

# Committing to Non-Stop Service

Dealers taking on managed access services essentially become their customer's security department.

By Karyn Hodgson, Contributing Writer

**M**anaged access control is a hot trend for dealers and integrators right now — a way to offer access to both a new class of customers and existing customers who may be feeling the pinch of the economy or are intimidated by increasingly complex technology. But with managed access the dealer has to take on a whole new level of responsibility, essentially becoming their customer's security department.

For those that can navigate those waters the rewards are definitely there.

"We are a RMR-focused company," says Brad Tolliver, vice president of electronic security, Per Mar Security, Davenport, Iowa. "With this format we can go in at a lower upfront install cost and create recurring revenue from it. It also exposes us to more potential clients because of the lower initial investment for the client."

Matthew Ladd, president and CEO, The Protection Bureau, Exton, Pa., — *SDM's* 2010 Dealer of the Year — sees it as a function of exercising the best experience. "We know access control, how the administration should go. A lot of times our clients don't have that

expertise. We found we could provide a service to our client that had a very good ROI on their end and generate RMR on our end. It was a win/win for both sides."

For Ron Oetjen, president, Intelligent Access Systems of North Carolina, Raleigh, N.C., managed access opened up opportunities to approach new types of clients.

"We were losing the smaller opportunities and were struggling to compete at those price levels. With managed access we can provide a high level of service to the small and mid-range businesses at a fraction of the cost."

Even with all of the positives, dealers and integrators who have a few years under their belts with this service stress the commitment required.

"Don't get into this unless you are willing to commit financially and for the long run," Ladd says. "It is not a quick process. It does involve a great deal of time on everybody's behalf. You have to staff the facility 24/7. You need to make sure your staff can really embrace the entire concept of what managed



PHOTO COURTESY OF DIEBOLD INC.

**ABOVE:** A good test of any managed access system is to become your own customer.

access is. Look at it business-wise and really ask if it is a good process for you or not. There is a big investment to make it a success.”

### WHAT WILL YOU DO FOR YOUR CUSTOMERS?

The first thing to consider when looking into managed access is what services you will offer. There are different levels of “managed” access and sometimes different terms. Some prefer the term “hosted” to mean that they are taking care of the access control end using a different set of employees and resources than their regular central station. Others use that same term to mean that they are literally hosting the client’s software and back end, but the client is still in charge of making changes and day-to-day running of the access control.

“We offer hosted access,” says Albert Skofich, camera/access department, Alarm Detection Systems, Aurora, Ill. “It allows the customer to use their web browser to get data or make changes. But we host the data here. We also offer the ability for us to make the changes via e-mail or a phone call, and that is reflected in the pricing.”

Expectations definitely need to be clear from the start, says Jacky Grimm, director, security solutions at Diebold, Canton, Ohio. “That is a big piece of the equation: What are you going to do for the customer and who is going to do it? The customer’s expectation is that if they outsource it you need to be available 24/7. That includes not only bringing the customer live for the first time, but also setting up the database for each and every site. There needs to be a lot of communication about how their environment works, schedules, who is going to be using what doors. There are often unspoken expectations and everyone has to understand what is standard.”

If the customer does want to generate some of their own reports or otherwise have some role in the managing of the system themselves, you need to make sure the system will support that. “One thing to think about is how user-friendly is the system?” says Kathy Miller, service coordinator, FE Moran, Champaign, Ill.

ADT, Boca Raton, Fla., offers both hosted and managed options depending on the customer’s needs, says Daiva Wood, manager for strategic products for access. “Hosted access is basically software as a service or cloud computing where the customer is responsible for entering all the data and managing schedules, but we manage the hardware, operating system and data.

“Managed access for us means we do all the data entry and scheduling for them. If the customer

doesn’t want to have anything to do with it they can outsource all of their access functions to us. But if they want to have a view into their system they can. It is very easy using the browser-based web interface. As much control as the customer wants we can provide that. We want them to be confident in their security,” Wood describes.

