
[4] https://dzone.com/articles/80-of-breaches-still-result-of-poor-patch-manageme

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. 800-367-2346 motorolasolutions.com