Replacing all access points with RFID badges that can be blocked instead of codes that have to be scrubbed from the system can help mitigate that situation.

Many agencies are trying to find ways to combat tailgating, the security breach when more than one person passes through a secured doorway on a single authorization. Most of this prevention depends on the personnel themselves. When those secured doorways cannot be manned, having employees understand the risk of tailgating is the next best thing. Monitor your access points with live feed cameras at all times.

"Wireless and Wi-Fi are the wild, wild west compared to landline networks," Larry Clement, IT Director of Orange County, Virginia, said in a phone interview, "Mainly because of the inherent way they work." They're made to connect to everything, to be open and trust all devices. Phones downloading data from questionable sources can be touching the same networks used by the consoles in dispatch or the report storage database for the sheriff's office next door. Since there's no such thing as a truly hidden wireless network — if it exists, it broadcasts a detectable signature — then separate carriers and firewalls can be used to better secure those data access points. Of course, landlines are the best option for any network connection when it's available;

"Considering the amount of personal and secure data that runs through any emergency communications center on a given day, the nonchalant attitude many of us may have can border on dangerous.