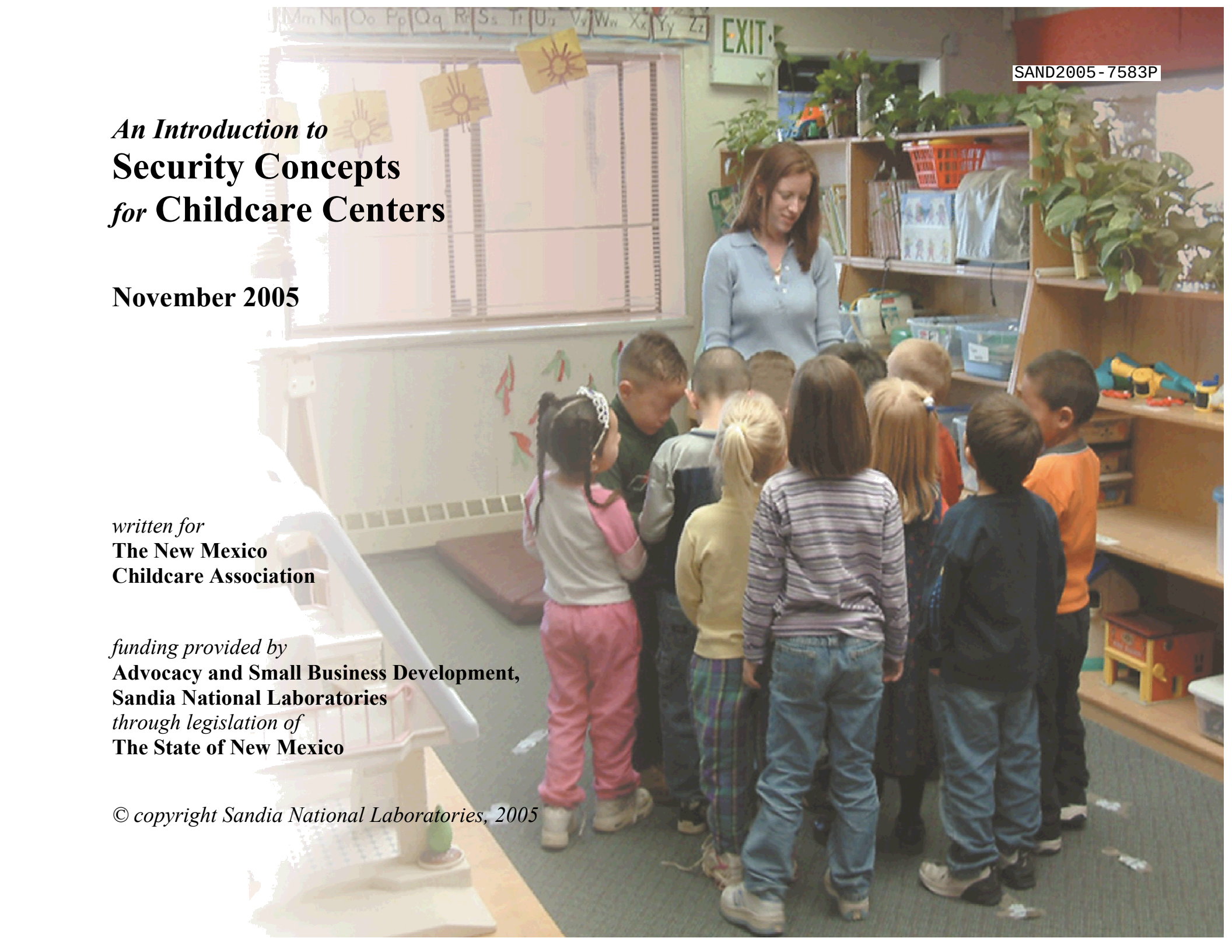

SAND2005-7583P

An Introduction to
Security Concepts *for* Childcare Centers

November 2005

written for
The New Mexico Childcare Association

funding provided by
Advocacy and Small Business Development, Sandia National Laboratories
through legislation of
The State of New Mexico

Acknowledgements

author: Mary Green, Sandia National Laboratories, Albuquerque, NM

graphics: Phil Wethington, Tech Reps, Albuquerque, NM

technical contributor: Tim Malone, Sandia National Laboratories

reviewed by: David Clauss, Sandia National Laboratories
Bob Waters, Sandia National Laboratories
Mike Itamura, Sandia National Laboratories
Sharon O'Connor, Sandia National Laboratories
Mike Itamura, Sandia National Laboratories

Special thanks to the New Mexico childcare providers involved in this project:

Kyle Smith, Southwest Childcare Centers
Hazel Darnell, Child Care Castle
Joy Haugan, Discovery Child Care Development Center
Mary Dickson, Jefferson Discovery Center
Helen Rogers, Cottage Pre-School
Carol Rapisardi, Covenant Classic
Crestina Gonzales, El Ranchito
Hazel Darnell, Child Care Castle
Eva Rivera, Tiny Tots
Mary Dickson, Jefferson Discovery Center
Loretta Fogerson, My School Daycare
Joy Haugan, Discovery Child Care Development Center
Judy Vallier, Angel Fire Resort Daycare
Jill Eiland, Kindercare Learning Center
Ethel Johnson, Southwest Childcare

Contents

This page left intentionally blank

Foreword

The goal of this manual is to present childcare providers with some available options for addressing a wide range of undesirable security events or situations. These options include facility enhancements, procedures, and technologies to discourage, mitigate, respond to, or resolve an incident.

In general, this document will focus primarily on security issues rather than safety issues, except to initially identify a spectrum of safety as well as security threats. Security incidents are situations that are malevolent in nature, while safety incidents are unintentional incidents or acts of nature.

Much of the discussion within this document most appropriately applies to larger childcare facilities rather than in-home businesses with only a few children. However, I believe that anybody who works with children on a daily basis will find items of interest and potential usefulness.

I was fortunate to be asked to write this manual as part of a project funded through legislation of the State of New Mexico to the Small Business Group at Sandia National Laboratories, using tax rebate monies. The customer and recipient for this task has been the New Mexico Childcare Association, a group of more than 100 proprietors of private childcare centers in the state.

For another part of this project, several Sandia security specialists worked on a pilot project at a local, private childcare center in Albuquerque. Several types of security technologies were applied at this center and the results were monitored and analyzed. The team made some interesting observations. See Appendix C for a summary of this pilot project.

Regarding my own background: I am <u>not</u> an experienced childcare proprietor writing about security; I am a security specialist writing about security in childcare centers. I have had the good fortune to be able to visit and work on security issues at more than a hundred K-12 schools across the nation during the past ten years. (Funding has been provided over the past seven years by the U.S. Department of Justice, through legislation sponsored by Senator Jeff Bingaman, NM).

My experience with childcare facilities is limited to security surveys at a couple of dozen centers over the life of this project. However, I was an extremely critical visitor to at least twice that number of childcare facilities some twelve years ago when I sought reliable and safe care for my own two children.

I welcome comments and criticisms from anyone who would wish to write me at my email address provided below. I realize that non-existent security budgets have driven many childcare centers to become very creative, and I would enjoy hearing about some of the creative approaches that are used today.

I would like to thank Ms. Kyle Smith and Ms. Ethyl Johnson, two icons in the New Mexico childcare business, who have taught me so much about their work.

And to all the childcare workers and providers doing their best out there: a great big thank you from all of us moms and dads who have needed you at an important time in our children's lives. Your work is indeed a labor of love.

Mary W. Green
Sandia National Laboratories
Albuquerque, New Mexico
mgreen@sandia.gov

Part I
Introduction

Chapter 1 Identifying the Security Issues for Each Childcare Center

Every person who works in a childcare facility needs to think about how vulnerable they and the children are to intentionally malicious acts. The adult staff present during most of the day is primarily female and most of the children are younger than five. Often the classrooms and playground are closed from prying eyes, which unfortunately means that people outside the school may not be aware of something terrible occurring inside.

Fortunately, open attacks on childcare centers resulting in injuries, murder, or kidnappings, while possible, are not common in the U.S. at the time this manual was written. Certainly, though, attacks of lesser consequences are not uncommon, such as theft, vandalism, assault, etc.

Protecting the children in this special environment, without creating a prison-like atmosphere, can seem like a tough and expensive task. It is also challenging to teach these young kids how to respond in an emergency without scaring them.

The goal of this manual is to present childcare providers with some approaches to consider for application against a wide range of undesirable events. But no facility can protect itself against everything. So how does a childcare center decide where to spend its limited time and money?

Most security specialists will tell you that the staff of any facility, whether it be a bank, a grocery store, a military base, or a school, must first identify their particular issues or concerns in order to develop a security strategy that adequately addresses these needs. Such issues are usually different for every facility and those issues will evolve over the years, just as the world evolves. These issues are driven by many different characteristics about a particular facility, which may include:

- the *location* of the facility (e.g., is it located within a new suburban office building or does it sit on a major street as part of a retail strip mall?);

- the *clientele* (e.g., if one of your parents has a bad day, are they the type that might have a few drinks before picking up the child in the evening and then decide to take out their frustrations on a teacher?);

- the *employees* (e.g., do your staff members view their jobs as a career or are they just there until something better comes along?);

- the *age and layout of the building* (e.g., was your building originally designed as a childcare center or was it a taco restaurant that has too many entry doors and too much glass?); and

- in-house *policies and procedures* (e.g., are there people available or hardware in place that could reliably stop a stranger from easily entering your center and wandering around?).

The design and implementation of a unique security strategy for a particular facility will be constrained by

→ **Affordability,**

→ **Acceptability,** and

→ **Effectiveness.**

The most *effective* security system will likely not be acceptable to parents due to intrusive entry search methods, intrusive surveillance, etc. The most *affordable* security system will likely not be as effective as desired, such as the lock on the front door. The most *acceptable* security system, using non-intrusive, high-tech methods to support security requirements, will probably not be affordable. The ideal security system will require a balance that must be periodically examined and tweaked by a facility's owner or manager, based on the current threats or most serious concerns.

A Systematic Approach for Security Assessments

Deciding where and how to spend a childcare center's limited security budget is not a straightforward task. Certainly it is not going to be possible to protect the center against any and all possible undesirable security incidents. So how does the manager or owner make decisions that will minimize risk while working within a limited budget?

There are several different systematic methods commonly used within the security industry to help make these choices for a particular facility. Most such methods involve:

- Determining which undesirable incidents are most important to protect against and who is likely to carry out these incidents;

- Identifying vulnerabilities that prevent a facility from effectively protecting against each of these incidents; and

- Selecting security measures that will minimize the level of risk, given available resources.

As this document does not include a complete tutorial for such an approach, the reader is encouraged to refer to Chapter 2 within the National Institute of Justice publication: *The Appropriate and Effective Use of Security Technologies in U.S. Schools*, 2005.

The remainder of this chapter, however, will provide the childcare owner/manager with a way to identify and categorize incidents and threats. *A facility that has not specifically identified the security issues they wish to address is unlikely to implement optimal security solutions.*

Identifying Issues of Concern

The manager/owner of a childcare center has likely already identified several issues that are of concern at his or her particular facility. Talking to other childcare managers/owners will bring up many issues that may or may not be applicable to a particular facility. Brainstorming with the teachers or caregivers at a center will provide even more insight into concerns that may need to be addressed.

To help a childcare staff start this identification process, an example list of undesirable events is included in the following section. However, it is important to realize that this list will not be all-inclusive for all childcare facilities. The final decision on what security issues are most important to address at a particular facility can only be developed by knowledgeable staff member(s) of that facility or by a security specialist who has worked with the staff long enough to understand their facility.

Examples of Undesirable Security Incidents

The list shown in Figure 1.1 includes common examples of undesirable security incidents. A more detailed version of this list, along with some common undesirable *safety* incidents, is shown in Appendix A. Appendix A includes a simple categorization of these different types of incidents along with some recommendations that a childcare facility might consider to lessen the severity of each incident.

1. Daytime theft inside the facility: This usually involves theft of money or wallets from teachers' purses or the theft of cash from a cash box in a desk. Perpetrator may be an *outsider* (a person who does not have authorized business within the facility) or an *insider* (a person who is authorized to be in the facility).

2. Parking lot theft or vandalism: This includes theft of wallets or purses while a parent runs into the childcare building to drop off or pick up a child.

3. An angry, irrational, or threatening parent: Many teachers have been threatened by an abusive parent.

4. An undesirable person gains entry to the facility or gets close to the children: Most playgrounds are more accessible than they ideally should be and most facilities do not prevent the initial entry onto the grounds or into a building by a stranger.

5. Abuse of a child by a teacher or other staff member.

6. Abduction of a child by a noncustodial parent or other relative: This issue is made tougher by the fact that a small child would not necessarily know that anything is amiss and would likely go with any family member.

7. Abduction of a child by an unknown adult.

8. Hostage situation: A potentially horrible situation that could be caused by a criminal on the run from another incident, a mentally unstable individual looking for attention, or an over-the-edge spouse/ex-spouse of a staff member.

9. Assault or rape of a parent or staff member after dark or whenever the facility area is deserted.

10. A drive-by shooting that sends bullets through a window or onto a playground.

11. Robbery/holdup: This could be by someone who has some information as to the general layout of the facility, how many adults (male and female) are usually present, where the cash box is, etc.

Figure 1.1 Examples of common undesirable incidents in a childcare center environment.

Likelihood vs. Consequences

Two terms that are commonly used for rating possible undesirable incidents should be understood. First, the **likelihood** of a possible incident occurring refers to its relative frequency. This is not to be mistaken for an actual probability; it is a term to be used as a relative comparison between different incidents. For example, if a childcare manager was considering the possible abduction of a child by a non-custodial parent versus the possible abduction of a child by a stranger, the manager might rate the noncustodial parent incident as more likely/more frequent than the stranger incident.

Secondly, the **consequences** of a possible undesirable incident refers to the costs that would be incurred if the incident did occur. These costs may be in dollars (for the loss of property or resources) or in terms of injuries or lives lost. For example, a manager may feel that the possible consequences of vandalism at a center might be a few thousand dollars in damages, which would likely be covered by insurance except for a deductible. On the other hand, the manager may feel the consequences of an unauthorized adult gaining entry into one of the buildings could result in the abduction of a child, the injury or death of one or more children and/or staff members, the loss of credibility with parents, or the loss of the center's license. Obviously, the consequences of the latter incident are greater.

Prioritizing Security Risks

To help the manager of a childcare center better develop a rough priority or ranking of the center's undesirable incidents, each incident on the list needs to be assigned a relative priority. The first step to accomplish this for a particular center is to examine each incident and make a judgment as to its *Likelihood* and its *Consequence* based on some rating system. This judgment could use a rating scale such as:

Very Low – Low – Medium Low – Medium – Medium High – High – Very High

A somewhat arbitrary numeric value can then be assigned to each of these ratings. One possible set of values that would be reasonable to use is:

Very Low	***1***
Low	***2***
Medium Low	***3***
Medium	***4***
Medium High	***5***
High	***6***
Very High	***7***

Once this scale is applied in the assignment of ratings, a *product* can then be taken of the assigned numeric values of the Likelihood and the Consequences for each undesirable incident. The higher the product, the higher the *relative priority* of that particular undesirable incident.

Example: Using the "*Very Low—Low—Medium Low—Medium—Medium High—High—Very High"* rating scale, if a particular undesirable incident for a facility was judged to have a Likelihood of *Very Low*, or 1, and a Consequences of *Very High*, or 7, then the product rating for this incident would be 1 x 7 = 7. For a different incident, if the Likelihood was judged to be *Low*, or 2, and the Consequences were judged to be *Medium High*, or 5, the product would be 2 x 5 = 10. Between the first and second undesirable incidents with product ratings of 7 and 10, respectively, the second incident would be considered to have a higher relative priority.

Keep in mind that these assigned values are truly arbitrary, and if one undesirable incident has a priority rating of 5 and another undesirable incident has a priority rating of 10, this does not mean that the second incident has twice the priority or twice the importance of the first incident. It simply means that, using the rating assignments that were determined by a knowledgeable person, the second incident has a higher priority than the first.

An example of this process to identify security risks and assign relative ratings at Main Street Childcare Center is shown in Figure 1.2. Each undesirable incident has been assigned a value for its relative Likelihood and Consequences in comparison to other undesirable incidents. When the rating products are calculated, the relative priorities, based on judgments of Likelihood and Consequences, will emerge.

This priority rating of undesirable events provides good information for a childcare center manager's use, but it does NOT imply that this priority order is the only order in which the issues can be, or need to be, addressed. Indeed, if a manager determines that it will cost the facility an unacceptable amount of funding to address the top priority, or if the only possible solution will be unacceptable to the stakeholders of the center, then the center may have to accept the risk associated with this undesirable incident.

Important Note: Keep in mind that the type of process that has just been discussed is a very subjective one. The Likelihood and Consequences ratings that are assigned may vary due to the difference of opinions between individuals. This lack

Main Street Childcare Center

Example:
4 x 6 = 24

	Undesirable incident	*Likelihood*		*Consequences*		*Relative Priority Rating*	
1.	Assault of a parent or staff member after dark	*Medium*	*4*	*High*	*6*	***24***	Highest priority cluster
2.	Abduction of a child by a noncustodial parent	*Medium Low*	*3*	*Very High*	*7*	***21***	
3.	Hostage situation	*Low*	*2*	*Very High*	*7*	***14***	Next highest priority cluster
4.	Robbery/holdup	*Low*	*2*	*High*	*6*	***12***	
5.	Abuse of a child by a teacher	*Low*	*2*	*High*	*6*	***12***	
6.	Parking lot theft	*Medium Low*	*3*	*Low*	*2*	***6***	3rd highest priority cluster
7.	Drive-by shooting sends bullets through a window	*Very Low*	*1*	*Medium*	*4*	***4***	
8.	Daytime theft of center or personal property	*Low*	*2*	*Low*	*2*	***4***	

Figure 1.2 This table shows one example of an identification of undesirable incidents, the associated ratings, and the subsequent relative priority for a fictitious childcare center. The undesirable incidents are listed in the resulting relative priority order. Note that three clusters of priorities emerge in this example, as shown on the right (e.g., Assault of a parent and Abduction of a child are in the highest priority cluster, etc.). However, keep in mind that even though an incident is identified as the highest priority, that does not mean that the childcare center will have the funding to solve or mitigate the concern. Likewise, if an incident is identified as a lower priority, but the center is able to solve or mitigate that issue inexpensively, the center may choose to solve the lower priority incident anyway.

of consistency must be recognized when using such a process; the results do not definitively dictate specific actions. Rather, rough *clusters* of ratings that emerge from this exercise may be most helpful in identifying the *highest* relative priorities, the *next highest* relative priorities, etc.