Grimm adds, “The system really needs to act like an extension of the customer’s own security department. Anything they would want their

## Network & Server Issues

A key part of any managed access system is the communication that needs to occur between the host and the client.

“You have to make sure that those who are setting up the program understand and are highly trained in IT, software, hardware and an overall understanding of what you are trying to provide clients,” says Matthew Ladd, The Protection Bureau. “Make sure you have high-caliber people who really understand networks and IT.”

Server failures prevent customers from being able to connect to their account and you from getting data from their site. This is a huge potential pitfall, adds Albert Skofich, Alarm Detection Systems. “You have to make sure you have redundant servers or at a minimum a backup server that you can restore very quickly, especially as you get more and more customers. You are dependent on your link, which is mainly the Internet from the customer’s site to your database. On your end you can guarantee that, but you are limited on the customer end. We still have customers ask about dial-up modems. We try to impress on them how important that connection is.”

Ron Oetjen of Intelligent Access Systems of North Carolina agrees. “I think our biggest hurdle has really been the upfront coordination with the customer’s IT group or the proper communication with technical folks. “Remote management is great once you get it working but it can be a bit of a problem when using Internet communication. Some IT-related programming has to happen.”

The ability to understand IT security concerns is absolutely key to success, says Jacky Grimm of Diebold. “You have to have the technical ability to do the due diligence and make sure your software is secure. You do not want to be the company that allows hackers into your customer’s business. You need to be able to talk about things like ‘Is there any open code? Do you have the license for all that code? How are the security patches?’ There are a lot of decisions just on the software you are going to run. Do you have network-savvy people that can help your potential customers come live? In the IP world we like to pretend that everyone has the same kind of network. That is a lie. Every implementation with a network is different. There is no such thing as cookie cutter.

“Then once you have a network connection you are not done. A customer may have a network that works just fine for their business application, but they don’t realize that the network is going up and down all day every five minutes. Someone needs to monitor that network connection to make sure it is working.”



*Managed access control means becoming the outsourced security department for several clients at once, a task that takes special training but can bring rewards for both dealer and client.*

people to do if they had it in-house you need to be able to do — and even anticipate some of the things they didn't ask you for.”

### **CHOOSING THE RIGHT SYSTEM & PEOPLE**

For dealers and integrators coming from the regular access control or alarm monitoring world, hosted or managed access offers new challenges right from the start.

“You have to have a good, solid system behind it all and really well-trained technicians,” Wood says. “It has to be a non-stop service. If you try to skip on any of that you are going to fail. It is not for the faint-hearted. What's more, even though an access control system may be great for access control, the way it is structured and the kinds of functionality it offers may not be suited to managed access at all.”

Many access systems will not work in a managed application, no matter how good or feature-laden they are.

“You need to find a system that has a partitionable database that is geared towards managed access control,” Ladd says. “Most systems are usually designed for one company, even ones with multiple locations and geography. You need to find an access system that can handle multiple companies so each database stays within their partition. The worst thing that can happen is to send a company a report that has another company's information on it.”

For most dealers offering managed access the solution is to pick one system and stick with it, Skofich believes. “We use one particular manufac-

turer. If a customer wants us to do hosted access they need to use that system.”

This is a change from traditional alarm monitoring and one that may come as a surprise to dealers and integrators, Grimm says.

“When you select an alarm monitoring head end you can generally monitor 95 percent of the hardware that is out there. That is not the case with access control. It is very proprietary and you have to choose your hardware carefully. There are only a finite number of systems you can use.”

And just like the systems themselves, it is not always realistic to expect your existing staff to run a managed access system, either. Choosing and training the right kind of employees is key, says Bill Fisher, central station inside technical coordinator, The Protection Bureau.

“I think one of the biggest things we had to overcome was to make sure our operators were trained correctly and had the background and ability to use the tools we were providing them to make this thing work correctly. We also had to make sure that moving forward we hired more technical, IT-based operators. All this stuff is IP-related so they need to know how communications work as well as how the access systems work,” he says.

