

By Kenneth Carlisle

Top Ten Security Mistakes HOAs Make

Regardless of whether you live in a densely populated urban area or a more suburban community, security is something most homeowners are concerned about—even if they are not sure how to best secure their own property. Most people know how to avoid the garden-variety, shady-looking miscreant on the street. But, how do you protect your building from unsavory characters?

Hopefully, by pointing out ten security mistakes commonly made by homeowner associations, this article will help you learn how to better protect yourself and your community. The goal is not to frighten but to inspire you to start taking practical action steps that will make you and your property safer.

There is one general mistake many of us make that is probably more important than any of the formal ones; that is “assuming crime won’t happen to you.” There is not a city, community or neighborhood that is immune from crime. Rather than assuming it won’t happen to you, be prepared.

The list of mistakes that follows is not arranged in any particular order. Don’t rely on this arbitrary ranking to give you a false sense of security should the top few mistakes not apply to your association.

Mistake #1: Not Conducting a Security Survey, Audit or Assessment

Without a good security survey “you don’t know what you don’t know.” A good security survey identifies problems by defining vital assets (what must be protected) and then identifying exposures, vulnerabilities and threats to those assets. This obvious approach is really just basic “Problem Solving 101.”

Once it is clear what the problems are, targeted solutions in the form of courses of actions and their costs to implement can be developed. By developing at least three courses of action, security measures, for each problem and considering the feasibility, effectiveness, consequences, and costs of each, we can create a decision document from which the courses of action that provide the greatest return on investment can be selected. Typically these solve or mitigate specific threats defined in the security survey. This gives us a real Security Plan that accomplishes security objectives in a cost responsible manner and identifies specific steps that will detect, deter, delay and deny criminal attacks.

What’s that? The Four Ds: Detect, Deter, Delay and Deny? Yes, yes! Now we have some practical criteria to apply. Rather than wringing our hands in frustration saying “But what can we do!” we

can sensibly ask “Will that security measure truly detect, delay, deter, or deny criminals an opportunity to hurt us?”

The Four Ds approach helps us more clearly understand that the true objective of “Security” is prevention of crime. This orientation is different from that of law enforcement, which has a primary focus on efficiently arresting and jailing criminals who have already committed crimes; this law enforcement approach is a reaction to crime.¹ We don’t want a home invasion to happen and then try to catch the criminal; we want to prevent it! We don’t want to have to go to court where the perpetrator is often released for a surprising number of possible reasons—e.g., as a child he was subjected to bad potty training. We want to prevent the event, the damage, the injury, the costs, the fear and the loss of owner’s equity. We want to live in a safe place.

Mistake #2: Implementing the Wrong Thing

Implementing the wrong thing is a common result of flying blind without a security survey. When quickly reacting to a criminal event, HOAs often end up putting band-aides on a sucking chest wound by implementing security measures that don’t solve the problem. For example, it may seem that hiring a

guard or installing CCTV cameras are obvious things to do. However, these solutions can often be double-edged swords and the “obvious” approach may be completely wrong.

As in any endeavor, the greatest costs are manpower costs. Therefore, do not be shocked to learn that a single security post with one person on a 24/7 basis costs about \$150,000² per year.

Consigning security requirements to cameras and remotely controlled locks in lieu of human staff is often much more economical; however, there can be drawbacks to that approach as well. For example, cutting costs by replacing the guard at the guard booth with improperly applied technology can lead to “piggybacking,” where residents let themselves in and three or four other cars come in behind, thereby allowing easy entry to potential criminal elements.

Better solutions can be realized by clearly recognizing when either guards or technology or both make the most sense. Here are some tips: (1) Retain a guard where a physical action or response must be employed to solve the security problem; (2) Install security technology to either replace or enhance the guard when a human response is unnecessary; (3) Understand that a guard only provides security where he happens to be standing; beyond his view and presence there is no security. A good use of well-designed technology, such as CCTV or alarms or even simply giving guards cell phones to call in police support, is to extend the strengths of real time human response to all areas of a large property.

