

best practices

REPORT #8

Community Security

*Published by
the Foundation for Community Association Research*

Acknowledgements

Thanks to each of the following individuals for their generous contributions to this report.

Foundation Representatives

Linda J. Schiff, CMCA, CTP, COMMUNITY ADVANTAGE of Barrington Bank & Trust Company, N.A.

Sandra Matteson-Pierson, LSM, PCAM, Capital Consultants Management Corporation

Task Force Members

Chuck Bartolomeo, INEX/ZAMIR

Jonathan Caudill, The University of Texas at Dallas

Kerry Colvett, The Wackenhut Corporation

Michael Dean, CS Security and Sound

Chuck Eberle, Applications by Design

Brad Kofford, Community Controls

Mark Montonara, Thorpe Enterprises, Inc.

Bruce Zuest, CPP, Monument Security Inc.

Contributors

Richard Means, PCAM, CCAM, The Keys Condominium Owners Association

Rick Sedivy, Doorking, Inc.

Foundation Staff

David Jennings, CAE, SPHR, Community Associations Institute

Jacob B. Gold, CAE, Community Associations Institute

Sara Drake, Community Associations Institute

Copyright and Use Permission

Published 2008. Foundation for Community Association Research

225 Reinekers Lane, Suite 300

Alexandria, VA 22314

Readers are encouraged to download and reproduce this report for community association managers, board members, individual homeowners, and community association-related industry professionals without permission of the Foundation for Community Association Research provided the following terms are met: this document must be reproduced in its entirety including the use permission statement; this document may not be added to, modified, amended, or otherwise altered from the original as presented here. Readers and users agree not to sell copies of this document or otherwise seek compensation for its distribution.

"This document is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal or expert advice is required, the services of a competent professional should be sought." —From a Declaration of Principles, jointly adopted by a Committee of the American Bar Association and a Committee of Publishers.

ISBN 978-0-941301-73-2

best practices

Community Associations Institute (CAI) and the Foundation for Community Association Research are dedicated to conducting research and acting as a clearinghouse for information on innovations and best practices in community association creation and management. As part of the Best Practices project, operations related to various function areas of community associations—including governance, reserve studies/management, financial operations, strategic planning, community harmony and spirit, energy efficiency, transition, and community security—are available at www.cairf.org as a free download or for sale in CAI's bookstore.

What are Best Practices?

The Foundation for Community Association Research is proud to offer function-specific best practices in the community association industry. The Foundation has developed best practices in select topic areas using a variety of sources—including, but not limited to, recommendations from industry experts and various industry-related publications. The subject areas for the initial best practices were selected through a survey of the CAI and the Foundation for Community Association Research national leaders.

The outcomes of the Best Practices project include:

- documented criteria for function-specific best practices;
- case studies of community associations that have demonstrated success; and
- development of a showcase on community excellence.

The benefits of benchmarking and best practices include: improving quality; setting high performance targets; overcoming the disbelief that stretched goals are possible; strengthening cost positions; more innovative approaches to operating and managing practices; accelerating culture change by making an organization look outward rather than focusing inwardly; and, bringing accountability to the organization because it is an ongoing process for measuring performance and ensuring improvement relative to the leaders in the field.

Accordingly, this project represents an ongoing exploration of best practices used in community associations. The series of best practices will set the bar, which applied research will then continue to raise.

best practices

Contents

| | |
|--|----|
| Introduction | 1 |
| Section 1 Your Association's Obligation to Undertake Security Measures | 3 |
| Section 2 Impact of Crime on the Community | 5 |
| Section 3 Developer Considerations | 7 |
| Section 4 Security Services | 9 |
| Section 5 Video Surveillance Systems | 12 |
| Section 6 Alarm Systems | 15 |
| Community Perimeter Security | |
| Residential Security | |
| Section 7 Access Control Systems | 17 |
| Controller | |
| Security Software | |
| Section 8 Vehicular Access Control | 22 |
| Resident Entrance Lanes | |
| Guest/Visitor Entrance Lanes | |
| • Radio Receiver/Transmitter System | |
| • Barcode Scanner Systems | |
| • Radio Frequency Transponders | |
| • License Plate Recognition Systems | |
| Exit Lanes | |
| Section 9 Pedestrian Access Control | 29 |
| Section 10 Automated Vehicular Gate Systems | 31 |
| Swing Gates | |
| Slide Gates | |
| Barrier Gates | |
| Safety Considerations | |
| Emergency Access | |
| Choosing an Installer | |
| Case Studies | 37 |
| The Polo Club | |
| Laurel Oak Community Association | |
| Attachment 1: Checklist—Tips on Securing Your Community | 40 |
| Attachment 2: Survey—Security Services | 41 |
| Security Acronyms and Key Terms | 45 |
| Additional Resources | 47 |
| About the Foundation and CAI | 50 |

Introduction

A community association board has many responsibilities—setting goals and approving budgets; conducting open, fair, and well-publicized elections; organizing events that foster neighborliness and a sense of community, to name a few. But a board's chief responsibilities, arguably, are to maintain and enhance the common areas and protect home values. Many communities seek to fulfill these responsibilities with security features, vendors, and systems that protect residents and property. The goal of this *Best Practices Report* is to give you an assessment and review of many community security systems and features—including useful tips and tools—to help meet residents' crime prevention needs.

Community security is not a one-size-fits-all venture. What may work for a high-rise condominium may not necessarily meet the needs of residents in a large-scale, planned community. A small, rural townhome association will approach community security needs and systems much differently than an urban, mixed-use development, which may employ security guards, video surveillance, and perimeter gating. Surveying residents about the community's security needs, desires, and goals is an important first step in the decision-making process—to get a sense of the security level members need and want. A board must also take into consideration the community's budget and make decisions that align with the association's financial and legal obligations and objectives.

There are many other key factors an association should consider when establishing a community-wide security program, including:

- What potential for danger or crime exist in your area?
- Are there any security-related requirements in the governing documents or local law?
- What exactly and who specifically does your community want to protect?
- Who will be responsible for researching, implementing, maintaining, and evaluating the security plan and system?
- Does the community have a common communications network, such as a website or blog, so that all interested parties, e.g., board members, management, and residents, can weigh in?

definition of physical security

According to Whatis.com, physical security is “the protection of personnel, hardware, programs, networks and data from physical circumstances and events that could cause serious losses or damage to an agency, institution or community. This includes protection from fire, natural disasters, burglary, theft, vandalism and terrorism. Breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security. First, obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms and cameras. Third, methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires or natural disasters.”

- Are there any insurance considerations or security-related liability issues?
- How will you measure whether a security system has produced superior results?
- Other factors to consider:
 - Convenience
 - Community involvement
 - Safety improvement
 - Ongoing evaluation of program

This report addresses various security-related options that are available to community associations, including security services, access control systems, alarm systems, gates, and surveillance systems. Along with suggestions about assessing the need for crime prevention, this *Best Practices Report* provides readers with professional, unbiased information about the most commonly used contemporary crime prevention strategies and a glimpse into the future of community-level crime prevention.

SECTION 1

Your Association's Obligation to Undertake Security Measures

Prevention is the most effective action against crime. Unfortunately, crime prevention usually becomes a hot topic in a community after someone is assaulted or robbed. Analyze your community association's authority, legal obligations, and security needs now before an adverse situation occurs.

What is the board's obligation to act? Does the board have the ability to make a decision to refrain from taking action, or does it have an obligation in all cases to take some affirmative action? Clearly, there is a difference between making a conscious decision not to take an affirmative step and merely doing so through inactivity—here is a brief review of the legal consequences of each.

The board's legal obligations in the exercise of its management powers are:

- To obey the governing documents
- To have a duty of diligence in the conduct of its activities, and
- To effectively carry out its fiduciary duty to the association and its members.

Common theories used to sue the community association for third party criminal acts include:

- Breach of duty to provide adequate security
- Breach of contract, and
- Misrepresentation.

Both the community manager and the board should understand how to properly discharge their responsibilities under the standards of reasonableness and the duty of care.

When applying the reasonableness standard, determine:

- Whether the decision is arbitrary or capricious.
- Whether it is non-discriminatory and even-handed.
- Whether it was made in good faith for the common welfare of the owners and occupants of the community.

When exercising due care, each board member should:

- Give the association the benefit of his or her best care and judgment.
- Exercise his or her powers in the interest of the association and the members.

The manager and the board also need to analyze their scope of overall authority. They should first look to the association's governing documents, as the articles of incor-

poration establish the purpose of the association, and the bylaws and/or declaration contain specific provisions regarding the duties of the board of directors.

The manager and the board should then conduct an analysis of their legal obligation. An attorney can assist them in reviewing the foreseeability of danger within the community, and case law decisions and trends. Courts in different states have both upheld and denied the association's duty to provide security. The courts have also ruled on an association's duty to properly investigate their employees.

SECTION 2

Impact of Crime on the Community

Community associations have a responsibility to protect the investments of the community members. A person's home or unit is typically his or her largest physical investment, thus protecting property value should be a main concern of any association. In addition, perceptions of personal safety influence current residents' decisions regarding relocation and rank high in prospective buyers' relocation choices.

Assuming that a community is faced with real—as opposed to “perceived” crime—the association can begin to address the impact of that crime by asking several fundamental questions.

Has crime increased resident instability?

Communities can measure *resident instability* in several ways. Two typical methods of measuring resident instability are residential mobility and owner occupancy. Resident mobility measures the frequency in which residents move in and out of the community, while owner occupancy is a rate assessing the number of resident owners. Combining these two measures provides community leaders insight about the prevalence of community instability.

Has crime affected property values?

Crime can have a negative impact on property values. For example, criminal mischief crimes, such as graffiti and destruction of property, directly reduce the value of the targeted property.

Has crime affected the quality of life within the community? Has it decreased community activity participation or is it over-represented in community meetings?

These questions attempt to measure the impact crime has on the quality of life within the community. Most directly, if crime in the community disenchant community members, and they believe the association is not addressing the problem adequately, the majority will take one of two approaches: (1) withdraw from social activities or (2) focus excessively and exclusively on crime in community meetings. Either of these responses is perfectly natural, however, both are evidence that crime has a negative effect on the community.

Community Response to Crime

When crime in a community association is real and increases in frequency, a board of directors will often take a look at its own efforts and response and determine if additional action is necessary. A community's response to crime can be assessed in several steps. To identify and measure a community's response to crime, four basic questions may be asked.

1. What is the community doing to prevent crime?

The initial step in analyzing crime prevention or crime control is to identify what measures are being implemented to address the crime problem, in other words, what is being done? There are several crime prevention strategies that community associations can implement—such as environmental designs, human capital investments, and electronic monitoring, all of which address crime in different manners. This is the assessment phase of a community's response to crime.

2. How does “perceived” crime influence the community’s crime prevention efforts?

The second phase of the community response to crime addresses how the community feels about the communal response to crime. Residents' perceptions of crime are the driving force behind community-level expenditures. Perceptions of crime do not always relate to the actual amount of crime within the community. Additionally, responding to crime does not address the residents' fear of crime; therefore, informing residents of community responses to crime is critical for resident satisfaction. Thus, it is imperative for communities to gauge the residents' perceptions of their crime prevention activities to determine whether residents approve of their response.

