# DUAL DANGERS: PHYSICAL AND DIGITAL RISKS INSIDE AND OUT OF THE ECC

## Security requires that personnel have knowledge of the risks and foresight regarding the solutions.

By Jessica Lohr

Adaptation. It's not just the name of the game in telecommunications; it's the arena and the whole rulebook. Every part of the system — from hardware to software, from personnel to infrastructure — must bend before it breaks. It must be designed or trained or built with that single purpose in mind: adapt and then overcome.

But adaptation isn't easy or simple. It's encompassing and, for the human element, often exhausting. Ensuring that technology complies with thousands of standards and requirements takes time and dedication. Information safety requires vigilance and preparation. Physical and digital security demands a mixture of everything else, as well as a fair bit of foresight.

The special challenges that emergency communications centers are facing in this day and age run the gamut, and it is only by working together and planning ahead that they can be anticipated and properly handled.

Whether you're in an existing ECC or excitedly awaiting the completion of a new communications complex, you've likely been drilled on safety and security since day one in your agency. But complacency and a sort of "alarm fatigue" can set in, even here.

### TRY TO FIND THE MISTAKES IN THE SITUATION BELOW.

Imagine pulling up for your shift. You turn at your building and weave around the parking control arm because you're running late and forgot your key fob. A landscaper cleaning the outer flowerbeds waves, and you wave back. You punch in your door code by muscle memory while video chatting with your friend. You head through the building, holding the door open for a janitor, because their hands are full. Finishing your call, you tap into the Wi-Fi and quickly download that email from an ex-coworker; swiping away the warning box that pops up is second nature. When the message opens, you forward it to your shift mate because the meme isn't one you've seen before.

And in the length of time it took you to arrive and sit at your console, you've violated a dozen safety and security protocols.

With the number of hours many of us work on the floor, it can be easy to forget that we don't live in dispatch. While we may spend an inordinate amount of time with our work family, it isn't where we lay our heads. But many times, we treat our workplace too casually. Considering the amount of personal and secure data that runs through any ECC on a given day, the nonchalant attitude many of us may have can border on dangerous.

Let's start at the beginning.

Parking security at ECCs has become more concerning lately. There have been news stories of telecommunicators being attacked on their way to or from work — even in the building itself. So ensuring that parking areas are safe and secure is quickly becoming a priority. Existing ECCs may have to work around site restrictions, but new construction can address this immediately. Parking control arms are exactly what they sound like: a single arm barrier to discourage drivers from moving forward. Rolling gates are more secure and can also be difficult to climb, which means better security in the lot. Using call boxes that require fobs or RFID badges are especially effective when paired with high metal gates. If the control arm is the only answer for your parking issues, try to make sure there is a significant barrier that prevents driving around it. While relations shouldn't suffer needlessly from it, a certain amount of information about the access methods into the building should be withheld from the general public. Blatantly violating those security systems in full view of citizens is not just against most policy and common sense, it's also irresponsible and can cause massive liability.

Door codes mean numbers, which means memorization. When an employee leaves or is terminated, who is responsible for making sure that code is immediately deactivated? If that falls to human resources staff, can anyone do it or just one particular employee? What if that person is on vacation? It can take time to address, and that means the security of the center is compromised. If someone accidentally or purposefully films a code being used, that's even more dangerous.