Many times we see systems where folks have implemented the wrong thing by being “penny wise and pound foolish.” For example, a “bean-counter” mentality can lead HOAs to buy on the cheap when it comes to security guards (if you pay peanuts you get monkeys) or technology. They take the lowest bid without considering security objectives or sometimes even the layout of the HOA community. I have seen HOAs buy dummy cameras (what about a dummy guard or perhaps a dummy owl) that don’t actually do anything but serve as props. This may seem clever,

but associations can pay a giant price later when criminals call their bluff or when someone unknowingly depends upon that dummy camera to provide security and is harmed because there is no real protection after all. A premises liability lawsuit against such an HOA typically results in a settlement in favor of the victim.

Another example of the wrong thing is when the relationship between security and livability is not fully considered. Recognize, for example, that security and freedom have an inverse relationship—greater security results in diminished freedom. A lack of understanding of such trade offs may result in installation of systems that are not in concert with the HOAs internal culture or external environment. The result is often antagonism as well as non-compliance with the security program. If a security program seems silly or dumb, residents will act counter to desired behavior and defeat its purpose.

Mistake #3: Ignoring Premises Liability Law

Security is no longer an amenity but a legal necessity. Speaking broadly, California law stipulates that property owners have a legal duty to provide a safe and secure environment. The legal theory of “premises liability” holds that owners and occupiers of property are legally responsible for accidents and injuries that occur on that property. Furthermore, the defendant property owner is negligent if he/she/it allows a dangerous condition on its property or fails to take reasonable steps to secure its property against criminal acts by third parties.”³

Not only does a good security program protect the physical investment and protect the owner in court; it also helps sell the property. Astute owners are well aware that good security leads to increased owner’s equity by protecting people and assets and by increasing resident satisfaction and owner’s reputation.

Mistake #4: Installing Dumb Security Measures

Dumb security measures are those that can be easily bypassed by friend or foe. Systems that present a perception of security without foundation frequently lead to a false sense of security.

Ah yes, this is the problem where you have the appearance of security rather than the real thing. The Transportation Security Administration (TSA) comes to mind, but that’s another story.

CCTV (closed-circuit TV) is often viewed as “the” security solution by the uninformed. We’ve already discussed how “dumb cameras” can be a dumb thing to do. CCTV can be a splendid security tool; however, if it is not monitored and no immediate response to events is forthcoming, then it is only useful for forensics. As any devoted viewer of video of convenience store robberies and bank robberies will tell you, CCTV does not provide for three of the FOUR D’s. Which ones? For the determined robber, CCTV doesn’t deter, delay, or deny. It only detects, perhaps aiding forensics and maybe not even then if the video only shows the top of a head or blurred pictures. Very common problems are poor cameras or poor camera placement—dumb. If you are using CCTV, the important question is “Are the images useful?”

Another typically dumb mistake is spending \$1,198.00 to protect \$1.98. Perhaps a good example is when vandals paint graffiti on a wall. Do we spend \$5,000 on CCTV to catch them or do we repaint the wall? Always consider both the objective and the cost. Will the course of action cost selected responsibly deter, detect, delay or deny criminal activity?

Mistake #5: Depending on CCTV

As discussed above, CCTV is not “the” solution. In fact, no single stand-alone measure is rarely “the” solution. Security measures should be aptly integrated to take advantage of a multiplier effect. For example, an access control door can be much more effective when it is also being monitored by a CCTV camera. A good door and camera system working together can detect door status (did someone leave it open?), detect early warning visual information about the area (who is coming?), deter (scare less serious intruders off), delay (it takes time to get through a good door), and give an alarm insuring appropriate human denial responses (alert a busy guard and detect for him how to best respond).

Cost and ROI are important factors as well. Effective modern CCTV systems can be very expensive so their value and return on investment should be carefully analyzed and compared with alternative measures. Will the large expense actually accomplish anything worthwhile?