3. Is the crime response successful?

The third step to assessing the community response to crime addresses the effectiveness of the community's response. It is plausible that a community could implement a crime prevention strategy but fail to meet its objectives or expectations. For instance, installation of neighborhood lights will not affect daytime burglaries because the lights will not be of use during the time the burglaries are occurring. If the community's crime prevention response is ineffective, inaction would prove more beneficial. Over-taxed association budgets necessitate effective programs that provide the most crime prevention per funding.

4. What are the side effects of the community’s crime prevention activities?

Identifying the side effects of a response to crime is the final step. Just as crime results in a community responding with programs to prevent or reduce crime, crime prevention programs can have unanticipated effects on the community residents. This concept is observable in all communities, but a prime example of this relationship is gated communities.

Gated communities provide a physical barrier between the community and the surrounding area as a form of crime prevention, however, residents are required to validate themselves and their guests when entering the community. This is a classic example of the social contract: the individual relinquishes certain freedoms for macro-level protections.

Assessing the impact crime has on the community and the community's response to crime can help an association develop a crime prevention program. Unfortunately, there is no one-size-fits-all method of obtaining data related to these questions. What may work in one community may not work in another; therefore, this process allows the individual community association to assess its own situation and take custom designed steps for crime prevention.

SECTION 3

Developer Considerations

A developer can have a substantial impact upon the security systems and features a community association ultimately chooses to obtain and implement. Will the community be gated? How much lighting should be placed around the community—and in what areas? Should the community be wired for security cameras and video surveillance equipment? Can landscaping, i.e. placement of bushes, trees, and shrubs, be used effectively to enhance residents' sense of safety? The developer has the opportunity to establish various security norms and practices right from the very beginning.

The Role of the Developer

Prior to the creation of a community association, the developer begins the development process. Once a tract of land has been identified, the developer must garner control of it. Typically, a developer will enter into a contract to purchase the land, subject to certain conditions. Once the ground is under control of the developer, the developer's due diligence begins.

Throughout due diligence, rough sketch plans are prepared. Frequently, a developer will share sketch plans with local officials to solicit their input before more costly hard engineering plans are prepared. The developer should consider hiring a professional management company on a consulting basis to provide input on the plans and ensure that the association will be able to reasonably maintain the common elements—and to offer their advice about whether to install security systems and features. Once the developer decides to proceed with the project, more detailed engineering plans are finalized. It is at this point that the developer begins to consider the rights, powers, and duties of a community association. For larger projects, clubhouses and other amenities need to be designed and located on the plans. These clubhouses and amenities very often will be owned and maintained by the community association. In addition, traffic (both vehicular and pedestrian) and parking considerations need to be taken into account.

IMPLEMENTING SECURITY: a look from the developer's perspective

To secure or not secure...

- Security can reduce liability concerns.
- Security can be a great marketing tool.
- Security can promote prestige within the community.
- Security may be used as a deterrent from outside communities.
- Security can be a good will ambassador.
- Security as an emergency responder.

Amenities

Developers often construct community associations with a wide variety of amenities that are designed to entice potential owners to invest in their associations. Gated communities are a perfect example. Many developers recognize that gated communities can command higher home prices and sell units faster than non-gated communities. A lower quality gate system may operate reasonable well in the community's initial stages of development due to reduced traffic flow. At some point, however, the developer turns

over responsibility for the amenities, including the gate system to the owners, and it is highly recommended that the community contract with a reputable gate access control contractor to perform a system evaluation prior to taking ownership of the system. In some cases, the developer may even finance some of the desired system modifications and updates. And where this is not a possibility, the community will be well informed about what is needed and be in a better position to budget accordingly.

A developer can turn to a number of sources for information about how to go about establishing a security program. Some of these sources include:

- Local law enforcement
- Security consultants
- Marketing studies
- Insurance consultants
- Other communities in the area

SECTION 4

Security Services

It is often misunderstood what role a contract security firm plays when providing security at a community association. Legally, there are many limitations to what actions a security officer can take—whether armed or unarmed.

Many limitations and liabilities arise from action(s) expected to be taken or as the result of a criminal action or serious CC&R violation reportedly taken place. The legal powers of a security officer are usually limited to that of a citizen or a client representative on private property. In comparison, the powers of a police officer and the release from liability they are subject to while acting in their emergency authority carries very little liability in the history books of case law precedent.

Employing a security officer to respond to emergencies within a community on streets, parks, clubhouses, pools, fitness centers, and potentially on an owner's or resident's property is a scenario that must have a scope of work clearly defined through professional legal advisors. The safety of the officer is paramount to the security contractor and at the same time the safety of the owner or resident is paramount to the client or association board. These two concerns can only be brought into alignment through well defined practices and training to those calls for service.

The role of the security officer before and after police, fire, or medical personnel arrive on a scene is different as well and must be addressed in any type of agreement, the scope of work, and in the training program that must take place onsite with the security officers, club house staff, management company, etc. Expectations for security officers must always include what they are expected to do, how they are to do it, when they are to do it, and most importantly, those actions and responses that are never to be done—this is where most firms incur grave liability.

And this legal impact is not confined to the security contractor. If a perceived legal violation has occurred, then most parties involved—security contractor, community associations, and management companies can all get drawn into the dispute. Other factors, such as public roads versus private property, limit the role of a security officer in different ways.

Observe and Report

At the heart of a security service's scope is the phrase "observe and report." The limitations as to what an officer can do in the case of criminal activity make proper observation and accurate and speedy reporting a critical part of the security team.

Deterrence

Ultimately, the best goal of any security system is to deter criminal activity. This is best achieved by striking a balance between high visibility and customer service. A mobile patrol through a community with flashing yellow lights is highly visible. But, some communities find that this is too disruptive of the aesthetic goals of the community. However it is achieved, designing a security solution that creates a high-level of awareness to the criminal element goes a long way to accomplishing the community's security goals.

Clearly Defined Objectives

A successful security solution within a community is built upon clear, two-way communication. Expectations are best managed with detailed “post orders” of what the community expects from the security team. But, it is equally important that some abbreviated form of these post orders be distributed to the community, or posted for reference on the community website, so that community members are not expecting support or activity from the security team that is clearly outside of their orders.

Ultimately, the work of defining these post orders should occur at the outset of a new contract. Even though it is a “living document” and will adjust to changing situations, it should be set up early and the security team should be clearly trained on them. It is important to cross reference the post orders with the community documents in order to make sure that they are not in conflict regarding rules enforcement, signage rules and restrictions, traffic rules, and parking enforcement.

key security considerations

Areas to consider when developing terms and conditions to a scope of work for a security program:

Residential Specific Issues

- Parking enforcement
- Speeding issues or the use of radar
- Privacy issues
 - Neighborhood Watch
 - Video surveillance
 - Residential information
 - Personal habits
- Liability issues
 - Entering private residences and alarm response and/or verification
 - Armed vs. unarmed guards and use of firearms
 - Full time vs. part time presence of security and when things happen before or after security is on duty
 - Onsite officers versus periodic or random vehicle patrols, or a combination of both
 - Legal issues for providing breaks and meal periods to officers assigned to a fixed post such as a gate house
- Serving many “masters”—setting up proper reporting procedures
 - Community management
 - Board of directors
 - Individual owners
 - Maintenance reporting and expectations to repair or clean facilities vs. providing a security presence and carrying out security specific duties

- Gated vs. non-gated
 - Authority for issuing codes, changing codes, and officers’ authority to override access denial
 - Access of visitors—registration of guests, contractors, real estate agents, and vendors
- Public facilities—schools, trails, parks, school bus stops, etc., within the community
- Construction issues—public and private and quiet hours and restrictions
- Animal control
- Clubhouse, pool, tennis court, basketball court, and golf course issues
- Special amenities management and reservations
- Pool monitoring and boat/lake patrols
- Who is responsible for setting up home alarm response and verification?
- Procedures, maintaining spare keys, alarm codes, etc.—management, security vendor, or both?

Labor Management

- Co-employment issues
- Background checks—fully use the investigative measures of the security firm
- Fraternalization
 - Rules being relaxed
 - Privacy issues—information, mail, etc.

hiring a security provider

One of the toughest decisions for any community association is the selection of the security provider. Associations who make the decision solely on price often find themselves dissatisfied with the service and end up moving from company to company.

To avoid this process and ensure that the board is obtaining all of the information and experience they deserve, here are some simple steps to help make this decision a success for the board and community.

1. Create an RFP (request for proposal)—outline the scope of work, expectations as to workload, and the specific qualities the community is seeking from its security staff.
2. Inspect the company’s office of operation. Determine if the personnel and resources are equipped to back up the community’s onsite staff.
3. Review the security officers’ training manual. Better yet, ask to sit in on one of their training classes. What type of ongoing, onsite training can be expected for the officers?
4. Ask the company for a complete list of existing clients. Contact board members to establish their satisfaction with the security personnel, and use a standard list of questions.
5. Ask for a copy of the liability insurance for each of the bidders. Verify that proper coverage exists.
6. Visit existing client communities and speak with security officers working for the proposed firm. Develop some key questions regarding their experience with the employer, their training, and the personnel who supervise them.
7. Ask the company to develop a “transition plan” as part of their RFP proposal. Review the plan with the board. How do they propose to move into the community? A change in the security vendor impacts every owner in the community. Planning for this transition makes the change much easier in the long run.
8. Are vehicles, uniforms, and equipment included in the proposal price?
9. Ask each of the security providers to talk to the board about two things that set them apart. This will afford them the opportunity to discuss unique aspects of their business or service—and the board might learn something about the provider they didn’t previously know.
10. If it is possible, ask the security provider to allow their site supervisor to meet with the board and community manager. As one of the key personnel of the company, this person will have direct interaction with the board, management, and community residents.

First Responder Roles

Part of the defined objectives should clearly address what expectations there are for any “first responder” duties. If life safety is part of the responsibility, the initial and ongoing training should have been planned into the contract and scheduled.

Definition of Key Terms

Proper communication both in the written and verbal sense requires a common acceptance of what the key terms used in the security industry actually mean in plain language. Deter, prevent, mitigate, restrict, detain, respond, react, engage, help, stop, local alarm, verify, assist, as necessary, loss prevention, risk, act, etc., are examples of terms that any individual may assume they know a definition to and what actions or non-actions these may require or infer. Training on definitions is critical and the scope of work for a security officer must be written with as much clarity as possible.

SECTION 5

Video Surveillance Systems

Surveillance systems are another useful tool in helping a board of directors combat crime and protect its community. The basic surveillance system consists of CCTV (closed-circuit television) cameras, cabling, recording devices, and monitoring devices.

When designing a surveillance system, a few questions need to be addressed.

- **What is the camera going to watch?**

Determine what the camera is going to be focused on. If it is going to be focused on the same object at all times, then a stationary camera will do. In larger areas, multiple cameras can be used to cover the entire area or a PTZ (pan, tilt, zoom) capable camera may be used to give the ability to scan the entire area.

- **When is the camera going to be used?**

If the camera is to view a service entrance, it may only be needed during the daytime business hours and may not require additional lighting. Whereas a camera being used at night must have light for an object to be seen.

- **How are the cameras going to be connected?**

There are several ways to connect a surveillance system. In new communities where the property backbone has not yet been installed, specific cabling can be installed during the beginning building phases. Depending on distances, the types of cable that can be used are coaxial cable (maximum of 1,500 feet), fiber optic cable (rated in miles), or Cat5 networking cable (maximum of 300 feet).