This page left intentionally blank

Part II
General Security Concepts, Methods, and Approaches

Chapter 2 Security Design Principles and Facility Layout

Security Design

In most of the growing communities in our country today, the city planners as well as the police departments are using the principles of *Crime Prevention Through Environmental Design* (usually referred to as CPTED) in the renovation and rebuilding of public areas. CPTED (pronounced sep-ted) incorporates certain philosophies that have been shown to reduce crime and vandalism in previously unsafe neighborhoods. These principles are straightforward and generally encourage a more visible, well-lit, and orderly community.

While the implementation of many of the CPTED ideas may require a major remodeling of an area, childcare center managers should keep these ideas in mind for minor upgrades as well. A few of the CPTED principles that are appropriate for childcare facilities are included below.

- A center's physical layout should allow staff a clear view of the property's exterior, including the parking lot and playground. Hidden areas should be minimized and natural or man-made barriers used to direct the flow of vehicular and pedestrian traffic (e.g., sidewalks, trees, large pots, etc.).

- Exterior areas should be well lit, but the lighting should not be uncomfortably glaring. Lighting that is evenly distributed across an area will usually require more lights than a builder would normally install. Ideally, the newer, softer light bulbs should be considered. Dark spots should be minimized.

- Landscaping should be neat, well maintained, and add to the general pleasantness of the area. Shrubs should be kept well-trimmed and located so that the outdoors is open and inviting, without hidden areas. Trees and larger shrubs should be pruned upward to prevent their low-hanging branches from blocking visibility, blocking light, or providing hiding areas.

- The exterior and interior of the facility should be kept scrupulously clean, always picked up, and very well maintained. This principle relates directly to the Broken-Window Theory: *If a window becomes broken, but is not quickly*

repaired, additional windows will soon become broken. An orderly facility gives the impression to others that there are responsible people who care about the facility and are looking after it.

- Fencing is important, especially for a childcare situation. Fencing that limits entry onto property and also establishes boundaries can add substantially to the controlled feeling of a facility.

  A word about fencing: Fencing does not have to be unattractive. If adequate funding is available, wrought iron fencing can enhance the appearance of many facilities, while providing a more difficult barrier to climb over. Less expensive, but still providing an excellent barrier, is a 6- or 8-foot chainlink fence with smaller mesh (e.g., one-and-a-half-inch squares). Unlike a typical five-foot chainlink fence, it is more difficult to pull oneself up and over an 8-foot fence with small mesh that will not allow toeholds, even for youngsters. See Figure 2.1, which illustrates the use of this type of fencing around an Albuquerque elementary school.

  A fence also helps defines property boundaries and forces a perpetrator to consciously trespass rather than allowing a stranger to idly wander onto a childcare center's unfenced property. The goal of fencing is to deter the casual or unmotivated trespasser. Few fences can keep out someone who is determined to enter the property. However, in some situations, a facility must be more aggressive. A thick planting of pyracantha or other thorny bushes, along a chainlink fence, can be almost impenetrable (see Figure 2.2). It may take three or four years to establish such a hedge, but the cost will be relatively low.

  Note: A fence that cannot be seen through can sometimes create an additional problem for a childcare center. For example, if the outside world is unable to view what is transpiring on the playground, then a perpetrator could use this to his advantage to attack without being seen. On the other hand, if the fencing can be seen through, then it is easy for anyone to case the center and figure out what kids go there, how many teachers are there, etc.

Facility layout

Few childcare centers are fortunate enough to be able to design the facility from the ground up. In fact, the majority of childcare buildings are structures that were originally built for a completely different purpose. Because of that, most childcare

Figure 2.1 This 8-foot, smaller-mesh chainlink fence is around an elementary school. The school's problem with outside gang confrontations on the playground was completely eliminated after the fencing was installed.

Figure 2.2 Pyracantha bushes can create an intimidating barrier where fences might be inappropriate or less effective than required.

managers have had to remodel creatively to enhance the usability of their facilities. A front office that allows for good visibility of arriving and leaving parents or visitors is one of the most critical design elements (see Figure 2.3).

Unfortunately, a secure facility layout does not necessarily lend itself to a safe environment. A good example is fire code restrictions. Many childcare managers wrestle with the problem of a primary egress (fire) door that opens out onto a street with heavy traffic, which is another dangerous situation for small children. One childcare facility owner was extremely creative with her building remodel; the primary exit door was altered such that the original exit door that led to the parking lot and busy street had its interior knob raised by almost two feet to make it difficult for children to exit on their own. Immediately adjacent to this egress door, she had a new panic-type exit door installed that opened only onto the fenced playground (see Figure 2.4). This kept the fire marshal happy, the parents happy, and the kids safe and secure.

Figure 2.3 One particularly important component of a good childcare facility design is an office location that allows an administrator to keep an eye on both the parking lot and the primary entryway.

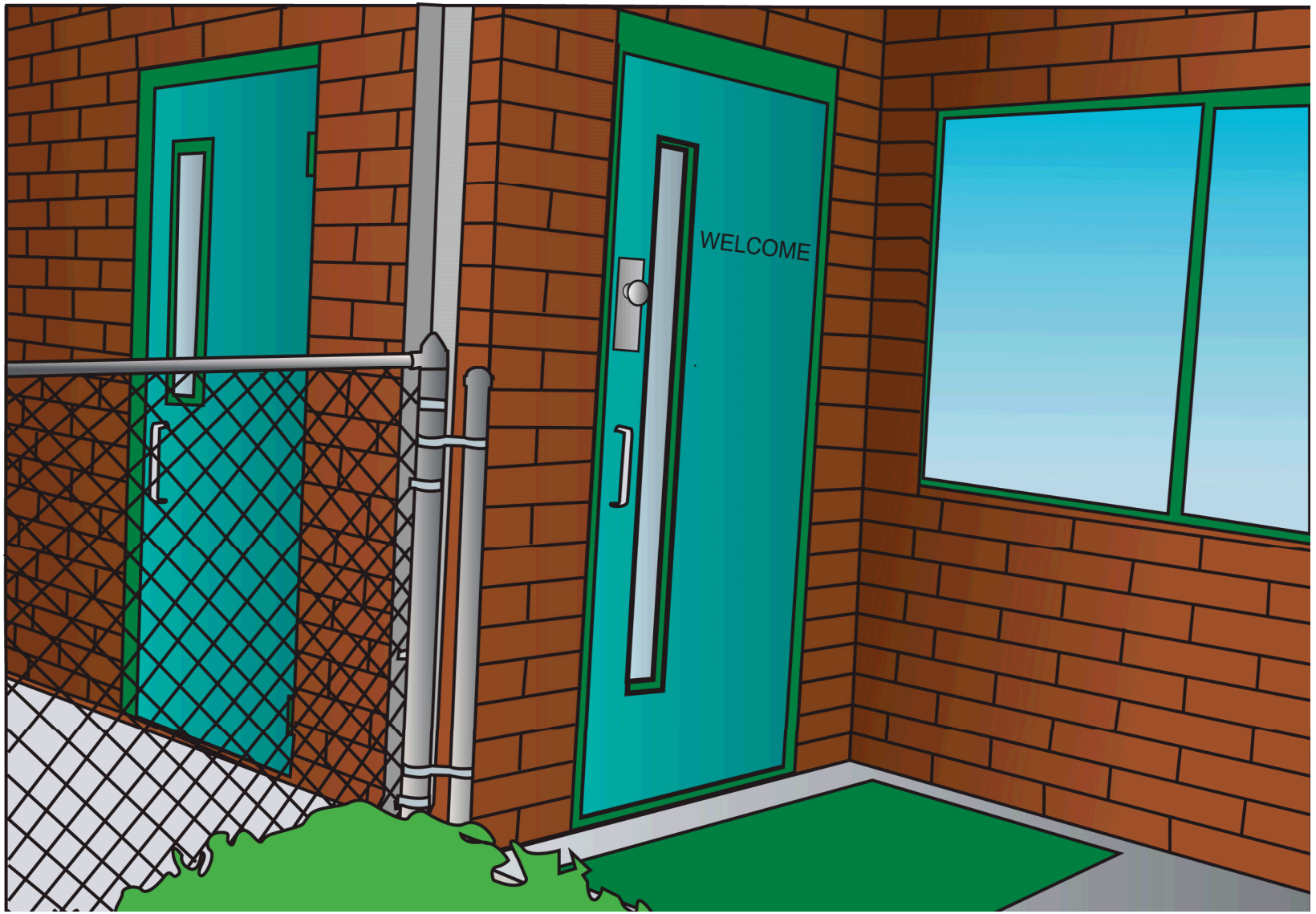

Figure 2.4 The owner of this childcare facility had the doorknob of the main entryway (right door – the primary egress door at the time) raised about 20 inches to make it more difficult for a child inside to open the door and get out onto the nearby busy street. An interior panic bar was installed on the left door to allow immediate and safe egress to the playground in case of fire.

Chapter 3 Common-Sense Approaches to Theft, Vandalism, and Assaults

Theft and ***vandalism*** can and will occur within most businesses, including childcare centers. This can cause caregivers to feel vulnerable as they realize that if someone were able or willing to rob or vandalize the facility, the perpetrator might also be able or willing to ***assault*** a child, a staff member, or a parent.

The application of security technologies can often help reduce or deter these concerns and will be covered in Part III of this manual. The recommendations listed in this chapter are common-sense approaches. Most are low in cost or free.

Theft

Daytime: Because childcare centers are typically very busy places with employees rarely idle, it can be easy for an outsider to wander in, size up the place, and then grab what they want. (It is not always a coincidence that the perpetrator might know where to quickly find purses and the cash box; ex-employees who leave under less-than-happy circumstances have been known to pass this type of information on to friends.)

Childcare workers need to realize that a thief can often be a female who wanders in and helps herself. A woman is less noticeable in a good-sized childcare facility, and an employee who does notice her will figure that she is just a mother or grandmother of one of the children.

For a childcare center, daytime theft may include money from purses or cash boxes, small items of value, vehicles, or items left in vehicles, etc.

Some key points to minimize the chance of daytime theft in a childcare center are to:

- Provide staff with a secure location where purses may be locked up during the day.
- Keep the cash box locked away, but minimize cash on site by depositing significant amounts of cash in the bank each day.
- If the office is right at the main entrance, keep the office locked when no one is there; have the office worker keep a key on a chain or stretch cord around their wrists;
- Teach staff members to be security-minded by challenging anyone who is not immediately recognized with: "May I help you?"

Nighttime: Attractive theft items can include copy machines, cash boxes, computers, small electronic equipment, tapes, CDs or DVD players, television sets, the business's van, etc.

Some key points to minimize nighttime theft at a childcare center are:

- Mark all valuable property with the school name using metal etchers, permanent markers, or anything that would be difficult for a thief to remove before selling an item.

- Deposit significant amounts of cash in the bank each day.

- Install good outdoor lighting, so that a perpetrator may be concerned about being seen.

- Alternatively, provide no outdoor lighting, so that a perpetrator cannot see well enough to perform his or her task at hand.

  (The reader will notice the contradiction between these last two bullets. There are security professionals who swear that good lighting keeps a facility safe and still other security professionals who claim a totally dark facility better deters theft and vandalism. It probably depends on luck and the perpetrator-du jour. But the bottom line here may be that poor lighting is probably worse than good lighting or no lighting.)

Vandalism

Vandalism usually occurs at night and may include graffiti, broken windows, broken playground equipment, beer cans and illegal drug paraphernalia left on the grounds, etc. These types of issues are often difficult to prevent.

Possible measures that may combat some of these problems some of the time include:

- Good outdoor lighting, so that a perpetrator may be concerned about being seen.

- No outdoor lighting, so that a perpetrator cannot see well enough to perform his or her task at hand.

- Exterior lights that come on when motion in the area is detected and will then stay on for a minute or two (See Figure 3.1)

Figure 3.1 *Exterior lighting that activates only when motion is detected can be a good deterrent to would-be thieves or vandals.*

- More delicate pieces of light-weight playground equipment can be moved inside at night, especially over weekends.

- Install a motion-activated sensor for the sprinkler system, so that it will come on for a few minutes if there is significant motion in the area.

Assault

And assault on a staff member or parent can be not only devastating to that individual, but also be devastating to the reputation of the childcare center where it occurred. The rape of a female, usually toward evening when most people are gone for the day, and especially after dark, can convince some employees to quit and some parents to take their children elsewhere.

A few suggestions to combat this issue include:

- Keep all doors into the facility locked when there are only a few staff and children left at the end of the day.

- Require that a staff member is never left alone in the facility at the end of the day.

- Install good outdoor lighting, so that a perpetrator may be concerned about being seen.

- Hire a staff member who has the strength, training, and ability to defend parents and other staff.

- Assign this trained staff member to accompany parents to and from their cars after dark, as well as staff members closing the facility.

- Encourage and support the staff to take self-defense classes.

- Inform staff and parents to report any stranger seen in the area who appears suspicious.

Part III
Security Technologies with Possible Applications in Childcare Facilities

Part III Security Technologies with Possible Applications in Childcare Facilities

Security technologies such as cameras, recorders, motion sensors, etc., may not necessarily solve the security concerns a childcare facility has. In fact, these types of technologies are often oversold to customers seeking a quick resolution to their problems. For this reason, a childcare manager or owner ideally should seek to

- Understand what it is they wish to protect;
- Understand what a general type of security hardware can and cannot do;
- Seek guidance and direction from a security professional who is trained in that field; and
- Make sure that the equipment will be correctly installed, operated properly, and be well maintained.

If the childcare manager or owner can accomplish the guidelines listed above, then the technology they bring into their facility could well be instrumental in helping them to deter, mitigate, respond to, or resolve issues of concern.

A thought to keep in mind: Deterrence is usually the main goal when designing a security strategy for a childcare facility. Deterrence is generally achieved by having a visible and effective security system in place. Catching somebody in the act of some malicious deed is probably not the best possible situation, especially for a childcare center. A more desirable approach would be to discourage the vandalism, theft, abduction, assault, etc., in the first place.

Part III of this document covers several security technologies, most of which have been used successfully in a number of childcare centers. Historically, childcare centers have not felt the need to incorporate security technologies into such a gentle environment. This is changing, however, as various threats have been brought to the public's attention. Certainly parents are going to feel more strongly these days that every reasonable security measure possible should be taken to prevent harm from coming to their children.

The following chapters discuss some of the more common technologies used today, along with the

strengths, weaknesses, applications, and expected costs. While this information should prove useful to the manager considering purchase of such equipment, certainly these few dozen pages will not make an expert out of anyone.

The technologies most commonly considered for use in childcare facilities include:

- Entry Control Systems,
- Covert Duress Systems,
- Burglar Alarms, and
- Video cameras and recorders

which are the subjects covered in the next four chapters of this document.

Chapter 4 Entry-Control Systems

It is likely that most serious threats against the occupants or property within a childcare center come from the outside (although that is certainly not always the case). Examples of unauthorized individuals that a center might be concerned about include:

- Ex-employees who left under unpleasant circumstances;
- Noncustodial parents or relatives of children at the center;
- Panhandlers, street people, or mentally disturbed individuals;
- Casual thieves looking for an easy mark or who are "casing the joint";
- A thief with knowledge of where money or other valuables are kept in the childcare building;
- Idle friends or family members of staff members who drop by to visit;
- A child molester who wishes to harm a child;
- A social or political activist (e.g., a terrorist);
- A would-be rapist; or
- A potentially violent spouse, ex-spouse, boyfriend, girlfriend, ex-boyfriend, or ex-girlfriend of one of the staff.

It is very important, of course, that an unauthorized individual never be allowed to enter a childcare facility unnoticed and unchallenged. This includes the playground area. Not only does unauthorized entry put the children and staff at great risk, but the potential liability of such a situation could be unacceptable in the event that an undesirable incident did occur.

Although it seems quite obvious, it is worth stating that as many exterior doors as possible should be kept locked on the outside, so that occupants can exit but outsiders cannot enter. Too often doors are left unlocked for the sake of convenience. Some doors will even be propped open for better air circulation. This does not support a secure environment.

But what about the front door where the parents come and go all day? The smaller childcare provider in a home will probably keep this door locked as well, knowing as she does when most

parents are expected. A larger childcare center does not necessarily have this luxury. While keeping the front door locked is the safest procedure, most centers don't have the manpower to be sending someone to answer the door all day long. And what if the locked door is then opened to someone who turns out to be one of the unauthorized individuals listed earlier?

The front door of the facility should be under constant observation by a staff member who is not trying to oversee children at the same time. This staff person can greet and/or challenge individuals as to their business, as well as to ask for identification. (See Figure 4.1). For many potential threats, this would likely be enough deterrence and the unauthorized outsider will make up some excuse to leave.

If the outsider seems to be acting in a suspicious manner or if the explanation for their visit seems questionable, but they refuse to leave when requested, the situation can quickly become serious. In order to seek help, the center's greeter must have at least one way of contacting help at this point. Whether the person(s) summoned will be able to discourage or stop the perpetrator at this point cannot be known. But at least there was some early warning provided by the staff member.

Experience tells us, though, that once a determined attacker has been able to enter a childcare center, it is unlikely that most staff members would be able to stop the perpetrator or summon help to arrive before the perpetrator has completed at least some portion of his malevolent goal.

Therefore the main entry door must remain locked at all times. This can create extra work for employees, as someone will have to answer the door each time a parent or other visitor needs access (whether that visitor is a malicious outsider or simply a parent dropping off their child).

