Warren County · Ohio
TELECOMatters
March 2015
our monthly newsletter of things that matter. all things Telecom.

School Emergency Button Activation Turned False Alarm… and Learning Opportunity

Imagine being on a routine traffic stop or sitting in a training class when you get dispatched for a School Emergency Button activation; an incident type only to be used when a school is in an active shooter situation. Your gut takes a hit but you clear your mind and get down to the business of rescuing and responding.

On Tuesday, February 24th at 9:47am, this is exactly what happened.

The school radio intended for a Montessori Academy in Deerfield Township was being programmed by a third party vendor, in preparation for eventual installation. When the accessory plug was pulled from the back of the radio, an emergency alarm was triggered unbeknownst to the vendor. The alarm was, however, very much recognized by the Warren County Communications Center Dispatchers and emergency responders who quickly went into action following their procedure - initiating a County All-Call for law enforcement and Deerfield Township Fire Rescue's Mass Casualty Incident 1st Alarm table. All (3) of Deerfield's stations reacted without delay along with their mutual aid agencies. Telecom also went into action knowing that it was a radio not yet active in a school, frantically calling the vendor and notifying dispatch.

In the 4 hectic minutes that it took to call off the emergency, WCSO's Lt. Faine and Deputy Doddy had already reached the school, reported an oddly-parked vehicle at the main entrance, addressed an individual exiting the building, interrogated the office staff, and were on their way deeper into the building. It was then that they heard Dispatch come across Primary reporting the false alarm due to radio testing. Deerfield Twp Fire also got the cancellation, while racing south to the presumed emergency.

As expected, responding agencies and anyone listening to the radio traffic were confused; and rightfully so. Telecom was not testing the radio, the radio was not at the school, and the school was not even aware that it had been pressed.

No school can begin use of their radio until they've been trained by Telecom, gotten their radio installed, and had their Memorandum of Understanding signed by a school representative, Fire Chief, Police Chief, the Director of Warren County Emergency Services, and the Board of County Commissioners. After these steps, their radio can be activated on the system.

Out of this incident, Telecom has put stricter policies in place regarding the implementation and maintenance of the school radios as they make their way to the schools; hoping to avoid this confusion again. Until the radio is active and approved by the Commissioners, test flags will be attached to the school's alias in CAD and the school's radio alias will begin and end with the words 'TEST' to visually alert Dispatch of a school not yet active.

The bright side of all this is that both WCSO and Deerfield Twp testify to the learning opportunity this gave them. As Chief Eisele says, "It's not a matter of *IF* this will happen in our community, but *WHEN*; so we need to be prepared." Agencies responded flawlessly, and proved they are prepared to protect the 56 schools we currently have on our radio roster; no hesitation, no doubt, they treated it like the real thing. They were able to gut check themselves and prove their readiness and willingness to serve and protect.

Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 adela.dingman@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

WARREN COUNTY WILL GO INTO SITE TRUNKING THIS MONTH…

as Motorola upgrades the radio system from 7.13 to 7.15 statewide.

Impact on radio users: you don't have to change your everyday talkgroup to talk with Dispatch; just know that you may lose contact with home if your radio leaves the Warren County towers.

In Site Trunking, Warren County gets disconnected from Columbus & neighboring MARCS towers, reducing our coverage to Warren County's (9) towers in a standalone status, like our old analog system. No talkgroup will talk back to Warren County until connection to Columbus/ MARCS is restored. Dispatchers operate from their consoles' BACKUP tab directing backup radios (shown right)

Dispatch Procedure

Dispatch Backup Radio		Use in Site Trunking
83 BKUP 1	→	83 SCHOOLS
83 BKUP 2	→	wandering, TACs
83 Clermont 1	→	Fire Primary
83 Clermont 2	→	PD Primary 2
83 Montg Co 1	→	PD Primary 1
83 Montg Co 2	→	Inquiry
83 MARCS 1	→	
83 MARCS 2	→	

Planned Site Trunking: Tuesday, March 24th 7:30-7:50PM & 11:30-11:50PM

Your talkgroup with Dispatch		Use in Site Trunking
PD Primary 1	→	NO CHANGE
PD Primary 2	→	
Inquiry	→	
Fire Primary	→	
Franklin PD	→	
Franklin Fire	→	
Lebanon PD	→	
Lebanon Fire	→	

Another radio failure we may someday face is… **Tower Failure**
Scenario: If Warren County's system of (9) radio towers 'goes dark', our radios will attempt to connect to neighboring county towers.

Impact on radio users: Most Warren County talkgroups are locked down to our towers only (Primaries, Inquiry, Local Ops/Commands), so users must use a backup talkgroup to communicate with Dispatch. See the diagram for your backup talkgroup, which will work off neighboring counties' towers.