For established communities, existing cabling can be used if it is available. If there is no existing cabling available and the addition of cabling is not an option, wireless point to point or mesh networks can be installed to transmit the video signal to a designated location. *(See page 46 for more information.)*

- **How much ambient light is available?**

If a camera is going to be installed inside a building or being used after dark, ambient light must be taken into consideration. Although some cameras have the ability to see in very low light, some light is still necessary. In areas that additional lighting is not possible or desirable, infrared illuminators can be used to create artificial light. Infrared illuminators create light that is above the capability for the human eye to see, but CCTV cameras can see light in this spectrum.

- **Where is the camera output going to go?**

Surveillance cameras can be used in many different ways. If an area just needs to be monitored, but does not need to be recorded, then the camera can be wired directly to a video monitor. If there are multiple cameras to be displayed, they can be wired to a multiplexer which splits the video monitor screen in multiple camera displays.

- **Does the camera need to have PTZ (pan, tilt, zoom) control?**

If the camera needs to see up to 360 degrees of view as well as up or down, or the objects to be viewed are both close to the camera and at a distance, a PTZ camera should be considered. These types of cameras have the ability to be remotely controlled to turn left or right, move up or down, and control the zoom and focus on the lens. These cameras require a controller to move the camera. The controller can be a matrix switcher with a keyboard or a DVR (digital video recorder) with telemetry controls.

- **How are the surveillance cameras recorded?**

Recording the surveillance cameras is accomplished by using a DVR. The DVR takes the video feed from the camera and stores it on a hard drive. The size of the hard drive determines the length of recording time for all the cameras and is divided between the number of cameras. Play back of the recorded video can be done locally at the DVR or remotely over an Ethernet network.

The main locations for community surveillance systems are the entry and exit gate, the community perimeter, and the community buildings.

Entry and Exit Gates

The entry and exit gates may have a license plate camera and an overview camera for each vehicle lane. The license plate camera is specially designed to capture the license plate of a vehicle without the concern of glare from the vehicle or the sun. This type of camera incorporates an infrared illuminator that shines on the vehicle and an infrared cut filter over the lens that blocks any glare so only the reflective property of the license plate can be seen. Due to the infrared cut filter, the vehicle is typically not viewable.

The overview camera is used to capture the vehicle as it passes through at the same time as the license plate camera captures the license plate. This overview camera should be a day/night camera with an infrared illuminator for capturing the type of vehicle at night. *(See Section 8 for a more detailed description of license plate recognition systems.)*

Community Perimeter

The community perimeter cameras should have a mixture of technologies and should all be monitored from a centralized location. A PTZ camera should be used to cover long distances of the community. This type of camera gives the ability to view 360 degrees around the camera location as well as zooming in and out to see long distances.

For areas that do not need a PTZ camera, stationary cameras can be used. These cameras are effective in areas like building access points, parking lots, or entry points.

Both of the types of cameras can be installed in plain sight or in a covert installation. Perimeter cameras that are installed in plain sight not only provide the ability to view objects around the perimeter, but they also act as a deterrent to possible intruders.

Depending on the ambient light of the objects to be viewed, infrared illuminators should be added as well. When adding an infrared illuminator to a PTZ camera, the distance the illuminator will project light should be compared to the distance the zoom lens can see and the objects to be seen at night.

Community Buildings

Community facility buildings may need surveillance systems as well. These systems can be inside and outside of the buildings.

The exterior cameras should cover the entry points to the building, any delivery areas, and the parking lot. Ambient lighting should be considered in these locations to ensure a clear image both day and night.

The interior cameras should cover the common areas and all exit points in the building. Any shopping areas should have a camera viewing the cash registers. Cameras should never be installed in restrooms, locker rooms, or any area that may be perceived as a private or personal area.

SECTION 6

Alarm Systems

Security alarms are yet another tool available to community associations to help prevent crime and secure residents. Alarms can be broken down into two categories:

1. Community perimeter intrusion detection system
2. Residential security systems

Community Perimeter Security

The perimeter security system for a community is the first line of defense against unauthorized access to the association. This security system allows the perimeter of the community to be electronically monitored from a centralized location.

As an intruder crosses the perimeter line, an alarm is activated. The alarm notifies the security guards or police of the location of the breach so they can dispatch the roving patrol to investigate.

There are several different technologies used in a perimeter security system. Depending on the terrain, a combination of technologies may be required. A few of the most commonly used technologies are:

- **Point to point beams.** These devices send several infrared beams between two points. As the beams are broken, the alarm is activated. These are installed in areas with direct line of sight.
- **Stellar cables.** This technology is used on top of walls or connected to fences. It has a shock sensitive cable that is attached directly to the fence or installed in conduit on top of the wall. As an intruder grabs the fence or places his or her hand on the top of the wall, the alarm is activated.
- **Outdoor motion detector.** These devices operate in the same fashion as an indoor motion detector with a much longer range of detection. Outdoor motion detectors can be used in areas that the photoelectric beams and stellar cables can not be installed.

These devices are hard wired to a centralized location and connected to a security panel in an individual zone configuration. Individualizing the perimeter zones allows a more exact location of the breach to be communicated to the roving patrol. Security panel controls the notifications to the guards or police via a security keypad, printer, or video monitor.

Residential Security

Although the perimeter of the community may have a security system protecting the association, the residences should be secured as well. With a young community it is easier for the association to establish a security system requirement policy. This policy simply informs the owners and developers what type of security systems are allowed to be installed in the community. Typically only proven security systems are specified in this security policy. Regardless of the manufacture of the security system, all residences should be monitored by the same monitoring center either on or off property. By limiting the types of security systems installed, it reduces the learning curve of the security

guards when it comes to the functioning of the security system should they need to disarm a residence, give a vendor access to a home or unit, or help an owner.

In most cases, the design of a residential security system is not complex. The standard security system consists of a security panel, door/window contact, motion detectors, an interior siren, and security keypads.

The door/window contacts should be installed on all opening doors and windows. These contacts will trigger an alarm when a door or window is opened while the system is armed.

Motion detectors can be strategically placed around homes or units in the main gathering areas, as well as the master bathroom. The master bathroom is a common entry point because of the easy access to the master closet where most people keep their valuable jewelry and money. Motion detectors are limited and should not be the sole source of security for the home. The system must be armed for the motion detectors to be used. Should an owner arm the motion detectors at night while sleeping, then get up to get a drink, the alarm would be set off when the motion detector senses the owner's movement. If this is the sole source for the security system, it leaves the residence vulnerable at night or while the owner is present.

A minimum of one internal siren should be installed with more in larger houses. The interior siren is used as a deterrent to the intruder and notification to the owner if they are present.

For more security conscious owners, additional options are available to increase the security of the home. Some of these technologies include glass break detectors, which detect an intruder breaking through a window instead of opening it, monitored carbon monoxide sensors, which detect carbon monoxide in the home, and monitored smoke detectors to detect smoke in the event of a fire.

Hard wiring is the best practice for security system devices, but wireless options are available as well. Although a home may have a security system, nothing will help prevent a successful home or unit invasion if the owner does not arm the system.

SECTION 7

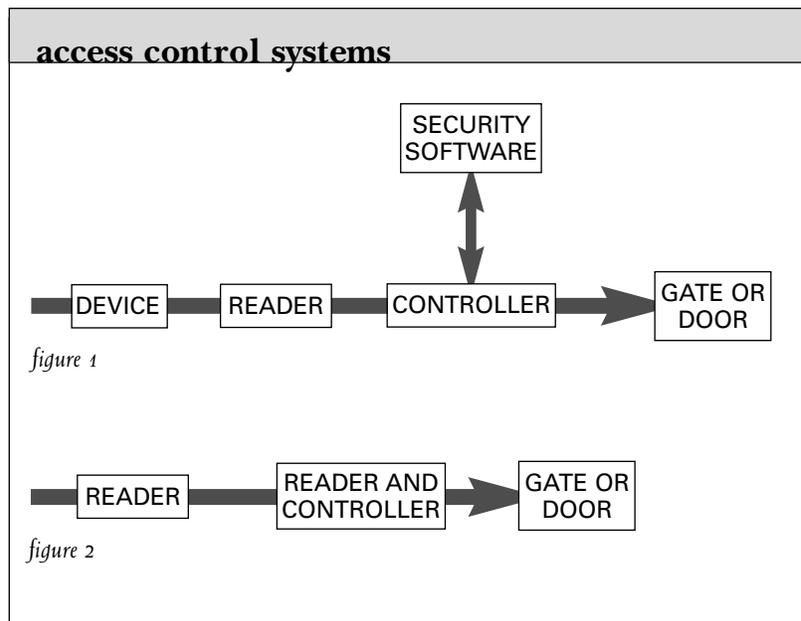
Access Control Systems

This section outlines various design considerations for implementing an access control system for your community. Before making decisions on what type of system is best suited for your community, it is necessary to understand how an access control system works.

In its simplest terms, access control systems include a device, reader, controller, and security barrier. The access control device is read by a reader. The reader sends the device number to a controller. The controller makes a decision whether to allow access and sends a signal to the gate or door for it to open. (See figure 1.)

In simple systems that are designed to open a single gate/door, the reader and controller might be combined into a single device. (See figure 2.)

Typically, access control and security systems can be configured as separate *stand alone* systems, each requiring their own database and programming. This is very time consuming and difficult to manage in larger systems. A better solution is to *integrate* the various gate/door locations, all operating from a single database.



Controller

The heart of an access control system is the controller. It is the part of the system that makes the access control decision. In other words, it decides whether the device should open the gate/door or not. If the signal from the device is valid, the gate/door opens. If the signal is invalid, the gate/door remains closed.

Some access control systems available on the market use a computer as the controller instead of a controller panel. The benefit of using controller panels versus computer based systems is that the access control decisions are made by the controller panels, which use solid-state circuitry that will remain in operation for years, while computers are more costly and much less reliable.

Controller panels can be used to control access at vehicular gates, pedestrian gates, or doors at amenity locations (swimming pools, workout facilities, clubhouse, tennis courts, etc.). The controller panels are programmed with computer software but operate independently without the need of a computer. They also have the capability to support multiple types of access control technologies. Therefore, the community has the flexi-

bility to select the type of device that is best suited for the given application. Virtually all types of reader technologies are compatible.

The use of any of the above devices can be controlled through the use of *access levels* and *time zones*. The access level feature allows the community to limit access to designated gates/doors if desired. For example, residents may be granted access at all gate points, while contractors, service providers, or employees may be limited to access through a specific gate location. The access levels may be customized to meet specific needs. Access may also be limited to specific times of the day and days of the week by using the time zone feature. For example, residents are allowed access 24 hours a day and 7 days a week, while club employees may be limited to the hours of operation of the club. Contractors may be limited to Monday through Friday from 8:00 a.m. to 5:00 p.m.

If your community is looking to control access at multiple locations, multiple controllers may be networked together to create a fully expandable system. The network uses hardware, fiber-optic cable, wireless networks, or broadband Internet service to permit real-time communications between the gate/door locations. When a device is activated, it is instantaneously active at all of the gates or doors. In the event that communications between the controllers is lost, each location will function independently using the last programming data. Upon restoration of communications, the panels will automatically download the transactions that occurred and upload any programming changes that were made while communications were down.