Luckily, it is fairly straightforward to allow staff and parents authorized and automatic access using one of many available entry-control technologies. Entry-control systems are intended to deny entry to unauthorized individuals and to allow entry to authorized individuals. These technologies are divided into three categories:

(1) What you HAVE,

(2) What you KNOW, and

(3) What you ARE (see Figure 4.2).

These categories are described in the rest of this chapter.

Figure 4.1 All visitors or workers at a childcare facility should be positively identified.

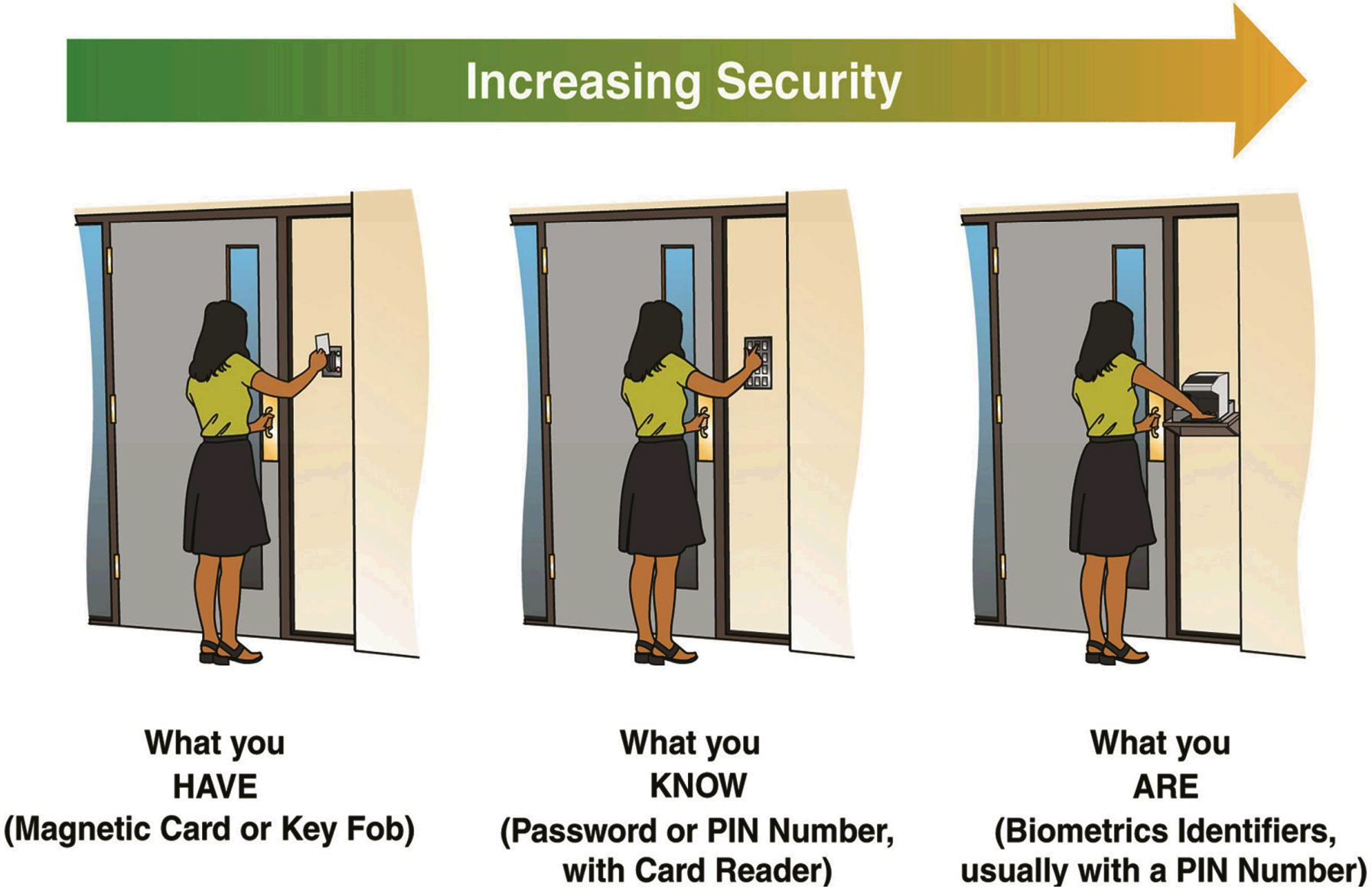

Figure 4.2 There are three major categories of technology methods for entry control.

(1) What you HAVE

For this group of technologies, a magnetic card or special key fob is electronically encoded to be recognized by some type of sensor located at an entry way. Recognition, also known as validation, of the item will then send a signal to release or engage the electronic locking mechanism on the door. This is the most easy-to-maintain type of entry control that may be affordable for a childcare facility. Each parent or adult who regularly drops off or picks up a child at the facility would be issued their own card or key fob, which has a unique electronic signature that is assigned to only that person.

One type of door control uses a magnetic card with a magnetic strip embedded on the card. This card is read by a card-swipe reader, similar to those used for reading credit cards in stores. Card-swipe readers are more susceptible to vandalism than some of the other types of scanning devices because the read-heads are fairly delicate. Any tenacious material (e.g., glue, honey, etc.) could be inserted inside the reader to temporarily or permanently disable it.

Another type of door control uses a card or key fob that emits a passive or active radio frequency (RF) signal and is then validated by a proximity reader installed at the door. Proximity readers can be protected from vandalism with a solid piece of plexiglass because actual contact of the card or key fob to the reader is not required. Depending on the cost of the system, the RF card or key fob can be validated from just a few centimeters away up to several feet away; this depends on the sophistication and cost of the system purchased. A small key fob that is designed to fit on a key ring is probably the best choice of proximity-type sensor for issuing to parents at a childcare center (see Figures 4.3 and 4.4).

Strengths

- No manpower is required to allow access to authorized adults.
- This is a relatively mature technology, so there should be fewer technical problems experienced by the user.
- Validation of a particular magnetic card or key fob can be turned off if the card is lost or stolen.

Weaknesses

- At a typical door, there is no way for this type of automated system to validate that only a single authorized person entered, i.e., an unauthorized person could have "piggy-backed" behind an authorized person who has

Figure 4.3 This mom is using the key fob that was issued to her for access into her daughter's childcare center. She keeps her key fob on her keychain, so that she always has it with her.

Figure 4.4 This is a key fob being held up to a proximity sensor. When the sensor validates the key fob, it will release the electronic door lock, thus allowing entry. Note the intercom box below the proximity sensor. This intercom allows visitors without a key fob to state their business and request entry. For this particular facility, the door intercom is answered by the office manager at an intercom unit on her desk. If the manager approves the visitor, she may simply press a release key on her intercom unit that will then release the electronic door lock for the authorized visitor.

already opened the door with a valid card or key fob.

- A card or key fob can be loaned to somebody who should not have entry.
- Regular updating of an entry control system's database will be required when parents and children enroll or leave the center.
- Most doors' hardware will need to be modified to accommodate a card-swipe or proximity reader and electronic locking mechanism. This upgrade can be costly.
- Cards or key fobs can be accidentally de-magnetized.

Suggested application

Install a proximity-type reader at the one or two primary doors used by parents and staff. Issue each parent or person who regularly drops off or picks up a child their own unique key fob to attach to their key ring. Charge each parent a deposit that will be refunded when they no longer have children at the center and the key fob is returned.

Estimated cost

Card-swipe readers or proximity sensors generally cost between $150 and $500 each. Pre-magnetized cards will cost anywhere from $3 to $10 each. Key fobs will cost between $5 and $15 each. The electronics, door hardware, and PC software, including installation, may cost between $1200 and $3000. Installation costs can vary widely, depending on the existing doors and frames. For new construction, the appropriate doors, doorjambs, panic bars, etc. can be installed initially, so the additional cost of the installation could be less than a few hundred dollars per door.

(2) What you KNOW

A typical example of this type of technology is a numeric keypad. The system will require that a personal identification number (PIN) or other passcode be entered on the keypad, which then releases the electronic lock. This is usually used in conjunction with a magnetic card and card reader. Alone, a PIN used on a keypad could be easily compromised by an onlooker.

Note: While there have been childcare facilities that have used a keypad as their entry control device, they generally have one passcode that all staff and parents share. Within the security community, this is generally considered to be a weak security strategy due to the compromise of the code that will likely take place (i.e., it is fairly easy to observe a code just by standing behind someone

inputting the code once or twice). This strategy is therefore not recommended.

Strengths

- A PIN and mag card can be turned off when no longer appropriate.
- A stolen mag card used alone is not sufficient to allow entry to an unauthorized person.
- Keypads are considered to be a mature technology and therefore will cause the user fewer technical problems.

Weaknesses

- More administrative effort is required to maintain both a card and keypad system (if they are not an integrated unit).
- It is possible for an unauthorized individual to piggyback behind an authorized person.
- Users can forget their PINs or their magnetic cards.
- Keypads are vulnerable to mechanical malfunction as well as vandalism.
- Installation may be difficult and costly on an existing door.

Suggested application

Issue a unique magnetic card or key fob and a unique PIN to each parent. Require that the card/key fob be used in conjunction with the keypad.

Estimated cost

A standard keypad will cost less than $200. More sophisticated keypads that may scramble the numbers on the keypad and only allow a narrow viewing area will cost $1000 or more. The standard keypad system and hardware, plus installation, may cost between $1000 and $3000. The magnetic card or key fob system will be an additional expense (see previous section) unless already integrated within the keypad system.

(3) What you ARE

For this technology, an electronic device verifies the identity of a person through the use of a personal attribute, such as the shape of a user's hand or finger, a fingerprint, voiceprint, the dynamics of a signature, an eye retinal pattern, or an eye iris pattern. (See Figure 4.5) These devices, known as biometric identifiers, can be extremely accurate. Biometric devices are most commonly used in high-security applications where unauthorized access into a facility is unacceptable.

Figure 4.5 *Illustrated here are several types of commonly used biometric identifiers that can help control entry into a facility with a high confidence of accuracy.*

Strengths

- This form of identification cannot be loaned to other people.
- There is no code to remember or card to carry.
- This type of identification verification is highly accurate in rejecting unauthorized persons and can be difficult to spoof.

Weaknesses

- It usually takes longer to use a biometric device than a card reader or keypad.
- Some devices can be very difficult for certain individuals to use.
- Some biometric devices may erroneously reject authorized personnel occasionally, depending on how the system's algorithms are set up.
- Not all biometric devices are user-friendly.
- Piggybacking is still possible if not used with a floor-to-ceiling turnstile.
- Cost is higher than other entry control devices.
- The initial enrollment of each individual can take several minutes.

Suggested application

Consider the use of one of the more user-friendly-type biometric units, such as a hand-geometry device. The unit should be placed where it will not be susceptible to vandalism.

Estimated costs

A stand-alone biometric unit can cost between $1200 and $6000 each. Installation will cost about the same as for most mag card or proximity systems. A system that manages biometric units at several doors can cost between $10,000 and $50,000, including installation.

Working with Security Vendors and Installers

Dozens of different manufacturers are offering many devices that produce a wide variety of products for the entry control market. When working with a security vendor, it may be helpful to keep several things in mind:

- Ask to see an installed and operating unit of the product being recommended.

- Visit other facilities where the vendor has already installed this product and ask folks at that facility how much they like the unit, how difficult it is to operate, and what kind of down-time (time during which the unit is inoperable), if any, that the unit has had since it was first installed.

- Be sure to have the vendor specify the complete installed and operating cost, including all hardware modifications that will need to be made to the door(s) to accommodate an electronic lock or switch.

- Make certain that the vendor will help you to install and operate any software necessary when first using the system and will provide user training.

- The owner/manager should be sure to specify to the vendor/installer that the system be installed such that it will fail safe if power goes out or the system breaks during the day. This means that during a power failure, all the doors will be unlocked and usable, both from the inside and the outside. For after hours, the doors should have a deadbolt that can be locked with a key when the facility closes and unlocked with the key when the facility opens. In this way, if the power goes out during the night and the system causes the doors to fail safe, the deadbolt will keep the doors secure.

Chapter 5 Covert Duress Systems

There can be events that occur in any business that put employees into a critical situation such that they are unable to yell or phone for help. This sort of incident can be most serious for a childcare facility as the staff members are usually women, so there is less chance of successfully fighting back and overcoming an attacker or malicious perpetrator.

Because of this innate vulnerability, the owners and managers of childcare centers may need to consider options to handle such a situation. The very best option is to discourage the situation in the first place. Steps to accomplish this may include

- Install fencing around the playground that is difficult for a would-be attacker to climb over.
- Hire a person trained in self defense to be the receptionist and greeter for visitors.
- Establish a protocol that allows all entrances to be kept locked, but provides easy access to authorized individuals.

Still, a determined attacker would be able to eventually circumvent these measures, given enough time and patience on the part of the attacker.

Consider, then, that a malevolent individual has breached the locks and fencing of the center and is now inside the facility, threatening one or more of the staff. At this point, staff members need some type of method or system to summon help in a clandestine manner, so as not to further provoke the attacker, if possible.

Communication technologies have advanced to the point that many **covert duress alarm systems** are affordable for use by schools and childcare centers. There are commercially-available products on the market, but to keep costs down, any clever handyman could help a childcare center install their own covert duress alarm. How such a system would operate is discussed below.

The covert duress system should allow a staff member to summon help quickly, using either a button/switch installed in the front office or other convenient location(s) (see Figure 5.1) or by using

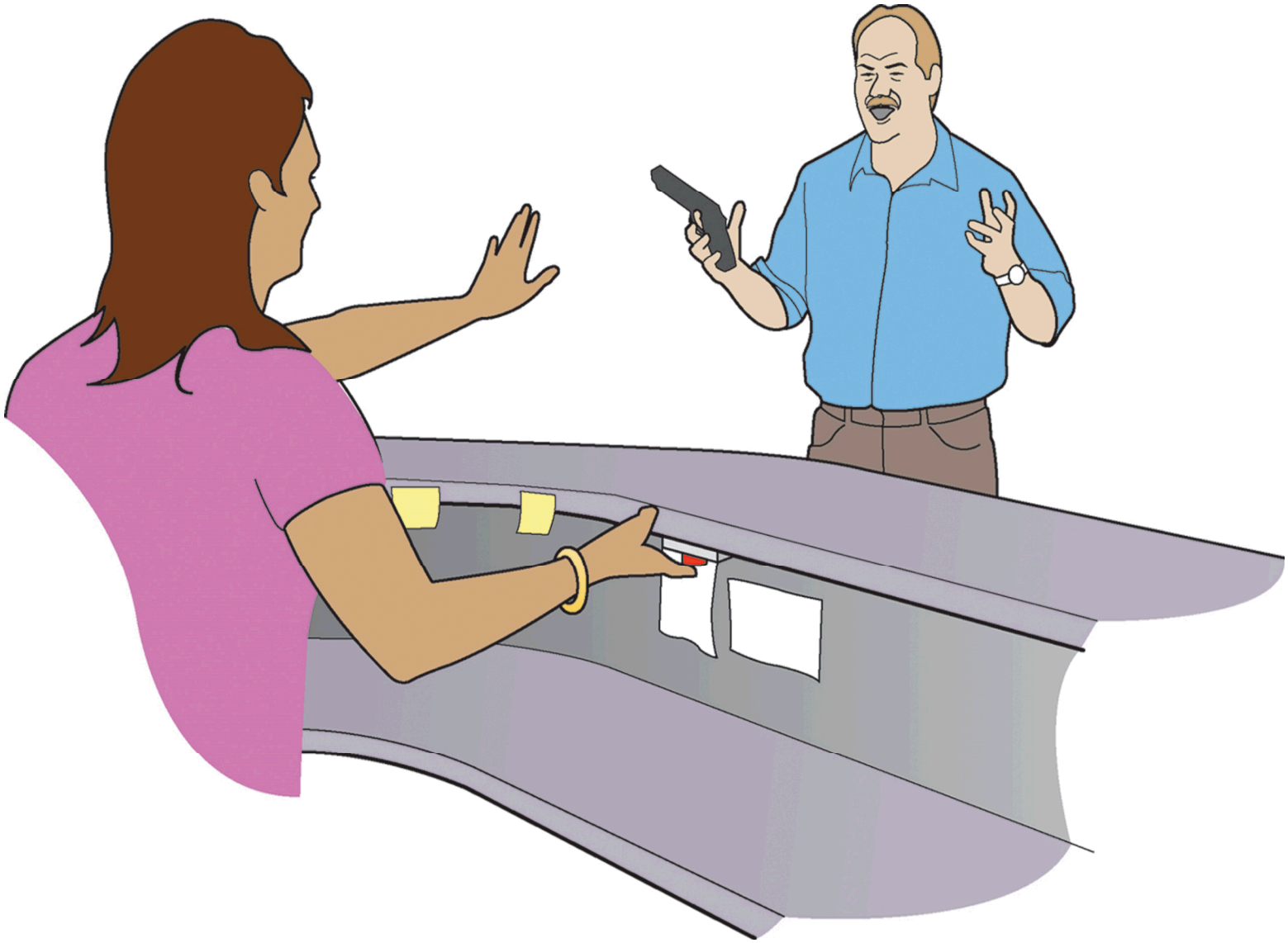

Figure 5.1 *A simple duress button-type system should be installed somewhere within the front office or at other strategic locations of every childcare facility so that help can be summoned quickly in the event of an emergency situation.*

a small wireless device that is worn by staff members.

Such devices usually send a signal to a dial-up modem attached to a telephone within the facility. When initialized, the modem secures a phone line, even if it means automatically hanging up a call-in-progress. The modem then dials preprogrammed telephone numbers; the total number of telephone numbers is determined by the particular modem, but it is usually four to eight phone numbers. The numbers are dialed sequentially. Each time a call to one of the preprogrammed telephone numbers is answered, the modem plays a pre-recorded message, then hangs up and calls the next phone number. An example of a message that a childcare center could record is:

> *"This is Middle North Childcare Center. We are experiencing an emergency situation. We are located at 17170 Broadway St., between Signal and Broadtown. Our phone number is 331-370-0706. Once again, this is Middle North ..."*

In most areas of the country today, such systems are not allowed to directly call the police or 911. Usually a facility will need to pay a monitoring company to receive these duress calls. The monitoring company will then attempt to call the center back to determine if the call was made accidentally. If no one answers at the facility, the monitor company will then contact 911 or the police on the center's behalf.