Oetjen emphasizes that companies offering hosted or managed access control need to look for an entirely different type of employee. “Some companies try to take their intrusion operators and tell them to also do remote card access. They soon find out it is a whole different animal. We stumbled with that also. In the beginning we weren't looking for the right people.”

Skofich agrees. “Central stations are infamous for turnover. You need to have a couple of key people that take care of the managed access system. We don't really have our central station manage the access system. They get calls from customers if there is a problem but all e-mails during business hours are directed to our service department and one specific agent makes those changes daily. We have two backups for that person. We tried to train our central station on the operation of the access system, but found that they have so much going on monitoring alarms it is not really a priority to them to change someone's card number on a door.”

Many dealers find that choosing the right system then sending the employees for manufacturer training is a good combination. “We do a base level of training in-house but for specific software training we send them to the manufacturer,” Oetjen adds.

“You want to train your staff to really understand how to configure the system and that is usually a



*Providing specialized training to a few key employees and tasking them with handling the day-to-day management of customers' access control systems is often the best approach.*

small number of people," Grimm adds. "Then you want to train your operators to go in and be able to make the changes requested by the customer. You have to train them really well. The last thing you want is to have a security director call you at 8 o'clock Saturday morning telling you he has been driving to all his various sites because everyone is locked out."

### Several Pricing Methods in Play

Pricing and billing can become a sticky issue for dealers just beginning to offer managed services.

"One of the toughest things is trying to figure out what to actually charge the customer," says Albert Skofich of Alarm Detection Systems. "We tried to figure out a formula. We standardized on a minimum price so if you have X number of doors or employees it will cost this much."

Most dealers use either a per-door or per-card formula, depending on what makes the most sense for them. "It really depends on the market," says Jacky Grimm at Diebold. "Some pricing models are per-card because that is a known number. For complex or really big systems pricing might be per-door and per-card."

It's all over the map, says Ron Oetjen of Intelligent Access Systems of North Carolina. "Everyone is still trying to benchmark and find that sweet spot, not charging too much but still making money. I have looked at several different models. We are working on a per-door schedule."

The dealer needs to work out the formula that will work best for them, says Matthew Ladd of The Protection Bureau. "We have a monthly fee that is developed based on the number of card readers and holders and the number of sessions they want. You have to make sure that whatever you decide is profitable for your company and also competitive and an advantage to the client. What is the client's ROI going to be? If you can make it in the neighborhood of eight months or less it will be an easy sale to the client."

### THE DEVIL IN THE DETAILS

If you have done all the work to get a good system with trained people to run it, the next step is to make sure you have processes and procedures in place to deal with the day-to-day details of running several different clients' access control systems simultaneously.

"You need to talk about things like 'what days are holidays and how do the schedules and access to areas change?'" Wood says.

"Schedules are a huge, huge part of this," Grimm adds. "Why? Because that is how everything functions. But also schedules change over time. Depending on where you are geographically, there is a lot involved in just getting everything to work correctly."

The crux of the daily management process, of course, is making changes based on customer requests. This can easily bog down an operator.

Ladd recommends setting up a procedure for the customer to follow. "If a client is calling you three to five times a day to add or delete a card, that can become very time-consuming for you. We found that it was very important to lay out to the customer the most efficient way to provide those changes. We created a 'session' that gives them X amount of changes per month. Any change counts as a session. It helps keep them organized. With any kind of managed system you have to remember you are placing the end user's administration with your organization and you need to make sure you can handle the volume and help the client be efficient."

Other dealers establish a time deadline per day, guaranteeing all changes received before a certain time will be changed on that day and after that time will be made the next day.

Managed access can truly be a benefit to both sides, but the hard work is on the dealer to get it right, Grimm says. "The trick is when you are bringing someone live you have to have a really solid system and processes so you are not making it hard for the customer. The cleaner you can lay it out the better off you are. If you do it right the customer will be a hero in their organization."

A good test of the system is to run the process internally first to make sure all runs as it should. "The best thing we ever did was be our own customer," Grimm adds. "We manage the access control for our own company. If you are not willing to do that you have no business being in the business. If you are your own company you experience everything that could possibly go wrong so you are prepared for it." ■