
ACTIVE THREAT
MITIGATION
Detect, Deter, Delay,
Respond and Recover

Page left intentionally blank

TABLE OF CONTENTS

Page left intentionally blank

INTRODUCTION

April 20, 1999, is a day that changed many lives in the United States. It was that day when two students entered Columbine High School in Colorado and began assassinating students at will. It was this event that brought school safety and police tactics back to the training table and dramatically changed the way schools and law enforcement operated. It also brought the term *Active Shooter* into our homes and vernacular. Since that day we have been witness to over 160 active shooter events in the United States, some at places one would never think of like schools, churches, movie theaters, and parks, and some in communities where "that stuff does not happen," like Wakefield (MA), Grundy (VA), Red Lion (PA), and Menasha (WI).

These events are very traumatic for all involved – obviously those directly at the time but also for the first responders and the community as a whole. National experts have been discussing these events in forums, trying to come up with an answer as to why they are occurring. Ideas have been tossed around with regards to gun laws, mental health issues, drug issues, propensity to violence, and so on. So far we have not come up with an answer or solution to prevent these from occurring. One way that that we can have an impact is in reducing the opportunity for these events.

Keep in mind that *active shooter* is becoming a household term, but we are seeing more *active threats* recently. In reality, if a person were to come into a business with a knife, bat, etc. our reactions should be the same.

In the world of crime prevention, we rely on the *Crime Prevention Triangle.* Similar to the fire triangle where it takes three things to create a fire (heat, fuel, oxygen), the same applies to crimes. If one is missing, a fire cannot happen. A criminal needs to have the following in place to be successful in committing that crime.

- **Ability** – A criminal is often savvy and has the tools or know-how to commit a crime. There's not much we can impact here.
- **Desire –** Criminals are going to have that desire. In these active shooter events, it is often some sort of hatred or vengeful act that precipitates this.
- **Opportunity –** This is where we come into play and by doing certain things, we can remove that opportunity or certainly delay it!

Security measures are often classified along the five steps of the security continuum: ***Deter, Detect, Delay, Respond, and Recover.*** In an active shooter situation if we wait until the response step (typically when law enforcement responds to a 911 call), there will likely already be a loss of life. Throughout this guide, we will look at these five steps and ways that they can be implemented in your building. While there is no single, fool-proof method, there are several well-established security principles that can provide a strong foundation for mitigating and reducing these situations.

Page left intentionally blank

ACTIVE THREAT EVENTS

So what is an *Active Shooter* event? The Department of Homeland Security (DHS) defines an active shooter as "an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearm(s) and there is no pattern or method to their selection of victims." Although DHS uses the term 'confined area,' we have started to see these events unfold in any populated area – again looking not too far with the event faced in Menasha, WI at a public park.

In 2014, the Federal Bureau of Investigation (FBI) released a report titled *A Study of Active Shooter Incidents in the United States Between 2000 and 2013* where they researched 160 events in an effort to gather information as to how these events unfold, which may help prevent or mitigate future occurrences. In an attempt to obtain the most applicable data, the researchers excluded any shootings that were clearly gang and drug related and only focused on these 'true' active shooter incidents.

The information graphic on the next page highlights some of the findings, but a big one to take note of is where these incidents are occurring. All too often we hear that these events "don't happen here," or they "only happen in the big city." Of the 160 events, 70% happened in communities with a population of 50,000 or less. An active shooter is the last thing on anyone's mind in all of these communities! That is why we need to raise our awareness of these awful events and have a plan in place to detect, deter, and delay!

Over the past 13 years, the trend has been increasing with regards to the number of these events. Anecdotally, it seems that we are seeing some breaking news story on an active threat a couple of times a month. That is backed up with the stats from the FBI's report, showing an upward trend over the past 15 years. The locations of these incidents are really starting to become varied. Early incidents were primarily limited to workplaces or schools, but in the past few years, we have seen events occurring in shopping malls, movie theaters, parks, and military recruiting centers.

