SECURITY SOLUTIONS FOR ENTERPRISE SECURITY LEADERS

How Access Control Fits into Multi-Tenant Housing Security Budgets

While video gets all the press, access control can be the key to incident prevention in housing facilities.

By Karyn Hodgson
September 1, 2013

Multi-tenant housing environments, whether they are condominiums, apartments, high rises or low income, must have security to protect the residents. But the types of security technologies available can make it confusing and tough to choose. Sometimes what you want and what you need is not the same thing. Developing a strategy to employ the right technology at the right time is key, as is understanding what a technology can – and can't – do for your facility.

Think of security technology as a three-legged stool consisting of access control, video and life safety (fire alarms, strobes, etc.). But not all of these are created equal: life safety is required by code, while the other two are discretionary. As a result, choosing how and when to implement access and video is where misconceptions, unrealistic expectations and mistakes most often occur. One of the most common errors is to put in a stand-alone video system without first making sure your doors are secure and monitored by an access control system.

"There are only five things that can be done to protect anything, from nuclear weapons to gold vaults to a residential community," says consultant and author of three books on security, Thomas L. Norman, CPP/PSP/CSC, principal of Protection Partners International in Houston, Texas:

1. Deter it from happening.
2. Detect inappropriate behavior.
3. Help assess what has been detected.
4. Help or mount a response to what has been detected.
5. Gather evidence of the event.

"Everything we do in security does one or more of those five things," he says. "Access control allows normal passage of appropriate users and deters or delays inappropriate users, creating a physical barrier that serves both to deter and detect crime, which is also part of response. Video can help in assessment and evidence. It might also be a deterrent, but it is a passive one."

Access control is an active deterrent. For example, providing video of an assault is not as effective as stopping it in the first place. So if you are starting with little or no security around a building, you need to control access first so you can create a safe haven for residents.

The Titans of Security:Access Control or Video?

There are situations where either video or access control are the obvious go-to solution. For example, if your biggest problem is graffiti or vandalism, and you want to collect evidence, then video makes sense. But if safety is a concern more than property damage, access control should be your first step.

“Access control is proactive and limits who can get access to a site,” says independent security consultant John De George, CPP, PSP, Security Management and Consulting of New York City. “Video is very powerful if you need to do investigation and investigatory efforts after an event has occurred.”

De George adds that video is often the go-to technology for users, not because it is best for every situation, but because it has more public recognition and acceptance. “Everything you see on TV looks to video for crime solving. It is kind of the security ‘glamour child,’ and that is why owners and property managers will often choose that first.”

Video is also easier to “do-it-yourself,” and is available from box stores or the Internet, whereas access control requires an installer with more specialized knowledge.

“After security problems begin, people tend to have a knee-jerk response to the event thinking they should ‘do something,’” Norman says. “The kinds of problems typically being responded to are ordinary crime as opposed to violent crime. In most cases there is a feeling that ‘if we only had video cameras, either we would see the guy doing it and intervene, or the criminal would see the cameras and be deterred.’ From my experience, both of those conclusions are false.”

Why? Because in most multi-tenant residential facilities, nobody is monitoring the video in real time in order to see it happening and stop it in its tracks. And unless the camera is placed in such a way that it will get a full-on clear picture of someone’s face, using it as an investigation or prosecutorial tool is not always a slam dunk – and criminals know that. That is why these cameras are often the first thing a criminal will attack or vandalize to avoid being seen.

Integrator Mike Bradley, president, Safeguard Security and Communication of Scottsdale, AZ, agrees. “Cameras are much better understood by the general public, but also very misunderstood in terms of what you get for your money. Our experience with the multi-dwelling unit (MDU) market is that video is primarily a forensic tool. Very few facilities have the budget to keep an eye on the video all the time. It is a deterrent to some extent and can be used in a forensic nature to follow up on events as needed, but even with the best equipment, the effectiveness of a camera system can be defeated. They won’t always be in the right place looking at events. You can’t have them everywhere and there is no guarantee.”

In other words, video alone, without other security measures such as access, may just move the problem to another part of the property.