Security Software

While the controller is the heart of an access control system, security software is the brain. In addition to programming and managing the access control system, security software provides many useful features and tools to improve security within the community. Automated access control systems provide the convenience for authorized people to access the community on a regular basis; they don't address people that are visiting the community. Security software allows the community to track guests, contractors, vendors, or service providers that would like to enter the association.

Many communities spend a great deal of money to be gated and to have onsite security officers. Using security software allows the community to get the most out of this substantial investment by providing security and management personnel the tools required to serve the community more effectively. The software allows the association to maintain standardized records on all residents, guests, employees, and contractors that enter the community. It also provides features that can't be offered manually, thus maximizing the return on the community's investment.

Benefits of security software:

- Operational consistency through the use of standardized data input forms, records, and reports.
- Expedite guest processing by automating the procedure, thus allowing guards to focus on welcoming residents and guests.
- Increase accountability of everyone involved with community security through reporting and monitoring.

- Financial rewards—Save money by using technology instead of manpower. Make money by generating and collecting revenue.
- Enhance community marketability by offering additional services; exhibiting an image of professionalism and commitment by using state of the art, cutting-edge technology.

Common characteristics of security software system design:

- User friendly—training new users should take less than one hour.
- The software should be customizable to meet a community's specific needs.
- Modular design that is expandable to adapt to a community's changing needs.
- Enterprise level database management system such as Microsoft SQL.
- Real-time networking to multiple gate and administrator locations via hardware, fiber-optic cable, wireless mesh, or broadband Internet service.
- Integrate seamlessly with controller panels and all access control technologies.
- Onsite and remote database backups performed automatically on a daily basis.
- Ability to import data from the existing community databases.
- Interface with other software programs used by the community.
- Transactions should remain active for 30 days—then they can be archived.
- Utilize name brand, high quality hardware with OEM (Original Equipment Manufacturer) warranty.

Software system features may include:

- Print customizable guest passes that include directions to where they are going.
- Multiple search criteria including searches by last name, first name, address/unit number, lot number, street number, telephone number, license plate number, guest name, employee name, access control device number, club member, or alarm code.
- Dial multiple resident telephone phone numbers automatically. This speeds up the process of contacting residents when a potential visitor is not on their guest list.
- Voicemail capability: Ability for residents to authorize guests via voicemail. This feature can save money by reducing security labor costs.
- Internet capability: Ability for residents to edit their guest list via the Internet.
- Residents should also be able to obtain reports of people that have been granted access to their homes or units. The security software should not subject the resident users to popup advertising.
- Software must have the ability to remain in operation even if communication with the central database is lost.
- Message board system for intersystem communications.
- Warning screens that can include resident specific messages and pictures.
- "Be on the look out" (BOLO) device and license plate warnings.
- Medical information and emergency contacts tracking.
- Special medical needs tracking.
- Second address tracking with the ability to use for mailings.
- Tenant/renter tracking.
- Numerous standard reports—should be customizable to meet association needs.
- Vehicle citations and violations with mail merge capabilities.

- Daily log to track guardhouse activity.
- Guard memorandums.
- Incident and field investigation reports.
- Party guest list management.
- Work order systems.
- Open garage door tracking.
- Out of town resident tracking.
- House check tracking.
- Package/delivery tracking.
- Calendar with event notification whenever users log into the system.
- Traffic statistics by gate location, traffic lane, or community wide.
- Handheld units: Ability for guards to process guests at curbside.
- Roving patrol units: Guards can access the security database in their vehicles.
- Driver's license scanning: Guards scan guest driver's licenses to grant access.
- Dispatch log: Track calls coming into the security department along with dispatch and response times.
- Resident communication system: Send email or text messages to residents to notify them of situations or events that affect the community.
- Video integration: Allows the CCTV system to put a face with the name of guests entering the community.
- Country club interface: Allows staff to greet members or guests by name.
- Photo-ID system: Create customized photo-ID badges.
- Alarm receiver integration: Monitor resident home security and fire alarms.

Investing in security software and systems can be a significant purchase for a community association. Here are some important things to consider when selecting a security software provider.

- Years of experience in providing security software to community associations.
- Number of communities that currently use their security software products. Security software and access control systems require a great deal of system integration. Broad experience with numerous communities and types of systems is essential.
- Number of features—the security software products available on the market offer a wide variety of features. Whether provided by a guard company, gate company, or software provider, the products range from simplistic to complicated. When deciding on security software, it's very important to not limit the association by selecting software with limited available features. Community needs and priorities often change. Features that the board doesn't think they'll initially use often become features that the community can't live without later.
- Speak to other communities that use their security software. Make site visits whenever possible to see the software in action. Service and the provider's ability to keep the software up and running are extremely important.
- Ownership of the community data—be sure to specify who maintains ownership of the software and the community's data.

- Software training—be sure to specify how residents will be trained, and determine what ongoing, refresher, or annual training is available.
- Data transfer—Many security software vendors offer the ability to import old data into their database. Any database, including security software databases, is only as good as the data it contains. The old adage, garbage in = garbage out, is true. If the community is not extremely confident that their existing data is accurate and complete, it will save time and money in the long run to collect new information to be input into the database. The community should maintain responsibility for updating its data to ensure it is current.
- Be sure to establish who will be responsible for ongoing maintenance, changes, and updates to the resident database, and how updates to the software will be handled.
- Help desk—investigate the availability of technical support. Is it 24 hours a day?
- Response time—what is the response time for technicians, parts, etc.?
- Employ Microsoft Certified System Engineers (MCSE).

SECTION 8

Vehicular Access Control

Many community associations have wrestled with issues of vehicles and security problems they pose for as long as there have been automobiles. Whether a community location is urban, suburban, or designed as a gated or open facility, all associations regardless of size eventually have to satisfy their collective level of comfort best fitting their community expectations.

Common factors in defining security entrance requirements are automated or attendant operation, gates, administration, tracking of vehicles allowed onsite, when, for how long, vehicle processing speed, and the timely accessing of information. Once these factors are known and a community security level is determined, various vehicle access and security monitoring technologies are then investigated and evaluated for deterrence, reliability, and ease of operation. Before any vehicle access system is purchased, the final task is weighing initial and continuing cost of ownership against overall system performance, protection level, and degree of difficulty of operation.

All vehicle access systems for a community association fall into four categories: attended, automated (unattended), open access, or some combination of these three. Available systems may be many and configurations can span the range from an attendant visually checking an owner's issued ID prior to allowing facility access to a fully automated license plate reader (ALPR) vehicle tracking and gate opening system.

Whether you are starting from scratch or evaluating your existing gate access control, there are important questions that need to be answered. The type of system that is appropriate for your community depends on what you would like to accomplish. The type of access control device is chosen based on who is going to use the device and the type of access point that the community wants to control. Vehicular access control encompasses three main areas:

- Resident entrance lane(s)
- Guest entrance lane(s)
- Exit lane(s)

Resident Entrance Lanes

The preferred access control method for processing vehicular traffic incorporates a passive read technology. This means that the driver does not have to do anything to operate the system. The access control device is automatically detected by the reader, thus eliminating the need for user input. The advantage of passive read systems is that the user is not required to stop the vehicle and roll down the window to present a card or enter a code into a keypad. The available technologies include radio receiver/transmitters, barcode scanners, radio frequency (RF) transponders, and license plate recognition (LPR) systems. These methods of automatically processing authorized vehicles are much faster and more efficient.

The selection of which system is best suited for your community ultimately comes down to a cost versus benefit analysis. When evaluating the actual cost of the system it

is important to consider the cost of the access control devices required in addition to the initial hardware installation. For larger communities, the cost of the devices often becomes the deciding factor. When determining the number of devices required for the initial system implementation, the community demographics must be considered. As a general rule of thumb, the community will need to purchase 2-3 times the number of homes/units in the community. This takes into consideration that most households have two vehicles plus the devices that are issued to employees, contractors, and vendors. If your community demographics are such that the typical resident owns more than two vehicles, this number may need to be adjusted higher.

A summary of the most common vehicular access control technologies, along with the advantages and disadvantages of each, is provided below:

Radio Receiver/Transmitter System

This technology is easiest to describe by referencing the standard garage door opener hand held transmitter. A radio receiver with an antenna is installed at the device to be controlled which receives the signal from the transmitters. Transmitters that use dip-switches to set the frequency, where all the transmitters have the same code, should be avoided because they are impossible to control. These types of transmitters can be programmed into many vehicles. The recommended transponder technology uses transmitters that have their own unique number or identity. Each transmitter can be programmed and deprogrammed with information about its owner/user, as if it were a card, barcode, radio frequency tag, or any other sophisticated access control device.

Advantages:

- Ability to read without the need for a line of sight from the transmitter to the receiver.
- Read capability not affected by dirt and harsh weather environments.
- Familiar technology.

Disadvantages:

- Transmitters are easily transferred from one vehicle to another. It is very common for transmitters to be passed among friends thereby reducing the level of control provided by the system.
- Long transmission range allows unauthorized vehicles to steal the signal and enables users to give an access granted signal for other vehicles.
- Transmitters can be lost, stolen, or broken.
- Cost of issuing transmitters.

Barcode Scanner Systems

Barcode scanner systems operate by projecting a beam across the roadway. The scanner reads a barcode label affixed to the side window of a vehicle. Typical barcode scanners are capable of reading a vehicle passing at up to 60 miles per hour with great accuracy. The effective read range is a distance of six feet from the scanner at a height ranging from approximately two to seven feet above the road grade. Therefore, barcodes may be used on vehicles ranging in height from a sports car to a semi-truck.

Advantages:

- Barcode labels are not easily transferred from one vehicle to another. The labels are made of the same type of reflective material as license plate stickers. They are specifically designed to fragment and self-destruct on removal. (It is possible to remove the label successfully, but it is difficult to do without damaging the label.) The barcode labels must be affixed on the outside of the vehicle's side windows.
- Barcodes can not be lost or stolen since they are affixed to the vehicle.
- Barcode labels affixed to the vehicle window allow visual verification by guard staff.
- Barcode labels are very inexpensive.

Disadvantages:

- A line of sight is required from reader to device. Snow, ice, or very heavy dew may obscure the barcode. The most common failure of the system is when the window that the barcode label is attached is down (so the barcode is not visible). The barcode labels should be installed on fixed side windows whenever possible to avoid this potential problem.
- Vehicles must be directed to pass the scanner within its read range.
- A barcode label affixed to windows is viewed as unsightly by many.

Radio Frequency (RF) Transponders

A radio frequency reader is positioned at roadside and angled to read entering vehicles. A radio signal is broadcast into a read area. The system reads a transponder that is usually placed on the driver side dashboard. When the vehicle's transponder enters the reading area, it interrupts the stream of radio signals. The electronics in the transponder modify the original radio signal so that the transponder's unique message is embedded in the signal reflected back to the reader antenna. The reader decodes and interprets the signal, and provides it to the access control system. These systems have a high read rate. The radio frequency readers are rated to read a battery-powered transponder up to 30 feet and a non-battery transponder up to 15 feet from the read head.

Historically, a major drawback for transponder systems was that the transponders could be moved from vehicle to vehicle. This practice greatly reduces the level of control afforded to the community. In response to this problem, the transponder system manufacturers have introduced deactivate (break) on removal transponders. These types of transponders are affixed to the inside of the windshield with double sided tape. Removing the transponder from the windshield causes the transponder to deactivate itself, thus eliminating the problem. These transponders can be reactivated by the supplier at a fraction of the cost of purchasing a new transponder.