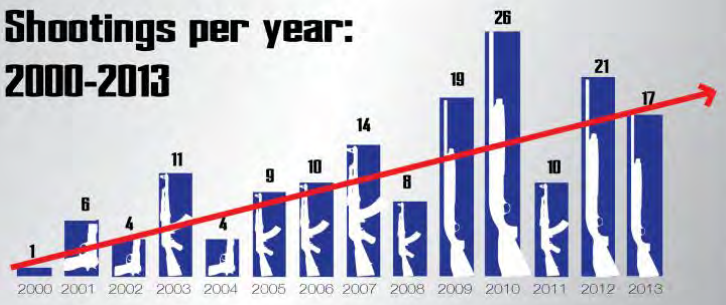
ACTIVE SHOOTER STATISTICS

FROM 2000-2013

IN **160** INCIDENTS...

486 PEOPLE KILLED **557** OTHERS WERE WOUNDED

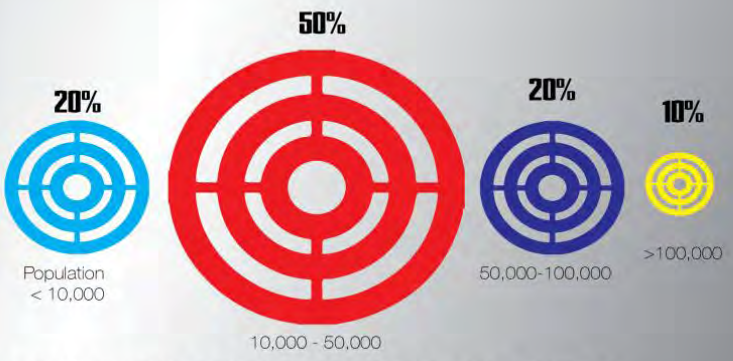
Shootings per year: 2000-2013



WHERE DO SHOOTINGS OCCUR?

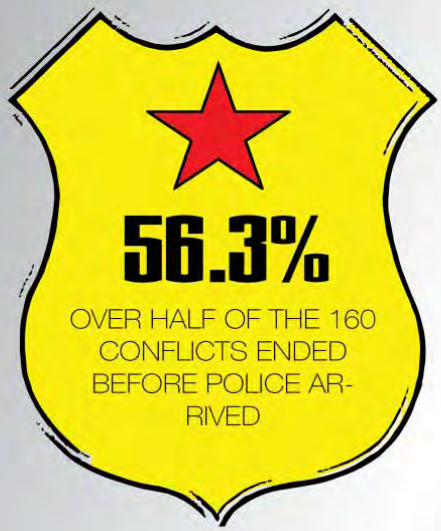
COMMERCE SETTINGS	EDUCATION	GOVERNMENT	RESIDENCES	HOUSES OF WORSHIP	HEALTHCARE FACILITIES	OPEN SPACE
45.6%	24.4%	10%	4.4%	3.8%	2.5%	9.4%

IN 158 OF 160 INCIDENTS, THE SHOOTER CHOSE TO ACT **ALONE**.



CITY POPULATIONS OF MASS KILLINGS*

(1992-2012)



SHOOTINGS HAPPEN FAST.

THE TRAGIC SHOOTING AT SANDY HOOK ELEMENTARY LASTED LESS THAN **5 MINUTES.**

Statistics from the U.S. Department of Justice, Federal Bureau of Investigation Study of Active Shooter Incidents in the United States Between 2000 and 2013. September 16, 2013. fbi.gov

*City population data taken from riskology.co and data from mass killings in the U.S.

We have taken a look into the *what, where, and how often* of these events, but what about the *who?* In 2012 the City of New York Police Department released a report titled *Active Shooter: Recommendations and Analysis for Risk Mitigation.* Unlike the FBI report referenced earlier, the NYPD looked at 230 active shooter incidents between 1966 and 2012. As with the FBI report, the NYPD found that 97% of the shooters were men or boys and almost all of them acted alone. The attackers ranged in age from 10 to 89, but when they looked specifically at schools, the vast majority fell into two categories: 10-14 years old (12) and 15-19 years old (33).

The following graphic takes a closer look at who these active shooters are.