Legal hassles are another concern. For example, recently in a HOA project a homeowner was enraged because a FastTrak toll-paying device was stolen from his car and the HOAs CCTV system did not provide useful video that would help recover it; therefore, in his opinion the HOA was liable for the loss and he threatened suit.

Mistake #6: Having HOA Members Provide Security Services

This is clearly a conflict of interest. In the FastTrak device case mentioned above one of the board members was an employee of a security company. The board thought CCTV would provide protection against vandalism and burglary; and they had the security guy acquire the cameras from his company at cost. He and another board member installed the cameras at no charge. These cameras were installed at an unused sentry booth, which had neither gate nor guard, at the entry to the property. The very angry homeowner whose car had been burgled demanded to know the following: who voted on the measure, how much money was spent, to whom did the money go, who selected that model camera and why, who decided the placement, what level of security did the CCTV provide, and when was the HOA going to pay for the theft from his car. Lastly, he was going to file charges because the HOA was violating his First Amendment Rights by not allowing him to publish a letter of displeasure in their newsletter or address all HOA members regarding his grievance and charges. Weee!

Now, having said all that, does everyone understand the importance of using independent third party providers?

Mistake #7: No Service Contract

If a system can't be serviced, it is garbage.

Warranties on security systems are normally one to three years; however,

they do not usually include labor. In my experience it is wise to have a service agreement with the original installer. This gives the installer a vested interest in making sure the system he installed actually works. Also, since modern systems are complicated, having a second company come out to provide service for another company's installation often results in finger pointing and greater costs. Finally, did we say, "If it can't be serviced, it is garbage."

Mistake #8: Not Taking Advantage of "Crime Prevention through Environmental Design"

The Department of Justice and law enforcement agencies have spent billions of dollars studying and implementing the concepts of crime prevention introduced by architect Oscar Newman's book *Defensible Space, Crime Prevention Through Urban Design*. Crime prevention through environment design builds upon five key strategies: (1) territoriality, (2) natural surveillance, (3) activity support, (4) access control and (5) education. These ideas are presented below to suggest a systematic intellectual approach to preventing crime by influencing offender decisions that precede criminal acts. It would be an egregious mistake not to consider them.

(1) Territoriality:

People protect territory they feel is their own and they tend to have a certain respect for the territory of others. Art, signs, good maintenance, fences, and landscaping are some physical ways to express ownership. Identifying intruders is much easier in a well-defined space.

It is important to know the people in your building and HOA as well as in the general community. Let trustworthy neighbors know when you're going away for extended periods of time. Let them know whether you are going to have somebody checking on your condominium or not. Reciprocate when they are gone.

Be aware that criminals often watch a potential target building for a considerable time prior to breaking in, taking note of the ebb and flow of traffic, residents' work schedules, and possible points of entry. Therefore it is important to recognize who belongs in your

space and who doesn't. Also understand the importance of not letting mail and newspapers pile up, always a clear sign that a home is probably unattended.

(2) Natural Surveillance (and General Vigilance):

Criminals don't want to be seen. Open areas that permit residents to easily see activity provide natural surveillance. Placing physical features, activities and people in ways that make it easy to see what's going on discourages crime.

We are living in the most difficult economic downturn since the Great Depression. Besides causing many other problems it also means that threats of criminal attack are now greater than they were five years ago. There has been a big rash of daytime burglaries. Just being aware of this fact can help increase general vigilance, thus making your building more secure.

Vigilance of residents is vital to any security plan for a building. In practice this means doing such things as risking being impolite by not holding the door for a stranger—even a well-dressed one who doesn't look like a thief. Explain that the building has strict entry protocols, and apologize—but don't let him in.