Other likely phone numbers to program into the duress system could be the owner's, a neighboring business, or a resource that would be able to check the facility and maybe even respond.

Figures 5.2 and 5.3 illustrate how a wired or wireless duress system could be installed, using components purchased at an electronics store. Prices for these components are included in the figures. These figures do not include the cost of the installation.

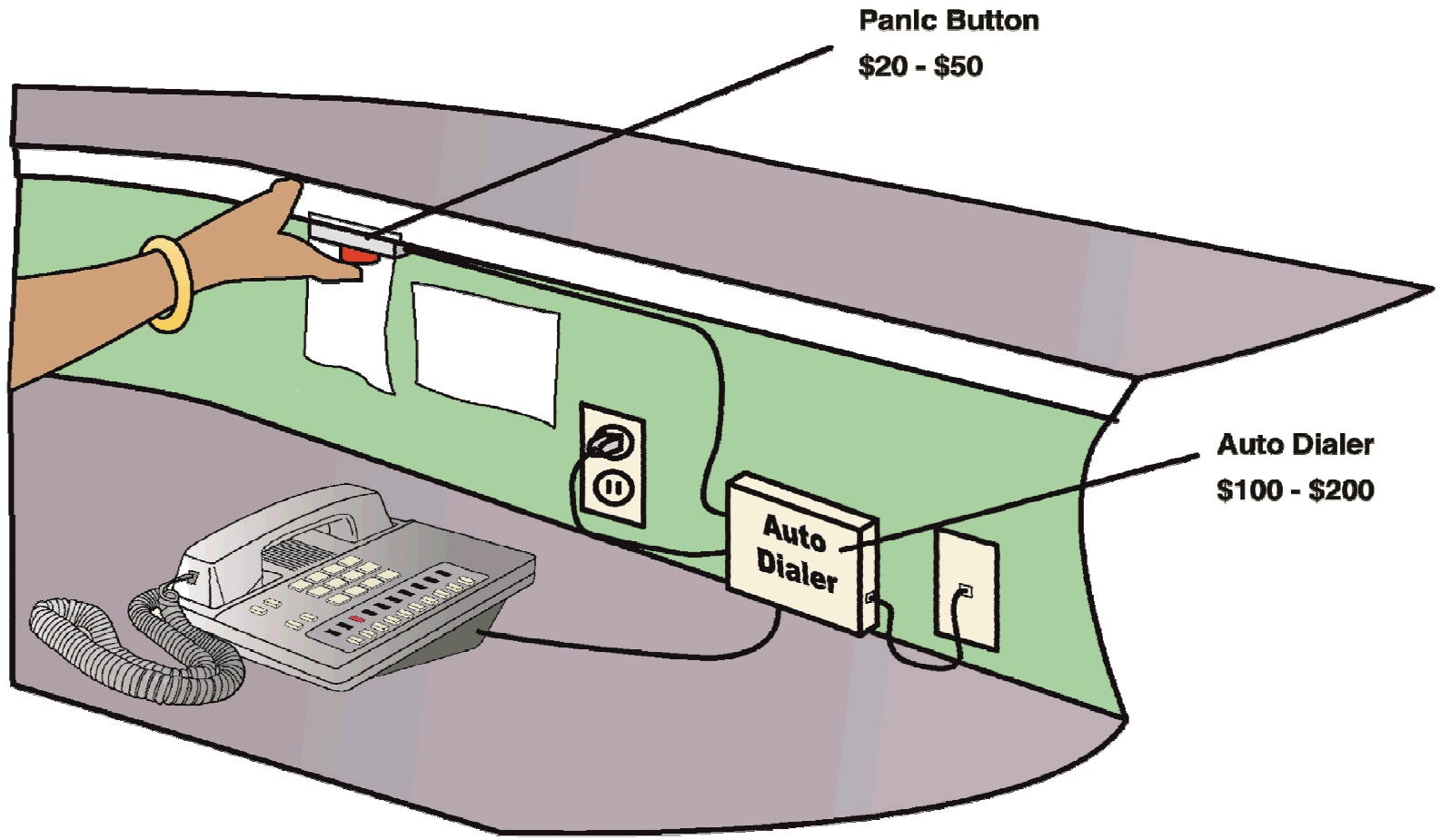

Figure 5.2 *This diagram shows an in-house covert duress alarm system, along with approximate costs of the components.*

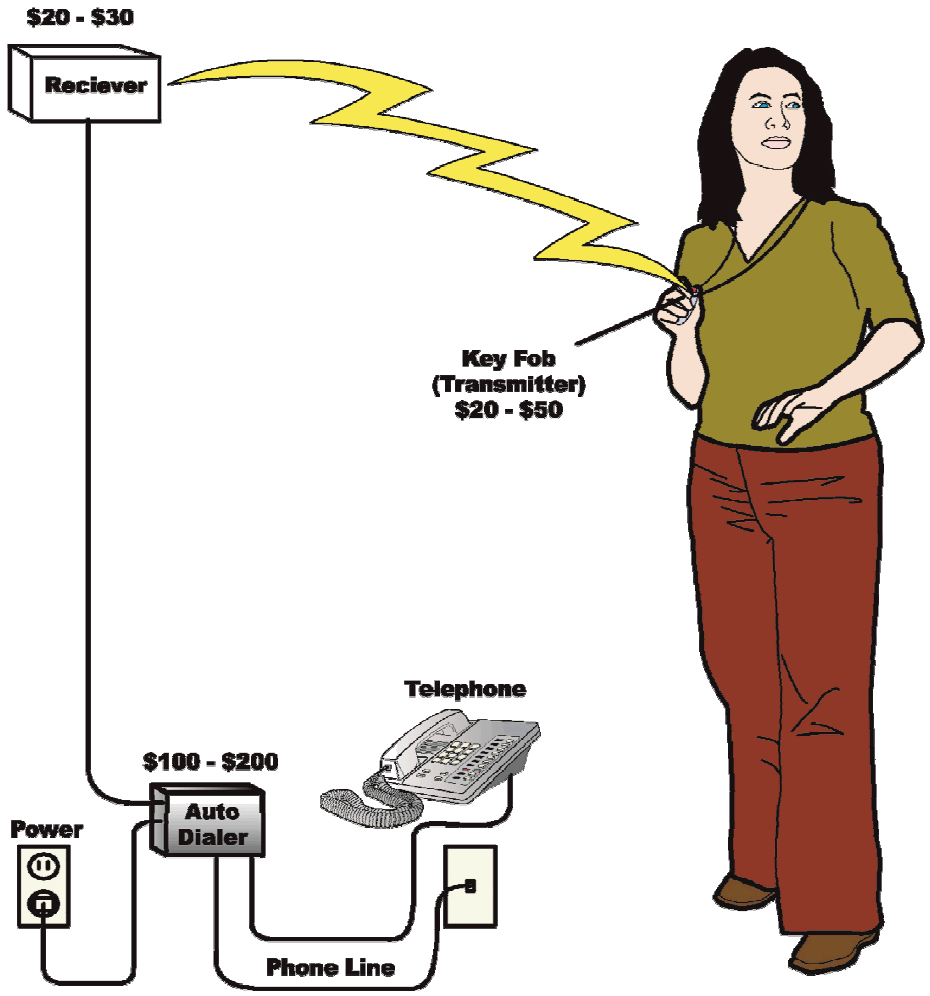

Figure 5.3 *This diagram shows how an in-house wireless duress system could be implemented. Each employee would wear an RF (radio frequency) -type key fob to transmit a duress condition. This type of RF system may require installation by someone who has experience with wireless systems.*

Chapter 6 Intrusion Detection Systems (Burglar Alarms)

Intrusion detection is simply a term for anything that will *notice* that someone has entered or is attempting to enter an area or building that they are not authorized to enter. One example of a very common type of intrusion detector found in many homes is the family dog – the dog is a type of sensor that detects (notices) a non-family member approaching or entering onto the family's property.

Similarly, today's technology has provided us with sensors (detectors) that can detect trespassers both inside and outside buildings. Nuisance alarms common to exterior sensors would be difficult to prevent in the typical childcare location, as these devices are normally only used in high-risk facilities. This chapter will cover interior sensors only.

A. Good reasons for intrusion detection in a childcare center

There are many good reasons why every childcare center should have an intrusion detection system, which is also known as a burglar alarm. Preventing the theft of equipment, money, or supplies is the first reason that comes to most manager's minds. The safeguarding of children's records (an important privacy issue) can also be a concern.

For many facilities, an equally important goal of an intrusion detection system is to detect a break-in over a weekend or holiday period. With no other method of alerting authorities that somebody is in the facility, the perpetrators could cause irreparable damage over a lengthy period of time without interruption. Some centers have experienced a break-in in which not only items of value were taken, but also the interior of the center was destroyed. The perpetrators concluded their visit by setting the whole building on fire. This type of incident can be devastating from credibility, financial, and employee morale perspectives.

Clearly, a basic but effective intrusion detection system is important for every childcare center.

B. The four components of an Intrusion Detection System

An effective intrusion detection system will normally have four primary components:

- Detection sensors,
- Communication and display,
- Assessment, and
- Response.

As mentioned earlier, **detection** is the capability to sense, or detect, that a person has entered or is trying to enter an area or building that they are not authorized to be in. In most office buildings, government facilities, and schools today, small **sensors** are installed in strategic locations of the building interior that are able to sense a change in certain conditions. Examples of changes in conditions that sensors detect are movement within a hallway or classroom, a door or window opening, or a window being broken.

After an intrusion is detected, this fact must be **communicated**, or transmitted, to a person or facility that is prepared to react in some way. For our guard dog example, the dog barks, which communicates to its owners the information that an intrusion of some sort has been detected. In most buildings, communication that a detection has occurred (also know as an *alarm condition*) travels via wire, cabling, or RF (radio frequency) signals to a panel that receives the alarms for that facility. The panel then uses phone lines or direct cabling to further transmit the alarm condition to one or more possible locations:

- An alarm-monitoring company,
- An administrator's home or cell phone number, and/or
- The police station (where allowed).

For most electronic intrusion detection systems, the communicated alarm will then be **displayed** to the person or organization that receives it. This display will use another electronic component – a computer monitor, a pre-recorded phone message, or an alphanumeric beeper message.

Note: One exception to the electronic communication and display component could be a system that simply initiates an audible alarm at the facility, with the intent of alerting someone in the immediate vicinity who can hear the alarm and then take action.

Once a detection has been displayed to the appropriate person or organization, the detection must be **assessed** to determine what caused the alarm condition. For our dog example, the owner could walk through the house, look out windows, or turn porch lights on, trying to determine why the dog is barking.

In an electronic system, the most accurate and convenient type of assessment will use a video surveillance system that is configured so that its images can be viewed remotely, usually via a special web site. If the person or organization can view both recorded and real-time video images of the area in which the detection occurred, they may be able to assess what caused the alarm. The source of the alarm might be a poster falling off a wall, a cat locked in the building, a balloon popping, or an unauthorized person breaking into the building.

Another type of electronic assessment consists of microphones installed throughout a facility. When the monitoring company receives the notification of an alarm, they can listen in through these microphones via regular phone lines. In this way, they may be able to determine if the alarm was caused by a person or persons actually in the facility. If the recipient of the alarm information does not have access to video or audio from the facility, then they are generally required to have the police or a security contractor travel to the site to determine if the facility has actually been broken into or if it is simply a nuisance or false alarm.

After assessing the alarm and confirming that it is an actual intruder, some action must be taken to stop the incident in progress. This **response** could consist of a trained security person or policeman confronting the suspect(s) and then making an arrest (or at least holding the suspect until the police arrive).

Note: The amount of time it takes to detect, communicate, assess and respond must be less than the amount of time an intruder requires to accomplish his goal; otherwise, the response is unlikely to interrupt and arrest the intruder.

It is important that childcare center owners and staff understand how dangerous it is for an untrained person to attempt to respond to an alarm alone. Even police officers these days are usually instructed never to enter a facility to assess an alarm by themselves. A responder never knows who they may come upon inside a building and many responders have been killed by a person who was originally just intent on theft. Furthermore, if a childcare center is aware that its manager or a

neighbor will respond to check out a possible break-in, the center could be incurring a huge liability if the untrained person is harmed in this duty.

C. Silent vs. Audible Alarms

A decision that every owner or manager must make is whether a center's alarm should be silent (only an electronic signal is transmitted to authorities) or audible (a loud horn or siren is initiated in addition to the electronic transmission). The answer to this question cannot be made easily. There are good and bad aspects to each approach.

<u>Silent alarms</u>
Pros:

- The intruder will not realize that a detection has occurred, and so may remain longer in the facility and possibly be caught by the responders.
- Neighbors are never bothered by the noise.
- The intruder may not be able to determine where he actually tripped a sensor, so the intruder may not have that information to help him in future break-ins at that facility.

Cons:

- Neighbors will not hear the alarm, so they are unlikely to look out a window to notice anything strange going on at the center.
- If it takes a long time for the police to respond (which is not uncommon due to the large number of nuisance or false alarms that must be responded to in most areas), the intruder will not be concerned about being apprehended and so may remain for a longer period of time to find more valuable articles or to further vandalize the facility.

<u>Audible alarms</u>
Pros:

- May scare off the intruder before the intended theft or vandalism is accomplished.
- Knowing that a facility has an active alarm system may serve as deterrence to other would-be perpetrators.
- Neighbors may hear the alarm and may look out their windows for anything suspicious.

Cons:

- The intruder will usually not be caught.
- The alarm may annoy neighbors if false alarms occur frequently, especially during the night.
- The intruder will know how far he can get into the building before he is detected. He can eventually do this enough times to be aware of the general location of many of the sensors and also to be aware of the period of

time before a response to the alarm will usually arrive.

- If an intruder decides to test your system, he could repeatedly set off the alarm until the owner of the center decides to turn the alarm system off as a problem system. Then the intruder could make a major raid on the facility without interruption or risk of being captured.

D. Sizing your intrusion detection system

An alarm system can have from one to hundreds of sensors. Most childcare centers will have anywhere from one to 30 sensors. Obviously, the larger the system, the higher the cost.

Alarm systems in childcare facilities typically follow one of five general approaches in sizing their alarm system:

1. A few motion sensors located in the main hallways.
2. Magnetic switches on all exterior doors in addition to #1.
3. Motion sensors in individual classrooms in addition to #1 and #2.
4. Magnetic switches on operable windows in addition to #1, #2, and #3.
5. Glass break sensors located near significant banks of windows (unusual for a school due to cost).

Option #3 above is probably the most common approach applied at childcare centers.

Note: The more sensors used, the more nuisance or false alarms may occur (see following section).

E. Nuisance Alarms vs. False Alarms

The bane of intrusion detection systems has long been their susceptibility to nuisance and false alarms. Nothing is more annoying to a police department than to dispatch two officers to a site that has reported an alarm, only to discover that the alarm was caused by some benign source, such as a cat locked in the building, a heat register that blew some classroom decorations around, or for no apparent reason at all.

Police stations across the country are beginning to either charge for the time spent responding to a non-break-in or refuse to respond to burglar alarms altogether, due to limited resources.

Childcare centers experience these same types of problems. This is generally because these facilities often choose some of the cheaper equipment available that is installed by the lowest bidder. These intrusion systems are rarely maintained and are almost never regularly tested after initial installation.

Two terms that a center manager should understand are nuisance alarm and false alarm. Contrary to common usage, these terms are not interchangeable.

A *nuisance alarm* is an alarm caused by a known source, such as a cat in the building or balloons floating in front of the heating register.

A *false alarm* is an alarm for which the cause is not obvious. A false alarm could be caused by intermittent sensor malfunction or by a non-obvious change in conditions, such as a heating system coming on. With no evidence of any other kind (such as rodents, pets, items hanging from the ceiling, etc.), it is advisable to check the placement of the sensor (such as a passive infrared sensor installed too close to a heating duct) and the sensor integrity (such as loose parts or wiring). It may be necessary to replace a sensor if no other reason for false alarms is found.

Using the house dog from earlier in this chapter, an example of a nuisance alarm would be when the dog barks at a neighbor's cat or at a car playing its radio at a high volume while driving by the house. An example of a false alarm might be when the dog sits and barks continuously for no apparent reason at all. Both types of alarms are annoying and may contribute to the eventual disuse of the system.

F. Installation of Sensors

When installing an intrusion detection system, where a sensor is located can make a big difference in the sensor's ability to perform well. It is important for the installer to be conscious of several characteristics of a site and of the sensors being considered, including:

- Are large pieces of furniture or other tall items in the detection zone of the sensor? Most sensors will require an unobstructed line-of-sight to operate properly.

- What is the pattern of detection for the type of sensor being considered? (The *pattern of detection* defines the shape and size of the detection volume – the space that is covered by the sensor.) This information should be included in the installation guide for each sensor.

- What doors or windows are most likely to be broken into? If everyone who has ever worked at a facility knows that tuition money is stored in the office, then the office window may be a likely entry point.

Many types of interior sensors have an adjustable sensitivity capability. However, it is not to be assumed that setting a sensor to its maximum sensitivity level will make your facility extra safe. On the contrary, the maximum settings will usually increase the number of nuisance alarms. For example, a sensor set at highest sensitivity may alarm on warm air from a heating duct or small rodents moving about the area that would otherwise not be noticed. Because of this fact, most sensors should initially be set at an average or medium sensitivity level or as recommended by the manufacturer. Adjustments can be made as experience with the system is gained.

G. Types of Sensors

There are several different kinds of intrusion detection sensors that can be used effectively at a childcare center. While each kind may work well in an appropriate location, no single kind of sensor is appropriate for all requirements. The installer needs to use the sensor that best minimizes nuisance alarms and maximizes the chances of detecting a true alarm condition for each location.

