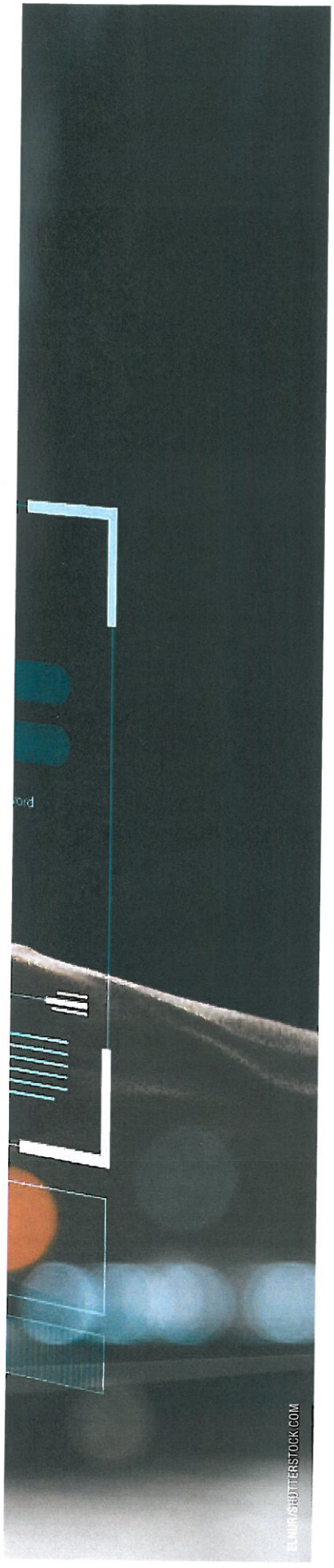
CDE #61715 and CDE#61716



SHOCK TO THE SYSTEM

How the Butler County Sheriff's Office Emergency Communications Section recovered from the technical impact of a cyberattack.

By Stephen Martini

PART I CDE #61715

The Butler County Sheriff's Office Emergency Communications Section serves 47 emergency response agencies in a county of 380,000 people just north of Cincinnati, Ohio. In the early afternoon of December 23, 2020, the center came under a cyberattack — a phishing attempt by a suspected Russian assailant.

The attackers gained access through a sophisticated phishing operation, demanded millions of dollars in ransom, and knocked out hundreds of computers and dozens of servers for several days, costing the county nearly $180,000 in repairs. We will focus on the technical and operational impacts of responding to and mitigating a cyberattack with the object of preventing future attacks.

THE BREACH

An employee of the sheriff's office clicked a link in an email that appeared to originate from a trusted vendor providing commissary services to the county jail.

"We had spoofed emails coming in from a vendor," said Butler County IT Director Ken Carpenter. "They were sophisticated, highly-targeted emails that were spoofed from a vendor that the jail regularly uses. It appears at some point (the vendor) had their email system hacked, and they (the hackers) were reproducing real content and using that for targeted, phishing-type emails to jail staff. It had all the proper signatures on the bottom of the email, and the 'from' name was correct. We had one person take the bait. They clicked it and basically infected their own system.

"We were using traditional anti-virus, anti-malware detection technologies and basically, it was a new malware that our detection solution didn't have definitions for until the following day. The malware then took bits and pieces of items that were in the Butler County employee's email inbox and used it to start generating more targeted attacks against our people."

Butler County Sheriff's Office Captain and 9-1-1 Coordinator Matt Franke stressed the authentic appearance of the phishing email.

"The key is it wasn't someone telling our employee that their Wells Fargo account had been locked, but they didn't use Wells Fargo," he said. "This one looked pretty good and unless you really looked at the sender and really dug down and actually got into the details, most people would not have recognized this soon enough. It was from somebody they normally deal with. It wasn't like it was unexpected or came from somebody they never talked to before."

The user didn't have much access beyond the basic servers storing public folders with publicly available data such as directives and news releases, which meant no data was lost as part of the attack.