Jeffrey Siegel, director, life safety division, American Security Systems, Inc. of Long Island City, NY, likens video to burglar alarms for homes. “If you are in a residential neighborhood and half of the homes have burglar alarms with signs on their lawns, the criminals will break into the houses without the signs.”

On the other hand, access control is not as well understood by residents and is sometimes seen as an inconvenience. Even if residents are asking for better security, if they don’t feel it is convenient they will try to circumvent it.

“Any system that is implemented, if it is not at least somewhat convenient or logical to the users, they will find a way around it,” says integrator Chuck Gladd, president of Gladd Security in Syracuse, NY. “The key is to button it up a bit, but don’t make it burdensome.” Going to a single front door entrance and making the rest exit only may save on cost, but only if the residents don’t prop the other doors open for the sake of convenience.

Access control requires more education both for residents and property managers, Gladd says. “I think there is an understanding that a vulnerability exists, but nobody initially understands what we can do with access control. There is an educational curve, but they are very comfortable with it and like it once they have it.”

Kenneth J. Gould, CEO of KJG Security Consulting in Staten Island, NY, adds: “We are never going to talk a facility out of doing video, and you absolutely should do video if you can, but card access gives you more control of your building. It is common sense. I don’t think security video is sufficient alone, because you need control of residents and who is coming in and out of your building, including the postman, utilities, residents and guests.”

Another very important distinction is that card access also gives better redundancy and reporting so building managers can help assure that only residents, their guests and other appropriate people enter the facility. These reports are confidential and can be used alone or ideally in conjunction with security video to monitor the facility without having to watch every coming and going on a camera or to try to figure out what happened after the fact.

Newer access control systems also often report if one or more components (including cameras) have failed so they can be fixed

immediately.

“The first purpose of access control is limiting access,” Bradley explains. “But the second is developing reports. The primary objective is limiting access to those that belong there and nothing does that better than access control. The bottom line is when you limit access you raise your security automatically.”

Why – or Why Not – Both?

In a perfect scenario, integrators and consultants agree that the best option is integration between access and video, and ultimately life safety as well. But in reality, budgetary constraints and other planning considerations sometimes make that less than feasible immediately.

“I think it is more of an apples or oranges consideration,” De George says. “Access control will allow only authorized individuals to gain access and video will provide surveillance. When you have both of these, you have situational awareness, which is the best of both worlds. I don’t think clients always make a selection of one or the other. Typically they realize they need both.”

When you marry video and access control together it is a stronger security tool and allows for maximum protection, and that should be the goal for any facility. However, deciding whether to phase-in both technologies simultaneously and start smaller, or to go fully with one technology then add the other in later is a question many multi-tenant facilities may face.

“In a situation where you can’t afford full-blown video and access control, you can purchase an access control system and have a few cameras off of that taking snapshots of who enters the building,” says integrator Frank Ross, senior account executive for B-Safe Inc. in Wilmington, DE. “If you do have the money, have video that is recording as well as integrating with access so you are getting that snapshot separately.”

Siegel also advises starting small, but with both technologies, if possible. “The systems we install are completely expandable. We give them the bare essentials. Once they discover the benefits of these systems, they quickly start adding additional cameras and secured doors.”

It is better to have something than nothing. With access control, the easiest thing would be to do one or two doors, initially (while keeping in mind user convenience). “Almost all access control systems are expandable,” Ross says. “We are finding a lot of places right now doing one front door and one back door and budgeting the rest for later.”

Similarly for cameras, one or two doors – even if analog technology to start – might be the way to go, initially. “You put something sufficient in at the time and can grow on it,” Gould says.

Whether you go with a combination or one at a time, it is okay to start small, Bradley says. “My advice would not be to steer them to one or the other. I think they need to look at their facility in terms of layers of protection, starting with the very highest risk areas and moving to the lowest. Where is the most traffic? Where is the highest likelihood of some kind of breach? Start small and move up. Both access control and video systems are likely to have babies over time. They tend to grow. Once people get an understanding of the value, they want more.”

The bottom line is access control and video work best when used together. If the budget allows for only one or the other, the facility manager needs to decide if the existing structure is already safe and secure. If not, then access control should be the first step. If the safety of residents and resident’s property is already assured, then video is a likely first step.