1. PIR Sensors

PIR (passive infrared) sensors are the most commonly used volumetric type of sensor. *Volumetric* refers to the fact that it protects or covers a certain volume of space, rather than a single line or a single door or window. A PIR is a type of motion sensor.

PIR sensors contain pyro-electric detectors that detect changes in thermal heat energy in a room or area. While the PIR does not see a person per se, it sees the hot spots of a person's body. A segmented lens which divides the PIR detection volume into multiple zones focuses thermal energy onto the pyro-electric detector.

The detection zones of an average PIR look somewhat like multiple fingers extending out from the sensor. Imagine very skinny pyramids that are slanted in one direction that make up each finger (see Figure 6.1). Walking through a pre-set number of these fingers is what causes the PIR to detect thermal energy changes and then generate an alarm.

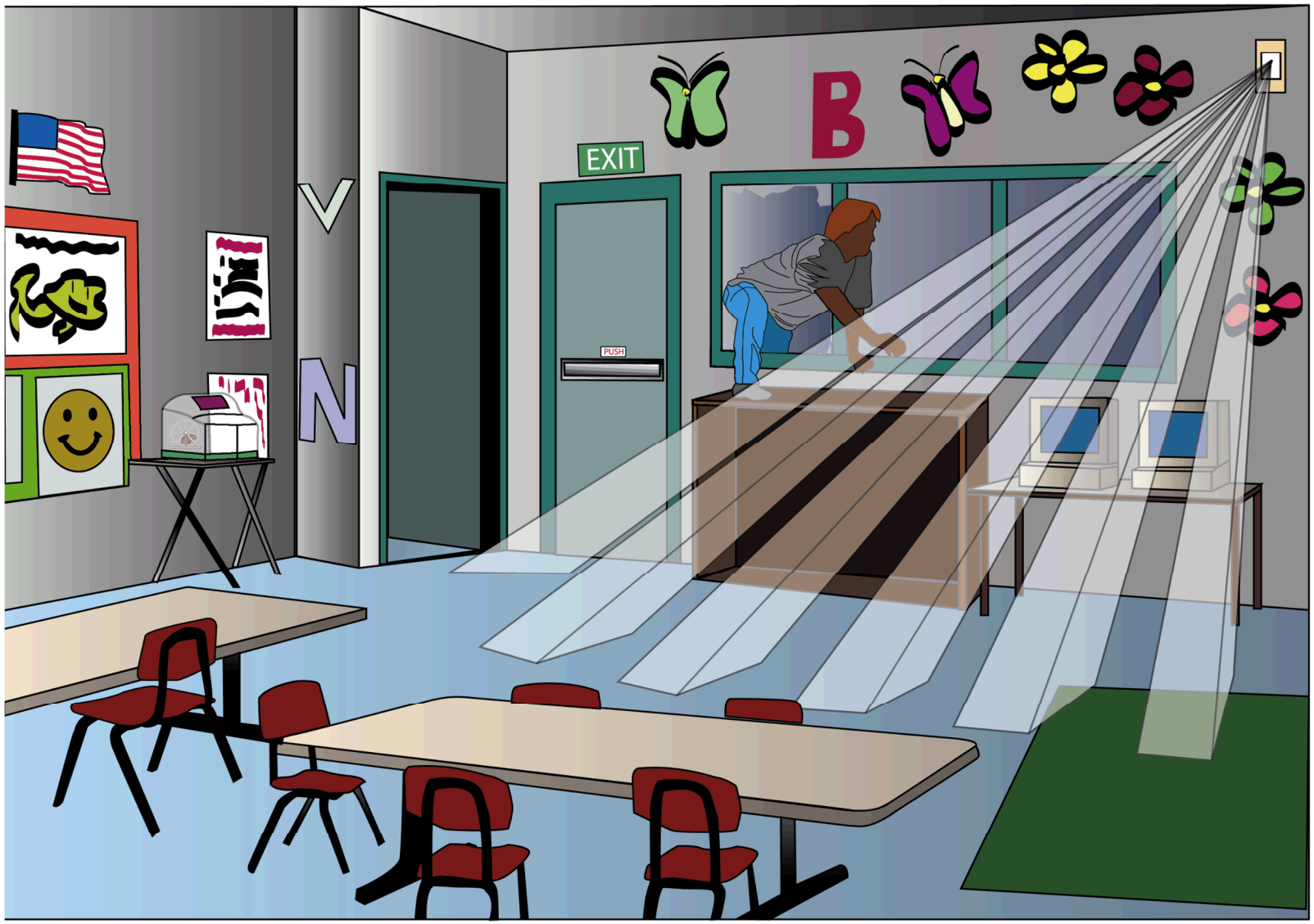

Figure 6.1 This diagram illustrates the segmented lens detection pattern of a PIR sensor.

Sources of nuisance alarms for PIR sensors can include:

- Rodents,
- Pets,
- Birds,
- Insects on or within the sensor casing,
- Being installed too close to or aimed directly at heat sources such as radiant heaters or heating ducts, and
- Possibly items hanging from the ceiling.

Prices for PIR sensors range between $25 and $100.

2. Microwave sensors

Microwave sensors are a type of active volumetric motion sensor that transmit a low-power microwave field. Detection occurs when the frequency of energy received back changes. Persons or other objects that reflect microwave energy cause slight changes in the frequency of the microwave energy when they move within the protected room. This is known as the Doppler frequency shift.

One particularly good feature of a microwave sensor is that it fills the entire space in a room. However, microwave fields can transmit through glass, dry wall, and other light construction. This means that movement in the hallway outside a sensored room will likely register as an alarm which may not be desired in a particular location.

Sources of nuisance alarms for microwaves may include:

- Movement of metallic objects, such as a Mylar balloon or a mobile made of tin foil;
- Fluorescent lights, when on and within the sensor detection area, though some microwave sensors have a filter that cancels out the frequency of flickering fluorescent lights;
- Pets, birds, less so for crawling rodents, and even less for insects; and
- Movement outside a sensored room, especially if the walls are of light construction or glass.

Price ranges of microwave sensors, which are primarily used in high-security applications, range between $300 and $500.

3. Dual-technology sensors

Sensor units that consist of two different sensor technologies are referred to as dual-technology (a.k.a. dual-tech). The most common type of dual-

tech sensor has a PIR sensor and a microwave sensor. Dual-tech sensors are usually set up so that both sensor technologies have to detect motion within a certain time window, usually a few seconds or less, in order to generate an alarm mode. This arrangement can reduce nuisance and false alarms significantly. The probability of detection for dual-tech sensors will be somewhat lower than for each individual sensor, but the reduction of false and nuisance alarms usually overrides this deficiency.

Price ranges of dual-tech sensors vary between $50 and $150. It is interesting to note that a sensor with both a PIR and a microwave is much cheaper than just buying a microwave sensor alone.

4. Magnetic switches

Magnetic switches are inexpensive position sensors for doors and windows. They consist of a magnetically sensitive reed switch and a magnet. The reed switch is mounted to the door or window frame and the magnet is mounted to the movable door or window. The reed switch changes state when a magnet is close to it, pulling the contact within the switch closed, thereby completing an electrical circuit. When a door or window is opened, the magnet is no longer close to the reed switch, which causes the reed switch to go back to its default state, breaking the electrical circuit. However, a knowledgeable perpetrator could possibly get past the sensor without causing an alarm. Still, a magnetic switch is a good sensor for a very reasonable price.

Prices for magnetic switches are in the $3 to $5 range.

5. Balanced-magnetic switch

A balanced magnetic switch (BMS) is a more sophisticated type of magnetic switch that is much more difficult to defeat. In addition to the reed switch and door magnet, there is a bias magnet installed next to the reed switch. Both the reed switch and bias magnet are within the same enclosure, mounted to the door or window frame. With the door closed, the door magnet and bias magnet form a balanced magnetic loop around the reed switch. The reed switch does not see magnetism and is in its default state, which is the door-closed, secure state for the BMS. When the door opens, the magnetic loop is gone and the bias magnet pulls the reed switch contacts into the alarm state.

The advantage of the BMS sensor is that, because the spacing and strength of the door and bias magnets is extremely precise, the sensor is much

more difficult to defeat than a simple magnetic switch.

Disadvantages of the BMS are that these devices are larger, less attractive, and much more expensive than a traditional magnetic switch.

The price range for a BMS sensor ranges between $50 and $100.

6. Glass break sensors

Glass break sensors serve as a type of boundary protection; they can provide the initial detection of a perpetrator before he enters a facility. For a school setting, glass break sensors can also serve to provide an alarm to authorities that windows are being broken – a common type of vandalism.

There are two types of glass break sensors:

Acoustic/audio – These sensors are mounted on a wall or in the ceiling up to 25' from the windows. They listen for the characteristic sound of breaking glass, which typically makes a low-frequency thud followed by a high-frequency, tinkle-type of sound.

Vibration – This type of sensor must be attached directly to the glass of each individual pane of glass. The sensor responds to the vibration of breaking glass.

Vibration sensors are more reliable than acoustic sensors, but one sensor per pane of glass is required and the vibration sensor is less attractive. Also, because an intruder will be able to see the vibration sensors on the windows, the intruder then knows at least one way *not* to attempt to enter the facility.

Glass break sensors cost between $30 and $100.

7. Wireless sensors

Wireless sensors, usually PIR or dual-tech detectors, use RF (radio frequencies) instead of wiring to send alarm signals to the control panel (see next section). This is particularly convenient where there are construction obstacles or no ceiling access due to environmental concerns. These sensors are generally powered by batteries that must be replaced every two to five years.

The primary advantage of using a wireless system is its easy installation. The disadvantages include the need to replace sensor batteries periodically and the possible loss of alarm signals due to interference. Because the effective installation of RF equipment is not straightforward, it is important to have these devices put in by an experienced installer.

Wireless sensor costs range from about $60 on up. Alarm panels that accept RF signals may also be more expensive.

H. The Alarm Control Panel

The alarm control panel is a gathering point for all sensor data. Many alarm panels can also provide a power source for the installed sensors. A typical panel installed at a large childcare center may handle between 8 and 32 different zones; each zone will receive the alarm signals of all the sensors in a particular location of a building.

For typical situations, the alarm control panel has a telephone dial-up modem which, when an alarm occurs, will automatically dial an alarm monitoring company. The alarm monitoring company has equipment to decode the message from the alarm panel and displays the information to an operator. Ideally, the alarm panel should have its own dedicated phone line, or at least a phone line that will always be available after normal business hours.

Note: If there is a concern about an intruder cutting the phone line, backup communications, such as a cell phone or the internet, can be used. However, this adds to the costs.

A keypad(s) connected to the control panel is used to perform daily functions and is normally located near one or more entry/exit doors. The keypad is used to arm the system when everyone is going home for the night, and to disarm the system in the morning when building occupants are returning. This same keypad is used to turn off the system when the building manager/owner, along with police officers or other trained security individuals, responds to an alarm condition. The keypad can also provide the information as to what zones were actuated to set off the alarm, thereby providing the location(s) of where an intruder is or has been within the facility.

Most alarm control panels allow the facility to have many *pass codes* – number combinations consisting of three to eight or more digits – so that employees can each have their own unique code. As these pass codes allow the alarm system to be turned off, it is important that they be kept secret and be shared among only a very few trusted individuals. It is good practice to change a pass code when compromised or when a staff member leaves the facility.

Alarm control panels can range in price from $150 to $800 for systems that will handle 8 to 32 zones.

Installation costs can range from hundreds to thousands of dollars, depending on the difficulties encountered when running the wiring to each sensor location. For small systems, say less than a dozen sensors, it may be cost effective for a facility to use a wireless system, provided that an experienced installer can do the work.

I. Working with security vendors and installers.

The burglar alarm market is such that there are many security companies that go out of business very quickly. Before committing yourself to a particular company, consider the following suggestions:

- Ask to see an installed and operating system similar to the one being considered.

- Visit other facilities where the vendor has already installed this product and ask folks at that facility how much they like the system, how difficult it is to operate, and what kind of down-time (time during which the unit is inoperable), if any, that the unit has had since it was first installed.

- Be sure to have the vendor specify the complete installed and operating cost. This quote should include system testing and the requirement that all wiring meet local codes. All wiring must also be run within the ceiling or walls; if that is not possible, wiring should be enclosed within conduit. Any wiring that will be located on the exterior of the building, run underground, or that will be susceptible to vandalism must be enclosed within tamper-resistant conduit.

- Make certain that the vendor will provide user training.

Chapter 7 Video Surveillance Cameras and Recording Devices

A. CAMERAS

1. Why video cameras?

One good reason to use video surveillance cameras at a childcare center is the deterrence factor they introduce to outsiders who do not belong there. The casual intruder who is looking for easy opportunities for illegal activities can oftentimes be convinced to look elsewhere simply by the presence of a strategically located camera.

A second good reason for using video cameras in childcare centers is to survey and protect the parking lot area. Staff and parent vehicles may be the target of theft and vandalism during the school day, while school vehicles are often hit at night.

Thirdly, video cameras inside a childcare center can help to later identify a perpetrator who is stealing from staff purses or from the center's cash box. This thief might be an employee, the parent of a student, an older student who attends the center after school, or even an ex-staff member.

A fourth reason to use video cameras is to hopefully mitigate the anger/actions of a frustrated or totally over-the-edge parent. If a video camera and TV monitor is installed in the front office of a facility and is always displaying the video being captured in real time in that area, angry parents may quickly deflate when they realize that they are being recorded. See Figure 7.1.

Lastly, the video camera system may record an incident that later becomes a major issue. It is not uncommon for parents, based on what a child tells them or from observing some sort of mark or bruise on their child, to accuse a staff member of abusing their child. At this point, the camera's recordings could serve as a record of classroom activities. If there is no truth to the parent's accusation, the recording will have saved much time and effort for the school manager and the staff member is cleared. But if there is even *some* truth to the accusation, it is also in the best interests of the childcare facility to identify a poorly trained or an inappropriate staff member as soon as possible. Not only is this best for that particular child, but if an abusive adult remains in the childcare's employ, there will likely be additional incidents in the future and one of them could be more serious.

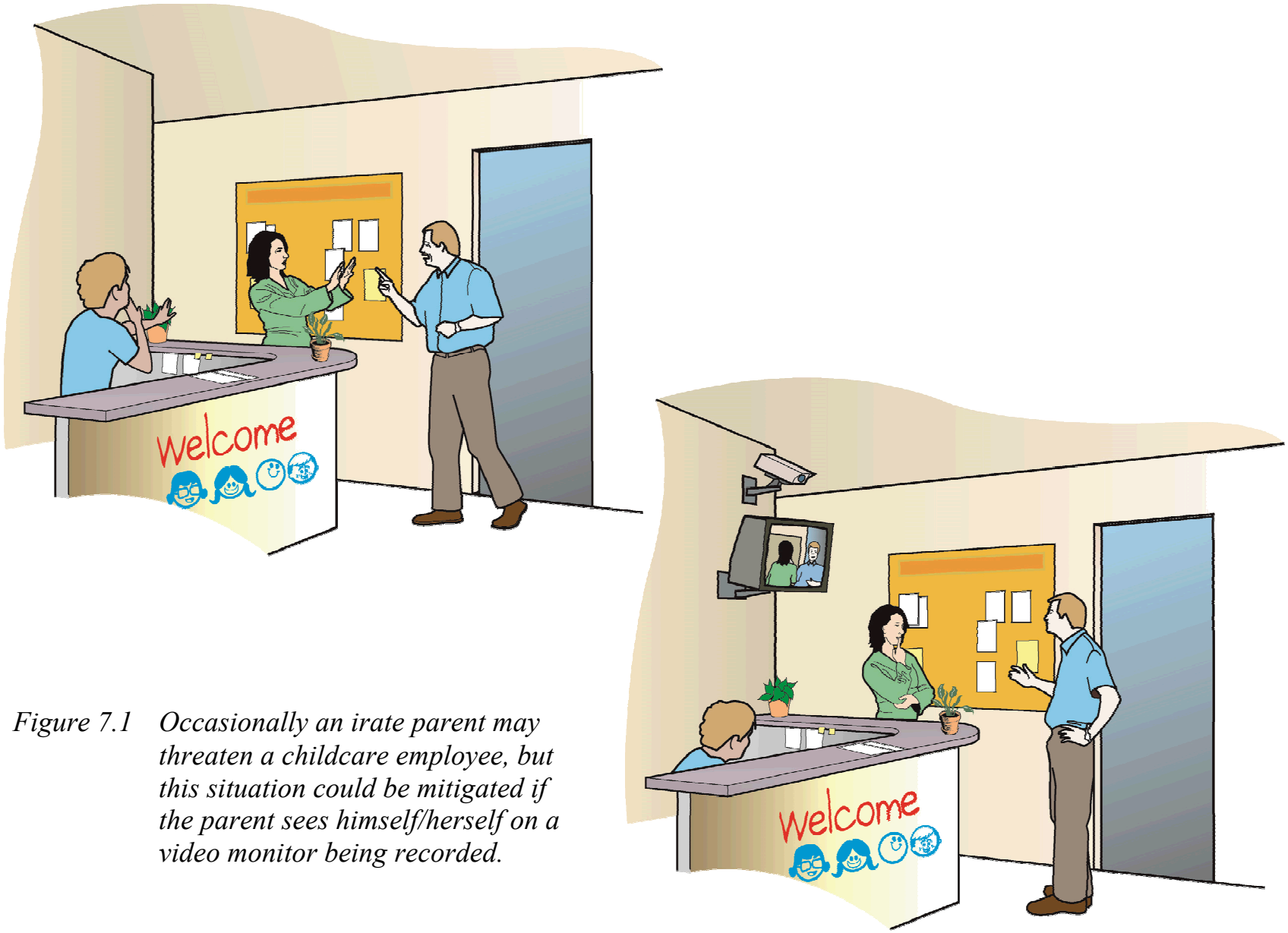

Figure 7.1 *Occasionally an irate parent may threaten a childcare employee, but this situation could be mitigated if the parent sees himself/herself on a video monitor being recorded.*

2. Why NOT video cameras?

Video cameras are not necessarily the best solution to many problems that a childcare center may be concerned with. For this reason, the childcare manager should consider the following cautions:

- A video camera system is a major expense for a childcare facility, and the cost of *installation* of the equipment is usually more expensive than the cost of the actual hardware purchased.
- It is difficult to choose effective video equipment without a moderate amount of technical knowledge.
- Video cameras can be stolen or vandalized.
- Video camera systems will sooner or later need maintenance or require repair or replacement.
- Even if a center can afford one or two cameras, it should be remembered that one or two cameras will only be able to effectively view a fairly small area.