Advantages:

- A line of sight from the reader to the transponder is not required.
- Read capability is not affected by dirt and harsh weather environments.
- Deactivate of removal transponders can't be passed from vehicle to vehicle.

Disadvantages:

- Metallic windshields found on some high end vehicles can interfere with the signal.
- There is possible signal interference from multiple transponders.
- Non-deactivate on removal transponders can be transferred from one vehicle to another and can be lost or stolen.
- Batteries must be replaced every 1-3 years in battery powered transponders.
- Cost of issuing the radio frequency transponders.

License Plate Recognition (LPR) Systems

LPR systems use infrared cameras to read license plates of vehicles entering the community. Imagers that contain their own infrared light source are preferred as opposed to imagers that require a separate light source. The LPR camera captures a series of pictures and sends them to a processor. The processor analyzes the image to determine which one has the clearest view of the license. Special algorithm software essentially reads the picture and converts the image to an alphanumeric code that can be handled by a typical controller. The read accuracy is greatly increased by comparing the license plate number read against the license plate numbers in the security software database.

Recent advances of automated license plate reader (ALPR) technology have made deployment within community associations as attractive as other more traditional gate opening devices. Significant cost savings can be realized by using a vehicle's license plate to open a gate rather than placing a specific triggering device in a vehicle. The cost savings directly increases with the amount of vehicles which are allowed access in the community. With some communities having several thousand vehicles the cost savings of vehicle triggering devices will more than pay for an automatic license plate reader system and some associations claim a vehicle crossover point, with one entrance lane, of 300-400 vehicles. Additionally, cost savings can be realized with the elimination of attended gate operators, and costs associated with system administration, triggering device storage, replacement, temporary passes, batteries, and lost or stolen units are eliminated.

Key components of an ALPR system are the plate reader, a processor, software, and a data administration networking package. Typically, a plate reader is aimed at a vertical plane "target zone" of approximately 3x5 feet and when any vehicle enters this zone the plate reading sequence starts. Within 200 milliseconds a visual plate image is converted to alphanumeric text, matched to an authorized list of vehicles allowed to enter, and a command is issued to trigger a relay to open a gate.

Low light, no light, direct sunlight, or approaching vehicle headlights will not effect the system's ability to read license plates, as the system imager uses unique near pulsed infrared illumination technology to "read" the reflective properties of license plates. For years, traditional markets such as law enforcement, toll roads, and pay parking have been making successful use of plate reader technology under all types of conditions.

Plate reading is easily accomplished within the gated community environment as there is a predetermined list of vehicles authorized to enter and the system will only open a gate based on these predetermined plate reads. After initial adjustments and some minor optimization, a good system installation should be able to read and match to the database vehicles authorized to enter.

Here are some important considerations to be aware of when assessing differing license plate recognition systems.

Intelligent matching—The system must be able to do some intelligent matching, should the need arise. For example, a plate ABC-1234 is on the approved list for a gate to open but the last digit 4 is blocked by a trailer hitch. The better systems can learn to make this plate adjustment by not reading the last number. Letting the vehicle in without the last number being part of the read does not compromise security.

Speed—The speed of accurate plate capturing, matching, and sending a command to open a gate must be fast. The typical elapsed time for this sequence of events is 200 milliseconds or less. In real life this is about the blink of the eye. Some LPR systems are not fully automatic, cannot process in real time, and should be avoided. As an example, for toll road violation deployments, 200 milliseconds would translate into a vehicle travel speed of more than a 100 miles per hour.

Environment—Environmental considerations also should be factored in the system selection process. In addition to reading plates in direct sunlight and 0 lux light level, a system should be able to endure all of the temperature extremes typically found in desert or frozen climate conditions. Imagers should also be resistant to moisture, humidity snow, and driving rain, specified as IP 66. (*See page 45.*)

When looking to deploy a vehicle plate reading system for access control and vehicle security tracking, other important considerations are:

- A. Is it easily interfaced to other security systems?
- B. Does the system interface with a card access control system, DVR's, CCTV?
- C. Can it alert an alarm when a vehicle of interest is present?
- D. Will it permit temporary vehicle access?
- E. Will it track the length of time a vehicle of interest is within the community?

In order to accomplish these considerations, additional applications would ride on top of the window's plate reading software. A community association will need to determine which features are important and if they are included by the manufacture in the initial pricing. The key advantage of any security interfacing is having total security vehicle control while not introducing an additional stand alone system for security personnel to learn.

Auto license plate recognition technology is rapidly becoming a very cost effective, single source tool for solving security and vehicle access challenges facing community associations today. Using plate reader technology provides a seamless, user friendly means of accomplishing a community's security needs. Accuracy and reliability should always be factors in any system selection. The most important requirement is selecting a system provider with local support and a comprehensive understanding of all hardware components and software application programming to meet the association's present and future needs.

Advantages:

- No special devices required since the vehicle's license plate is used as the access control device.
- Offers the ability to gather information from all vehicles.

- Long term guests can be allowed to use the resident entrance lanes for future entries by entering the license plate numbers into the security software. This can greatly reduce the traffic volume in the guest entrance lanes.
- Can manage vehicles of interest, i.e., plate numbers attached to public court orders of protection, thus eliminating potential problems at the gate.
- Can track and manage the length of time a vehicle is allowed in the community. For example, a delivery truck authorized to enter for one hour or a guest pass for a weekend. Alarms can be automatically generated whenever a vehicle exceeds its time limit.
- In facilities where vehicle access is open, the ALPR system can be used as a monitoring and logging tool rather than an access control device. For example, a multi-use facility would have a combination of CCTV cameras, ALPR system, and DVR integrated so when an incident occurs within the community, and only a partial license plate was remembered by an owner, the system could search the database by partial plate numbers and obtain visual positive ID evidence of the driver and vehicle using an integrated system consisting of ALPR, DVR, and CCTV. If there is a match, even down to just three or four consecutive characters, an image of the plate will be called up to allow the operator to verify that it is indeed the plate of interest—right down to the state of issue which can be determined from the image itself.

Disadvantages:

- Hardware can be expensive, depending upon the provider and system.
- Line of sight device—license plate must be visible to the camera.

It is beneficial for the community to sell access control devices to frequent guests of residents, employees, contractors, vendors, and regular service providers on an annual basis. The community may require these types of guests to purchase the device to gain access into the community or it can be offered as an optional convenience. The device may be programmed with a deactivation date of one year from the date of issuance, thus generating a source of recurring revenue for the community. This revenue source can be used to offset the cost of operating and maintaining the system. In some cases, the sale of access control devices can even pay for the cost of the system.

The community maintains control of who enters and at what time through the access level and time zone features included in the controller and security software. This process also affords the opportunity for the community to verify that vehicles that regularly access the community have proper registration and insurance.

Another benefit is improved traffic flow at the gate locations since these vehicles are processed automatically by the system. This reduces congestion through the guest entrance lanes and allows the security staff, where available, to process guests in a more efficient manner. As a result, the required number of guard staff may be reduced, thus lower labor costs.

Guest/Visitor Entrance Lanes

The type of guest/visitor lane access control system that is appropriate is determined by whether the gate location is manned by security staff or unmanned. If the gate location is manned, the use of security software is recommended. If the gate location is unmanned, a

visitor telephone entry system is recommended. If the gate location is manned for part of the day and unmanned for the remainder, as is often the case with construction entrances/gates, both would be required.

Manned Gate Locations

Historically, security guards working in the guardhouse of a gated community used a pen and paper to record guest information when they entered the association. This practice was extremely slow and the data obtained was essentially useless because it required manual labor to look back through the paperwork to obtain information. If guest lists were available, they were also kept on paper in rolodex fashion. Sharing information and guest lists between multiple guardhouses was virtually impossible.

Computers and security software offer a much faster and more efficient way to authorize and record guest information as they enter the association. The sophisticated security software described earlier in this report is designed specifically for this function.

Unmanned Gate Locations

Visitor telephone entry systems provide a means for people with an access control device to gain access into the community. The visitor's telephone is installed at curbside along the guest entrance lane. It contains a directory, which typically includes the last name and first initial, of all of the residents that live behind that gate along with a code number. The visitor locates the person he or she wants to visit on the directory and dials the appropriate code. The telephone unit dials the resident's phone number that is associated with that code. The resident answers the telephone as usual and determines whether he or she wants to admit the guest. To grant access the resident uses his or her home telephone to send a signal to the telephone entry unit to open the guest entrance lane gate. If the resident does not answer the telephone or denies access, the unauthorized guest must exit the property. A suitable turnaround area is required for vehicles to exit the community without having to back up.

The use of visitor telephone entry systems is a time consuming process. As such, they are not recommended for busy gate locations. Sufficient stacking area is required for vehicles waiting to use the system so they do not block the resident entrance lane or overflow into the adjacent roadway.

Exit Lanes

The majority of gated communities do not control vehicles exiting from the community. The reasoning behind this follows the premise that since the vehicle was authorized to enter the association, it should also be allowed to exit. Adding access control to exit lanes can double the cost of the overall system and the labor required by security officers. Many communities do not have gates on the exit lanes and if they do, they are opened automatically. However, controlling vehicles and pedestrians exiting the association can greatly increase the level of security provided to the community. In this case, the security software can generate reports of vehicles that are in the community at any given time.

SECTION 9

Pedestrian Access Control

Some communities control pedestrian access into the community at various entrance points and amenity locations inside the community. Here are some common tools security providers offer to help control pedestrian access.

Keys

Keys are typically only used for single doors that have a very limited number of people that need access. They are not recommended for community wide access.

Some communities task their security departments with maintaining keys for home/units within the association. If this is a consideration for your community, make sure your security software has the ability to track all of the keys.

Keypads

Keypads are electronic devices similar to the numeric pushbuttons on your telephone. The user types in a preprogrammed code to gain access through the gate/door. Keypads can be challenging to control in communities. It is very common for the code to be shared with unauthorized people. For example, a resident gives the code number to the door on the workout room to a friend so they can use the facility while they are out of town.

Access Cards

There are a wide variety of access control cards available on the market. Some examples of cards include magnetic swipe, barium ferrite, barcode, and proximity. All require the user to present the card to the reader to gain access. Each card can have its own identity, usually a number, which allows management to assign cards to specific people. Cards are ideal for resident access through pedestrian gates or into amenity locations such as the swimming pool, workout room, or tennis court.

Access cards are not recommended for use in vehicle access control systems for several reasons. First, the fact that the user must present the card to the reader is inconvenient and greatly slows access into the community. The second is that cards can be easily passed from person to person, thus eliminating the control that the community is trying to achieve.

Photo IDs

Photo IDs are ideal in situations where community management staff is present or when the security department can make spot checks. Staff can verify that the user of the card is the actual owner of the card. The photo-IDs can also double as an access control device, including magnetic swipe, barcode, and proximity cards. A community's security software should have the capability to generate custom photo-IDs should the need arise.

Biometrics

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Examples of human traits used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins.

Using biometrics for identifying and authenticating community residents offers some unique advantages. Only biometric authentication bases an identification on an intrinsic part of a human being. Tokens, such as smart cards, magnetic stripe cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed.

Biometrics are generally not used in access control systems for gated communities. This is largely due to:

- Cost.
- The amount of training required to use the system.
- Potential maintenance issues.