Good lighting is one of the most effective and cost responsible enhancements to natural surveillance that one can take. Consider the reason retail stores often keep their lights on all night even when closed. It makes it harder for intruders to hide from law enforcement, building residents, passers-by and cameras. Finally, as a caveat, keep in mind that there is a difference between lighting in general and good security illumination. Mood lighting may be nice for lovers but security illumination makes it uncomfortable for evildoers.

(3) Activity Support:

Encouraging legitimate activity in public spaces helps discourage crime. It helps create a feeling of ownership. It also helps neighbors get to know each other and thus better know who is possibly an unwelcome stranger. Any activity or place that gets people out and together – a homeowners' social, a

neighborhood watch group, or even a pleasant common area where people naturally meet each other over time – helps prevent crime.

(4) Access Control:

Access control is a significant concern. It includes such practices as not letting guests into the building prior to getting approval, establishing the identity and purpose of non-residents before granting entry, and not holding an access door open for unidentified individuals. Below are more points about access control that a security conscious HOA should consider.

Well-located entrances, exits, fencing, landscaping and lighting can direct both foot and automobile traffic in ways that discourage crime. Think about easy or especially effective ways this can be arranged in your particular situation.

Condominiums and multi housing properties are popular for intruders because of amenities such as swimming pools, gyms, spas, recreational facilities, playgrounds and parks. These amenities are often found on the outskirts of the property, which make them harder to supervise. Therefore, HOAs should pay particular attention to controlling access to them.

Another simple concept: make sure the doors are locked. How often are service doors left propped open and left unattended by someone waiting for a delivery? Or, how often is a front door opened wide while a resident goes to her car to fetch parcels or to move a sofa out of his apartment? Doors should never be propped open and left unattended for any reason for any period of time. This includes doors from basements or underground garages and roof doors as well the more obvious lobby and other ground-floor access doors.

Key control is also an important component of door control. Your building or HOA should have specific policies with regard to how keys are to be stored and who is to have access to them. We have even seen policies providing for large penalties (used to reimburse for complete common area rekeying) in critical situations such as large retirement communities for the very elderly.

Consider what vendors should be given keys to common areas? Should cleaning ladies or caretakers be given keys to apartments? Keep in mind the various unseen vendor personnel and caretaker's relatives who may be getting secret access without official approval. By the way, according to the pros, keys to your home should never be labeled with apartment numbers; rather, they should be coded so that only the few individuals responsible for them know which doors they open.

(5) Education:

Education influences the environment by increasing security awareness in ways that help residents, individually and as a group, to recognize and prevent potential crime scenarios.

Motivation reinforcement is another benefit of the education. If residents, managers and directors are not all onboard even the most well thought-out security program is useless. The security of the property is everyone's collective concern—not just the security team.

Effective education usually involves participation. Some good ways to increase participation include a neighborhood watch program, training seminars, and quarterly meetings where residents meet with security staff to discuss what is happening on the property and in the neighborhood. Also consider regularly adding brief educational content about security, such as status and practical ideas for improving safety, to your HOA newsletters and regular member meetings.

Mistake #9: System Grows Like Topsy⁴

This mistake is usually not recognized until after the fact; i.e., after several unrelated security measures have been instituted in reaction to a variety of unsettling events.

Typically something happens—a crime. Then an urgent call goes forward to do something. In response to each new call a new security measure is hastily installed without serious consideration of unintended consequences or return on investment. As time goes by and more and more disturbing events occur the security systems grow in a haphazard fashion. Elements fall into disuse or just don't work. Costs climb

sky high. Sometimes, even ineffective bureaucracies can take root and start growing all on their own (just like in government?).

Then people start asking “Why was this done, what does it really accomplish, how much did that cost”? Security may become the laughing stock of the community, which rapidly loses confidence in it. Residents cease to follow security protocols because they are too hard, don't make sense, and are inconvenient. Then security really goes to pot!

Oh! What to do! Stop! Stop feeding the monster or it will only get larger and uglier. Assess what is there—do a security assessment with objectives and goals, evaluate costs versus benefits, remove equipment and protocols that are not working.