3. Color vs. black & white

There is very little difference between the price of color video cameras versus black & white video cameras today. While black & white cameras often have more lines of resolution so that the image is more detailed, in most situations there is more information provided by a color camera. Examples are the person who picked up a certain child the day before wore a blue coat, had light-colored hair, and drove a dark beige car or the child that pushed Tommy off the monkey bars had on a green jacket.

The only reason a childcare center might want to consider a black & white camera is for night-time viewing; black & white cameras can operate with more efficiency and somewhat less lighting at night than color cameras can. There are video cameras on the market today that use a color camera mechanism during the day, but switch to a black & white camera mechanism after dark. This type of camera is more expensive and is designed for facilities that desire optimal viewing both during the day and after dark.

4. Lines-of-resolution

At the time of the writing of this document, 450 lines-of-resolution for a color camera is considered *high resolution* and has become almost a standard. This produces a quality image (provided that the surveillance system's recording device has the ability to record this resolution – be sure to ask!) that would likely satisfy the requirements for most childcare centers.

5. Fixed cameras vs. pan-tilt-zoom cameras

Most security surveillance cameras installed today are a type known as a *fixed* camera. These cameras cannot move or zoom and always view the same scene.

It is not uncommon for many facility managers to believe they will gain much more oversight capability through the installation of a *pan-tilt-zoom (PTZ)* camera rather than a fixed camera. This type of camera will allow a person at a control station to alter the direction that the camera is pointing either to the right or left (360 degrees) and up or down and to make the image zoom in or out. While these capabilities may be excellent, there are many problems associated with the use of PTZ cameras:

- PTZ cameras may cost from five to 10 times as much as a normal camera.

- PTZ cameras have mechanical parts that will wear out and need more maintenance and repair than a fixed camera.

- PTZ cameras can only use their optimal capabilities of changing the view if someone is available and located at the camera system console to operate the joy stick that controls the PTZ camera.

- When the PTZ cameras are not being controlled by an operator, they can be placed in a random or specific pattern to scan an area. When a security incident does occur in that area, the probability that the camera will be viewing the wrong scene at that time is high. (See Figure 7.2)

- If a PTZ camera is not installed within some type of opaque dome, the direction it is pointing can be seen by would-be perpetrators and they can then use this information to their advantage. (See dome enclosure in upper right-hand portion of Figure 7.3). While this is also true of a fixed camera, the significantly lower price of fixed cameras may allow a facility to install multiple cameras in a risky location, so that the entire area is always being surveilled and recorded.

For these reasons, many facilities across the country have chosen to install more fixed cameras rather than fewer PTZ cameras.

Figure 7.2 A pan-tilt-zoom camera that is set to automatically pan an area may completely miss capturing incidents of concern.

Figure 7.3 These are all examples of cameras in use today.

6. Camera location and installation

Depending on the neighborhood where a facility is located, a camera that is installed outside (such as overlooking a parking area) may be stolen or vandalized at night. This may be because the perpetrator doesn't want to be seen as they conduct their unofficial business at the facility or because the camera has value and may be resold.

Therefore, it is important that an exterior camera be mounted in such a way that it cannot be easily vandalized or stolen. Usually this is accomplished by installing the camera as high as possible, preferably around 16 feet or higher.

Another way to protect a camera is to locate it where a perpetrator attempting to vandalize or steal it will be recorded before they successfully render the equipment inoperable; i.e., they cannot approach the camera without being seen by one or more cameras. However, the design of some facilities or the needs of the facility may dictate a less-than-optimal installation location. (See Figure 7.4).

The camera should never point directly into the sun, either in the morning or evening, as this will likely wash out the image during these times. The best way to avoid this problem is to mount the cameras high and pointed downward such that they are looking below the horizon.

It is important for the childcare manager to understand that a single camera cannot view a very large area. A rough rule of thumb is that a camera can capture and provide a recorded image that allows the viewer to distinguish between individual faces within an area no bigger than about 50 feet by 50 feet. Most childcare center parking lots are larger than this. Remember also that cameras cannot see through objects or around corners.

Usually it is not a good idea to mount a camera at the top of a tall metal pole; many slender metal poles sway significantly in medium to high winds near the top of their height, which could cause problems with the internal electronics of most video cameras. The large wooden utility or wooden light poles (a foot or more in diameter) are more stable and can be reliably used for camera mounting, provided a source of electricity is available. One thing to remember about wooden poles is that they can twist over time due to drying out, so that cameras may need to be re-aimed if this occurs.

Many facilities mount their cameras on the sides of their buildings resulting in a very stable configuration. It is also much easier to run interior power and data lines to and from a camera mounted

Figure 7.4 *For most applications, a camera should be installed at a height of about 16 to 20 feet (while still capturing an effective view of the scene) to protect it from theft and vandalism. However, the design of the facility or the requirements of the scene to be captured may dictate a less-than-optimal installation location. The camera shown above was installed at a height of about 10 feet as the building is only one story and the cost of installing the camera on a pole would have been prohibitive for this center.*

on the side of the building rather than one mounted to a pole located away from the building.

Depending on the weather in the area, most exterior cameras will require a housing to protect them from rain, freezing temperatures, hail, sand, dust, and rocks thrown at it. Some neighborhoods may be more prone to having cameras shot at, in which case a facility may need to consider upgrading their camera housings so that they are more bullet-resistant. (See Figure 7.5.)

B. VIDEO RECORDING UNITS

The most expensive part of a video system (besides the installation) is the recording unit. Up until just four or five years ago, these units consisted primarily of an industrial-quality VCR in combination with a multiplexor. The VCR had many problems associated with it due to the mechanical parts that often wore out and the limitation of the tapes to record 24 hours or less of high-quality video output before the tape needed to be changed out. For a very simple system consisting of only one or two cameras, a multiplexor is not necessarily required.

7. The DVR (Digital Video Recorders) unit

Today, almost all new camera surveillance systems use a digital video recorder (DVR) that is basically a custom-designed personal computer (PC) with special software and at least 100GB (gigabytes) of storage. The DVR records, stores, and manages camera images on the PC's hard drive.

Many DVRs include video motion detection (VMD) and will only record a particular camera's images when it detects motion in the camera scene. This usually saves a tremendous amount of storage space.

Another advantage of the DVR is that large or multiple hard drives make it possible to store many days or even weeks of video recordings before the system starts recording over the oldest saved images. And because there are almost no moving parts within a PC, there are typically fewer hardware problems to deal with.

There are many manufacturers selling DVRs at this time. Options and capabilities vary widely. One good way to choose a DVR brand is to find one or more businesses that use a particular type of DVR that they have had positive experiences with. Make

Figure 7.5 The cameras above are in tamper-resistant housings; shooting and destroying cameras was a regular occurrence at this location before these better housings were installed.

certain that the vendor has agreed to help install and get the system running, in addition to training your staff.

8. <u>Monitoring and Monitors</u>

Too many facilities believe that when they purchase a good video surveillance system, they will be able to stop undesirable incidents in progress simply by monitoring the cameras. This is simply not possible in most situations. First, most childcare facilities do not have the manpower available to devote someone to watching the playback monitor full-time. Second, it is difficult for people to consciously watch a monitor for more than 20 minutes before their minds wander or their eyes glaze over. In high-security facilities, video and alarm systems are integrated so that video is displayed only when an alarm occurs. Security officers who must watch monitors continuously are switched out every 20 minutes to prevent this sort of problem.

In general, childcare facility personnel will only be able to watch the real-time playback during short, specific times of the day. This will be when they are expecting something specific to happen, such as a teacher's desk being broken into during recess or cars being vandalized during the lunch hour.

In general, then, childcare facilities must realize that one of their biggest benefits from the video surveillance system, other than deterrence, comes from the ability to replay a recording later to determine exactly what occurred during an incident and who was involved. This is also referred to as *after-the-fact* viewing.

Contrary to what is commonly seen in many department stores, it is highly recommended that all of the scenes from a facility's cameras NOT be shown playing live on a monitor where anyone could view it. This is so that a would-be perpetrator, who could be a parent, worker, child, visitor, or even a staff member, could get a good idea of what areas can and cannot be seen by the cameras. This would allow them to make sure that their own undesirable actions take place in an area that is not effectively covered by any of the cameras.

Every video surveillance system needs a monitor to play back recordings and to view live video. This monitor should generally be co-located with the recording unit in a locked room or cabinet away from prying eyes. Another possible location is next to a staff member who may have the opportunity to glance at it frequently during the day. In this latter

case, the monitor should be placed so that only appropriate personnel can view it.
Monitors for playback can vary widely in price, depending on the size and quality of the playback image. A small monitor could be as inexpensive as $150, while a larger flat-screened monitor could cost as much as $600 to over $1000. The buyer needs to be certain that the monitor has at least as many lines of resolution as the cameras to obtain the best possible images.

9. Hardware and installation pricing

The price of cameras has come down significantly in the last five years. Today, reliable high-resolution color cameras can be purchased in the $200 to $800 range. (Good cameras can also be purchased for less than $100 if buying directly from a manufacturer and IF the buyer is knowledgeable about cameras.)

The housing to protect an exterior camera may add an additional $100 in cost or a housing may already be built into the unit as part of the camera unit. Housings can be more expensive if they are bullet-resistant or if they contain a built-in heater for low-temperature locations.

Prices of DVRs range from around $1000 to over $12,000. Most DVRs will be able to handle and record 16 cameras at one time. A few more expensive models can handle 32 or 64 cameras. A childcare facility should be able to purchase a $2000 or $3000 DVR that is reliable and offers all the features they would need.

Installation of the cameras can be extremely expensive, as it consists mainly of labor and will likely include the cost of a licensed electrician. Depending on where the cameras and recorders are located relative to each other, installation costs could be anywhere from $1500 to $20,000 for just a dozen cameras. The actual wire is relatively inexpensive, except for very long runs or where special wire is required.

Note: It is important that none of this wire be exposed such that a perpetrator could simply cut the wire to disable the camera(s). Even for the short length of wire that exits the wall next to the camera mount and enters the camera 12 inches away, this wiring should be enclosed in a flexible metal conduit to prevent easy vandalism.

10. Equipment life and maintenance

It is believed among many security experts that if a video camera is going to fail, it will do so in the first few weeks of use. Many of the warranties for video cameras cover just the first 90 days. It is important that the purchase documents include a clause that

makes the warranty period start at the time of acceptance by the purchaser. Usually if a camera does not fail during this early period, it will run for years with no problems. If a camera does cease operating, it could be caused by a power surge or a lightning strike. The installer should include one or more surge protectors in all systems. While camera repair used to be a big business, the lower-priced cameras of today may likely encourage a facility to simply swap out an inoperable camera for a new one.

11. Maintenance

The only regular maintenance a fixed video camera may need will be:

- To re-aim the direction the camera is pointing if the mounting bracket has slipped or someone has tampered with it;
- To re-focus the camera if the focus has drifted; and
- To clean the outside of the lens or the glass of the housing that protects the camera.

While this maintenance is fairly simple, it is a good idea to have the vendor or installer show facility maintenance folks how best to accomplish this. (The only challenging part of camera maintenance may be getting a maintenance person up to the higher-mounted camera locations, for which the use of a man-lift is highly recommended.)

Note: It can sometimes be difficult to get a security vendor or installer to come back out to a site for maintenance of equipment, even if the facility offers to pay additional money. Be certain that any contract that is drawn up includes provisions for repair, both before and after any warranties may expire, as well as on the actual installation. Response time to a center's calls is also an important negotiating point.

DVRs are still a relatively new product on the market and new versions of the system software are being distributed to users fairly often. These newer software versions do need to be installed, as older versions will not be supported by the manufacturer after a certain amount of time.

Hardware problems usually mean that a repair person will have to visit the site or that the user will need to ship the PC back to the manufacturer for a couple of weeks or so. Most DVR companies are anxious to make a name for themselves in this exploding new market, so they usually try to be fairly responsive to calls from the field for help.

Some manufacturers of DVRs offer a one to three-day training course on their product. Often, this training will be held in a different state, and travel costs may be prohibitive to a childcare business. However, it is sometimes possible forsomeone who enjoys working with computers to read the manuals and teach themselves most of what they will need to know.

12. Working with Camera and Recorder Vendors and Installers

It is a good idea for childcare facility managers to talk to as many vendors and users of video surveillance systems as possible before deciding on a brand and model that is most appropriate for their facility. The manager should not pretend to be knowledgeable about the products on the market but should always listen to any information that the sales representative can give; a potential buyer can learn a lot about the different companies and their products in this way. After a few interviews like this, the manager will begin to understand what features may be important for the purchase of the center's system.

Once the selection for a new DVR has been narrowed down to only one or two vendors, be certain to call and visit customers of those vendors, if possible, both to determine if the equipment is working as expected and to ask these customers if they are truly satisfied.

This page left intentionally blank.

Part IV
Critical Incidents, Disasters, and Emergency Response

Part IV Critical Incidents, Disasters, and Emergency Response

Unfortunately for childcare centers, no affordable security or safety measure exists that would always prevent undesirable incidents from affecting the facility and/or their students and staff. Just about any determined adversary who is willing to spend the time planning, surveying, and learning about a particular facility is probably going to be able to carry out an attack or assault that is going to cause damage or great bodily harm. And there may be little a childcare manager can do to prevent acts of nature from occurring, such as a direct hit by a tornado or quickly rising flood waters.

Because of these challenges, the most important preparation that any manager of a childcare center can do is to plan for a crisis. If an emergency situation does occur, the staff and students must be ready to respond. Certainly all parents are going to want to feel that, in the event of an emergency, good insight, planning, and practice is going to improve the chances that their child is harmed.

The three most basic responses that a childcare staff will likely need to accomplish for most critical situations are:

- Intervene to mitigate the situation, if possible;
- Get the children out of harm's way; and
- Summon help.

These responses will not necessarily occur in this order.

It is therefore crucial that childcare managers identify and understand the critical types of incidents that may occur in their areas, along with the possible ramifications. For example, if the center is located on a main street that usually has plenty of fast-moving traffic, then there is the chance that someday a vehicular accident out on the street could propel a vehicle onto the childcare center's parking lot, playground, or even through a wall of the facility. How should staff react in such an event?

Instead of waiting for the next emergency situation to see how the staff *does* react, the manager needs to provide and reinforce guidelines as to how the staff *should* react.

Note: It is certainly not possible for every possible undesirable scenario to be imagined and specific

instructions be developed to handle each particular incident. What is necessary is that the childcare manager be able to identify the major categories of events along with a few basic reaction plans to be implemented by the staff and the children.

The information provided in the next three chapters is mainly applicable to larger childcare centers. It is hoped that the smaller in-home childcare providers will also benefit from this information. Even in-home childcare providers need their own well-thought-out emergency plans.

Chapter 8 Being Prepared

For most Emergency/Crisis Plans, there are certain decisions that have to be made in advance and certain actions that have to occur during a crisis event. For a childcare center, these decisions would likely include, but not be limited to, the following (not necessarily in this order):

Before a crisis occurs

- Assign the person who will be in charge as well as an alternate.
- Determine desired procedures for various crises.
- Develop different code words or phrases for children and staff to respond to.
- Identify the emergency resources that are to be called to provide the response/services needed.
- Identify primary and secondary modes of emergency communications.
- Identify evacuation locations.
- Prepare calling lists with important phone numbers and place in appropriate locations.
- Train staff on a regular basis.

When a crisis has occurred

- Intervene, where needed and helpful, without causing further harm to anyone.
- Get the children and staff out of harm's way, using appropriate evacuation/shelter locations.
- Call for help; assign someone to meet responders at the street and direct them to location of problem.
- Notify childcare owner/manager if not present.
- Notify the families of involved children & staff.
- Prepare an early statement for the media.
- Notify the rest of the families, if appropriate.
- Prepare a document to be distributed to all families to explain entire situation.
- Document everything that has happened including names, times, locations, what was said, etc., as soon as possible.
- Debrief with staff – what went wrong, what needs to be improved or changed in the future.

A Discussion of Some of These Actions

An **Emergency Coordinator** for each facility should be assigned. The Emergency Coordinator does not have to be the person in the front office who greets visitors and collects childcare fees. If the manager of the facility is almost always on-site, then the manager may likely be the best candidate. If one of the staff members has been a nurse, policeman, medic, firefighter, or member of the military in the past, he or she might have more experience in handling crisis situations and may be more accustomed to maintaining a level head in an emergency. It might be a good idea to ask employees how they feel about handling this type of job assignment – there may be someone on the staff who would welcome the challenge and the mental exercises that this task brings.

The Emergency Coordinator should know who on the staff can provide CPR the most effectively (usually everyone employed at childcare facilities these days) the most effectively and who would be able to render appropriate first aid before professionals arrive on the scene.

It will be the job of the Emergency Coordinator, in the event of a crisis, to give directions and make assignments, place phone calls, etc. There should be a **fully-trained alternate** assigned for this task in case the regular Emergency Coordinator is not available during the critical time.

When a crisis really does occur, three things need to happen concurrently and immediately, as much as possible:

- Someone needs **to intervene into the situation** (i.e., stop the incident in progress or rescue, as appropriate) *if* it is possible and helpful, and *if* it will not result in the further harm of anyone.
- A call must be made **to obtain help**.
- The children not directly involved need to be relocated so that **they are out of harm's way**, using predetermined evacuation strategies.