SECTION 10

Automated Vehicular Gate Systems

Gated communities are rapidly expanding throughout the U.S. and are commonly found in many community associations today. The type of gate chosen by a community is largely based on aesthetics, cost, and physical space available. The three most common types of vehicular gates are swing gates, slide gates, and barrier gates. Some other types of vehicular gates include vertical lift gates and cantilever gates. These gates are not routinely used in community associations.

Swing Gates

Swing gates hang from hinges mounted to a post or column and operate similar to a door. They are the most common and are generally considered to be the most attractive type of gate. The downside is that they are the most expensive to maintain. The maximum recommended gate panel width is 12 feet and the weight of the gate panel must be considered. Gates that are too heavy increase the wear and tear of the gate operator. In most gate applications two gate operators are required, one to open each wing of the gate set. Having two gate operators doubles the expense and requires twice the maintenance. Swing gates are the most susceptible to damage since anxious drivers often hit them as they enter the community with their cars. Swing gates are:

- Designed and installed so as to not create an entrapment area between the gate and other fixed objects.
- Installed in such a way so that the pillar or column covered by the swing gate when in the open position does not exceed 4-inches.
- Characterized by smooth bottom edges.

Slide Gates

Gates that slide horizontally along a track are known as "slide gates." The preferred method of installation has the track that the gate rides upon, typically a steel angle iron, imbedded in a concrete foundation. Thin tracks that are bolted into the pavement should be avoided. Slide gates require the most physical space to install since a "pocket" for the gate to retract into is required. The slide gate backtrack area can also interfere with sidewalk routing or other obstacles. Some consider slide gates to be less attractive but cheaper to maintain. Only one gate operator is required and it has fewer vulnerable parts to break. When a car clips a slide gate, the usual result is the gate getting knocked off the track as opposed to bending or breaking a control arm or weld point.

Slide gates are the most dangerous because of the potential pinch point between the sliding gate and the support column/post. Signage must be placed on both sides of the gate in plain view. Common characteristics of slide gates include:

- Weight bearing rollers are guarded or covered.
- All openings in the gate are guarded or screened from the bottom of the gate to a

minimum of 48-inches above the ground to prevent a 2.25-inch diameter sphere from passing through the openings anywhere in the gate, and in that portion of the adjacent fence that the gate covers in the open position.

- Gaps between the gate and fence, or other stationary objects do not exceed 2.25-inches.
- Smooth bottom edges.
- Positive stops to prevent the gate from sliding past its design limits.
- Will not fall if the gate becomes detached from its supporting hardware.

Barrier Gates

Barrier gates, also known as swing arm or parking lot gates, have a boom that rotates vertically to allow vehicles to pass and are most common for manned gate locations. They are not recommended in unmanned gate applications due to their lack of security and susceptibility to being damaged.

High-speed highway toll road style barrier gates open and close in less than one second and are recommended for resident entrance lanes. These types of barrier gates are designed for high traffic areas and meet the stringent standards required for all state highway toll plazas. Unlike typical parking barrier gates, these gates are engineered to operate thousands of times per day. The fast operating speed allows for improved vehicle passage and reduces the possibility of tailgating. This also tends to reduce the number of collisions with the barrier gate boom since unauthorized vehicles are discouraged from attempting to run the gate.

For guest/visitor entrance lanes, slower gates can be used. These barrier gates should also be high quality but can be designed to operate in applications where the vehicle processing speed is not as demanding.

Here are a couple of other things to keep in mind related to vehicular gating:

Vehicle detectors and sensors. All vehicular gates, regardless of type, use vehicle detection sensors. The most common type is a loop sensor, which is typically placed in a saw cut in the pavement or installed under brick/stone pavers. A continuous loop of wire is placed into the saw cut and seal, or placed in conduit under pavers. An electrical current is run through the loop, creating a magnetic field. A vehicle detector, typically placed inside the gate cabinet that is being controlled, senses the presence of the vehicle over the loop by detecting a change in the magnetic field. Placement of the loop sensors is critical for proper operation of the system. Vehicle sensors are named after the function that they perform as described below:

- **Close loops**—Send a "close" signal to the gate once the presence of a vehicle is no longer detected.
- **Safety loops**—Hold the gate open when the loop sensor detects the presence of a vehicle. They are designed to keep the gate from closing on a vehicle.
- **Free exit loops**—Send an "open" signal to the exit gate(s) when the presence of a vehicle is detected.

Tailgating. Tailgating is when a vehicle follows an authorized vehicle through an open gate before it closes. A security breach occurs when an unauthorized vehicle follows a resident or other authorized vehicle into the community. Tailgating is most common with swing and slide gates due to the nature of how they operate. After an authorized vehicle passes through the gate, the close loop signals for the gate to close. However, if another vehicle pulls up onto the safety loop prior to the gate fully closing, the safety loop will signal the gate to reopen. This is amplified by the fact that swing and slide gates typically take between 12-15 seconds to close.

The best way to prevent tailgating is to install a barrier gate in front of the swing or slide gate. The barrier gate is synchronized to operate in conjunction with the swing/slide gate. The barrier gate remains closed while the swing/slide gate opens. Once the swing/slide gate is fully open, the barrier gate opens to allow one vehicle to enter and closes immediately after the vehicle has passed. Then the swing/slide gate closes.

Safety Considerations

The continuing proliferation of automated gates for use in controlling who enters and exits the community has necessitated that safety guidelines be established for their use and installation. Manufacturers and the installing dealer will help determine the type and specifications necessary for the equipment that should be installed for the particular applications.

Safety standards are written for everyone's protection. The professional system installer should provide a safe gate operating system. To comply with the manufacturer's installation instructions and industry safety standards, the installer may present some options of specific safety devices that can help ensure a safe gate system. Some of these safety devices and gate construction criteria are listed below.

- Secondary entrapment prevention device or devices are installed in areas where an entrapment hazard exists. These devices include contact (electric edges) and non-contact (photo-electric) sensors.
- Warning signs are placed in a visible area on each side of the gate.
- Gate controls are installed so that a person operating the controls cannot come in contact with the gate or gate operator.
- The gate operator is appropriate for the construction and class of the gate.
- Rollers are guarded.
- Pinch points are eliminated or guarded.
- All openings in slide gate systems are guarded or screened from the bottom of the gate to a minimum of 48-inches above the ground to prevent a 2.25-inch diameter sphere from passing through the openings anywhere in the gate.

Never install a vehicular gate operator that does not carry the mark of an internationally or nationally recognized testing laboratory (NRTL), such as Underwriters Laboratories Inc. or Interek Testing Services NA, Inc. This ensures that the gate operator has been tested by an independent third party laboratory and has met all the safety requirements of applicable safety standards as designated by the country of origin. See www.osha.gov for more information.

Emergency Access

When an automated vehicular gate system is installed in a community in general access areas, there must be a method to allow emergency vehicles (fire, police, ambulance, paramedics, etc.) access to the community without the gate hindering their entry. The access system must allow for entry through the vehicular gate under three different and unique situations:

- The system is in service and under normal operation.
- A power failure has occurred and battery powered convenience open systems are employed.
- A power failure has occurred and the convenience open system has failed—due to a dead or low charged battery.

Situation 1—Normal Operation

Under normal operation, there are many devices that can be integrated with the vehicular gate system to allow emergency vehicles access to the community. When any of these devices are activated, the vehicular gate is commanded to open and remains open until the device is deactivated. Typically, the emergency vehicle access device will bypass the primary access control device—a telephone entry system, for example—and is wired directly to the gate operator so that the gate will open, should the need arise. Some of these devices are listed below.

- **Click-2-enter.** This system consists of a special radio receiver that allows fire departments, police departments, and ambulance companies to open the access gates by using their two-way radio installed in their cars or trucks.
- **Special keys and key switches.** With this system, emergency vehicles each have a special access key that activates an emergency override key switch. These key switches are typically labeled "Fire Dept." and are installed in a location at the gate that is visible and easily accessible.
- **Lock boxes.** Lock boxes are essentially the same as the key switch option in that a special padlock (to which only emergency vehicles have a key) is placed on the lock box to lock it shut. When the padlock is removed or cut off, the lock box automatically commands the gate to open and will hold the gate open until the lock box is re-closed and locked. Lock boxes are typically labeled "Fire Dept." and are also installed in a location that is easily visible and easily accessible.
- **Siren sensors.** These devices detect the "yelp" mode from an emergency vehicles siren. When the yelp is detected, the gate will open.
- **Strobe light sensors.** These devices respond to the flashing strobe light from the emergency vehicle. When the strobe light is detected, the gate will open.
- **Wireless transmitters.** Like garage door openers, wireless transmitters open the gate from a distance of 75 to 100 feet. These transmitters are specially programmed with a code that is unique to emergency vehicles.

Because of the many different devices and options that are available, community leaders should consult the regional building department to determine which method of entry is preferred by the local authorities.

Situation 2—Power Failure with Battery Powered Convenience Open System

Many manufacturers of vehicular gate operators now offer battery powered convenience open systems that provide a method to open the gate when primary AC power is removed. This type of system is completely self-contained in the operator and is completely independent from the primary drive system. In essence, this provides a redundant drive system when the primary AC power is removed.

Operators equipped with a battery powered convenience open system typically operate in one of two different methods:

1. When a power failure occurs, the system immediately commands the gate to open and remain open, or
2. When a power failure occurs, the system remains in a stand-by mode until a command from either a wireless transmitter or manual switch is received to open the gate.

In the second option, it is important to note that the radio receiver is powered from the batteries which allow the receiver to remain in operation during a power failure. This design feature assures that any emergency vehicle using the wireless transmitter method of entry will be capable of commanding the gate to open even during power outages.

Battery powered convenience open systems in vehicular gate operators provide a trickle charge to the batteries during normal operation. It is advisable that maintenance personnel and community managers check these systems on a monthly basis to assure that the batteries are in good condition and have enough power to open the gate. Batteries in these systems are good, on average, for about two years before they will need to be replaced.

Situation 3—Power Failure and Battery Powered System Failure

This is the “worst case” scenario that must be addressed during the design of the vehicular gate access system. In other words, system designers and installers must assume that at some point in time there will be a primary power failure and the battery powered convenience open system will fail to open the gate because of dead or low charged batteries or because of some other system component failure. Under these circumstances, the gate operator must assume a fail-safe mode. Simply stated, the operator “fails” in a safe condition allowing the gate to be manually pushed open without the need for any keys, cranks, or other mechanical devices. This is an essential feature for both emergency and non-emergency vehicles. Obviously, emergency vehicle personnel cannot waste time looking for keys, cranks, or attempting to force the gate open with bolt cutters, the “jaws of life,” or other mechanical devices. They also cannot wait for maintenance personnel to arrive to activate gate release mechanisms that are typically located on the inside of the gate. Likewise, community association boards cannot allow a situation to develop where residents are “locked” out of their homes. Many fire department regulations require that fail-safe gate operators be installed to allow emergency vehicle access during power outages.

Automatic vehicular gate systems provide convenience and limit traffic in gated communities, condominiums, and private homes and businesses. When vehicular access is restricted, there must be a means to allow emergency vehicles access in the overall

design of the system. This design must include failure modes under the worst-case scenario, and the access system must have in place equipment and products to overcome the worst-case situation.

Choosing an Installer

While the equipment manufactured for automated gates is designed for long life, it is still a mechanical product and will need service and maintenance to ensure its longevity. It is therefore vital that the company chosen to install your equipment has the experience, tenure, and expertise in installing and servicing an automated gate system. The following minimum guidelines should be addressed when choosing a system installer.