Dispatch will direct their backup radios to these alternative talkgroups to communicate with agencies. Dispatch will broadcast over the backup talkgroups that they are in use in lieu of the standard talkgroups; with updates as available.

Your talkgroup with Dispatch		Use in Tower Failure
PD Primary 1	→	PD Hailing
PD Primary 2	→	PD Hailing
Inquiry	→	PD Hailing
Fire Primary	→	Fire Hailing
Franklin PD	→	Franklin PD 2
Franklin Fire	→	TAC 17
Lebanon PD	→	Lebanon PD 2
Lebanon Fire	→	TAC 19

Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net 2
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 adela.dingman@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

ATTENTION LAW ENFORCEMENT AGENCIES!

The Radio Team starts a tour of programming on Monday, March 2nd. After your radio is programmed it will have this tag, directing you to use LAW1 for all INQUIRY purposes.

LAW1,2,3 are being added to your Zone C; so find LAW1 and get familiar. Probation and Warden will use it as their main line to Dispatch; law enforcement will use it to run plates, SOCs, etc. The temporary change is due to an encryption key transition that won't be complete until all radios are programmed. **DO NOT USE INQUIRY after being programmed.** Telecom will announce the 'Return Normal use of Inquiry" to Chiefs and known Training Officers via email and post it on our social media and website once the last agency has been programmed.

*When in Site Trunking later this month as explained on Page 2, your Inquiry will be 'LAW1' if you've been programmed before March 24th.

Last Month's Training [Get on the list!]

Feb 3: WCSO Corrections [Radio]
Feb 5: Lebanon PD [Radio]
Feb 11: WCSO Corrections [Radio]
Feb 11: Mason Fire [Radio] [MDC] [ePCR]
Feb 12: Royalmont Academy [School Radio]
Feb 24: WCSO Corrections [Radio]
Feb 25: Montessori Academy [School Radio]

California likes our Training Material!

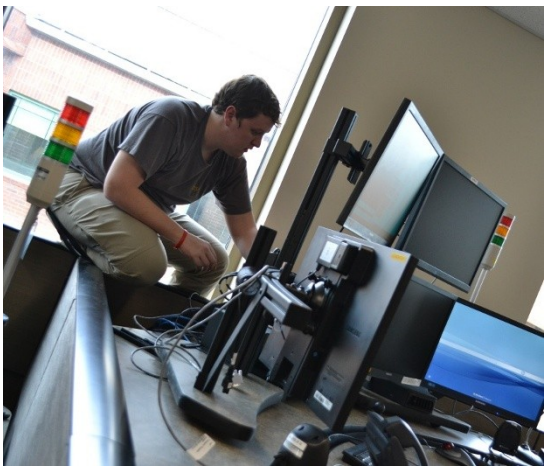
Sunny California's Office of Emergency Services / Public Safety Communications in San Luis Obispo contacted Telecom on February 20th looking for APX6000 training material. We provided them a PowerPoint, stripped of any sensitive Warren County information (emergency button details) that will lay the groundwork for them fleshing out a training specific to their programming.

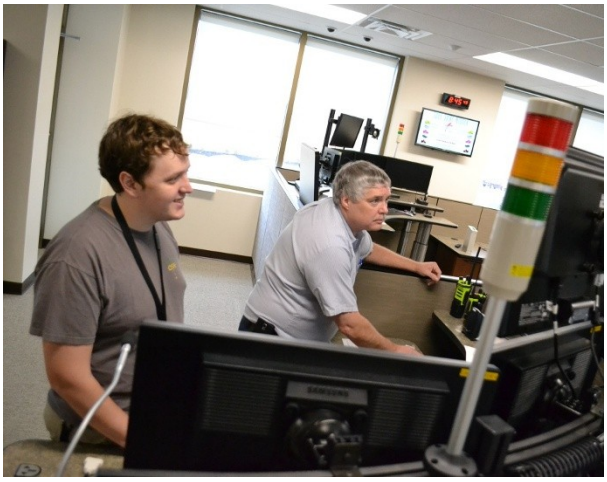
We hope our own agencies are as eager to use our training material as our followers out west!

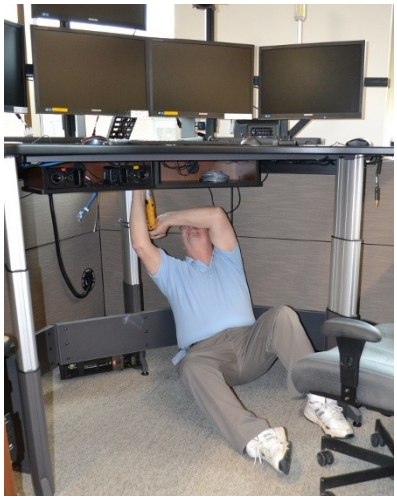
Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 adela.dingman@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

