Tricks and Traps:

Planning Electronic Access Control

What do you want from your access control system? The same things everybody wants: controlled access and egress, consistent information collection, simple and accurate database management and some degree of system integration. It seems like a short list, but without careful planning it could be the most expensive short list you ever develop.

This article proposes to help you avoid "black holes" in the planning and implementation process that frequently add to the cost of EAC projects. It will show you how to break down the wish list in order to look at each "wish" individually. Then it will help you assess how to blend a new system into daily operations and attain the protection and facility management you're after.

Controlled Access and Egress

Identify the facility type. Assess the physical structure, including its layout and component parts.

Take a firsthand look at the surrounding area. Are there adjacent facilities that compound the problem of securing yours? Maybe the adjacency is not another building, but to a lake or heavy timber. Would it simplify the solution to expand the perimeter? Is there a real need to secure the entire facility? What are the long range plans for the facility? If it will be expanding, the system must expand with it.

Identify levels of security required. Assess day-to-day operations at the facility. Some areas may be open to virtually anyone. Some public areas may remain open after hours. Other areas may be extremely sensitive due to life safety issues.

Make lists. Assign levels of security — by number or color — to each area of operation. One excellent method is to use colored markers on a floor plan.

Identify and classify users. List users and group them by operational areas. These groups can be further broken down by levels of responsibility. These usually parallel required security clearances, but not always.

Examine each individual's required access level and don't assume that a position of responsibility automatically grants access. For example, an office manager in a large psychiatric clinic is not automatically granted access to medical records because of HIPAA restrictions.

Identify existing or proposed systems to be integrated with a new program. Do we have a system in place? Can we make it communicate with a new one? At what level do we need the systems to talk? Possibly the systems could share credentials, which would lower the initial cost of a new system.

Many surveillance systems use open architecture or have alarm inputs and outputs that can be used to trigger video recording upon activity within the EAC system. If event recreation is a goal, integration of alarm, video and EAC can generate virtually indisputable evidentiary data. This integration can be very expensive if it becomes an after-the-fact add-on.

Existing mechanical and electrical hardware should be considered; examine existing door hardware to determine whether it will complement the new system or interfere with code compliance. This is a potentially costly hidden expense that never seems to be anyone's responsibility.

Consistent Information Collection

Determine what information the system will collect. Will you have visitors to credential? If so, what information should be collected from them? What information do you want to store and for how long? Should the same data to be collected for everyday users and visitors?

Determine how data will be used. Human resources, accounting, marketing and security all need information that can be extracted from the EAC system. Sometimes this is identical information presented in different ways.

If data to be collected is evidentiary, the time and date stamp must be accurate and must match other systems reporting the same event. If information is shared with accounting for time and attendance purposes, the system must have provisions to calculate time and allow for missing data. If human recourses will be controlling the input of information, some provision should be made to mask parts of this information from other personnel.

Determine the risk of losing information. Is the system host-bound? What happens in the case of a communication loss? Will the data be stored while the network is down? Will the system tell you if data is missing?

In most cases, some provision for storage away from host is required. This may be a buffer built into the individual controllers, or a database server dedicated to the system, or both. Provide for power loss at both the controller and the host with batteries and UPS. Consider threats from acts of God, as well as from both internal and external interference.

Simple and Accurate Database Management

Determine how you will gather information. When selecting the software that will control your new EAC system, consider day to day operations and how management controls normal processes.

Most security and human resources directors have too much on their plate to do the input for every access credential issued. For that reason, the best EAC systems will allow a clerk to input data without actually granting access. A system allowing data input and management from multiple workstations should also allow multiple levels of data input and management.

Decide to share the database. Discuss with other departments the possibilities of sharing databases. Many times an employee database already exists and can be imported into the new system, saving a great deal of time and expense in the setup process. The EAC system could share "who's in" information with reception. Time and attendance is a growing function of EAC systems that feed information to accounting software.

Beyond normal security concerns, the EAC system can solve many management issues automatically, for example, greenhouse quarantine areas that require 24 hours to pass prior to reentry. Some EAC systems can control building services such as lighting and HVAC based on time or on the presentation of a credential.

Remote management of locking devices is becoming increasingly popular. Schools can open all the doors at a given time, lock them when classes start and control access by visitors, all from the office.

EAC has become more than just a solution for the security staff — it can have many applications in many other departments as well.

Let the system talk. Reporting capabilities should be of high concern when selecting a new EAC system. Information previously unavailable to management and staff is now a few mouse clicks away and able to be automated. Attendance problems can be reduced dramatically when a supervisor can show exactly when an employee came and went.

EAC systems can record temperature change, fire and intrusion alarm activation, open/close data and much more. It can record the number of times a door was opened, who opened it, and how long it remained open. It can tell you when the air conditioner came on and whether the freezer stayed cool enough during a power outage.

Beware of overpurchasing. Today's systems can do it all. For this reason, it's especially important to know what you need before deciding which one you need. It's very easy to end up paying for what you won't use, and just as easy to end up not using what your dollars got you. Don't pay thousands of dollars for access control software to monitor three roll-up doors in a warehouse.

A responsible provider can help match your needs to the proper product. The steps involved in source selection and system design can be put into a bulleted list or a complex specification. In any form, the information you relate to the consultant will ultimately decide the cost of your system and whether it meets your requirements.

Remember, no provider knows your business or facility as well as you do; the more accurate the information you collect, the less consulting will cost and the better your ROI will look.