1. Do they have significant experience in installing and servicing automated gate systems?
2. Will they provide you with a list of similar installations covering at least the last several years?
3. Perform a credit check on the company with one of the major credit bureaus. Because of lien laws it is important to have a financially viable company that has a history of paying for their equipment. Remember to obtain lien releases before paying for any installation in full.
4. Have they been certified by any of the major manufacturers or industry associations through training programs? If so, which ones and are they the manufacturers of the equipment they are going to be installing?

The automated gate system is the first impression many will have of the community. Because the gate system involves a large moving mechanical device, carefully select the professional who will be installing the system—especially since the safety of all residents are at stake.

Case Studies

The following case studies, the Polo Club of Boca Raton and Laurel Oak Community Association, are intended to showcase how a community association can effectively implement a security program. In each of these situations, the board, management, and owners have worked together for the best interests of the association and successfully established a safe and well informed community.

case study #1

The Polo Club of Boca Raton

- Size:** 1,708 homes
- Age:** 1985
- Location:** Boca Raton, FL
- Board Size:** 11 members
- Contact:** Alexander Raimondi, CCM, CAM, Chief Operating Officer and General Manager
- Email:** alexr@poloclub.net

The Polo Club of Boca Raton is one of the most exclusive country club communities in south Florida. Located seven miles from downtown Boca Raton on 900 meticulously manicured acres, with two 18 hole golf courses, 29 Har-Tru tennis courts, 145,000 square foot clubhouse, and 30,000 square foot spa and fitness center, the member owned residential community is comprised of 24 associations with more than 1,800 homeowners.

The Polo Club residents value their privacy and have high expectations for their security program. The primary goals of the security program are providing value to the residents and offering them a sense of safety and security. To meet the residents' desire for controlled but quick entry to the system, the community installed an integrated access control system providing a record of all resident, visitor, and contractor community ingress and egress, gate arm integration, and video capture technology.

Safety and security go hand in hand at the Polo Club. Realizing that the Polo Club patrol officers are the most familiar with the community and in emergency situations are the first on scene, the Polo Club patrol includes a trained team of non-transport emergency response paramedics around the clock. These trained officers respond to over 200 calls annually and have saved numerous lives during the past four years. While 911 is always called first, having trained responders available has undoubtedly improved the survival rate of Polo Club residents. The patrol vehicle is equipped with a paramedic automated external defibrillator (AED) unit, comprehensive state required medical supplies in accordance with Florida administrative code, a public address system, and light fire suppression equipment.

In the past individual homeowners contracted with various alarm monitoring companies to monitor their home alarms and dispatch local law enforcement. The response time

ranged from 20 minutes to one hour. To address this need the Polo Club installed a redundant alarm receiving system in the main gatehouse and, utilizing the buying power of the association, contracted with a single alarm monitoring company, reducing the total costs by two-thirds and assuring residents of a less than two minute response time by the onsite roving security personnel.

Looking for ways to provide public relations oriented service to the residents has led to providing a security officer in the clubhouse on a daily basis and providing a special response team to provide surveillance of areas not accessible by road patrol officers—fence lines, golf course areas, and densely covered vegetation areas. With more than 500 employees the Polo Club also utilizes their security team to assist with employee terminations and crime awareness seminars.

The Polo Club management team attributes the success of their security program to a focus on developing strong relationships through effective communication between residents, management, and the security staff. Utilizing an outsourced security provider with clearly defined experience and background requirements has given the Polo Club long tenured security officers that know the community and the residents.

By providing customer/resident driven solutions that go beyond the traditional security functions, the Polo Club has become a model for security programs that residents count on for protecting not only their property but for improving their overall quality of life.

case study #2

Laurel Oak Community Association

| | |
|--------------------|----------------------------------|
| Size: | 400 homes |
| Age: | 1989 |
| Location: | Sarasota, FL |
| Board Size: | 5 members |
| Contact: | Ruth Johnston, Community Manager |
| Email: | loca10@comcast.net |

Laurel Oak Community Association (L.O.C.A.) in Sarasota is an upscale gated community designed with privacy in mind. Located on 813 acres of wetlands and nature preserve property, the 400 single family homes are located on lots ranging from one half acre to three acres. The community includes two Gary Player golf courses, 12 Har Tru tennis courts, a 45,000 square foot clubhouse, and a family of native deer that reside in the nature preserve. The community has two manned gates and a fully integrated gate access control system.

Laurel Oak is devoted to the interests of the homeowners and strives to help the community continue to live up to its mission statement: "We envision Laurel Oak as a safe and beautifully-maintained community, committed to high levels of owner satisfaction, mutual respect, and a spirit of community among our diverse residents, all harmoniously integrated with the Laurel Oak Country Club." As the association manager, Ruth Johnston has the primary responsibility for oversight of the security program. According to Ms. Johnston, the most important part of the Laurel Oak security program is communication—ongoing and frequent communication with residents and daily communication with the security officers.

Laurel Oak residents receive a weekly email from the L.O.C.A. manager every Friday, regardless of where they are living. The emails contain brief information on everything going on in the community and include a security focus. The emails focus on positive reminders, keeping residents aware and up-to-date. The ongoing communication provides reinforcement and the ability to quickly communicate any concerns. Residents have a reliable source of consistent information that replaces speculation and hearsay. Additionally, the association maintains an extensive community website that includes a wealth of information for residents, including the ability to easily update or change their gate access information. The website also includes important security and disaster response plans that are updated annually along with hurricane shutter guidelines, community documents, and resources to assist residents.

Ms. Johnston believes the key to communication success is establishing partnerships that bring value to the residents. The gate officers know every resident on a first name basis and work with management to keep residents feeling informed and cared about. Whether providing residents with periodic safety classes, preparing disaster recovery plans, or assisting the local Girl Scout troop with a fundraising drive at the front gate, the security officers are an integral part of the community, sharing experiences and keeping a safety and security focus for the residents.

ATTACHMENT 1

Checklist: Tips on Securing Your Community

- Analyze your community as a whole—include both the surrounding communities and the community association in this analysis.
- Conduct an annual safety survey.
- Call a security meeting with the members.
- Point out effective interior security measures, in meetings and in newsletter articles.
- Conduct daily or weekly tours of the property, both on foot and by car.
- Check street lighting nightly.
- Communicate with neighboring properties.
- Review your use of exterior lighting.
- Control access into the community association, by limiting the number of entrance areas, or via gates.
- Use effective landscaping and maintenance measures.
- Establish a neighborhood watch program, including an out-of-town watch program and regular member recognition for their participation.

ATTACHMENT 2

Survey: Security Services

The responsibility for making a prudent decision on a security provider can best be served by thoroughly investigating the proposing companies. While many considerations factor into the decision of which security company to employ—such as community type, budget, and resident expectations—here are a series of questions that can help guide a community association through the evaluation process. The point system ranges from 0-5, with 5 representing the most satisfactory answer and 0 being unsatisfactory.

| CRITERIA | 0 | 1 | 2 | 3 | 4 | 5 | NOTES |
|---|---|---|---|---|---|---|-------|
| Human Resources | | | | | | | |
| 1. Determine if the company has their own background investigation process and evaluate the extent and quality of the background investigation. | | | | | | | |
| 2. Does the company use an outside lab for drug screening of all personnel? | | | | | | | |
| 3. How does the company recruit officers? What programs are in place? | | | | | | | |
| 4. Seek proof of the company's vacation and benefit package in detail. Determine what percentage of the health insurance premium is paid by the company. Ask what other plans are available. | | | | | | | |
| 5. Does the company have safeguards in place to ensure prescribed pay rates are adhered to and full background checks are successfully completed prior to assignment to a particular account? | | | | | | | |
| Training | | | | | | | |
| 6. How does the company provide training to its employees? What kinds of resources does it use? | | | | | | | |
| 7. Does the company provide continuing education to all security officers? | | | | | | | |
| 8. Has the organization been recognized by any industry groups or publications? | | | | | | | |
| 9. Does the company issue a standard invitation to all prospects to make unannounced visits to training classes for the purpose of examining materials, speaking to students, and evaluating the overall learning atmosphere? | | | | | | | |

ATTACHMENT 2 / CONTINUED

Survey: Security Services

| CRITERIA | 0 | 1 | 2 | 3 | 4 | 5 | NOTES |
|--|---|---|---|---|---|---|-------|
| Operations and Support | | | | | | | |
| 10. Does the company have their own 24-hour communications center to support all after hours activity? | | | | | | | |
| 11. Does the company have radio system/communication capabilities that meet the needs of the customers? | | | | | | | |
| 12. Does the company provide a formal transition plan to encompass all activities during the transition? | | | | | | | |
| 13. Evaluate office management. Inquire about their backgrounds, job duties, and length of employment. | | | | | | | |
| 14. Determine if the company provides an ample supply of uniforms, weapons, and other equipment at no charge to the officer, as well as replacement of damaged uniforms when necessary. | | | | | | | |
| 15. Determine the company's policy regarding outside supervisory visits, including from office management. Determine the frequency and review documentation. | | | | | | | |
| 16. Determine the company's relationship with local law enforcement. | | | | | | | |
| 17. During national disasters, hurricanes, landslides, earthquakes, fires, etc., what are the company's capabilities dealing with these circumstances? How are they provided and at what cost? | | | | | | | |
| 18. Ascertain the number of support offices in the immediate area. | | | | | | | |
| 19. Review office copies of operational orders from existing clients. Ascertain if they describe in-depth all of the instructions and duties for the site. Check for thoroughness and attention to detail. | | | | | | | |
| 20. Will the company remove any officer from the community at your request? Ask what the procedure entails. | | | | | | | |
| 21. Does the company have an incentive award program in place for outstanding performance and heroic deeds? | | | | | | | |
| | | | | | | | |

ATTACHMENT 2 / CONTINUED
Survey: Security Services

| CRITERIA | 0 | 1 | 2 | 3 | 4 | 5 | NOTES |
|---|---|---|---|---|---|---|-------|
| Validation | | | | | | | |
| 22. Require the company to bring in working security officers from various communities to be interviewed by your team. Ask any questions that you feel appropriate. | | | | | | | |
| 23. Determine if the company sends you evaluation questionnaires regarding their performance, as well as the frequency. | | | | | | | |
| 24. Regarding firearms, what programs are in effect beyond state requirements to enhance judgment and safety training? | | | | | | | |
| 25. Determine if the company has been designated and certified by Homeland Security to be a qualified provider. | | | | | | | |
| 26. Does the security company have a policy for protecting the information of residents? | | | | | | | |
| 27. Gather opinions from other clients regarding the company's performance over an extended period of time. | | | | | | | |
| 28. Ask to see letters of commendation received throughout the years from clients and the public. | | | | | | | |
| 29. Ascertain the company's experience in working with community associations. | | | | | | | |
| 30. Ask the company about client cancellations and the reasons. Judge the veracity of the company's explanations. | | | | | | | |
| 31. Does the company have a working relationship with various minority subcontractors to be utilized when required by bid specifications? Ask for proof. | | | | | | | |
| Value Added | | | | | | | |
| 32. Beyond uniform protection, does the company have the ability to provide other services when needed that include investigations, undercover, loss prevention surveys, engineering services, consulting services, and risk assessment services? | | | | | | | |
| 33. How encompassing is the liability coverage provided and does the company provide a hold-harmless agreement to the client? Determine the amount of coverage. | | | | | | | |
| | | | | | | | |

ATTACHMENT 2 / *continued*

Survey: Security Services

| CRITERIA | 0 | 1 | 2 | 3 | 4 | 5 | NOTES |
|--|---|---|---|---|---|---|-------|
| Value Added, <i>continued</i> | | | | | | | |
| 34. Determine the company's experience utilizing technology in conjunction with manpower. Examples: computer access control, instant mobile reporting utilizing a PDA system, capability of tracking real time incidents, and location of security officer. Does the company have an affiliation with an electronics company for surveys and installation? | | | | | | | |
| 35. Ascertain what innovations, if any, the company has made to enhance the security posture of all of their clients. | | | | | | | |
| 36. Does the company provide upward mobility and promotions for their security officers throughout the organization into supervision, middle management, and senior management? Ask them to provide examples. | | | | | | | |
| 37. Request that the company provide a state regulatory contact for you to inquire about licenses, complaints, and violations. | | | | | | | |
| 38. Investigate the financial stability of the company. | | | | | | | |
| 39. Does the company belong to and/or are they active in professional organizations such as ASIS, CAI, or BOMA, etc.? | | | | | | | |
| 40. Is the company involved in the local community, charitable organizations, or chamber of commerce? | | | | | | | |

Security Acronyms and Key Terms

AC (Alternating Current)—AC refers to the form in which electricity is delivered to businesses and residences. Audio and radio signals carried on electrical wire are also examples of alternating current.