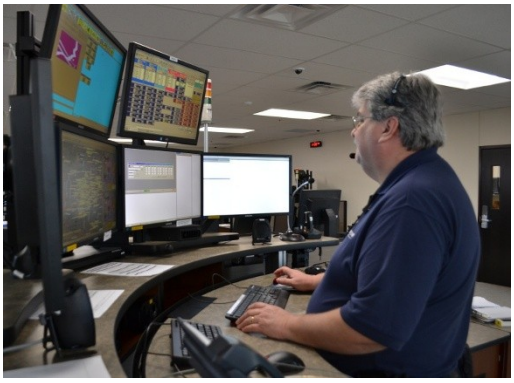
Telecom in Action! Relocating the Comm Center

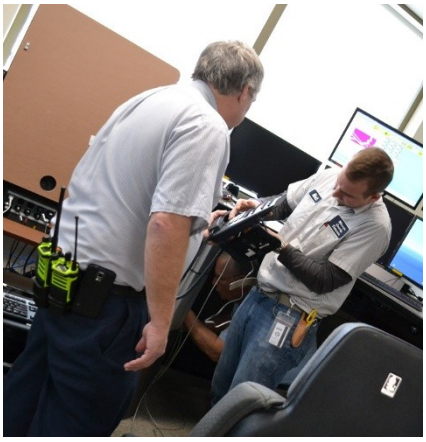
Disassembling the old center; moving 911, CAD, and Data to new building in phases so that Dispatching/call taking was never interrupted; connecting and repairing phones; ensuring every program and application works properly; running cable behind and through stations; cables, cables, cables! climbing up and crawling under workstations; and more!











MALWARE EXPLAINED!

(malicious + software) programs that infect your computer and cause harm.
Most common: virus, trojan horse, worm, adware, and spyware.

Malware can provide a backdoor into your computer for a hacker; destroy all your data, including programs, and the operating system; steal all your personal information and send it to an identity thief.

Signs of Malware Infection

- Sudden changes in how a computer or programs behave such as crashing, freezing, or missing files.
- The inability to use common programs.
- An unusual amount of pop-up windows
- Computer seems to be running slower than usual.
- Your anti-virus software keeps turning itself off.
- When you visit a web page and are directed to a site you didn't expect.
- The computer unexpectedly shuts itself down.
- Unusually low system memory.

Steps to take to prevent a malware infection

- Install a robust anti-virus software!
- Frequently perform a full-system scan with an anti-virus program.
- Avoid using unknown removable media, such as flash drives.
- Avoid visiting questionable websites.
- Be cautious when opening emails. If they include an attachment that you're not expecting, contact the sender and ask them about it.
- Avoid clicking on anything suspicious in an email or a website.
- Do not surf the Internet, read email, or perform your day-to-day computer functions when you're logged in with an admin or root account. Use these accounts for maintenance duties only.

Removing Malware

1. Start your computer in safe mode.
2. Run a full system scan using your anti-virus software.
3. If suspicious files are detected, let the anti-virus remove them.
4. If the software can't remove them, manually remove the file or files.
5. If necessary, obtain help online from experts. As a last resort, reload your computer.

Recovering From A Malware Infection

Manual removal may be necessary if the anti-virus software does not recognize the malware or if the anti-virus software has been disabled.
Microsoft Windows has a feature called System Restore which lets you roll back the system files to a previous date when there was no malware problem. Sometimes this may get rid of the malware, but further methods of removal may be required, depending on what malware has infected the system. In order for System Restore to work, it must be turned on in the computer's settings.
Apple's Mac OS has a similar feature called Time Machine. The feature allows you to backup your data and will keep track of changes, enabling you to go back to how the files were on a previous date. The backup files are kept and updated on a separate drive each time the drive is attached.

Viruses - software which can infect a computer and disable applications, corrupt data, or cause the computer to stop working properly.
A virus will be attached to a program, an email or document. In order for the virus to activate, you have to open the infected file.

Remember: Malware and viruses are not interchangeable terms; that is, while a virus is a type of malware, not all instances of malware are viruses.

Trojans - signs your computer is infected with a Trojan:

- Any of the symptoms mentioned earlier.
- A downloaded program fails, producing an error message or the computer begins acting strangely.
- Viruses or malware are detected on your computer.

A Trojan differs from a worm in that it does not spread itself. Usually, Trojan horses are created to obtain some information or data from the computer, or to gain access to the computer.

Worms - capable of replicating itself and spreading to other computers through a network. A worm stands alone and can replicate itself through entire networks without being attached to any file. They can spread through infected files on a flash drive, memory card, external hard drive, CD or DVD or through email. But the most common method for worms to spread is through network connections, including an Internet connection.

