landline traffic can be isolated much more effectively.

AND HOW DID YOU FARE AT THE END OF OUR SCENARIO?

Thankfully, your IT department has just sent out some new quarter training on best security practices within the agency, and you realize your errors immediately. A few emails and phone calls ensure the system is free of malevolent programs and your security code is reset. There is some headshaking about driving around the arm, but it's already in the budget to replace it with a gate in the future. You set an alert on your phone to ensure you check for your fob before each shift. All in all, no harm really done.

When asked about how best to prevent the scenario put forth, Clement advised, "Monitoring is important. You have to know you've been compromised in order to do anything about it."

It's likely that you've been trained on many of the concerns in the previous scenario. Some potential security breaches may be easily overlooked, however. Whether physical or digital, there are always areas where we, as an industry, can do better.

There are some physical security considerations that may not have made the top 10 concerns a few years ago, but now are crowning that list. "Doors," Director Chris Cord, of Orange County (Virginia) Emergency Communications Center, said with a smile. "At Lexington, in our first center, we had glass doors to get into the secured hallway. There was a second glass door leading to communications. Glass doors are not secured entries. They rectified that [issue] at the new center. Granted, the entry to the building was glass, but the doors to communications were solid."

Clement had another take on the physical security issue: generator yards, or similar work areas outside of ECCs, are often not gated or fenced adequately. "A malicious person could easily go out and chop off the cable," he warned. Such an act could bring the entire agency down during a weather event, or it could be a part of an organized attack on the public safety presence in that jurisdiction.

That is one of Cord's particular aggravations with government buildings. Looking over a blueprint of his agency's wing in a new consolidated public safety building, he said, "Signage is an issue. Don't put signs on the building. Don't broadcast the purpose of the agency. It just highlights the building as a target." He referenced a recent situation in Louisville, Kentucky, where protesters marched on the local ECC and attempted to burn the employees out. "It's a good example of why there should be no identifying marks."

Clement pointed to cameras as a potential security weakness. Poor technologies are often embedded within the cameras, he explained, things that seem dated and don't use best-practice protocols, such as default passwords. Identifying those issues before they cause problems can be difficult. And while the core software may be updated, its system could have been built on a version of Java or similar program that is now out of date. Closing that gap can be impossible.

Virtual private networks are another security system that may not be as safe as you think.

> **Make sure you follow your agency's social media policies, your IT department's guidelines and, of course, common sense.**

"VPNs are always a compromise between security and business," Clement said. "They need to be encrypted and set up properly, especially when you're talking about a CJIS environment. You have to come up with a solution that meets those requirements but is also easy on the end user."

The COVID-19 pandemic has generated a special type of challenge that many agencies have never faced or maybe even planned for. Security of the actual ECC is a continuing concern. But what about the new hurdles COVID has created with at-home access and communications? "We can offer a portable 9-1-1 console for off-site work, which includes a laptop, SAM box [sound arbitration module] for the headset, the ability to remote into programs, and a hand-held radio. But there are issues with that, too," Cord said. Clement agreed. "Network isolation — maintaining the integrity of the data — is the biggest concern in security for new and existing ECCs. Zero trust networks are the new thing; it isolates everything on the network, and the network can only talk to specific devices." Many agencies are struggling to find a compromise between the two imperatives.

COVID has also unveiled a new twist on an old danger: social media. The pandemic is opening up public safety to more digital scrutiny. So many people use online programs to have conversations, to maintain that needed human connection, that too little digital presence can be as dangerous as too much. Hacktivists don't just pay attention to which government employees are online, they also build profiles of those who aren't. As a good preventative measure, personnel who choose not to use social media should still create accounts under their email addresses to control that base account. Maintaining awareness of who in your agency does and does not use Facebook, Pinterest, Instagram and the like is vital. If you get a social media message from a coworker asking why the audio recorder program isn't letting them log in, and to verify the password, go directly to that person instead of replying. It may be an attack. Either way, Clement says, "The best way to deal with it is not to feed the animal." Make sure you follow your agency's social media policies, your IT department's guidelines and, of course, common sense.

Overall, what does this all mean to the telecommunicators in the ECC? At a glance, it can feel like the industry is under constant barrage from both internal and external factors. Some fixes can take long enough to move from concept to reality that it seems like they'll never come at all. But those fixes are the heart of the adaptation that identifies ECCs and similar agencies. Yes, it takes time to correct problems, but it sometimes takes longer to even identify them. According to a Verizon data breach report, it can be up to 18 months before a system breach is even found.

That is where the human element comes into full play.

Employees need to be aware of their actions and vigilant in their personal and professional defenses, and they need to follow and take their security awareness training seriously. Agency IT and management need to work together to create a targeted program and have an incident response plan set up for both digital and physical assault. Deficiencies and weaknesses need to be identified and repaired before they can be exploited. "It's not a matter of *if* you're going to [be compromised]," Clement stated.

When it happens, we can all do our part to be prepared. ●

Jessica Lohr *is Communications Supervisor at Orange County (Virginia) E911 Emergency Communications Center.*