Mistake #10: Ignoring Building Codes

Government building codes often require installation of specific security measures. For example, San Francisco Building Code, Chapter 10A. Security Requirements stipulates, “Apartment houses (Group R, Division 1 and R, Division 2 Occupancies) and buildings containing more than two residential condominium units shall meet the security requirements of this chapter.” It goes on from there to mandate several specific security measures.

Here's a related tip for the wise: Be sure to always get the fire marshal's blessing on access issues before making expensive security changes. Ignoring or hiding something from a fire marshal will only make him angry and capricious. And they definitely can and definitely will force changes in anything at all that could possibly affect fire safety.

So! What's your point? The point is that if the worst happens and building codes have been ignored, then the ensuing lawsuit and/or other penalties can bankrupt a blissfully ignorant HOA.

Conclusion

There you have it, or at least a good start. As one can see these ten mistakes often tend to overlap, run together, and have quite a bit of each other in them. That's the point: good security is not just one thing; it is an integration of sev-

eral interrelated concepts, actions and items that tend to be mutually supporting and to have a multiplier effect.

The idea is to get started stacking the odds in your favor. Just knowing the most common security mistakes is a beginning. Choosing small or easy things that will convince criminals to move on is a good next step. Often even little improvements can help you sleep more peacefully at night and let you enjoy an evening out without worrying if your heirlooms will still be there when you get back home. I have also shown you how to start developing a more serious security plan should you have attractive valuables, large legal

risks, or can otherwise anticipate problems.

I know! Feeling concern every time you leave your property is basically un-American. Years ago we Americans felt safe at home and saw such issues as problems only in foreign countries where homes had bars on the windows and had surrounding walls with broken glass atop. But now criminals can often be found literally on our own personal American doorsteps as well. So, let us begin to put things right again and stop being ignorant and thus easy victims for miscreants.

A good security assessment is the underlying secret behind effective security. Many mistakes can be quickly fixed,

some very easily, when confronted by a well-done security survey. Call it a survey, audit, assessment, whatever you wish. But do one. Soon! **EJ**

Ken Carlisle is the principal consultant at www.SecurityNet.com. He holds the professional designation of Certified Protection Professional from the American Society for Industrial Security. He has provided security-consulting services to a variety of both large and small organizations.

1 Law Enforcement does recognize the importance of "crime prevention" and many departments even have Crime Prevention or Community Service officers formally trained in this subject. However, Police Departments are usually on tight budgets and thus are so busy responding to crimes already committed they can only spend a few hours at most on a security audit. A truly useful security survey may often require days to accomplish and even more days are needed to develop, implement and maintain an effective security plan derived from it.

2 Normal full-time hours for one person annually are 2,080 hours. Twenty-four hours, seven days a week requires 4.5 personnel. To pay a guard \$10.00/hour, a guard company will charge the HOA approximately \$16.00/hr. Therefore, 2,080 hrs. X 4.5 men X \$16 = \$149,760. This does not include overtime, holiday pay, or in some cases the costs of training or special uniforms.

3 Further, defendant property owner is negligent if he/she/it allows a dangerous condition on its property or failed to take reasonable steps to secure its property against criminal acts by third parties." (*Delgado v. American Multi-Cinema, Inc.* (1999) 72 Cal.App.4th 1403, 1406, fn. 1) "Even when proprietors... have no duty... to provide a security guard or undertake other similarly burdensome preventative measures, ...there are circumstances (apart from the failure to provide a security guard or undertake other similarly burdensome preventative measures) that may give rise to liability based upon the proprietor's special relationship." (*Delgado*, supra, 36 Cal.4th at pp. 240-241)

4 The phrase "grewed like Topsy" (later "grew like Topsy"; now somewhat archaic) ...of unplanned growth, later sometimes just meaning enormous growth. Ref: Stowe, Harriet Beecher (1852) *Uncle Tom's Cabin*.