Read more online, including an exclusive on how to design an access system based on priorities, at www.SecurityMagazine.com/MultiTenantHousing

---

Tech Talk

Access control encompasses a wide range of technologies from telephone entry to cards to biometrics. Deciding which is best for your facility is a matter of personal choice, but there are some things to keep in mind.

“Whether it is a key fob or biometric, the most important thing to know is what you want to do with it,” says John De George, an independent security consultant with Security Management and Consulting. “If it is a multi-tenant residential building you really want to secure access to the building. You want something that provides historical data on an access or other event. Most of the major suppliers today have very similar, very advanced capabilities.

“But you do want to look at the credential itself. Will your residents be more comfortable carrying a card or would they be happier with a key fob?”

In some markets, multi-technology cards or smart cards may even be a good choice if you want to tie things like vending, laundry or retail capabilities in. Also keep in mind that in areas where vandalism is a problem, there are access control readers (and cameras) specifically designed to be difficult to tamper with.

Where budgets are tight, a digital entry system based on a keypad with codes, or a phone entry system at the door or gate are cost-effective options.

The simpler, the better, adds integrator Mike Bradley, president of Safeguard Security and Communication. “We have experimented with biometrics and other types of higher end, harder to defeat types of access technology but often there are too many people coming and going. The reality is if you can keep it simple, keep the readers easy to use with conventional credentials like key fobs or prox cards, you are much better off. That’s not to say some of these technologies might not become a good option in the future. Wireless technology and cell phones are emerging access control technologies right now that could be relevant to this market”

“The industry is moving to access control systems for multi-tenant buildings where they can dial their cell phone,” says integrator Frank Ross, senior account executive for B-Safe Inc. “People have always had phones, but now they have cell phones. Phone lines will be going away and the choices will be cable or wireless. Newer systems are able to hook up to the Internet and dial through that.”

Designing for Security

Whether or not a multi-tenant housing facility has the funds to go all out on the latest and greatest integrated system, or must start with minimal solutions and budget over time, the very first thing they should seek out is a risk assessment to determine the highest priorities and understand where they need to focus both now and down the road.

“Typically what happens in these situations is a contractor gets called, does a physical survey and makes a suggestion for one type or another because there isn’t the budget for both,” says consultant and author Thomas L. Norman, principal of Protection Partners International. “But what hasn’t been done is a risk analysis by a properly qualified individual so the organization understands what the real risks are. When you don’t do that, you are working from a perception that is inherently vague and can vary according to the opinions of the people sitting around the table. Nobody has any empirical evidence as to the real risk source or how to mitigate the damages being done, so fundamentally the whole process is flawed and doomed to fail. There is often no comprehensive strategic approach to multi-tenant facilities. It is all tactical about what do we need to do to solve today’s problem.”

Independent Security Consultant John De George of Security Management and Consulting, agrees. “One of the approaches I take more than ‘I have X dollars to spend’ is to go in and do a threat and risk assessment (TARA) and come up with a basic strategy for securing the building. Once you have that entire package identified, then you can look at ‘how much can I buy in the first phase? How much funding do I have initially?’ I would suggest that if in fact you don’t have enough budget, you develop and install over several budget years instead of one.”

In fact, the right integrator is as important a choice as the technology or manufacturer, De George says. “My experience as a consultant suggests that what is more important is not what or whose equipment you buy. The key issue is who do you buy it from and who installs it and who will support it going forward? You need to rely on your integrator and choose one with a good history, whether they are a large scale or local or regional integrator. The integrator is the one who will be there literally in the middle of the night when you have a problem with your system.”

Another key aspect to designing a security plan is understanding that security is about more than just the technology deployed. One suggestion is to follow the four principles of Crime Prevention through Environmental Design, CPTED, which cites:

1. **Territoriality**– Appropriate users protect and respect their own territory.
2. **Natural Surveillance**– Criminals don’t want to be seen committing crimes.
3. **Activity Support**– When legitimate people are engaging in activity, criminal activity is less likely.
4. **Access Control**– The location of entrances and exits, fences and lighting aid in natural direction.

Karyn Hodgson is a long-time security industry reporter with previous assignments at Security Magazine and SDM Magazine. Karyn is the managing editor for SDM Magazine. She can be reached at 630-694-4025.