ACTIVE SHOOTERS

Who, How and Why

97%

were men or boys

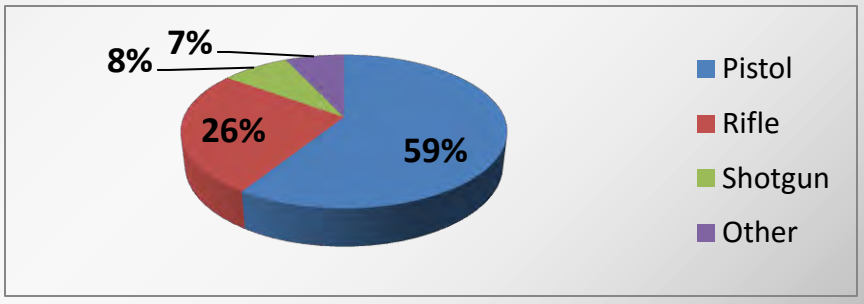
ALL shooters had a perceived or real grievance

However 26% had no connection with the location they chose for their attack!

Most shootings are planned days and weeks in advance and are not reactionary or the cause of a 'mental snap.'

A few shooters have set up *pre-planned defenses* to *trap victims* and *prolong their attacks*.

Most powerful weapon used

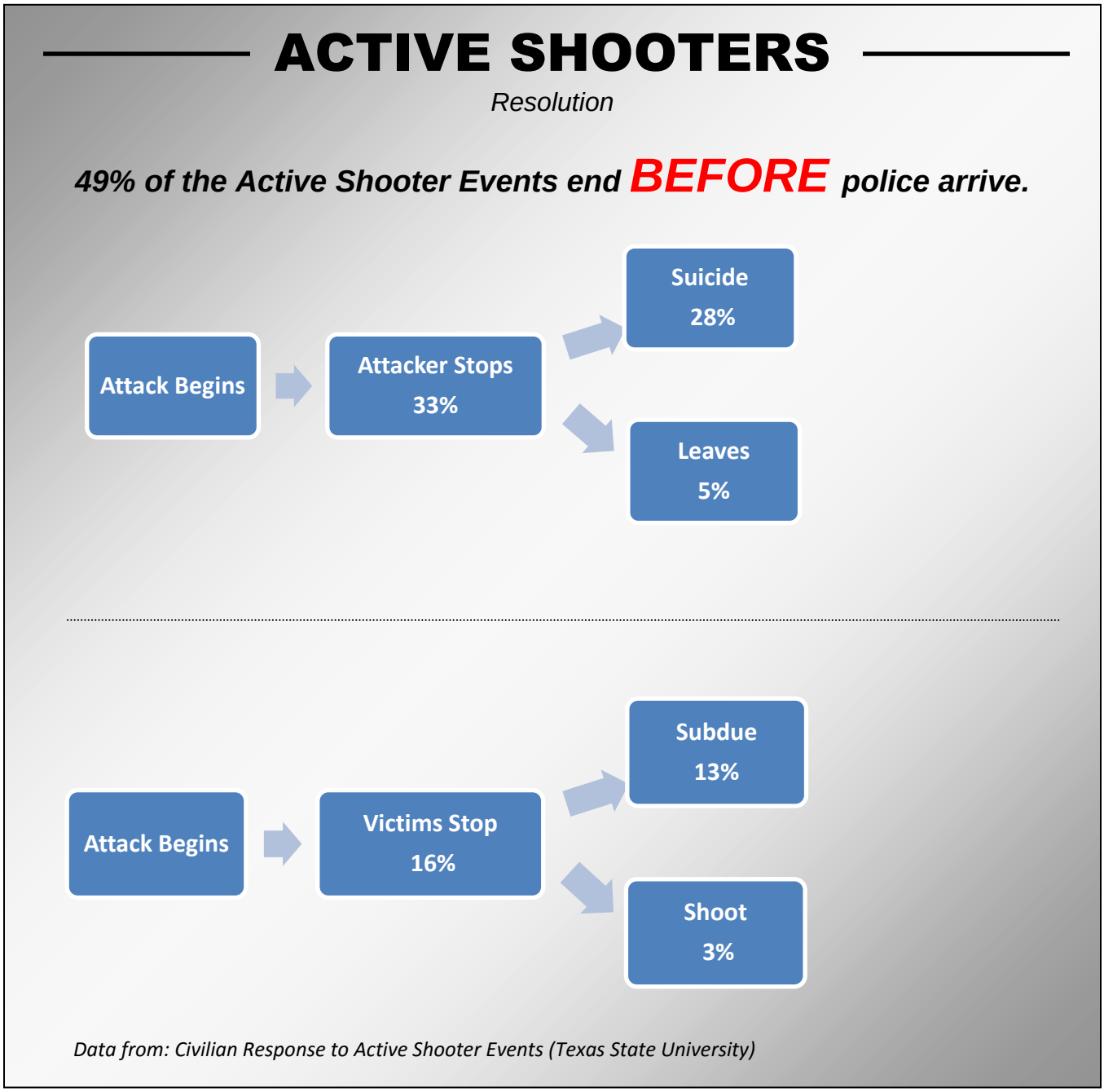


Data from:
Active Shooter: Recommendations and Analysis for Risk Mitigation.(NYPD)

Civilian Response to Active Shooter Events (Texas State University)

As we have learned, most of these events are planned days, if not weeks, in advance. That is because the shooter wants to inflict as much damage and casualties as possible. They know that they have only a short window of opportunity to achieve their goal. The tragedy at Sandy Hook Elementary School lasted only five minutes! On average law enforcement arrives on scene within three minutes. Therefore, the shooter is not worried too much about gaining access to locked rooms or those where the door is barricaded. We will look at that later in this book.

The following two graphics take a closer look at how these events end – both before and after the police arrive.



ACTIVE SHOOTERS

Resolution

51% of the Active Shooter Events end AFTER police arrive.

Data from: Civilian Response to Active Shooter Events (Texas State University)

Let's take a look at these incidents that are specific to businesses.

ACTIVE SHOOTER EVENTS

COMMERCE AREAS

Businesses Open to the General Public