"That was good," Carpenter said. "I hate to say it was lucky, but there's a little bit of luck involved

in that. The issue that we ran into is these cyber criminals schedule these attacks before holidays on purpose."

During holidays, the support teams that commonly monitor and mitigate attacks are away. They can be slow to catch the problem or begin mitigation efforts, allowing hackers the opportunity to do extensive harm.

THE FIRST 24 HOURS

Telecommunicators in the emergency communications center (ECC) noticed something was wrong when one CAD computer displayed a blue screen error (commonly referred to as the "blue screen of death"), and Supervisor Angie Mondello called Carpenter, who was at the hospital with his wife and baby. "I was an incident dispatcher — which is just an extra person for the law dispatchers who may need help — and one of my dispatchers said, 'Angie, my screen just went blue,' so I told everyone to get their phones out and take pictures of what they had on their screen," Mondello said.

Carpenter looked at the server remotely on his phone and saw files actively being encrypted — an immediate sign of an intrusion. He shut down the servers remotely. Franke praised the IT director's quick thinking. "I can't give this guy enough credit for picking up on it," Franke said. "The tech who lived closest then went to the center to physically unplug equipment."

Carpenter then called a variety of partners, including the FBI. "I basically said, 'Look, we haven't had a chance to evaluate this yet to determine what this is or if it could traverse to your network, but there's something happening, so you may want to look,'" he said. "Our radio vendor did a detailed scan of our radio system to ensure nothing had crossed over. A few servers were impacted, specifically those that allowed administrators to change aliases, program and inhibit radios. We were without that capability for a while.

"Our 9-1-1 staff looked into the 9-1-1 system, and our partners were reviewing their firewalls. We found it was confined to our (Microsoft) Windows domain — our group of servers. It looked at our domain, got an inventory of our computers and tried to spread to those. Fortunately, it didn't end up impacting 9-1-1, the radio or our partners (which was a possibility). Initially, we didn't know that so we had to treat it as if it did. My first call was to our local FBI field office.

Comfortable that the impact was limited to their domain, the ECC immediately reached out for help. During their initial phone call, Franke told Carpenter to take care of his family and committed to taking care of the problem. Still, three hours later, the two were side-by-side at the ECC, where Carpenter took charge of the investigation, and the pair worked to create a response plan.

"We didn't want to do this alone, so we started reaching out to cybersecurity professional firms who said, 'If you pay us $250,000 right now, we'll start helping you'," Carpenter said. "That was crazy. Then they told us we needed to call our insurance company and start there, and they'll get you somebody."

Butler County Sheriff's Office Chief Deputy Tony Dwyer served as part of the team and worked directly with the insurance company and cybersecurity experts. "The experts don't know us, and we don't know them," Dwyer said. "There's a stage where you're feeling each other out over conference calls and asking them questions. They don't want us to do anything because they don't know if we're an agency without qualified personnel, so they instructed us not to touch anything or do anything.

"First, we had to get on some conference calls and build some familiarity between personnel on both sides. As they got to know each other over the days and weeks, they came to understand that we learned how to protect something without exposing our network to more risk. Within the first few days, as the teams became more comfortable working with each other and sharing data, they told our team you can run with this or run with that. It did take a while and slow things down, but you have to play friendly with everybody.

"I couldn't just override this feedback — I could have, but it would not have been a good decision to say 'No, we're not going to do that because we must get this going again.' We did have to push them a little bit and say we know what we're doing and what we need to do, but you may have to tell me why we can't do it, or we'll have to do what's in the best interest of our agency. A bit trying at first, and then it sped up after that."

The attackers gained access through a sophisticated phishing operation, demanded millions of dollars in ransom, and knocked out hundreds of computers and dozens of servers for several days, costing the county nearly $180,000 in repairs.

