Access Control Users Looking for Answers on How to Handle Ever-Changing Technologies

Voice of Customer Research Shows End-Users Need Help in Balancing Security Requisites with Technology Scope

Rick White, Ingersoll Rand Security Technologies General Manager

Change is not new. Indeed, back in 500BC, the Greek philosopher Heraclitus proclaimed, "*The only constant is change."*

Two of our nation's most endeared presidents have built upon his decree. John F. Kennedy supported Heraclitus by stressing that "Change is the law of life. And those who look only to the past or present are certain to miss the future."

Ronald Reagan then built on Kennedy's warning by observing that "Freedom is the right to question and change the established way of doing things**."**

No people understand this more than security directors of organizations, big and small, about to undertake the process of developing new security platforms to protect their people and assets. This underlying theme was uncovered in interviews conducted by Ingersoll Rand Security Technologies with over 800 end users in the access control market.

In the respondents' perfect world, the access control solution installed today would be customized to exactly meet present security and safety issues but be able to accommodate other technologies, including emerging technologies that will let this system easily, quickly and affordably grow and adapt as needed. With the confidence that they can stay technologically current without compromise or risk, security directors would like the freedom – now – to choose among solutions deploying any and all technologies, including those yet to be developed.

Why, they ask, should they have to specify only proximity or only smart card credentials? Why do they have to choose between only offline or only online solutions? If online, why must they choose between only wired or only wireless? Why must they isolate technologies when they could choose them all, working under one system with only one database, to provide a holistic security and safety solution?

According to Voice of the Customer inputs, users want a new model for security and safety that lets them customize today while, at the same time, lets them easily migrate

or upgrade in the future. In other words, they want their next access control system to be flexible, adaptable and scalable. It must provide the right products for their own specific applications now and in the future, regardless of whether the initial solution is keypad or card reader, offline or online, or stainless steel or brass. They want components to match existing hardware both in color and style. They look forward to eventually incorporating emergency lockdown, WiFi, network on a card, mesh networks and all the other new technologies that are being discussed in the media and at tradeshows without complications.

And, although such systems can become complex, they do not want to see the complexity. It's not technology itself they see as foreboding; it's how to incorporate new technologies into their present systems. New tools should be simplified, made easy to use and easy to install. Such attributes aren't important only to them. After all, these decisions are now being made in conjunction with IT and finance managers who have different sets of measurable goals and objectives.

Where Are We Now?

Let's review the typical access control system in use today. In all too many cases, it was installed in stages. As a result, it is comprised of different brands and disparate products, many of which do not integrate into the same system or talk with each other. Too often, the hardware and software systems are proprietary, refusing to let security managers to mix and match best of breed components or customize the solution to their specific needs. The system requires too many separate databases and a plethora of software interfaces that create confusion, lower the level of security within the facility and decrease staff productivity.

Such a dilemma is good for physical access control, though. Pain creates change. How soon we forget. Remember the "good old days" when graphical windows-like interfaces didn't exist? We didn't know if it was our video card, motherboard or printer that was creating the glitches that drove us mad. Similar scenarios now face users with their access control systems, or aspects of it, and they no longer want to try staying one step ahead of obsolescence with bandaged solutions. It's time to move on.

Where Are We Going?

Voice of the Customer inputs couldn't have been more specific. Indeed, these security professionals challenged every preconceived, current practice in the security industry.

For instance, instead of locating components such as credential reader or request-to-exit around the door, as has been traditionally done, why can't new integrated lock

designs incorporate these components into the lock itself, providing more value for their investment and a smarter solution, all in one product?

What if such a new security platform could be developed from the ground up using open architecture and interchangeability as its keystones?

That would mean that electronic locks would provide seamless integration with their existing software. The lock hardware would be as easy to upgrade as its software. The lock itself would provide a migration path to future technology needs, not only protecting the facility but also protecting its investment. Users could upgrade their locks without ever taking them off the door, saving installation costs. With interchangeable reader modules, they could switch from one credential reader to another quickly, easily and affordably.

They could do likewise with interchangeable network modules, going from standalone, offline locking to a networked access control system with yet another switchover, to provide instant lockdowns throughout the facility when needed and change access rights from their offices. They could use wireless on those openings where it has been traditionally too expensive or cumbersome and use hardwired where it was most cost effective, all under one system and one database.

No compromises today…no compromises tomorrow.

Free to Move Boldly

The tug between incorporating new technologies now or waiting until later is not restricted to access control decision-makers. We all face such decisions in our daily lives. When do I buy that new PC, flat screen or smart phone? Do I wait for the new version which should certainly have more features that interest me? Will I have to abandon everything I already have – from computer files to recorded movies to phone records – just to enjoy the new features?

As the consumer products industry is finally making it easy for its customers to employ the latest technology today while being able to migrate easily to the best of emerging technologies of tomorrow, so can the access control industry.

After all, access control buyers simply want a solid return on investment and a lower total cost of ownership. They want to be able to buy now with minimal risk to themselves and their corporations, being able to show their budget oversight committees that to buy now provides the best security for their facility and their access control investments.