The 44 incidents that occurred in business environments generally open to pedestrian traffic resulted in 124 people killed (including 2 company co-owners in 1 incident) and 181 people wounded (including 1 manager). The most incidents occurred on Tuesdays (10), with others occurring on Fridays (9), Mondays (6), Wednesdays (6), Thursdays (5), Sundays (5), and Saturdays (3).

The majority of the shooters in these incidents were not employed at the location. Specifically:

- 30 shooters (68.2%) were not employed by the businesses, though 7 had a relationship with at least 1 current employee;
- 12 shooters (27.3%), including 1 woman, were employed or previously employed by the businesses (8 current employees [2 possibly facing termination, 1 terminated the day of the shooting] and 4 former employees); and
- 2 or more shooters from 2 incidents fled the scene and remain at large, so their connection to the incident location is unknown.

Businesses Closed to the General Public

The 23 incidents that occurred in business environments generally closed to pedestrian traffic resulted in 69 individuals killed and 73 wounded. In 12 incidents, supervisors/managers and owners of companies were killed (10) or wounded (5). The most incidents occurred on Wednesdays (7), with others occurring on Tuesdays (5), Thursdays (4), Mondays (3), Fridays (2), and a Sunday (1).

These incidents almost exclusively involved employees. In all, 22 of the 23 shooters, including 2 females, were employed or previously employed at the business. The sole shooter not employed by a business had a relationship with a current employee. The 22 shooters who were employees included:

- 14 current employees;
- 4 employees fired the day of the shooting;
- 3 former employees; and
- 1 suspended employee.

