Technology at the administrator's side- empowerment or security hole?

The usefulness of technology for the public organization is clear and accepted by all but the worst Luddites in our society. Modern county services simply could not be administered without computers, the Internet and the ubiquitous "Cloud". The sheer volume of transactions are such that the traditional files, folders and cabinets we used to store and process information are a thing of the past. The utility of the technology has also enveloped the administrator with multiple devices that are making decisions and actions easier:

- A desktop computer in the office that can connect to secure email systems and enterprise management systems such as personnel, budget and procurement.
- Perhaps a laptop to take when travelling and to make working at home an easier chore by using a VPN connection to ensure reliability and security of the transactions.
- A tablet to make reading long reports easier and to appreciate colorful photographs or plans that can be enlarged with the pinch of two fingers.
- A smart phone that is coordinated with the email system and calendaring function, so that a promise to a resident to meet or address a concern is not forgotten but enters into the same system the staff people also see.
- … and now smart watches that can bring events and decisions right to the wrist, reminding those who are not afraid to date themselves of the infamous Dick Tracy watches that doubled as TVs and phones.

Five platforms to make life easier—but also five "attack surfaces" through which the bad guys can attack the security of the IT systems and hack in to compromise files of hundreds or thousands of individuals. So what can an administrator who wants to have the latest technology and the best ways to stay in touch with issues in the community do to balance these two twin dimensions of empowerment and security?

In my experience that spans several decades, two general truths have helped navigate the constant churning and changing landscape of managers. The first is simple: never stay put, and keep changing and adapting to the wondrous technological opportunities that open up on a continuous basis. Yes, expand your reach by using the five platforms of connectivity and knowledge-sharing that are available today. And when smaller (or bigger) devices beckon, try them, at least until you discover that they will be of no help to you. SO not blind use, but openness to try and keep those technologies that truly empower you to do more.

The second is more difficult: remember that with connectivity and true interoperability comes the responsibility of safeguarding the privacy and security of the information which can be lost in a flutter of a butterfly's wing. When paper files ruled the world, it would take trucks and winches to steal them and use them for purposes other than those intended. Today, a simple bit of software attached to an innocent-looking email can unleash an instantaneous attack under which millions of data bits can leave the government's hands and end up in dangerous hands. So the responsibility to understand the basic essentials of cyber security, to know what to look for in phishing scams or how to identify suspicious attachments is incumbent on you and all your staff. The need to constantly train in the latest techniques is high, and everyone should put aside feelings of "I know it all" or "I don't need to know, because I pay others to do so"…. Our phones and tablets have become the open doorways for smart and determined hackers to do damage to ourselves and the organizations we serve.

So it is a balance between empowerment on the one hand and security on the other that must be in our minds. If we begin to shun modern, creative and open systems that put us in touch with our employees and those we serve, we will be bowing to defeat without a fight. And on the other hand, if we rush on adding systems and devices without taking the time to understand the risks, and most importantly to train ourselves to mitigate the risks, we are simply waiting for the bad event to occur—for it is not if, but when such a breach may happen if we are not strong and capable to respond to the challenge.

Technology has taken many twists and turns, and is now becoming intimately enmeshed with our personal life; so it is wise to take the time to understand both the potential, as well as the risks involved, and to become wise users—nothing else will do! n