Dwyer praised the efforts of the insurance company and their quick response in the moment of crisis. "Our insurer stepped right up — they had a plan," he said. "They had been through it. They had a law firm and an expert on speed dial. They contacted the law firm that ran the legal portion. The law firm contracted with cyber experts who walled off the bad actors. When disaster struck, there was a plan on the part of our insurer in place that didn't take time to put up — it was ready to go. That was pretty amazing because generally, we're the ones running everything in disasters, and this was one situation where I had to lean on others. We're not used to that. We were dealing with insurance, an attorney and a cyber expert. It worked out pretty quick."

The scale of the infection wasn't clear, and Carpenter knew they could address the attack one of two ways: either try to figure out the specific malware and the specifically impacted machines or assume everything is harmed and disconnect all access.

"We had dealt with other agencies before who tried to figure out exactly where the malware may have gone and exactly what might be impacted. It turns out that later on, they just get hit by it again because they didn't fix all of their vulnerabilities — they didn't clean everything up all the way," Carpenter said. "So, kind of on the spot, we decided to take the exact opposite approach. We took everything down. We shut down every server, every network component, every computer and we set out to restore all the servers back to the incident, rebuild all the computers."

The decision rendered 400 computers and 50 servers — many virtualized — entirely out of service. The most critical was the computers running the computer-aided dispatch (CAD) system in the communications center.

While Dwyer coordinated with the insurance company, Carpenter balanced liability concerns with operational needs. "The insurance company wasn't concerned with us getting back online," Carpenter said. "They honestly weren't that focused on the

SONG_ABOUT_SUMMER/SHUTTERSTOCK.COM

impact of us not having the full capability of our technical operations. They were worried about what data could be leaked that could cause them to be sued later.

"We spent the first three days not allowed to work on our server, not allowed to start restoring, not allowed to do anything — just capturing forensic data. The breach caught us entirely by surprise, so we spent three days capturing forensic data. The cybersecurity experts said we could only conduct our forensics using a certain hard drive. It's the holiday season, and they were sold out everywhere. We sent people to stores as far as Columbus, cleaning out all the locations and just driving further and further until they could get enough drives. It was a lot of scrambling."

Franke focused on logistical support to set up a process to rebuild workstations quickly while forensic evidence was captured from servers and potentially infected machines.

"It was a double-edged sword," Franke said. "On one hand, because it was a holiday, the work volume was decreased. But on the other hand, because it was a holiday, our resources were diminished as well. On the first day I gave a guy my credit card, and we sent him to Best Buy to buy external hard drives, and he was in uniform, fighting the Christmas Eve shoppers. He went to four or five computer retail stores to buy power strips and all sorts of things to equip an administrative conference room that we took over to set up a space to rebuild workstations 40 at a time (four rows of ten each). We didn't have all the electrical we needed to do that. We were stringing electrical extension cords and power strips together to make this work."

RESTORING SERVICES

An information technology team typically staffed with just three people swelled to 15, drafting anyone willing and able to help rebuild workstations. "During those first three days we had a team of people rebuilding workstations that we didn't have to keep down," Carpenter said. "We had a stack of 400 computers. We called in anybody that we could, and they were rebuilding them. The first thing we did was rebuild CAD workstations even though we didn't have a CAD server.

"We identified all the people we thought could help and then we worked through the process of assigning them roles. Then they had to be trained. We had a lot of people who repaired radios in our radio shop who were used to rebuilding computers. Instead of our computer guys working to fix computers, they were training other people how to fix the computer. We had a jail sergeant who was in school for IT stuff — we pulled him in. Everybody we could find, we pulled in to get this going as quick as we could.

"The guy who normally does our ankle bracelet monitoring reached out and said, 'I don't have anything going on over the holidays, and I don't know what I can do, but I'm glad to help.' We said, 'We'll take you!' He just went and collected computers, and when they were fixed, he took them back and plugged them in. He did that for like two weeks, and that was super helpful."

The group of trained professionals and volunteers worked across a variety of locations to restore services.