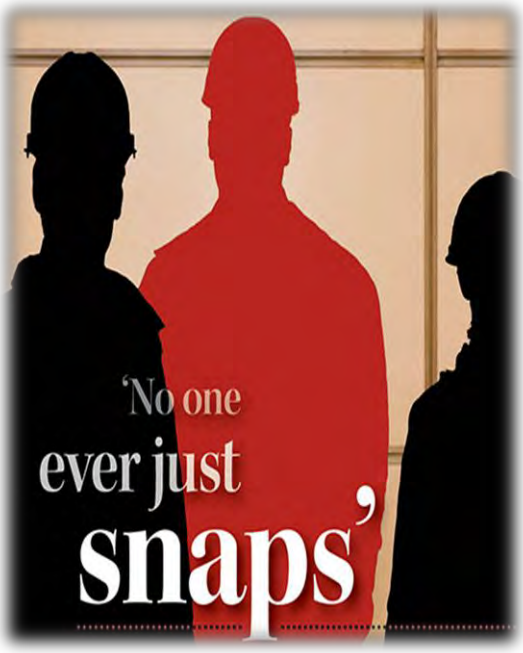
Malls

The 6 incidents that occurred in malls resulted in 17 killed and 18 wounded. It appeared the shooters were neither employed by businesses in the affected malls nor had relationships with mall employees. The most incidents occurred on Sundays (2), with others occurring on a Monday (1), a Tuesday (1), and Wednesday (1), and a Thursday (1).

Source: FBI: A Study of Active Shooter Incidents in the United States Between 2000-2013

Detect

It is quite apparent that the number of these mass shootings in the United States is concerning, but the question remains – *How do we stop them?* Research has shown that no one really can tell when these occur, but in many instances, there were 'red flags' that alerted many that the shooter had some anger or worrisome traits. These are the signs and symptoms that we need to pay attention to and not dismiss.



Research has shown that over two-thirds of the active shooter incidents since 2000 have occurred in either a business or school setting. Of those incidents, half of the shooters had some sort of connection to the location, such as being a student or employee. Therefore, if we recognize some of these 'red flags,' there is a chance that we can intervene and hopefully prevent a future incident!

Who is the Threat?

The first step that we look at in mitigating these incidents is to identify the potential threats. Essentially there are four types of threats to a business which are highlighted in the info box below.

Potential Threats to a Location

Violent acts by criminals who have no connection to the location. This could be the person who chooses the location to commit a robbery, burglary, and so on.

Violence directed at the business/organization by someone associated with it. This could be clients, customers, patients, students, and so on.

Violence committed by employees or past employees. This could be directed to other employees, supervisors of just the business as a whole.

Violence committed by a spouse, relative or acquaintance of an employee. This could result from a domestic disturbance or some other threat.

As we progress into the next chapter of this book, where we address physical prevention tactics and techniques, let's first take a look at identifying and addressing the warning signs of a potential threat.

Current and Past Employees

Recent OSHA data shows that 43% of workplace violence involves current employees. This means that while there are many examples of workplace violence involving fired employees, such incidents are almost twice as likely to be committed by a current employee rather than a terminated one.

We have all heard of the Homeland Security's slogan – ***See Something, Say Something*** and really need to heed that advice. There are so many more sets of eyes and ears out there than there are in law enforcement or positions of authority. If something catches your attention that doesn't seem right, notify someone! Back in 1999, the shooters in Columbine had planted 76 improvised explosive devices (IEDs), of which 30 were detonated, yet none were noticed ahead of time!

The same thing goes with employees and comments or behaviors they exhibit, so we need to follow the slogan *Hear or Sense Something, Do Something* as well. The info boxes to the right cover some of the triggers of stresses for people. Supervisors and co-workers also need to pay attention to a change in work performance as well as changes in attitude.

Friends of the shooter at the Charleston, SC church in 2015 had noticed some odd behavior. His roommate told authorities that 'he wanted to make something spark up the race war again' and another friend had taken one of his guns away from him after he went on a tirade. Neither one of these incidents were passed along to authorities to look into.

We need to instill in the minds of workers that by notifying someone of this behavior does not necessarily mean that the person is getting into trouble. It is just like in school when we were told the difference between tattling and telling!

