ALLEGION™

Cracking the code: The relationship between integrators and IT

Have you ever experienced a scenario like this one?

You're working closely with the security director of a medium-size business to design an access control solution that gives them a higher level of security and functionality. Even better, the solution doesn't just offer physical security, but also allows them to implement cyber security measures as well—a component the security director wants to add within the next three years.

Problem is that your solution comes to a screeching halt when the security director brings IT into the discussion. Their external IT consultant isn't familiar with your security recommendation and doesn't believe it's compatible with the company's IT infrastructure.

If you can relate to this scenario, you're not alone. With electronic access control growing significantly in the marketplace—expected to top $3.5 billion globally in 2014—integrators are crossing paths with IT more frequently now as IT managers become increasingly involved in physical security decisions.

With demands on bandwidth and internal networks, it makes good business sense to involve IT. These interactions become complicated, however, when they happen as an afterthought, as is the case in the above scenario.

IT becoming key part of access control projects

"On many projects now, integrators are realizing the need for closer working relationships with IT, whether it's an in-house staff or an external consultant," says Erik Larsen, National Integrator Account Manager at Allegion.

And it's a trend that's likely to continue. In his June 2014 "Between Us Pros" commentary, Scott Goldmine, editor of Security Sales & Integration magazine, noted that security system integrators are shifting from being strictly focused on hardware and electronics to more services, software and networks—a shift he believes will only accelerate.

A focus group at ISC West revealed much of the same. Participants reported seeing more security purchases being rolled up into IT because the hardware solutions need to access the network. With stresses on bandwidth and networking for access control and video storage, decisions can no longer be made in isolation from IT.

ALLEGION™

So, what can integrators do to make the involvement of IT work for them instead of against them?

1. **Start early.** "I've seen the best success when a company's security and IT leaders are involved from the beginning. They set the tone for working together and jointly developing a solution," says Larsen. "When security understands the IT infrastructure—and, how, for example, the addition of locks or cameras impacts the network—and, on the other side, when IT understands the liability and reputation risks of not having the proper security solution in place, that's when they can move forward implementing the right solution." Integrators, Larsen says, who advocate for that level of interaction and involvement are more likely to avoid the pitfalls that can hamper the integration process.

2. **Speak their language.** "Key to success is being able to demonstrate to IT that you can speak their language at a basic level and that you know about the system being utilized," says Matt Seymore, Sales Manager with M3T. "This shows them you're there to help them avoid problems, not create them."

3. **Add IT expertise to your team.** As IT becomes more integrated into security, you'll want someone on your team who can effectively communicate about your security platform, while also providing guidance on IT decisions, from both a technical and sales perspective. M3T used to have an external IT partner but, as they saw the role of IT increasing in projects, they decided to add to their own staff. Today, they have multiple IT associates in-house.

4. **Learn their capabilities.** Before project kick-off, M3T makes a point of asking several questions, such as:
   - What IT security policies are in place?
   - What access control points are available to use?
   - Can the system support security beyond PCs?
   - How is cabling installed?
   - Is the server environment virtual?
   - Do you maintain backups or do you want the integrator to do that?
   - How do you onboard a new application?
   - How do you want to handle maintenance of the security solution?

5. **Think long-term.** It's important to view the partnership with IT beyond just installation and implementation—and even maintenance. Consider how you and IT can partner throughout the life cycle of the security solution to provide ROI protection. "Once the security solution is deployed, the integrator and IT should continue to partner and make plans for three, five and 10 years down the road," Larsen says, "Together, they can continue to leverage the network as security needs—and technology—continues to evolve."

If you want an Allegion integrator sales rep to assist your client, contact us today online or by calling **888-758-9823**.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a $2 billion provider of security solutions for homes and businesses, Allegion employs more than 7,800 people and sells products in more than 120 countries across the world. Allegion comprises 23 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®. For more, visit **www.allegion.com.**

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

010447, Rev. 07/2014
allegion.com/us