"We essentially had servers in two separate buildings," Franke said. "We had two people at each location looking at the servers. Four people were dedicated to rebuilding the workstations (desktops, laptops, mobiles). You didn't always have to have a high skill

level — you just had to…follow the checklist. We were essentially starting over. We called everybody back on December 23 while we were trying to figure it out, but by Christmas Eve it was pretty much voluntary — you didn't have to come, you didn't have to stay any amount of time.

"It ended up we had about 12 or 13 that essentially worked 16-hour days for the next four weeks —all the holidays. We didn't force anybody — if they needed to take a couple of hours off, fine, but they essentially committed to give up a month of their lives to make this work. That's what surprised the insurance company and the cyber experts. We were actually able to do things in weeks that normally took months."

The impact potential was extremely broad. The Butler County Sheriff's Office Communications Section's partner public safety agencies each had interfaced or satellite connections to the affected CAD servers that needed to be considered.

"We support the radio and 9-1-1 system for all of the ECCs in Butler County," Franke said. "There are other centers out there, which is why we had to confirm which network was impacted and then tell the other ECCs that we were not sure. Everybody is dependent on us for radio and 9-1-1, and a smaller number are dependent on us for dispatch services (CAD, RMS, mobile and other services), so we've got a network that is more complicated than just an office email system. About 50 servers were impacted, even though most are virtualized.

"If the mobiles for the police department were impacted, we had to go get them. Which fire station did we have to go out to get the station alerting system up and running? Does the sheriff's investigator who works in children's services have a computer on the network that needs to be rebuilt? Do we need to access that office on Christmas Day and get that computer off the network? There was a lot of the chaos we were going through because we were not sure where the impact was or how far reaching."

Carpenter recalled challenges obtaining specific machines. "We had one bomb expert — our explosives technician — who, because of some materials he had in his office, had his lock keyed separately. No one had a key. Someone had to pop the ceiling tiles out and climb down the wall to get into his office and get his computer because he couldn't be reached by phone over the holidays.

When disaster struck, there was a plan on the part of our insurer in place that didn't take time to put up — it was ready to go. That was pretty amazing because generally, we're the ones running everything in disasters, and this was one situation where I had to lean on others."

— Butler County Sheriff's Office Chief Deputy Tony Dwyer

"We run the mobile computers for a lot of smaller agencies that don't have their own IT departments so they were all impacted. We called one of the departments and told them they had to shut down their computers and bring them in. The chief refused, telling us 'You can't tell me what to do'. All kinds of strange interactions — it was a challenge."

When it was time to restore services, challenges arose again. "After the forensic data, we attempted to restore the CAD server, but we needed assistance from our vendor," Carpenter said. "Christmas had passed, and we were heading into New Year's. We had talked with our vendor who said they would handle it, but it was like a fight — it was New Year's Eve when we were trying to bring the CAD server back up, and they didn't want to assign us anybody. We said we were willing to pay the after-hours holiday price, but it was a major battle from a technical standpoint."

For the next six weeks, information technologists worked 12-hour days six days a week to restore county systems. Carpenter then spent the rest of the first four months of 2021 working to ensure Butler County is better prepared for the next attack.

"We didn't have everyone engaged for the full four weeks. We scaled down as we got the critical stuff out of the way and the bulk of the work done," Carpenter said. "Then we started giving people days off. After that, we went another four weeks with a lot of little things that people didn't have access to that maybe only one or two people needed. It took another six to eight weeks until we were 98% restored."

Franke nominated Carpenter for recognition and receipt of an Ohio APCO Chapter Gold Star Award, a program created to honor outstanding and individual performances that occur on duty. In his nomination, Franke stated, "Cybersecurity experts predicted it would be weeks before our critical systems could be back online and six months before any hope of complete restoration. Fifteen members of the Technology Services Division worked diligently to accomplish it all in less than two months; but it was the dedication, determination, intelligence and ingenuity of Director Ken Carpenter that provided the leadership necessary for us to achieve those successful results." Not surprisingly, he won the individual award, while the information technology team nominated by Dwyer received a Gold Star for outstanding team performance.