Triggers of Stress

- Losses, including death, divorce, custody disputes, or job loss
- Emotional and mental health problems
- Drug and alcohol abuse
- Workplace Problems
- Family problems, including childcare, teenage behavior problems, elder care
- Financial problems, including debts or bankruptcy

Work Performance Issues

- Excessive absenteeism or tardiness
- Difficulty with coworkers or withdrawal from contact with others
- Accident/injury prone
- Poor work quality
- Sudden or significant deterioration in work performance
- Difficulty accepting constructive criticism or guidance

Troubled Employee Indicators

- Displaying unpredictable and/or inappropriate behavior.
- Negativity, poor attitude or harsh criticism of others.
- Excessive dwelling on a situation
- Excessive vigilance about minor breaches of rules or procedures.
- Irritability, belligerence, hostility, anger, temper tantrums.
- Inability to get beyond anger, disappointment, sadness, or guilt.
- Strained relationships.
- Isolation, social withdrawal, or secretive behavior.
- Depressed, anxious, or angry mood.
- Fatigue or exhaustion.

Threat Assessment

Now do all of these threats that we see or hear lead to something bad happening? Fortunately, no! However, it only takes that one to make a world of difference. So now that an employee has told human resources or a supervisor about some concerning behavior, what happens next?

Many states are now requiring school districts to form a threat assessment team. Businesses should look at this strategy as well and form a team to look into these threats and make an assessment as to their credibility. Consideration has to be given to making assumptions and immediately going to the extreme so as to avoid 'profiling' or misidentifying an individual.

The threat assessment team needs to be created ahead of time and should contain a diverse group of people. School districts across the country have had a head start on creating these teams and we will focus on that group, but with a few tweaks they certainly can be adapted to the business setting. Note how we use the word *team.* This is truly a team effort and each member brings valuable expertise to the group.

Threat Assessment Team

Core members

- Senior respected and trained member of administration and/or human resources.
- Safety team member
- A mental health professional (counselor, social worker, EAP)
- Local law enforcement

Contributing members

- Immediate supervisor
- Co-workers
- Other outside contacts (social worker, therapists, consultants, etc.)

Retired police Lieutenant Dan Marcou wrote an article for PoliceOne.com on the ***Five Phases of an Active Shooter.*** Nearly every active shooter goes through these five phases, and if these are recognized and attention is called to them, maybe we can prevent these tragedies. Those five stages are outlined below.

Five Phases of an Active Shooter

Fantasy Stage

During this stage the shooter has daydreams of the shooting. He fantasizes about the news coverage. He idolizes other shooters. He might draw pictures of the event and make postings on social media. He may also discuss his desires with friends and enemies.

Planning Stage

In this stage the shooter is deciding on the "who, what, when, where and how" he is going to carry out his action. He may write these down or even discuss them with others. He will plan a location and time that will afford the most victims or target specific individuals. The shooter will also make plans on how to obtain his weapons and his mode of travel to the location.

Preparation Stage

This is the stage where the shooter starts to put his plan into place. He will be obtaining weapons, maybe stealing them from family members or other locations. He may also plant weapons, explosives or other items around his location of attack. This is where the *See Something, Say Something* motto comes into play! Past incidents have shown shooters notifying friends or co-workers not to go to school or work on this particular day.

Approach Stage

This is the stage where the shooter is on his way to the location. This is potentially a very volatile stage, but many would-be shooters have been stopped in this stage thanks to tips or alert officers on a routine traffic stop.

Implementation Stage

This is the actual event. Remember that the shooter has one goal in mind and that is to commit as much carnage in a short period of time and will do so until he is finally stopped either by law enforcement, a citizen, or himself.

