

For campus security, an integrated system is more than just technology

By Chief James Overton

As potential attackers are becoming smarter and more brazen, it doesn't take long to become sold on the benefits of an integrated security system. That's especially true if you're the one charged with protecting high-traffic areas such as school campuses.

Now how to create one? For starters, it's important to realize that an integrated approach means a lot more than just ensuring technologies work seamlessly together. Rather, a real integrated system requires the entire organization and all its nuances to work as a cohesive unit.

Think about the electronic components of an integrated system. It is well-documented that being able to supplement security personnel with a system that seamlessly combines intrusion, access and video technology into a single interface improves situational awareness and enables faster response times.

It's not uncommon, for instance, for a large university to employ dozens of digital video recorders dispersed across campuses to support camera networks. The ability to manage those DVRs from a single location certainly streamlines operations. But a real integrated system takes it a step further and folds in access control to provide personnel with an all-encompassing platform that can tie access control events with relevant video.

Here are some basic, yet often overlooked, rules of the road to follow when preparing your campus for an integrated approach either from scratch or via retrofit.

Make security top-of-mind, for all

A security director should never be the only security advocate within an organization. If someone applies for a grant for a new building, he/she should include the security costs needed to protect it. Unfortunately, many people don't think that far ahead. Ensuring non-security personnel understand the importance of securing new buildings during the initial planning stages is crucial. This step also obviously makes financial planning for security upgrades much less painful. It's also especially important to include IT staff in initial discussions, given recent advancements in IP technology for things like video systems.

Consolidate Resources

Many organizations have several divisions with separate budgets. It's important to pool resources when appropriate, especially considering that stronger security benefits the organization as a whole. An example of this is incorporating outside

cameras. If a single department needs two cameras, the security director should inquire with other departments to determine if there is a need from them as well. The same is true for access systems - you wouldn't buy a new access control panel for only two new doors, after all. But it's possible that a different department in another building could also benefit from a more-comprehensive system. Using common resources to purchase larger systems often provides bigger bang for the buck.

Never make a rushed decision

Buying the first thing you see after a publicized emergency is a huge, and unfortunately common, pitfall. For example, in the wake of tragic incidents such as the Virginia Tech shooting in 2007, many organizations rushed out to purchase mass notification systems. It's crucial, however, to conduct thorough research to ensure you purchase the right system. Contact organizations similar to yours to gauge their experiences. Ask vendors for technology demonstrations that test the product as best they can in front of you. Admittedly, this can slow the procurement process, but it's very worth it to replicate the success of others.

Never underestimate training

You can have the best technology, but if you have bad or incomplete training, it's about as effective as having no technology at all. Take the time and make the effort to invest in your staff and ensure everyone receives the training necessary to use the technology properly. Fortunately, this is something most vendors do for their customers. Vendors and manufacturers should either conduct mass trainings or "train-the-trainer." It's also important to include IT staff in these trainings.

Bring everyone on-board

It's crucial to ensure you have organizational and/or community support. In a university environment, for instance, an access card system is rendered useless if students are propping doors open. And cameras won't do any good if people can easily move objects to block them. Take steps to inform those within your organization and campus community of your efforts and why they're important. These steps can include ensuring security technology is addressed in new student/faculty/staff orientations. Also take time to address any privacy concerns and clearly communicate that all measures will be taken to comply with reasonable expectations of privacy, which greatly enhances the learning environment.

Choose a partner

Security is about more than just buying and installing products. When it comes to vendors, look for good references. It's important to evaluate the relationships dealers have with their suppliers. This is because you ultimately need to view your vendor as more than just a hardware supplier that issues contracts. Rather, treat your vendor like a true partner that advises your organization on one of its

most critical functions.

Get your money's worth

In terms of working with vendors, be honest with yourself. Don't ask for a pie-in-the-sky solution and then push for price cuts. You truly do get what you pay for, and security is not a place to cut corners. By the same token, carefully evaluate the vendor's track record of service, reliability and responsiveness. It all evens out in terms of price if you make sure you get your money's worth.

An integrated security system requires multiple components to be in synch with one another to provide adequate protection. The same holds true for the campus as a whole.

James Overton is Chief of Police at the Delaware State University Police Department in Dover, DE.

Editorial, <http://www.securitydirectornews.com/?p=article&id=sd200909p9FQ96>