PART 2 CDE #61716

THE CALL

"You know that phone call that comes at the worst possible time with the worst possible news? This is that call." This is how Carpenter, the Butler County, Ohio, IT director, began a phone call to Franke, the Butler County Sheriff's Office captain and 9-1-1 coordinator, around 4:30 p.m. on December 23, 2020.

Carpenter knew the scale: the ECC was actively under a cyberattack. He also knew it was the worst possible time, two days before Christmas. And at the same moment that labor and delivery nurses were loading his wife and newborn daughter into a wheelchair to head home, he was answering a call from Mondello, the communications supervisor, advising CAD computers were displaying blue screen errors, commonly known as the "blue screen of death."

A few minutes later, the network supporting public safety response communications countywide would go down and stay that way for seven days. Four hundred computers and 50 servers — many virtualized — were entirely out of service. The most critical were the computers running the CAD system in the ECC. "Once one computer went down, every computer went down," said Mondello. "I had everybody who at that point wasn't busy take pictures of their screens on their personal cell phones to start writing the calls down on cards that had officers assigned — any of the pending calls. I ran over to the call taker room and passed out cards. They seemed to have their computers on that side; they lasted a little longer than we did. They were

able to help write down active and pending call screens for people who were too busy."

The team — six or seven on duty at a time, staffing three police radios, two fire radios and two call taker positions — and a visitor conducting a sit-along and considering a career in the ECC was enlisted to serve as a runner between the call takers and the radio dispatchers. Butler County ultimately hired her as a dispatcher. "Within just a few minutes, everything was on cards. The evening shift was the newest crew — and absolutely fine with it. None of them had worked back in the day when we used cards. They transitioned quickly — no one was freaking out. You wouldn't have even known anything was going on that day. They stayed calm but going 'blue screen' we all knew something had happened besides just CAD going down."

The process stayed in place overnight, but it was not sustainable long-term. "Operationally, the dispatcher's planned to go back to paper cards that we used to dispatch on before we ever had computers," Carpenter said. "They were always stored in a closet — there are boxes of them packed away — supposedly they practice and train on them and in the event of an incident or major outage or technology incident — they could return to those. They quickly found their practice, training and testing weren't applicable for a situation where you're fully dispatching from paper cards. It didn't work."

SIMPLIFYING PROCESSES MADE COMPLEX BY TECHNICAL CONFIGURATIONS

The following day, Mondello led a conversation about how the team could adjust their manual dispatch practices, utilizing a clothespins and paper run cards system. "Dispatchers, in general, try to think that we need to have a different plan," she said. "We always think there has to be a different way of doing this. So early in the morning when we weren't extremely busy, we all started brainstorming. Back in the day when I worked in the city of Hamilton we had a Rolodex, and we would put numbers and cards in it. I was talking about that, but we knew it wouldn't work because we dispatch too many people. I knew I wanted something that attaches to a card, so we went to Hobby Lobby and bought every single box of colored clothespins," she said. "We dispatch for 15 different fire departments, so we bought 15 different colors — every station for the next 24 hours had their own color. They could stay in their own block and be a little more organized. It sounds confusing but visually, it made so much sense."

Law enforcement officers were assigned blue clothespins that were adorned with flags identifying the specific unit and changed each shift. "It was really impressive how adaptive they were, and the public never noticed an impact," Carpenter said.

Dwyer was amazed by the creativity of the public safety communications team. "In our line of work, we are used to dealing with tragedy and destruction and all kinds of things thrown at you from mass casualty issues to active shooters — this is something from a different book," Dwyer said. "We weren't prepared for the cyberattack that took us offline for a period of time. Literally, our IT guys just kind of unplugged and started fresh. As a police agency, you're used to handling lots of disasters, but not at this level internally. And then our job is to serve the public and even though we were dealing with a massive problem, we wanted to continue our services as close to what the citizens are used to — we were able to pull that off. We had to set up individual email stations allowing officers to go to the station, log in to their account and send emails so that vendors and others that we needed to email with didn't see the impact; we were just a little slower."