ALPR (Automated License Plate Reader) or LPR (License Plate Reader)—Captures or stores license plate information by converting the video image to a computer journal entry of manageable text, by using special plate illuminators, combined with real time video analytics processors.

CAT5 (Category 5 cable)—A twisted pair cable type designed for high signal integrity and used in networking applications.

CCTV (Closed-circuit television)—The use of video cameras to transmit signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted, though it may employ point to point wireless links.

Coaxial cable—A type of wire that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cabling is the primary type of cabling used by the cable television industry and is also widely used for computer networks, such as Ethernet.

Controller—The heart of an access control system. The controller is the part of the system that makes the access control decision. It decides whether the device should open the gate or door.

DVR (Digital Video Recorder)—This device transforms analog video signals from security cameras into digital format, suitable for storage on a hard drive. It also helps the user manage the stored video files, as well as providing motion detection settings and PTZ security camera control. DVRs can often be remotely accessed over the Internet.

Ethernet—A family of frame-based computer networking technologies for local area networks (LANs). The name comes from the physical concept of the ether.

Fiber optic cable—A cable made up of super-thin filaments of glass or other transparent materials that can carry beams of light. Because a fiber-optic cable is light-based, data can be sent through it at the speed of light. Fiber-optics are less susceptible to noise and interference than other data-transfer mediums such as copper wires or telephone lines.

Infrared illuminator—A light source working in the infrared frequency range.

IP 66 (Ingress Protection)—A designation system used to classify different types of housing according to their degree of protection. The protection classification offered is shown by the letter IP and two digits. The first digit indicates protection for persons and equipment (6 means dust tight), and the second digit indicates the protection against water (6 means protected against heavy water jets).

MCSE (Microsoft Certified Systems Engineer)—A certification offered by Microsoft proving expertise in designing and implementing the infrastructure for business solutions based on the Microsoft Windows 2000 platform and Windows Server System.

“Mesh” networks—A decentralized and simplified network created through the connection of wireless access points installed at each network user’s locale. Wireless mesh networking could allow people living in remote areas and small businesses operating in rural neighborhoods to connect their networks together for affordable Internet connections.

Motion Detectors—These devices are used to detect motion on security cameras. Simple motion detection triggers the camera to either record or set an alarm. Motion detection by frame region instructs the camera to respond only if a certain area of the screen detects motion. Outdoor motion detectors operate in the same fashion as indoor motion detectors with a much longer range of detection.

Multiplexer—A high-speed switch that provides full-screen images from up to 16 analog cameras. Multiplexers can playback everything that happened on any one camera with no interference from the other cameras on the system.

NRTL (Nationally Recognized Testing Laboratory)—A U.S. Department of Labor Occupational Safety & Health Administration (OSHA) program that recognizes private sector organizations for meeting necessary qualifications. The NRTL determines that specific equipment and materials meet consensus-based standards of safety to provide the assurance, required by OSHA, that these products are safe for use in the U.S. workplace.

OEM (Original Equipment Manufacturer)—A company that acquires a product or component and reuses or incorporates it into a new product with its own brand name.

Point-to-point networks—These devices send several infrared beams between two points, usually host computers. Point-to-point is sometimes referred to as P2P, or Pt2Pt, or variations of this. As the beams are broken, the alarm is activated. These are installed in areas with direct line of sight.

PTZ (Pan, Tilt, Zoom)—PTZ cameras allow you to adjust the position (“pan” is side-to-side, “tilt” is up-and-down) and focus (“zoom”) of the camera using a remote controller.

Stellar cables—This technology is used on top of walls or connected to fences. It has a shock sensitive cable that is attached directly to the fence or installed in conduit on top of the wall. As an intruder grabs the fence or places his or her hand on the top of the wall, the alarm is activated.

Additional Resources

Books available from CAI

Before Disaster Strikes: Developing an Emergency Procedures Manual, by the Institute for Real Estate Management.

This two-piece set includes a book and a diskette to download key resource material. Learn how to minimize injury, loss of life, or damage to property, or prevent an emergency altogether. This valuable book contains information how to develop emergency plans, teams, and manuals; how to assess security systems; when and how to evacuate; public relations; and how to report and document an emergency situation.

Neighborhood Watch: What Residents Can Do About Crime

How do associations form Neighborhood Watch groups? Find out how to get started, keep residents involved, and gain support from police, local government, and civic organizations. This brochure is perfect for association residents that want to make their neighborhoods safer.

Spotlight On Security For Real Estate Managers, by Lawrence J. Fennelly, CPO

Security is a matter of concern for most association managers. In this new second edition of *Spotlight on Security for Real Estate Managers*, various security issues are addressed, such as vandalism, protecting residents, liability and the role of security in maintaining property values. It explores different approaches to crime prevention, provides tips for identifying security risks and cost-effective strategies for maximizing security. This book also includes a section on how to perform your own security survey and a sample security checklist.

True Stories of Survival and Triumph in Communities Like Yours, Common Sense from Common Ground: A Collection of Articles from CAI's Award-Winning Magazine

Community associations all across America face tragedy every day—financial ruin, natural disasters, terrorist attacks, lawsuits, even murder. And yet they not only survive, they rise above disaster and become stronger communities because of it. Read their inspiring stories, and see how much goodness lives in communities just like yours.

Other Books/Articles of Interest

Behind The Gates: Life, Security, and the Pursuit of Happiness in Fortress America, by Setha Low (2003).

Crime Prevention Through Environmental Design, by Timothy Crowe (2000).

The Design and Evaluation of Physical Protection Systems, by Mary Lynn Garcia (2001).

Effective Security Management, by Lawrence J. Fennelly, CPO (2004).

Encyclopedia of Security Management, by John Fay (1993).

Fortress America: Gated Communities in the United States, by Edward J. Blakely (1999).

Handbook of Loss Prevention and Crime Prevention, Lawrence J. Fennelly, CPO (2004).

High-Rise Security and Fire Life Safety, by Geoff Craighead (2003).

"Gated Communities and Property Values," by Michael LaCour-Little and Stephen Malpezzi (2001).

Introduction to Security, by Robert Fischer (2004).

Physical Security: 150 Things You Should Know, by Louis Tyska and Lawrence J. Fennelly, CPO (2000).

Risk Analysis and the Security Survey, by James Broder (2000).

Security and Loss Prevention, by Philip P. Purpura (2002).

The Ultimate Security Survey, by James L. Schaub and Ken D. Bicy (1998).

Understanding Crime Prevention, by the National Crime Prevention Institute (2001).

Additional Resources, *continued*

Web Resources

American Fence Association, www.americanfenceassociation.com
Building Owners and Managers Association (BOMA) International, www.boma.org
The American Society of Landscape Architects, www.asla.org
ASIS (American Society for Industrial Security) International, www.asisonline.org
ASTM International, www.astm.org
Community Associations Institute, www.caionline.org
Door and Access Systems Manufacturers Association, www.dasma.com
Foundation for Community Associations Research, www.cairf.org
International Association of Professional Security Consultants, www.iapsc.org
LiveSecure.org, www.livesecure.org
The National Association of Security Companies, www.nasco.org
National Crime Prevention Council, www.ncpc.org
National Ornamental and Miscellaneous Metals Association, www.nomma.org
Project Safe America, www.psn.gov
Security Magazine, www.securitymagazine.com
U.S. Department of Homeland Security, www.dhs.gov or www.ready.gov

Other Best Practices Reports (available at www.cairf.org)

Community Harmony & Spirit
Energy Efficiency
Financial Operations
Governance
Reserve Studies/Management
Strategic Planning
Transition

Foundation for Community Association Research

The Foundation for Community Association Research is a national, 501(c)(3) non profit organization devoted to common interest community research, development, and scholarship. Incorporated in 1975, the Foundation is the only organization recording the history of, and identifying trends in, residential community association living. It supports and conducts research and makes those findings available to people involved in association governance and management.

The Foundation's mission is to promote positive change for all stakeholders who live and work in homeowner, community, and condominium associations by:

- Discovering future trends and opportunities.
- Supporting and conducting research.
- Facilitating and promoting cooperation among industry partners (owners, managers, and product and service providers).
- Providing resources that help educate the public.

The Foundation has fostered the growth of associations by providing educational and research support through CAI's 58 chapters. We are committed to providing quality research and publications for promoting academic interest in community associations.

To learn more about the Foundation, call CAI Direct at (888) 224-4321 (M–F, 9–6:30 ET) or email foundation@caionline.org.

Community Associations Institute (CAI)

Community Associations Institute (CAI) is a national, membership organization dedicated to fostering vibrant, competent, harmonious common-interest communities. Founded in 1973, CAI and its 58 chapters provide education, tools, and resources to the volunteers who govern communities and the professionals who support them. CAI's 28,000+ members include community association volunteer leaders (homeowners), professional association managers and management firms, and other professionals who provide products and services to community associations.

Our vision is reflected in community associations that become better—even preferred—places to call home.

CAI serves the community association housing market by:

- Advancing excellence through seminars, workshops, conferences, and education programs, some of which lead to professional designations.
- Publishing the largest collection of resources available on community associations, including books, guides, *Common Ground* magazine, and specialized newsletters.
- Advocating community association interests before legislatures, regulatory bodies, and the courts.
- Conducting research and acting as a clearinghouse for information on innovations and best practices in community association development, governance, and management.

CAI members receive a variety of benefits, including discounts on CAI publications and events; an award-winning magazine; specialized newsletters on community association management, governance and law; members-only website content and resources; and networking and referral opportunities through the national office and local CAI chapters.

For membership or other information, call the national office at (888) 224-4321 (M–F, 9–6:30 ET) or visit the CAI website at www.caionline.org/join.

ISBN 978-0-941301-73-2

To comment on the Best Practices initiative, submit research for the project, or suggest a future Best Practices Report topic, please email foundation@caionline.org.