Networked access control: Can you support what you’re selling?

As networked access control systems have become more affordable and the technology more user-friendly, demand has grown. This is a great business opportunity for integrators for several reasons:

- Networked systems are suitable for clients of all sizes, from just a few openings to thousands of doors.
- Earning potential from the initial sale is considerable, both in terms of product and labor.
- Opportunities are strong for building ongoing relationships and revenue streams.

Whether you’ve been installing networked solutions for years or are new to the game, you can make a big difference in your bottom line by understanding the stakeholder concerns, having the right infrastructure in place, identifying the right clients for your capabilities, and knowing how and where to get product and service support.

Understanding the stakeholders

Along with the transition from keys to cards has come a transition in who owns the budget to pay for a networked access control system. No longer is this a decision made solely by the security department. Today’s clients—from universities and hospitals to corporate campuses and manufacturing—also include the IT department. In fact, it’s the IT department who often has the power to make or break the deal.

According to Brent Dusenberry, Director of Operations for Standard Electronics in San Diego and Santee, CA, demonstrating your expertise to the IT team is critical to making the sale and ensuring a smooth implementation.

“As soon as security goes on the network, it immediately involves IT,” says Dusenberry. “But they don’t always want to add more to their plate. So the more questions you can answer up front, the greater your credibility and the more comfortable they will be.”

Ensuring your company has the right infrastructure

The demands of networked access control solutions require your business to be as technologically sophisticated as your clients’ IT departments—if not more so. Joe Baumgarte, Engineering Specialist at Allegion, says companies supporting client-networked solutions must provide protection against different types of attacks, including both hacks and physical attacks.

“Hacks are very sophisticated today. They are looking for specific data, like credit card numbers,” says Baumgarte. “But physical attacks, like an employee removing a hard drive, can also compromise security.”

To warrant your clients’ confidence, your company must provide redundancy on your own servers and in your Internet service. You must offer extensive training and customer support capabilities. Dusenberry says that, when it comes to networked solutions, you can’t sell something and then figure out how to implement it after the fact.
“If you are going to offer a hosted, access-managed solution, you need to have your IT in-house, on point and ready to go,” says Dusenberry.

He points out that the costs to build your company’s IT resources—both in terms of people and hardware/software—can outweigh the profit on a job if you aren’t prepared for the high expectations of clients.

“Exposing a company’s network is virtually always viewed by IT as a risk. Recent hackings of companies like Target and Anthem have made IT professionals even more wary of opening their network to an outside host in order to support a security system,” says Dusenberry. “As an integrator, you have to be able to make them comfortable right from the start.”

**Identifying the right clients for your capabilities**

Networked access control is no longer an option just for large businesses with big budgets. Commercial clients can include hospitals, corporate campuses, manufacturing facilities and multi-tenant office buildings. These larger organizations are more likely to have both a security team and an IT department, but they still may need your help identifying their current security risks and needs.

Large organizations with this kind of structure are more capable of handling the ongoing maintenance and operation of an in-house access control system. But in many cases, an already-overloaded IT department may look for another party to take on this responsibility.

Smaller clients may include businesses like law offices that are concerned with securing the main entrance, as well as those with staffs working varied shifts, like independent medical clinics or offices, retail shops and restaurants. Small clients are often good candidates for ongoing service relationships because their small size means the access control system needs management only a few times a year.

“Small companies may not use the management aspect of their system every day, so they aren’t always proficient in it,” says Dusenberry.

Targeting smaller organizations can be another way to gain entry into the networked access control market without making a large capital investment in your business.

**Accessing the support you need to succeed**

So how can integrators, who don’t have their own IT infrastructure, get a piece of the growing networked access control market? Allegion is one place to start. Baumgarte encourages integrators to bring in product experts from Allegion to help gather the answers you will need to get IT on board.

Dusenberry points out that you can partner with larger or more experienced integrators who offer wholesale support services, such as 24/7 telephone and tech support, off-site hosting and other services needed to support your client. This enables you to add these services to your portfolio without investing in the personnel and equipment it takes to offer these services.

No matter what your approach to growing your business and enhancing your IT capabilities, it’s critical to get your systems and people in place before you make the sale. This will help ensure your clients are confident in your capabilities and reduce the likelihood that you’re scrambling to pull together a solution you’ve already sold.

**Top tips from the pros**

Both Baumgarte and Dusenberry have a few tips for integrators to keep in mind when selling, installing and maintaining networked access control solutions.
• Find a balance between security and usability. Baumgarte says, “If you turn the security way up, it’s difficult to use. Make it too easy and it’s easy to abuse. You have to find the balance.”

• Consider effective systems, which include off-the-shelf technologies that are readily available, even for mobile management. These products often make a client feel more comfortable about what you're installing, especially if they recognize a brand name like Schlage® or are confident these products have been used successfully in other systems.

• Ask the important questions in the early stages of the sale. The answers will help you identify the best solution and the client’s need for ongoing support. Here are just a few examples:
  - How do you back up your infrastructure?
  - Where is your data stored? Is it off-site?
  - Who is in charge of distributing keys?
  - What happens when an employee is fired or quits?
  - What is your policy for changing access privileges?
  - Who will be in charge of operating/maintaining your system?

• Educate your client. Systems that will include cashless vending require more client education. You will need to talk about encryption and how it protects them. Many integrators discourage clients from including cashless vending or other personal data in their access control system because of the inherent risk of hosting credit card or bank account numbers, social security numbers and other data that could be stolen and misappropriated. As a hosting integrator, you and your client are equally responsible for the security of this data.

Want to brush up your knowledge on security certificates and encryption? Allegion can help. Share these online videos with your team today.

• What Makes Cloud-Based Products Secure: Certificates
• What Makes Cloud-Based Products Secure: Encryption

To find out more about how Allegion can help with networked access control solutions, visit us online at www.allegion.com.