In the comm center, the dispatchers followed a simple process handing calls from call takers to an incident dispatcher, then on to radio dispatchers. "Call takers took completed CAD cards to the incident dispatcher, who searched the ESRI tool to determine the appropriate response jurisdiction and assign the proper station and appropriate units using the corresponding clothespin, then passing the call to the radio dispatcher," Mondello said.

When the units cleared, the clothespins went back to the incident dispatcher who returned those units available for the next call. "It actually made fire dispatching a lot of fun that day, trying to figure that out," she said. "Like incident command, I was initially thinking we would use a big whiteboard but then having all the magnets and not being able to put the cards in the place — just being able to clip the units on the card kept it very organized. We were going to sink or swim and we had to swim."

Those efforts didn't go unnoticed or unappreciated. "In dispatch, everything is run with computerization," Dwyer said. "They had to revert back to the old pen and paper and the way they did it was phenomenal. Our staff were put into a unique situation and they rose to the occasion. We didn't get any complaints about delays, everyone just hunkered down and did their jobs and the public really didn't see a delay in 9-1-1 responses or anything else. Dispatch was just racked with difficulties — staffing and everything else — to just manage it as best as they could. Our first thought is we must keep serving the people — we didn't want them to suffer any secondary problems. It was amazing to see how they responded to losing their technology. They came up with creative ideas and kept the train going while we attempted to recover our data and get back to operational norms."

The ECC used a variety of complex technology configurations such as response configurations within the CAD to send a second medic at a specific fire station as the second due-in for all calls in the jurisdiction, and radio configurations simulcasting specific messages across various talk groups with the single push of a button. "We've been concentrating for years on the what we do but we need to spend a little bit more time on the why we do, what we do," Franke said. "We've simplified a number of things, almost to our detriment, so our personnel doesn't understand what goes on behind the button or icon. We need to re-establish that everything is set up for a purpose."

What functionality is lost almost immediately when technology fails and that button doesn't work? What actions should the telecommunicators expect to take if a brief outage stretches into multiple operational periods? "We have a Motorola radio system configured so expertly that technicians came to see how they tied together the console subsystem so intricately for all ECCs," Franke recalled. "Motorola technicians came in to see our setup because no one had used their system like this before. But the part I forgot is if it doesn't work, no one understands what we're doing. We made it so simple that all you must do is push a button or enter this command and everything beyond the scenes does this, but you have no idea what you just accomplished. You need that cold bucket of water dumped on you to remind you that as good as technology is, you can't become so dependent on it that you can't operate without it."

Franke continued, "We were able to manually dispatch all these fire units, but

we didn't have all these complicated response recommendations, so we were kind of back in manual mode. Getting our response partners to understand that was complicated and took us several days. With= three shifts of fire personnel there were guys coming back with no idea what we'd done for the past 72 hours, and we had to explain once again the limited resources we were working with.

Complex response configurations loaded in CAD became very challenging to conduct on paper. Without assistance from technology, it won't be as nice as you want it to be, but it will be functional. Telecommunicators were constantly having to contend with responders' needs and citizens on their worst days while also dealing with the effects of the actual cyberattack. Both were important and more difficult because the process to solve problems wasn't straightforward.

To assist with complex decision making, fire departments sent battalion chiefs or captains to the center on a rotation for the first few days to assist with decision making. "We told them that we could come close, but they felt they might do better. They were in the same place — they were used to using a map a certain way; even they got caught because in the areas where they reconfigured the medic districts that wasn't intuitive for them either, so they were kind of having to look things up just like we were. Everyone understood the realities of the problem on both sides of the radio. They understood exactly what we were going through and what we were doing, what we had and what we didn't have."

