SECURITY Technology & Design

Is Outsourcing Right for You?

Avoid missteps in choosing your method of access control.

By Lauris Friedenfelds

I am frequently asked my opinion as to who has the best security system or solution. As a consultant, I have to answer that no one manufacturer or provider has the answer for all security challenges.

A truly unbiased consultant learns to look for the most appropriate solutions for each challenge. In my many years of developing security solutions for my clients, I can honestly say that not one has been identical to another. Like a fingerprint, each program has been unique, with unique threat and vulnerability issues, preferences and cultural challenges.

All security programs should be developed to address the threats and vulnerabilities identified in an assessment. Mitigation strategies should be developed based on this assessment.

One of the early decisions to make in the development of a security program is whether to use an in-house security management program or to outsource this function.

What Are Your Options?

Many of my clients have opted for an in-house security program. It provides them a sense of comfort and control. They are willing to make the investment in staff, and they have often already implemented traditional access control technology as a capital investment. But what about outsourcing the technology? Outsourcing access control?

Central stations have been contracting to monitor intrusion and fire detection systems for many years. Companies that cannot justify maintaining their own a security staff have often relied upon central stations to provide alarm monitoring services.

Successes and Failures

In the late 1970s and early 1980s, some central stations began offering access control components—basic card readers—in their systems. The reader programming and reporting was typically executed locally, but a few central stations began to bring the programming and management into their own shops, calling it outsourced access control service. The entire concept grew more complicated than anticipated for some of these firms, and many eventually dropped the offering. There is still at least one national firm—and there may be more of which

I'm unaware—that has been successful in providing this service.

I have personal experience with two firms that provide or provided outsourced access control. I was employed by a firm that tried to offer this solution in the 1980s. Having a provider's understanding of the service, I am aware that visitor or exception-based entry requests come in waves. Staffing the center to quickly handle these requests was difficult, because high-traffic periods were unpredictable.

When the center had to ask visitors to wait for access (possibly outside, exposed to harsh weather), it of course led to complaints. What's more, the center couldn't effectively verify that the person requesting access was truly the authorized cardholder. This firm eventually decided that the liability risks for a central station providing this offering were not congruent with their business.

The other access control outsource firm with which I'm familiar is the national firm that offers access control as their main service. They have a good concept on staffing, their system equipment is oriented for this type of service, and they keep pace with innovations in the access control industry.

I have been privileged to tour their corporate headquarters and their main monitoring station. They combine the management of access control with the management of intrusion detection in an effective manner. They are the access control, intrusion detection and management staff that your firm may not need to put on your payroll. They have been successful in providing this service as an outsourced service since the late 1970s, so they have good experience to do this work.

Who's It For?

Outsourced access control is most likely to find fertile ground in office buildings where there is a need to provide access control to the building, yet there is no on-site security staff. These programs are most successful in multi-tenant facilities with only a limited number of legal entry points, typically with little visitor activity and a building population that does not desire the visible presence of a security officer. They are successful in urban settings where local police department response is quick.

As with every security program, a good understanding of the risks and vulnerabilities associated with the facility is imperative. An assessment should be executed by the security professionals within the firm, public law enforcement or an independent security consultant. Avoid the offer of a free assessment from a provider's salesperson. The result is typically a design of their offering and not a true independent evaluation. Rarely will they indicate that their system is not the proper application for the building.

What to Look Out For

There are some issues that should be considered.

• Delay. Granting visitors access from off-site usually requires audio and video devices to communicate with the off-site operator. Visitor access rights need to be planned and announced prior to the arrival of a visitor, or the process becomes cumbersome. This may not be unlike what occurs in many office building lobby operations, but since it involves off-site people it has the potential for longer delays.

• Some aspects of security are best handled by staff. If the risk and vulnerability assessment recommends the screening of packages entering the building, for example, you will still need on-site staff. Similarly, most outsourced access control programs provide little if any video surveillance. Again, if the assessment indicates that video should be provided, outsourcing may not be the answer.

• Watch out for sales talk. If you're interested in outsourcing, be aware that there is a good amount of sales talk in some program descriptions. Remember that good service comes at a cost. Evaluate the cost by comparing it to the cost of adding the function to in-house staff. Execute the cost comparison on an apples-to-apples basis. Do not allow salespeople to add costs to your in-house estimate.

Some may sell outsourced programs by saying that they allow you to avoid technology obsolescence, but access control technology does not become obsolete as quickly as you may believe. I have seen systems function without problems for more than 10 and even 20 years. That said, changing needs and expectations may render systems ineffective well before their components fail.

Ensure that the monitoring of the intrusion system and access control is executed by a UL-listed central station. The UL certification indicates that the construction of the facility meets standards, there is adequate staffing to ensure vigilant monitoring, and there are adequate system backups.

Outsourced access control provides a good security solution in many instances. Its application should be based on the results of an independent risk and vulnerability assessment that indicates this type of program would be appropriate. The best security program involves well trained, active security staff supported by technology.

Compare the cost of the service with the cost of providing this service with in-house staff. Review the contract with your legal or risk management support staff to ensure that you are comfortable with the limitations of liability in the agreement. In the final analysis, the decision should be based on the appropriateness of the program. **STD**

Lauris Freidenfelds is a vice president of Sako & Associates Inc., a provider of security and media technology consulting, design and construction management services. He is based at the company's headquarters in Chicago and can be reached by phone (312-879-7230) or e-mail (lfreidenfelds@rjagroup.com). *For more information, visit the Sako & Associates Web site at* www.sakoinc.com.

Where Outsourced Access May Be Most Effective

• In office buildings with no on-site security staff

• In multiple-tenant facilities with a limited number of legal entry points

• In urban settings where local police department response is quick

Potential Problems with Outsourced Access

• Delay in making and relaying access decisions

• Absence of additional capabilities such as video and screening

• Sales talk—Choosing an inappropriate provider

Tips for Making the Right Decision

• Base your choice on the results of an independent risk and vulnerability assessment

• Compare the cost of outsourcing and staying in-house—apples to apples

• Review any proposed contracts with your legal or risk management staff

Reprinted with permission from *Security Technology & Design* magazine · February 2006