For most critical situations these days, dialing 911 will provide whatever type of support is needed. In case your particular area does not have the 911 feature that automatically provides emergency personnel with your location, be sure that all staff members know the address of the childcare center and that they remember to provide it when phoning for help. The address should be posted next to

every phone, along with the phone numbers of key individuals. If possible, assign somebody to stand at the street curb to **flag down arriving help** and direct them as quickly as possible to the location of the situation or victims. (If it is already after dark, this person must take a flashlight along to be more visible by first responders.)

Once help is on its way and the rest of the children are out of harm's way, **the parents of the involved children must be contacted**. An up-to-date list of phone numbers and alternative phone numbers should be readily available. The need for a carefully worded phone call cannot be over-emphasized. You do not want to unnecessarily panic the parent of a child who has a broken leg, but you also do not want to downplay a serious incident. And in the event of a more tragic incident, the Emergency Coordinator should have already developed (and confirmed with the center manager) the appropriate wording that is to be used. This serious call to the parent, to be made by the Emergency Coordinator, the manager, or the owner, could be something like this:

> *"Mrs. Johnson -- this is Tracey from the Middle North Childcare Center. I'm afraid your son Mark has been in an accident. A car rammed through the fence and onto the playground. The EMTs are with him right now and we don't know the extent of his injuries, but we are having them take Mark to St. Mary's Hospital on 9th Street, as it says on your emergency sheet."*

At this point, the Emergency Coordinator should try to provide whatever information the parent needs, but only the information that is truly confirmed. Make certain that you provide them with at least two phone numbers where they can call back (which may need to be different phones if there are several parents still to call) and that the center has the parents' cell phone number. Keep phone lines open if at all possible unless speaking with the parents whose children are directly involved.

If the emergency is something as straightforward as a broken leg, then at this point, the Emergency Coordinator needs to start **writing down all details** that can be remembered about the situation, including the approximate time the incident began, the time help was called, when help arrived, who was there when the incident occurred, what they said, what each person saw, how the child/children appeared, etc.

If the emergency was a more tragic event, and many of the children are very upset by what they saw or heard, it may be appropriate to **contact the rest of the parents**. Explain to each parent that, while their child is fine, there has been a serious incident (with a very short explanation), and they may wish to come and pick up their child at the present time, though the center will be open until regular closing hours. Explain to them that you cannot go into the details at this time as there are many parents to call, but that some of the children were particularly upset. Assure them that there will be a printed letter available for parents by a certain time, which will explain more completely what has occurred.

For larger centers, **a website for parents** to log onto when there is a local disaster can be very useful. The developer of the website should design an option for the manager or Emergency Coordinator to enter a few quick lines when necessary regarding what has occurred and what the parent may want or need to do at this time. (See Figure 8.1.) Another option is to have an **emergency hot line** for parents to call to listen to a pre-recorded message with basically the same information. (See Figure 8.2.)

It is important that the staff of the center realize that only one person, likely the owner or manager, should EVER **talk to the media** unless that person has been fully briefed on the appropriate response. Mixed messages early in a tragic event can alarm parents needlessly. Ask all staff to be pleasant to the media but to refer them to the appointed voice of the childcare center.

Preparing **a written explanation for parents** as to what has occurred may be difficult, as there should be no assumptions made. The explanation should contain as much confirmed information as possible so that parents do not feel that information is being withheld from them. The manager and/or owner of the center will have specific instructions as to the explanation's content, due to potential liability issues.

Lastly, within a couple days of the incident, the entire staff should get together for **a debriefing of the event**. This meeting should allow everyone to discuss and understand exactly what happened, how each person reacted (without placing blame), how the children reacted, and what needs to be changed or improved in the future.

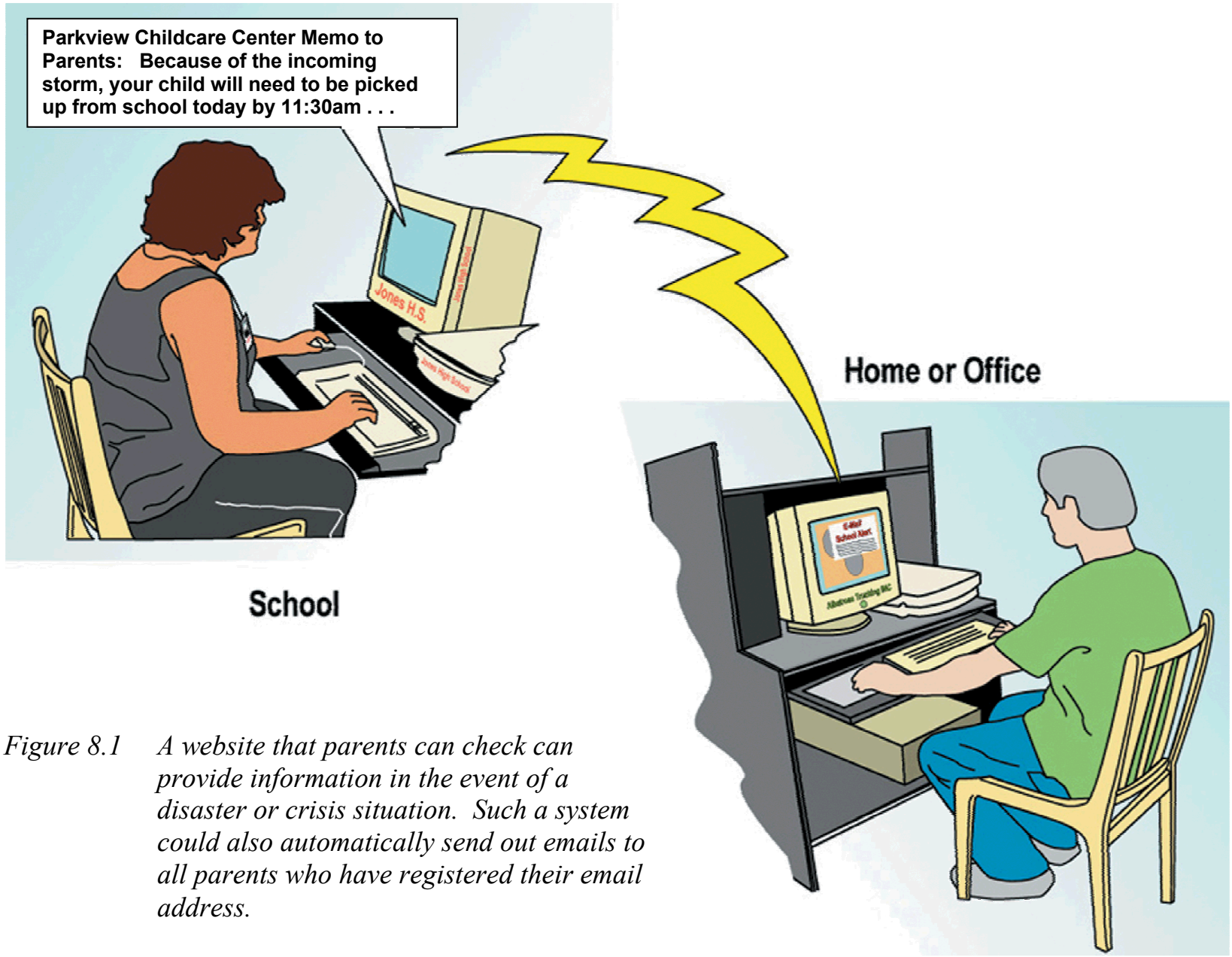

Figure 8.1 *A website that parents can check can provide information in the event of a disaster or crisis situation. Such a system could also automatically send out emails to all parents who have registered their email address.*

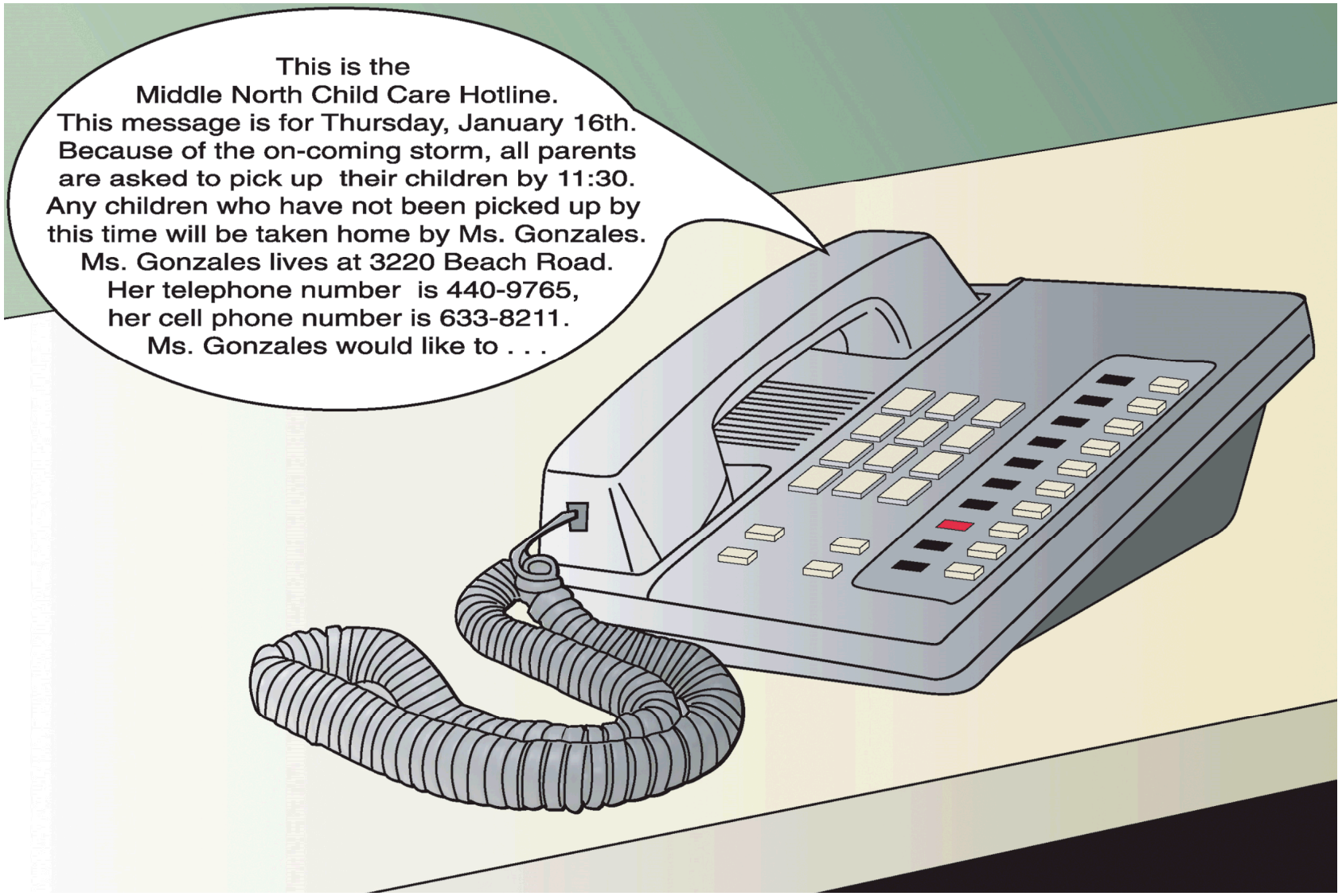

Figure 8.2 An emergency hotline can provide information quickly to calling parents. This is particularly useful if parents are stuck in traffic but have a cell phone with them.

Chapter 9 Training Employees, Children, and Parents

While a facility's emergency plans will change over time, the owner, manager, and Emergency Coordinator must agree on the general categories of emergencies they wish to prepare for and how the occupants of the building should respond to these emergencies. These procedures should be written down as the Emergency Response Plan, in a simple, concise, and, if possible, illustrated manner. (See Chapter 10 for one possible Emergency Response Plan.) **Keep in mind that an imperfect plan is probably better than a nonexistent plan, at least until more time is available to perfect the plan.**

An initial two-hour training session with the entire staff is probably a good way to get started and should be repeated twice each year and whenever new staff members are hired. New issues that come up need to be included in the next revision of the Emergency Response Plan and training session. Ideally, there should be no more than just a few different response actions that management and staff feel are appropriate. These response actions should coordinate with the center's defined threats.

Training the children to react to particular codes will likely be fun for them. The children should not be unduly frightened, but they should be taught that this sort of drill can be a serious thing, rather than only a fun thing. Different types of actions should be simple to understandable for most of the children who are over three years old. Some examples:

- *"Code Red"* – children and staff should quickly lie down very flat and put their hands over their head (see Figure 9.1);
- *"Code Blue"* – children and staff should quickly leave the classroom and move to the back of the playground; and
- *"Code Green"* – children and staff should get under heavy furniture or interior doorways and cover their heads.

More than three or four types of actions may become difficult for the smaller children to keep straight. The rest of the children will likely do well in learning the codes, especially if they are timed to see how quickly they can get into the correct formation each practice session.

Figure 9.1 Here a class of four-year-olds practices an emergency drill.

While parents do not need to be trained – unless they regularly volunteer at the center – they do need to be kept informed that the school is practicing these different types of exercises. Parents should be encouraged to ask their children about how they were taught to respond to the various codes.

Chapter 10 A Sample Emergency Plan

Too often, an emergency plan for a school is never prepared, even though everyone agrees that one is needed. Why? Because it is often felt that such a plan must be very comprehensive and it may seem to the staff as if too much needs to be known and decided on before a good plan can be pulled together correctly. Then the plan has to be published, the staff trained, and the plan updated as necessary. Many childcare managers feel they will never have that kind of time available.

Better than *never* writing the perfect emergency plan would be developing a simple initial plan that is easy to prepare and requires a minimal amount of training. One example of such a plan is shown in Figure 10.1. This Emergency Plan Poster could be posted in all classrooms, offices, and staff areas. The information on the poster that might change each year is left blank. The poster can be laminated to be reusable by simply changing the information in the blanks with a dry-erase marker. This type of poster, plus staff training sessions on a regular basis, can produce an excellent initial emergency plan that is always available, easy to understand and use, and easy to update as needed.

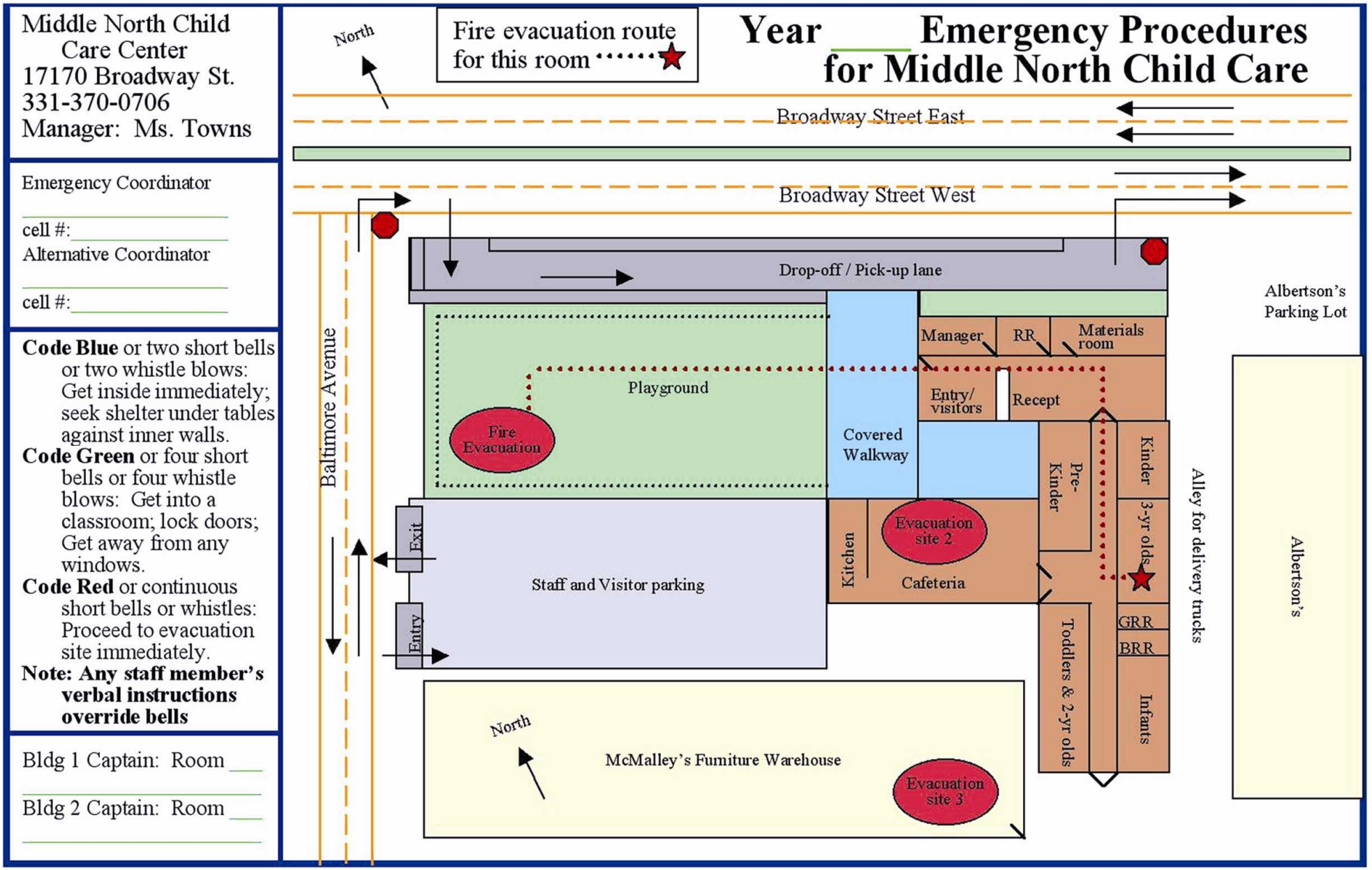

Figure 10.1 This is an example of an Emergency Plan poster that could be laminated, posted in every classroom, and updated with a dry-erase marker as required.