A few fire departments requested an additional step from the comm center to replace CAD paging. "One of the departments brought in another solution for us — they thought it was a solution, but it was just another step we had to do to ensure they got the pages," Mondello said. "Once the incident dispatcher placed the clips on the card, that same dispatcher would use another laptop and type out the whole call so that it would be paged to the fire departments. Only certain departments asked for that. They expected it, so we made it happen — if we forgot or didn't have time to do it, they dealt with it.

While CAD was a focus, the loss of mapping was another hurdle to overcome, so a GIS professional was positioned in the ECC to assist for the first few days. "Our CAD is map-based and the map is everything — it plots the location, everything," Franke said. "What we discovered is that just because they use the map every day doesn't mean they know how to read a map or manually find things on a map because they're used to a computer showing them everything. It was an assumption I made, 'Well, they know the map, so they'll be able to do this' but it was a totally different procedure."

After just seven days, the CAD server was restored, and normal operations returned to the communications center.

Carpenter agreed, stressing the challenge of providing map data without a network connection.

"We hadn't planned for mapping," he said. "We had to scramble to get them a lot of mapping resources. Until their CAD was up, we had to get them PDFs of maps and spreadsheets of the old-style street listings and response areas."

Cyber experts and the insurance company were cautious about allowing any connections to the internet whatsoever. "We couldn't listen to that entirely," Carpenter said. "If it was up to them, we probably would not have taken down a single computer. But the first thing we did was pull firewall logs and identified computers that were suspect. We kept those back and all the others we started rebuilding. We rebuilt the dispatch workstations first in the days when the servers weren't allowed to be touched. We still had the network down, but we took the cellular cards from the patrol units not in use and put those in the dispatch computers and gave them internet. We gave them spreadsheets of everything that we could. We gave them access to county GIS mapping resources (the cloud version of ESRI), as well as access to Google maps. That occurred either late the second day or the third day providing basic internet access and cloud functionality to the dispatchers." Providing even basic computer functionality back into the ECC was "the best Christmas gift ever," Franke said.

COORDINATING WITH EXTERNAL PARTNERS

The impact of manual work was not limited to the ECC. "The officers in the cars were just doing everything on the radio and their reports on paper, but that's an inconvenience that doesn't really impact response," Carpenter said. "But we didn't have enough paper. There are enough forms for when one computer goes down, but when 100 computers are down and officers are coming in to get a big stack of forms because they don't know how many they'll need, that was an issue. We were hustling printer companies to get more forms made."

Filling out the forms was also time consuming for those unfamiliar with the process.

"We had a lot of cops out there who never had to do a report on paper," Franke said. "They're used to that cursor jumping to the correct box and they manually had to figure that out for themselves. We had a generation of people on both sides of the mic that hadn't had to work in a manual scenario."

After just seven days, the CAD server was restored, and normal operations returned to the communications center. "We'd been telling them we could do it pretty quickly, but they didn't believe us because we had other agencies in the area that had similar incidents, and it would take them a month or two to come back online," Carpenter said. "I think they thought we were overly optimistic or lying to them, so they were genuinely shocked that after seven days (over two major holidays), we were back. We'd seen other agencies go through this, and their technology teams were still going home at 5 p.m. with systems down and, for pretty much all our staff, that was unbelievable. We couldn't imagine doing that. I guess we just have dedicated people."

Throughout the process, Dwyer said the commitment he felt from partner agencies was strong.

"The people we work with and dispatch for are good folks to work with," he said. "When we had our problem, we notified those affected immediately. I dealt with the police chiefs and command staffs from the other agencies. We had so much going on that they just stepped up — I didn't get calls from city managers or other council members. Individual chiefs were briefing their people — they understood. The city of Hamilton had gone through something similar, so they felt our pain. We kept our partners apprised of what we were doing to fix it and our timelines, then they ran with it within their own entities, and no one really complained. They didn't want to add to the problems we had." ●

Stephen Martini, ENP, RPL, *is Director at Metro Nashville Emergency Communications Center.*

CDE EXAM #61715 AND #61716

This CDE article is the only CDE article in the November-December issue of PSC magazine. It is double the regular length with double the questions and is worth two continuing education credits rather than one.

