7 Best Practices When Upgrading Access Control Systems

Posted on 12/9/2014 11:42 AM by Dennis Raefield

Businesses today face complex security threats, including violent crime, weather emergencies, and even terrorism. These issues require comprehensive access control solutions that safeguard against unauthorized individuals and serve as a key component of incident and emergency response. However, faced with tight budgets — and wary of long, drawn-out installations — some leaders are still hesitant to commit to an upgrade of their legacy access control technology, leaving their organization vulnerable to these and other potential threats.

Technological advances over the past few years have significantly impacted the growth of access control systems, which have evolved in nearly every aspect. Some systems can even be updated overnight by simply swapping out the server and replacing controllers with new IP-based solutions that communicate with your existing readers, credentials and infrastructure.

Retrofitting facilities with modern access control technology doesn't have to be complicated or pricey – in fact many new systems are affordable, simple to install, and easily-scalable. Take a look at these 7 easy tips to help ensure the process goes smoothly.

1) Give Your New Access Control System Its Own Network

Today's access control systems are IP-based, which means the devices sit on a network just like your PCs, tablets and printers. While it's technically possible to lower installation costs by utilizing the same network as your other devices, it's best to place the new access control system on a separate network as a precautionary measure to isolate the network against cyber-attack. Having a dedicated network can mean establishing a physically separate network, implementing a virtual environment or applying your technical expertise to segment an existing network. This last option effectively places your facility's access control data into its own secure tunnel.

Before you make a decision, consider that many IP-based access control systems require power-over-Ethernet (PoE) switches to function. Unless you already had a specific need for such switches, chances are your current switches won't work, and a new network will be required.

2) Go IT-Centric

In an IT-centric environment, solutions leverage software running on standard industry hardware as opposed to hardware that is supported by firmware. The facility's existing IT infrastructure (TCP over IP) can be leveraged, using software to control its access control system in the same way users control network security for logical access to computers.

Because much of the hardware required in a traditional access control system is unnecessary under this kind of set-up, end users can eliminate many of the antiquated devices that are typically required. For example, consider this: a solution that runs on the IT network does not require proprietary access control boards or panels to perform the authentication check at the door that traditional solutions necessitate. Instead, the user only requires the computers operating in their data center running software with a simple interface at the door to connect the electric-strike. This method can not only deploy an easy solution for users, but also takes advantage of the existing IT infrastructure.

3) Consider Redundancy

If you're retrofitting an outdated access system and need to control a large number of openings on many floors, establish highly secured areas or provide security for multiple buildings, you should consider including backup servers in your upgrade plans. After all, if you only have one server and it goes down, your access control system is immediately rendered ineffective.

The beauty of many of today's modern access control systems is that it's easy to connect multiple servers via a network and gain redundancy. In the event of a failure of the primary server, a network interface or bridge device can reach out to the secondary servers to maintain functionality and full operation of the overall system, ensuring your people, openings and assets stay secured.

4) Look for Integration Options

Years ago, an access control system was just that – access control, it didn't integrate with other solutions in the way that current technology is capable of doing. Today, due to the nature of IP-based technologies, it's common for access control systems to integrate with optical readers, fingerprint scanners, building management, and tie into video surveillance systems. Indeed, integration has reached exciting new levels (along with significantly lowered costs). For example, it's now possible to click on access control transaction data and have corresponding video of the event pop up for viewing. Whether or not you need such integration today, make sure you're aware of the options available with the system you select.

5) Don't Miss Out On the Latest Features and Functionality

When it's time to evaluate a new access control solution, you might be overwhelmed by all your options — particularly if you haven't been keeping up with today's modern capabilities. Keep your decision relatively simple by focusing on the key features and functions. For starters, many users are now interested in remote access. That is, you don't have to be sitting in front of the access control server to view transaction data and control the system. In fact, you could be anywhere around the world and access or administer your systems. Related to this, you'll want to ensure your system can issue notifications (e.g., email or text alerts) to key personnel when and if certain events occur. Take the time to thoughtfully create a plan of which events should issue notifications and to which employees.

In the future, you might want to use smart phones as your access credential. If they're connected to your network, they can effectively become your access credential with all the same roles and access privileges assigned to a standard card. Such a solution removes the need for employees to carry cards that can be easily misplaced. Users can even mount an RFID device on a vehicle's dashboard, enabling drivers to scan the bar code and remotely open a door or gate – this also eliminates the need for below-ground wires to keep costs low.

6) Prepare Your Data for the New System

If you want your access control upgrade to be quick and seamless, you shouldn't have to manually enter all your user data into the new system's software. Fortunately, today's IT-centric technology has the ability to import data from a variety of sources and the database from your outgoing system can most likely be easily accessed and exported to a common format.

Today's systems should have the ability to utilize established standards which help streamline processes like inputting data and setting up user permissions and responsibilities that apply throughout an organization's IT systems. The best practice here is to do your homework on how to export the data from your old system securely and ensure the new system can accommodate the incoming data. It may seem like common sense, but it's often these small things that can be overlooked and add time to an upgrade.

7) Ensure Your Systems Integrator is Asking the Right Questions

While the previous best practices can help ensure a successful access control upgrade, this one might be the most important because it's tied to your specific needs. Assuming you're working with a professional to handle the implementation of your new system, it's important that they are asking you in-depth questions about your needs. Consider every best practice we've covered in this article. If your integrator isn't talking to you about each item here in detail and how it affects you, that's a red flag.

These questions are important for a professional to ask for two reasons: First, they'll ensure you get a system that achieves your goals. Second, gathering all the necessary information upfront ensures your system is upgraded quickly, on time and within budget. Your goal is to seamlessly and affordably adopt a new access control system. A good systems integrator can mean the difference between a worry-free upgrade and an IT nightmare.

Dennis Raefield is president and CEO of Viscount Systems.