Appendix A A Spectrum of Possible Undesirable Incidents, Threats, and Improvements

The list below consists of possible security and safety incidents that could occur in a childcare center. ***Security*** incidents are defined as those generally caused by the malevolent acts of one or more persons. ***Safety*** incidents are defined as unfortunate but unintentional incidents or acts of nature. Safety concerns are included in the discussion below as some incidents can be both maliciously caused as well as occur accidentally.

Along with each security threat are a few possible solutions that a childcare manager may want to consider. Many of these suggested solutions are discussed in more detail within the rest of this document.

Keep in mind that this list is not exhaustive, but probably does address the majority of perceived threats or concerns in a childcare environment.

Security incidents

1. Daytime theft inside the facility. This usually encompasses theft of money or wallets from teachers' purses or the theft of cash from a cash box in a desk. Perpetrator may be an *outside*r (a person who does not have authorized business within the facility) or an *insider* (a person who is authorized to be in the facility).

   Possible enhancements to upgrade security:
   → Better control of who enters the facility.
   → Surveillance cameras in certain interior parts of the school.
   → A policy that all staff purses and school money are to be kept locked away.

2. Parking lot theft or vandalism. This includes theft of wallets or purses while a parent runs into the childcare building to drop off or pick up a child.

Possible enhancements to upgrade security:

→ Surveillance cameras in the parking lot.

→ Notes sent home to parents reminding them to not leave valuables in their vehicles and to always turn off the engine and lock the car while in the facility.

3. An angry, irrational, or threatening parent. Just about any teacher or manager can tell you stories about a parent who has become threatening and/or abusive.

Possible enhancements to upgrade security:

→ Procedure to discuss problems with parents only in the front office and while in the presence of another employee.

→ Camera with a playback monitor in the front office so that a parent realizes that he/she is being recorded.

→ Some method of signaling to another employee to become involved with the ongoing discussion or to phone for police.

→ A duress system.

4. An undesirable person gains entry to the facility or gets close to the children. Most playgrounds are not as inaccessible as they could be and most facilities do not prevent initial entry onto the grounds or into a building by a stranger.

Possible enhancements to upgrade security:

→ Better control of entry into facility.

→ More effective fencing around playground areas that cannot be easily climbed and/or seen through. (The ability of outsiders to view or not view the children is a double-edged sword. See more discussion in Chapter 2.)

→ A duress system.

5. Abuse of a child by a teacher or other staff member.

Possible enhancements to upgrade security:

→ Staff should be encouraged to speak up if they feel that there is something unacceptable going on between a staff member and one or more children.
→ Video cameras in classrooms such that recordings could be reviewed later by a manager.
→ Bathrooms designed with short swinging saloon doors to allow more visibility to others.
→ Background checks of all employees before hiring.

6. Abduction of a child by a noncustodial parent or other relative. This issue is made tougher by the fact that a small child would not necessarily know that anything is amiss and would likely go with any family member.

Possible enhancements to upgrade security:

→ Entry control systems that prevent easy entry into a center by people other than those who have custody or authority to pick up.
→ Information easily accessed by staff as to who may pick up a child plus a required procedure that staff always ask to see ID if they don't recognize an adult.
→ An alert given to all staff when a bitter child-custody case is underway or has just been settled.

7. Abduction of a child by an unknown adult.

Possible enhancements to upgrade security:

→ A robust entry-control system.
→ Good fencing.
→ A duress alarm system.
→ A camera system for after-the-fact identification of what the suspect looks like and what kind of vehicle was used.

8. Hostage situation. A possibly horrible situation that could be caused by a criminal on the run from another incident, a mentally unstable individual looking for attention, or an over-the-edge spouse/ex-spouse of a staff member.

Possible enhancements to upgrade security:

→ A robust entry-control systems.
→ A duress alarm system.
→ Good fencing.
→ Making certain that all employees know to make a school's manager aware of any domestic problems, so that staff can be notified and be on the alert.
→ A camera system that can be viewed by emergency personnel off site. (Talk to your camera vendor for more information about this type of option.)
→ Teaching children where to evacuate to when a bad incident occurs.

9. Assault or rape of a parent or staff member after dark or whenever the center is fairly deserted.

Possible enhancements to upgrade security:

→ Make certain that all exterior doors are locked after dark.
→ A procedure that all parents and their children be accompanied to and from vehicles during risky periods of the day.
→ Announcements to parents to always lock vehicles and to report suspicious individuals.
→ An entry-control system.
→ Good lighting.

10. A security incident in the neighborhood spills over to the childcare facility.

Possible enhancements to upgrade security:

→ Training the kids about how to respond to a few situations or simple code words given by their teacher.
→ A covert duress alarm system.

→ A robust entry-control system.

11. A drive-by shooting sends bullets through a window or onto a playground.

Possible enhancements to upgrade security:

→ Enclosure of the playground by material that might deflect bullets, such as a brick or cinder block wall.
→ Training of the staff as to how to respond to such a situation.
→ Training of the kids as to how to respond to a few easy commands given by a teacher or staff member.

12. Robbery/hold-up. This could be by someone who has some information as to the general layout of the facility, how many adults (male and female) are usually present, where the cash box is, etc.

Possible enhancements to upgrade security:

→ A procedure that does not allow visitors or prospective clients to visit after dark or without an appointment made ahead of time. (Several robberies at childcare facilities have been the result of adults who asks to see the center for possible placement of their own children late in the day.) A phone number should always be obtained to confirm the visit.
→ A robust entry-control system.
→ A video surveillance system.
→ A procedure for the manager or money handler to keep a small amount of cash in a cash box in a drawer that all staff is aware of. Meanwhile, larger amounts of cash are moved, as it accumulates, to a different location, one that few staff members are aware of.

13. A parent picks up their child without signing them out. Occasionally a parent takes their child from the center without anybody's knowledge. When the child is discovered to be missing, there is no record to indicate that the child had been picked up. (This isn't really a security incident, it is more of a safety/procedural incident. But at the time, it can seem very much like a crime has been committed!)

Possible enhancements to upgrade security:

→ Surveillance cameras in the parking area so that the facility manager can check to see if or when a child left and with whom.;

→ No access possible onto the playground except through the center's building.

→ An entry-control system that requires the use of a code, magnetic card, or proximity sensor so that everyone who enters the facility is automatically recorded, including the time of entry. (However, keep in mind that an entry-control system would not solve this problem if the parent entered the facility immediately behind another adult (called piggybacking), so that the door was already open and did not require the parent to use his/her own code or card.)

Safety incidents

14. Child is hurt. Could occur outside or inside through carelessness (the child's or a staff member's) or by the child doing something forbidden.

15. Child hurt by another child. Normally this would be considered a safety issue, especially if the offending child is less than two years old, but a significant injury or repeated incidents will be considered a security problem by the offended parents and could be a liability for the childcare center if not dealt with properly.

16. Child is stung by an insect or bitten by an animal.

17. A fire starts in the kitchen or elsewhere in the building.

18. A child is served something to eat that he or she is highly allergic to.

19. The children are served something that causes widespread food poisoning or worse.

20. A child is hit by a car in the parking lot while arriving or leaving the facility.

21. A child leaves the center unnoticed and gets lost or gets hit by a car.

22. Life-threatening weather hits the area (e.g., tornado, flooding, etc.).

23. A fire that spreads quickly (e.g., electrical fire that starts in the ceiling).

24. A serious vehicular accident occurs in front of the childcare center and the involved vehicle(s) are propelled onto the center's property or through one of the facility's walls.

After reviewing the above examples of possible concerns/threats and adding any others that are required, the manager of a childcare facility needs to decide what the facility's most likely threats might be and what type of truly devastating concerns they should be prepared to respond to. Once the staff of a facility identifies the most likely threats, they are better prepared to decide on the optimal upgrade of the security system. The bulk of this manual describes some of the possible approaches to handling various problems or issues which the childcare manager may wish to consider.

Appendix B An Example Security Checklist for a Childcare Facility

- ☐ All exterior doors are locked when not in use.
- ☐ Floor plan and site layout of facility is available to give to emergency responders.
- ☐ A list of threats/concerns has been developed, along with long-term and short-term (if necessary) plans for addressing each security concern.
- ☐ The center has a procedure in place and/or technology installed to control entry into the buildings or onto the playground by unauthorized people.
- ☐ A covert duress system (button/switch) has been installed in the front office and/or has been issued to each staff member (as appropriate).
- ☐ A regular weekly meeting is held to alert all staff about any child custody battles, angry ex-spouses or ex-boyfriend/girlfriends, and other issues that may exist. How the staff should handle a possible unauthorized visit should be decided upon.
- ☐ An Emergency Crisis Plan has been developed.
- ☐ Staff has been trained on the Emergency Crisis Plan.
- ☐ Children have been trained on the codes they may need to know in the event of an emergency.
- ☐ Appropriate exterior lighting has been installed.
- ☐ A regular process exists for a staff member to check the playground for trash or other undesirable items left on the playground each morning and especially after a weekend.
- ☐ A full roster of home and work phone numbers for parents, plus a list of adults who may pick up a particular child, is kept by every phone.
- ☐ All important emergency phone numbers are kept at each phone.
- ☐ Procedures are in place to protect women and children leaving the center after dark.

Appendix C A Summary of the Childcare Pilot Project

Goal of project: Sandia National Laboratories will:

- Analyze the security needs of a fairly large, private childcare center.
- Survey the center, along with several other centers, to get a feel for common issues.
- Meet with center's staff and some of its parents to determine what security upgrades might be of benefit to this facility.
- Have Sandians or local security vendors install any hardware and track the usefulness of each security upgrade.
- Use the funding that was available to investigate various possible solutions for a number of different undesirable incidents that were identified by several childcare centers.
- Evaluate, for this pilot childcare center, the appropriateness and usability of at least three kinds of security technologies.

Facility: A childcare center in Albuquerque, New Mexico, with approximately 125 children enrolled was chosen. This facility has two separate buildings that sit directly on a very busy Albuquerque street. A significant portion of the students attending this center have either all or a portion of their tuition paid for by a state-sponsored program.

Issues identified for this center and their calculated relative priority: See Figure C.1.

Note: This table of undesirable incidents has already been arranged in its relative priority order.

Figure C.1 Rough Priorities for Issues Identified at the Pilot Project Childcare Center

Note: This analysis uses the rating:

Very Low(1) – Low(2) – Medium Low(3) – Medium(4) – Medium High(5) – High(6) – Very High(7)

Pilot Childcare Center		Likelihood		Potential Consequences		Relative Priority Rating	
1.	Unauthorized outsiders enter the buildings	*Medium*	*4*	*Very High*	*7*	***28***	Highest priority
2.	Assault or robbery after dark	*Medium Low*	*3*	*Very High*	*7*	***21***	
3.	Abduction of a child by an unknown adult	*Low*	*2*	*Very High*	*7*	***14***	Next highest priority
4.	Abuse of a child by a teacher.	*Low*	*2*	*High*	*6*	***12***	
5.	Unauthorized outsiders near or on the playground	*Medium Low*	*3*	*Medium*	*4*	***12***	
6.	Child wanders out of buildings into busy street	*Low*	*2*	*High*	*6*	***12***	
7.	Drive-by shooting	*Very Low*	*1*	*Very High*	*7*	*7*	Third highest priority
8.	An angry parent threatens a staff member	*Low*	*2*	*Medium Low*	*3*	***6***	
9.	Nighttime break-ins and false alarms	*Medium Low*	*3*	*Low*	*2*	***6***	
10.	Daytime theft of money from staff purses	*Medium Low*	*3*	*Very Low*	*1*	***3***	
11.	Child taken by a parent who does not sign out	*Low*	*2*	*Very Low*	*1*	***2***	

Measures taken to address each issue:

(1) Unauthorized outsiders on the playground: A 6-foot wooden fence was installed right outside the existing 4-foot chainlink fence along the back of the playground that borders an alley. This alley does border some low-income housing further down. It was not unusual to see strangers wandering down this alley and sometimes stopping to look at or talk to the children. The staff of the center felt uncomfortable about this close proximity and visibility of the children and the staff. (This upgrade was funded entirely by the center.)

(2) Unauthorized outsiders entering the buildings: A proximity sensor system was installed at the two doors that open onto the parking lot from the two buildings. Parents were each issued their own key fob with a unique code. The key fob was designed to be attached to each parent or guardian's key ring. Next to each of the proximity sensors, a doorbell/intercom unit was also installed that allowed visitors (or parents who had left their key fob at home) to state their business to the receptionist in the main building or to a teacher in the toddler building. A button on each of the intercom units next to the receptionist in the main building and the teacher in the toddler building allowed the staff member to release the electronic lock on the respective door so that the visitor could enter if the staff so desired.

(3) A child wandering out of the buildings and into the busy street: A small corral-like structure made of wood (about 5 feet by 10 feet) with a small gate was built in the toddler building, right inside the main door. When the gate to the corral is opened, a buzzer sounds to remind the teacher to look toward that area, as the little gate has been opened, and either a parent or child is entering or exiting. (This upgrade was funded entirely by the center.)

(4) An angry parent threatening the staff or a teacher: Two video cameras were installed in the two rooms of the front office. All staff were encouraged to meet with parents only in this area until the parent's intentions were discovered. While it was recommended that a monitor be located next to one of the cameras, this upgrade was never accomplished.

(5) Daytime theft of money from staff purses: Three cameras were installed in strategic classroom areas and a digital video recorder (DVR) was installed in a large locked closet within the office area, so that camera recordings could show who entered or exited a particular area when no one else was present.

(6) Robbery or assault on a teacher or parent after dark: Center owner hired a young man to work in the front office after dark and to escort parents and staff to their vehicles. (This upgrade was funded entirely by the center.)

(7) Abduction of a child by an unknown adult: The Sandia team felt that solving the problem of unauthorized access into the buildings would go a long way in solving this problem. Sandia also installed two exterior cameras that would cover the two main exterior doors, so that if an abduction did occur, the cameras could catch it and allow the DVR to record it.

(8) Nighttime break-ins and false alarms: The 20-year-old intrusion detection sensors originally installed in the center were replaced with dual-tech sensors to minimize false alarms caused by items hanging from the ceiling (mobiles, etc.) that often triggered the older-technology sensors.

(9) A child is taken from the facility by a parent who does not sign out: While this type of incident can cause great fear and anxiety for staff on occasion, the ultimate consequences are almost nonexistent. It was felt that cameras installed for other requirements would help support this concern within certain areas of the campus.

(10) Drive-by shooting: Children were taught to immediately lie down on the floor if they heard a loud noise similar to a gun being fired or when a staff member yells a particular code phrase. (This upgrade was funded entirely by the center.)

(11) Abuse of a child by a teacher or other staff member. While this particular issue rated fairly high in the rough priority analysis (see Figure C.1), the pilot project ended up not upgrading the security to address this potential concern. It was felt that any possible upgrade would be too invasive or too expensive to be practical.

Results of Upgrades and Lessons Learned:
Note: The ratings given below are primarily subjective, based on feedback from the staff and the project team. No significant statistics could be produced, given that there was only one pilot center involved in the project.

- Fencing: The staff felt much more comfortable that a stranger in the alley behind the playground could not easily get to a child on the playground.

  Rating: Very Helpful

- Proximity sensors on doors for entry control: Parents really liked this upgrade and the staff felt it was the most important upgrade the center received. Unfortunately, despite repeated calls, the installing company would not return calls when repair to the system was needed. Sandia team members supported the center as well as it could (given no funding was available for this) and the center is currently trying to locate a private source for maintenance. Also, the team felt that the reliability and quality of this type of system in the price range affordable by child care centers was poor.

  Rating: Extremely Helpful (except for times when the system was not working, which was about 4 days over a 6-month period.)

- Small corral-like structure installed within the toddler building: The staff felt good about this upgrade, as they were always alerted to parents and kids coming and going. The only issue mentioned was that the gate/corral/door area can become slightly jammed with parents and kids during peak drop-off and pick-up times of the day. The only outstanding issue for this upgrade is that the gate swings toward the room instead of toward the door, and the Sandia team has recommended this gate be altered soon to swing toward the door.

  Rating: Extremely Helpful

- Digital video recording system, plus cameras in the reception area and in main teaching areas: While the staff does seem to like the idea of these two cameras recording the reception area at all times, it is difficult to say whether the sight of these cameras served as a deterrence and thwarted a potentially angry or threatening parent or whether these types of events would just never have occurred during the life of this project. The cameras in

the main classroom areas were helpful once, when an intrusion detector alarmed one night and part of the playground chainlink fence was knocked over. It was possible to determine why this happened. One issue identified by Sandia that did not result in any negative consequences was that because the monitor for the digital recording system was kept in a locked closet, the center staff never noticed that both the cameras in the reception area ceased working after the first few weeks. By the time Sandia discovered this when checking on the system, the cameras were no longer under warranty and Sandia replaced these two cameras.

Rating: Somewhat Helpful

- Cameras in the parking lot (looking at the two main doors): Only one incident arose during the life of this project in which these cameras were helpful; a parent picked up their child directly off the playground one afternoon without signing the child out. When the child was noticed missing, the staff panicked. The office manager was able to play back the video recordings and the staff was able to see what had occurred earlier.

  On the other hand, over a weekend during the summer of 2005, the bus belonging to the childcare center was stolen and taken for a joyride. At first, the center owner was upset that these particular cameras did not record the thieves during this incident, as the cameras were viewing the front doors. It was pointed out to her that these cameras had not been installed to record this type of undesirable incident – they were installed only to address possible issues involving parents and children entering or exiting the center. (The childcare owner is currently planning on installing an additional camera in the parking lot that will be directed at the bus in the parking lot.)

  Rating: Somewhat Helpful

- Replacement of the center's old intrusion detection sensors: To the team's knowledge, no nuisance or false alarms were generated after the sensors were upgraded to dual-tech sensors.

  Rating: Very Helpful

- Implementing procedures to address a possible drive-by shooting: Luckily, these procedures were never needed for an actual incident, but the kids found the practicing fun. The center owner felt that measures of this sort would rarely be used, but if they were ever needed, they would be invaluable.

  Rating: Helpful