Spyware - is sneaky software used to monitor your computer usage, or take over full or partial control of your system without your consent or prior knowledge. You typically have no knowledge that spyware is installed, running, or transferring data about your activities. It can

- Install keyloggers that log all your keyboard key presses in an effort to capture passwords and other sensitive information such as bank account or credit card numbers.
- Scan your entire hard drive looking for specific pieces of information, such as SSN, credit card numbers, or bank account numbers.

Signs of Infection

- Any previously discussed symptoms.
- Your homepage is set to an unknown website, and you can't change it.
- A new user account may appear.
- Internet "pop-ups" (advertisements) appear.
- Your web-camera is activated (and you didn't do it).
- You can't get to certain websites anymore (like an anti-malware program download site).

Removing Spyware

Like other types of malware, spyware can often be removed by scanning your computer with the proper software. Some anti-virus software looks for spyware as well as malware. Since spyware has different patterns or signatures than malware, standard anti-virus software may overlook spyware. There are anti-spyware software programs designed specifically to help protect against, detect, and remove spyware.

- Perform a full system scan with anti-spyware software. If spyware is detected, allow the anti-spyware software to remove it.
- If your anti-virus or anti-spyware software doesn't detect any spyware but you are sure your computer is infected, research your computer's symptoms and get help online.
- Contact the anti-virus or anti-spyware scanning software's help desk. They can often walk you through the process of removing the spyware.
- Take your computer to a local computer repair shop. They can remove the spyware for you.
- If all else fails, reload your computer from scratch. This should be used only when all other options have been tried, since it will result in the deletion of all data on your computer's hard drive.

Director 695-1318 paul.kindell@wcoh.net | CAD/RMS 695-2800 paul.bernard@wcoh.net | Data Systems 695-1810 gary.estes@wcoh.net
Radio Systems 695-2860 gary.hardwick@wcoh.net | Telephony 695-1320 adela.dingman@wcoh.net | Training 695-2802 allison.lyons@wcoh.net

(Malware Explained) continued

Adware

Adware may be more of a nuisance than a real threat. Adware is a term for software that is installed on a computer in order to display advertisements. Generally, adware is not harmful to a system like a virus can be, but is mostly just annoying to many users.
Like any advertisement mechanisms, adware is designed to influence your buying decisions. The authors of adware programs get paid by the websites they get people to visit – as you can imagine, they are very motivated to get you there.

Signs of Infection

The most common sign of infection would be a constant stream of pop-up windows that are trying to get you to buy something from, or click to a particular website. Identifying signs include:

- Constant pop-ups on your screen as you are surfing the Internet.
- Internet searches that take you to a different search page than what you expected.
- Your home page is changed to a different page.

These behaviors or changes are unacceptable to many users. Some users are not bothered, however, and permit adware to be installed on their computers.

Preventing Adware

The best way to prevent adware is to be very selective of the sites you visit and the software you install on your computer. Only install software on your computer from software manufacturers you know and trust.As a general rule of thumb, if you have to pay for it, it probably will not contain adware. If the program is free, though, it may be bundled with adware. If you have any doubt, use a trusted search engine like Google, Ask.com, Yahoo!, MSN, etc. and check out that program's reputation.

Detecting Adware

As mentioned earlier, the symptoms to watch for include noticing that your computer is running slowly and experiencing many pop-up advertisements on your computer. These symptoms can indicate several types of bad software, though, so how can a person know for certain that he/she has adware installed, or which type of adware is installed? One way to detect adware is to use a software product, such as anti-virus or anti-spyware, that will search your computer and detect and remove suspicious programs.

Removing Adware

Adware can be extremely difficult to get rid of, or it can be removed relatively easily, all depending on the type of adware that has been installed on your system. Many anti-virus products now scan and remove adware automatically. Since this is not always the case, other ways of getting rid of the unwanted adware may be needed. Consider the following:

- Contact the adware scanning software's help desk. They can often walk you through the process of removing the adware.
- Take your computer to a local computer repair shop. They can remove the adware for you.
- Attempt to uninstall the adware just like any other program on your computer. This means using the operating system provided menu for removing programs.
- Download adware scanning software from a reputable company. The adware scanning software will typically try to remove any adware it finds on the system.
- Purchase adware scanning software from a local store. Usually anti-virus manufacturers also sell adware and spyware removal packages that can be used to clear up unwanted adware.

NEW TWO-FACTOR TOKENS ARE COMING!

We are in final stages of implementing new two-factor tokens. *Budget $25.00 per token.*

We do not have an ETA of when we will begin issuing the new tokens yet.

Each user will go through enrollment - more on that as we get closer. We will provide each Agency with a report showing the utilization issued tokens.

After completing audit of licenses by Microsoft, we will have to change how we handle the shared tokens, we are still looking at options but do not assume we will be able to issue station or MDC tokens. We will let you know as soon as we can confirm how this will be done.

Please contact Data Systems Manager, Gary Estes with questions 695.1810 or gary.estes@wcoh.net