QUESTIONS

1. How much did the cyberattack cost Butler County to resolve?
   a. $18,000
   b. $180,000
   c. $1,800
   d. $18,000,000

2. Telecommunicators first recognized a problem when one CAD computer displayed a blue screen error.
   a. True
   b. False

3. What did telecommunicators use to document active and pending call status at the time of the attack?
   a. Screen shots stored on the computers
   b. Memory
   c. Pictures taken with personal cell phones
   d. Nothing — all information was lost

4. Who served as a runner during the first hours of the cyberattack?
   a. An experienced public safety telecommunicator
   b. A visitor completing a sit-along, considering a career as a telecommunicator
   c. A new trainee
   d. A police officer

5. What did the telecommunicators use to track unit status?
   a. Clothespins
   b. Paper clips
   c. Toy cars
   d. Magnets

6. Call takers wrote calls for service on cards, then handed the cards to the incident dispatcher who determined the jurisdiction and assigned units, then passed the card to the radio dispatcher to be dispatched.
   a. True
   b. False

7. The public did not notice a significant difference in response times during the cyberattack.
   a. True
   b. False

8. Despite using this resource every day, some telecommunicators did not know how to use the manual solution for:
   a. Phones
   b. CAD
   c. Pagers
   d. Maps

9. How long was the communications center without CAD?
   a. 2 days
   b. 5 days
   c. 7 days
   d. 10 days

10. Clear and consistent communication about the reality of the situation and steps they were taking to fix it helped the county avoid challenges with partner agencies.
    a. True
    b. False

11. What type of cyberattack did Butler County experience?
    a. Trojan
    b. Phishing
    c. DDoS
    d. DNS Tunneling

12. The email the employee received was from a stranger they had never met.
    a. True
    b. False

13. Once the email accessed the domain server, the hackers generated:
    a. Copies of Butler County's private data.
    b. Messages to the Mayor threatening to harm the system.
    c. Additional emails from Butler County employees.
    d. All of the above.

14. When Butler County IT Director Ken Carpenter discovered files on the CAD server were being encrypted, he first:
    a. Called the FBI.
    b. Remotely shut down the server from his cell phone.
    c. Called the 9-1-1 coordinator.
    d. Started rebuilding individual workstations.

15. Cyberattackers plan attacks ahead of holidays hoping technology staff are not available to respond.
    a. True
    b. False

16. The insurance company was primarily concerned with avoiding any additional data leaks and obtaining evidence, rather than restoring operational functionality.
    a. True
    b. False

17. The insurance company provided which three solutions when contacted?
    a. Insurance advice, legal expertise and cyber security expertise
    b. Insurance advice, cyber security expertise and operational consultations
    c. Legal expertise, cyber security expertise and temporary staffing solutions
    d. Insurance advice, media consultation and cyber security expertise

18. How many computers and servers were impacted by the attack?
    a. 19 computers and 20 servers.
    b. 400 servers and 50 computers.
    c. 250 computers and 12 servers.
    d. 400 computers and 50 servers.

19. Employees with which kind of experience assisted with restoring functional workstations?
    a. Technology professionals
    b. Jailers taking technology coursework
    c. No experience, willing to serve as runners
    d. All of the above

20. All the computers impacted by the attack were located in the same building.
    a. True
    b. False

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online! To receive a complimentary certificate of completion, you may take the CDE exam online. Go to http://apco.remote-learner.net/login/index.php to create your username and password. Enter CDE in the search box, and click on the "Shock to the System," then click on "enroll me" and choose "Shock to the System (61715 Part 1)" and "Shock to the System (61716 Part 2)" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.