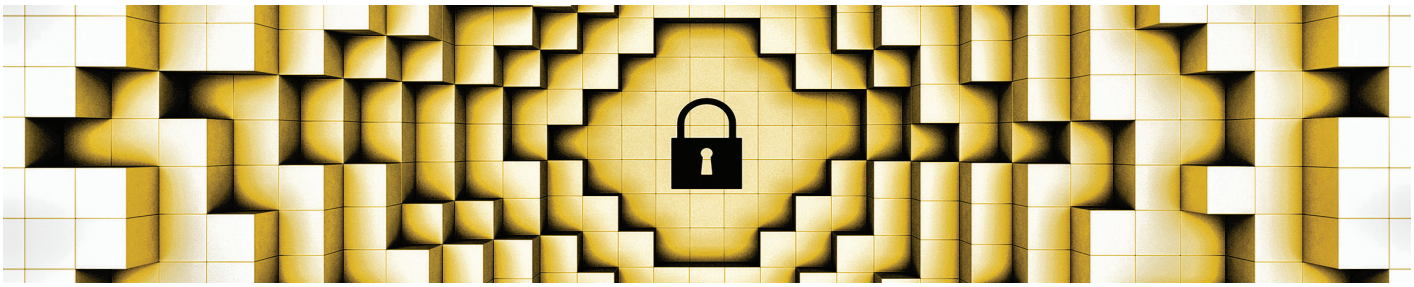

TIPS FOR SUCCESS

Data Security

Let's get physical

by Mike Taylor
Florida League of Cities

As technology becomes more critical to city services and processes, protecting data and systems is paramount. While most cities have a detailed data security plan that addresses protecting the systems and data from a technical side (strong passwords, firewalls, etc.), there is another critical component to data security that is often overlooked: physical security.

Physical security components include facial recognition, weather monitoring and protection, building automation and control, entry access control, irrigation monitoring and many other monitoring and security options that can quickly increase data security budgets. However, there are many simple procedures that will go a long way in adding an extra layer of security to protect your city's data.

LIMITING ACCESS

In your city, are all access points to rooms that contain critical components locked and secured? Most cities do a great job of keeping their data centers secure, but what about those "out-of-the-way" or forgotten places that contain critical equipment. Because of space limitations, sometimes servers are installed in a closet, hallway or other empty space. More often than not, these areas are not secure. Anyone could log in and install malware or accidently unplug or power down the unit. At a very minimum, servers and other critical devices should be in a secure environment behind locked doors and in a location with no external windows.

However, a locked door doesn't always mean critical infrastructure is secure. Access to rooms where servers and critical components are stored should be limited. Too often, these devices are locked in a secure location, such as a server room, but anyone with a master key has access. Plus, if the master key is on a key ring sitting on an employee's desk, it could easily be stolen or "borrowed" for a short time, enabling someone to access and damage the system.

Access should be limited to select staff. If someone else needs to enter the room, he or she should sign in and be accompanied by approved personnel. It would be ideal to have a physical security plan that only allows entry via a fob or proximity card or through the use of biometrics, or that incorporates a high-tech motion-activated camera system; however, this is not always financially feasible. At the very least, securing the equipment by locking doors and limiting access can go a long way.

KEEPING IT CONFIDENTIAL

Another aspect of physical security is keeping documents in a safe and secure location. During the course of a day, documents containing confidential information are moved from workstation to workstation. They are often stored in plain sight while waiting to be worked on. Cities collect forms that contain confidential information, such as social security numbers and credit card information. These types of documents should be stored in a locked area or filing cabinet until processed and then be properly destroyed when appropriate. If documents need to be retained, they should be stored in a secure location.

The same precautions should be taken for various types of media that contain confidential information. When critical systems and data are backed up, often the backups are stored on portable media such as magnetic tapes or external hard drives. These devices and media should always be stored in a fireproof safe in a secure location, preferably not in the same building where the servers reside. Only authorized personnel should have access to this storage location. When it's time to destroy the media, the data should be thoroughly erased (known as formatting) so that it cannot be accessed.

UNAUTHORIZED CONNECTIONS

Finally, open network jacks are an often-overlooked aspect of physical security. When a building is constructed, extra network jacks are installed to allow new personnel immediate access to the network.

However, if these jacks are left "active" when not in use, anyone could come into city hall, plug in and be on the network. There have been many reports of guests, vendors and others plugging into a network and unleashing a virus. Network jacks should only be made active when needed.

These are a few tips a city can incorporate into its physical security plan to help make a more secure environment. Physical security involves planning, but keeping computing devices and documents in a secure location will help improve the overall data security in your city.

Mike Taylor is associate director of technology planning and development for the Florida League of Cities. QC