

# Essential Access Q&A

By Jerry Cordasco, Contributing Writer

**H**ere is some basic homework for you to do, some important questions to be asked and answered in advance, before you make a selection.

Preparation is key; if a buyer or specifier goes in unknowledgeable, there can be a quantum difference between expectations of the system and what it actually delivers. You want to obtain the system that is best for your business – neither too simple to work well, nor so complex that it intimidates your people. Selecting a vendor, getting the system installed, getting it to operate effectively on a day-to-day basis – a lot of problems are inherent here, but problems will be reduced with prior planning.

## ■ Are you ready to “sell” the system?

Sell the system? You’re the buyer, aren’t you? You have made up your mind to do it, but what will the people in your organization or building think about access con-

trol? How will they learn to work with it? If the people in the building perceive it as a nuisance, chances are they will fight it.

If they forget their cards, they cannot get in. If you are using badges, they could consider them an intrusion. Some will not like their pictures.

Silly? Probably. But all are obstacles to be overcome. You can avert a lot of headaches by doing your public relations ahead of time. Put out notices explaining the importance of security for employees as well as employer; hold a meeting where questions can be answered, get them on your side.

## ■ Have you set the parameters?

Before you can select an access control system you have to figure out how you want your building to operate.

One of the first parameters to set is timing. It is more complicated than you might think. You cannot just leave the outer doors locked because you have people coming and going all the time during

the day. You have to have a timing system that unlocks them at a certain time and locks them up again at a certain time.

What do those times need to be? Is 8:00 a.m. okay? Are visitors coming in earlier? Maybe it should be 7:30. Is the receptionist always there at 8:00? If not, do you have an inner barrier to keep people from wandering in before the receptionist gets there? Typically you will also want your inner doors to lock and unlock on schedule.

Some manufacturers offer a software feature called “first in unlock.” The time schedule for unlocking the door will not go into operation each day until someone first opens the door using a valid card. The fact that a valid person is in the building will tell the doors it is okay to unlock at 8:00. If no one has used a valid card at the doors by then, they will not unlock.

Privileges are typically set using access levels or some other similar function. This connects users to doors to days of the week to times of day. It is essentially how you determine who can get in where during what time. In some facilities, this setup process can be fairly simple. In larger facilities, there may be access levels specific to a person or groups of people based upon their position or function.

## ■ Does the facility have visitors?

How will they be handled in the system? Will they each be registered? Will they be given badges? What will you do if the badges are not returned?

## Checklist for an Access System

### Which doors will be protected?

- What types of doors?
  - Exterior
  - Interior
  - Will existing door hardware support electronic access control?
- Will they be monitored for prop conditions?
- What type of exit devices will be used?
- Push button, motion detector, built into the door hardware?

### Any special ADA considerations?

- Location of readers
- Types of doors

### Will the system use your network?

- Has your network administrator been involved in the system design and review?
- Virus protection
- Gateways, routers, bandwidth requirements
- PC requirements
- Data backups

### Who will administer?

- Entry and deletion of cardholders
- Initial distribution of cards
- System operating parameters

### Who will service the system?

- During business hours
- After hours/weekends

### Who decides who will get in; where and when? (Access levels)

### How will you name your readers and other devices so that they can be easily identified?

### What are your holidays? Can the system support all holidays? How will the system operate on holidays?

### What doors will lock and unlock automatically and when?

### What information will be captured in the employee database?

■ **Will your system interface or integrate to other systems, security and non-security related?**

Will you expect the access control system to activate cameras? Trigger a signal to a remote monitoring center?

■ **How will you handle door propped open alarms?**

Doors being propped open are the single largest weakness in an access control system. Without having someone monitoring the alarm screen constantly, it is possible that a propped door may go unnoticed, compromising your security. The system can be designed with audio alerts to prevent this.

■ **Will your system use the organization's network or will there be a dedicated network for security?**

Have you gotten together with your IT department or network administrator to discuss requirements and issues? That and many similar functions need to be set to attain the individuality that makes the system work well for your needs. For example, where will the system be administered from? Who will enroll the employees? How will you take out employees who are terminated? Suppose it is an ugly termination and you did not get the card back? What do you do when someone loses a card?

■ **Is your building in shape for the system?**

Procedural decisions aside, there are mechanical aspects to consider. If the door does not close, the access system will not work. This problem can arise if the door system is not properly coordinated; if the locking mechanism or door closer does not work properly; or if there is too much air pressure in the building and the door cannot close against the excessive pressure. Someone knowledgeable should check the mechanical aspects out in advance. Or if the problem arises after the access system is in use, whose responsibility is it?

■ **To badge or not to badge?**

Who will be authorized to use the access control system? There are many different options for credentials. Some security operations or buildings probably will not need badges because everybody pretty much knows everybody else. If you have no intention of badging, access cards will cost less. You could even consider a key-ring attachment like the supermarkets offer, since people will be less likely to forget or lose it.

But if you have a building or offices with more than 100 people, or where a lot of visitors are common, you probably do not want to take the chance of having

unauthorized people wandering around the building. This is the time to think seriously about badging.

■ **Are you ready to enforce?**

Badges are only valuable if you enforce the use of them and educate all employees about what to do if they see people who look legitimate otherwise but have no badges. The appropriate thing to do is challenge unbadged strangers politely. Ask to help them. Escort them to where they want to go to make sure their business is legitimate.

This is a nuisance, of course, but employees must take responsibility for helping with policing or the effectiveness of the system becomes significantly less, and badging does not do any good at all. It is all part of the mentality that must be adopted to make access control work, for the security of the business and of the employees themselves. ❖

**About the Author**

*Jerry Cordasco is vice president and general manager of Exton, Pa.-based Compass Technologies Inc., and director of security products for its parent company, Wheelock Inc.*

**Checklist for an Access System**

**How many locations will the system be administered from?**

**Will all operators of the system have the same level of access?**

- If no, what info will each be able to view and edit?

**Will you utilize badging?**

- How will photos be captured?
- Who will design the Badge?
- Will visitors require badges?

**How will you train your employees on the use of the system?**

**What reports will be required?**

- How will the reports be used?
- Does the system provide appropriate standard reports?
- Will "custom" reports be required?

**What process will be used when an employee is terminated?**

**Are there any high security areas, which require special consideration?**

- Will in/out readers be used anywhere (anti-passback)?

**What type of readers will you use?**

- Proximity
- Magnetic Stripe
- Biometrics
- Barcode
- Smart Card

**Will you use keypads (PIN) in any locations?**

**Will the system interface or integrate with any other systems in the facility?**

- What systems?
- How?

**What database will the system use?**

- What security will be placed upon the database?

**Will anyone be monitoring alarms?**

- Will certain alarms be routed to specific locations for monitoring?

**Will the system be required to report alarms off-site?**

**Will the system use graphical maps/floor plans?**

- Who will create the maps/floor plans?
- Who will keep these current?

**How will the system react to a power failure?**

**Is any license or certification required?**