Source: Retired Lt. Dan Marcou

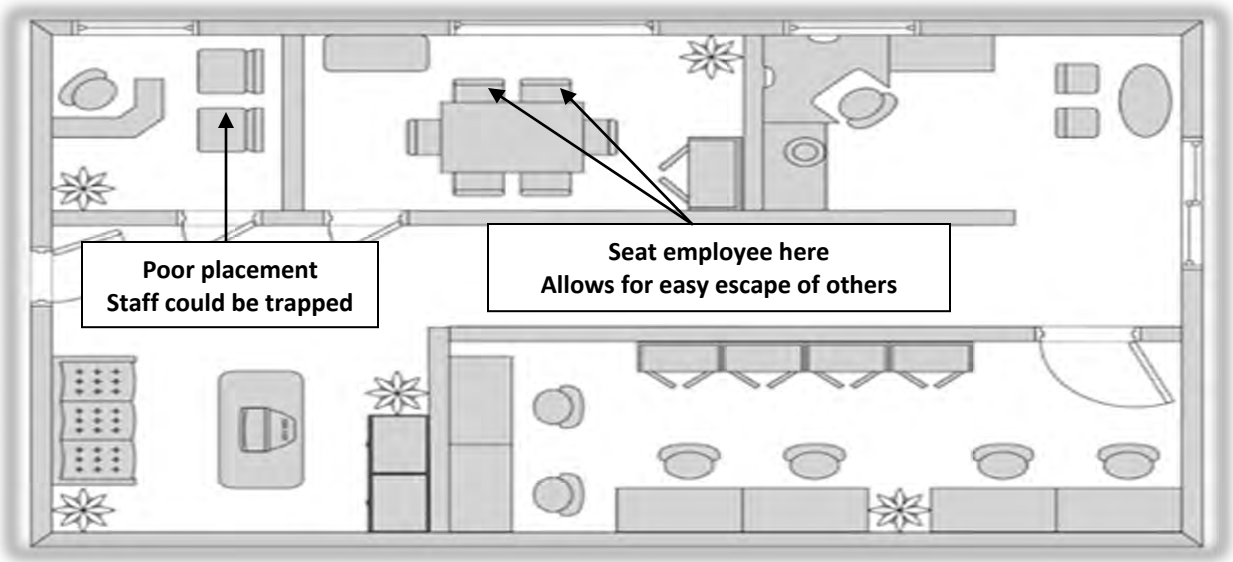
The threat assessment team is only as good as what is brought to their attention! We have all heard of the Homeland Security's slogan – ***See Something, Say Something*** and really need to heed that advice. There are so many more sets of eyes and ears out there than there are in law enforcement or positions of authority. If something catches your attention that doesn't seem right, notify someone! Back in 1999, the shooters in Columbine had planted 76 improvised explosive devices (IEDs), of which 30 were detonated! We have also seen reports of suspicious packages left in areas that have turned out to be explosives.

"Shooters will often say something or post threats online, so we need to follow the slogan *Hear Something, Do Something* as well."Friends of the shooter at the Charleston, SC church in 2015 had noticed some odd behavior. His roommate told authorities that "he wanted to make something spark up the race war again" and another friend had taken one of his guns away from him after he went on a tirade. Neither one of these incidents were passed along to authorities to look into.

Now do all of these threats that we see or hear lead to something? Fortunately, no! However, it only takes that one to make a world of difference.

Disciplinary Meetings

Often these meetings are a negative encounter and there should be thought given to seating arrangements in order to prevent any type of entrapment by the employee and human resources person. Meetings with employees are should not be held in an individual office and rather in a conference room. The conference room should also be close to an exit so that the employee can be escorted outside easily.



Page left intentionally blank

Deter and Delay

Target hardening is a common term that can be found in crime prevention manuals and heard in seminars around the world. This is part of the *opportunity* side of the crime prevention triangle that we discussed in the introduction. Those who wish to cause harm will look at properties that are easy to strike; they look at the risk versus reward, the likelihood of getting caught, or the plan failing.

Target hardening is critical in deterring acts of crime and violence. Shortly after September 11, 2001, the New York Police Department (NYPD) was receiving intelligence that the Brooklyn Bridge was a prime target for terrorists. The NYPD conducted a security assessment of the bridge and found that there were areas of its infrastructure with unrestricted access. Immediately the NYPD put plans into place to secure this iconic structure through a variety of measures, including securing access points through physical measures and increased surveillance.

Unbeknownst to the NYPD, there was a sleeper foreign terrorist in the United States who was making his way to the Brooklyn Bridge to commit an act of terrorism. Once he arrived, he immediately noticed the increased security measures and determined that his plot would not work. His response to his leaders was that the area was "too hot." This is a great example of how Crime Prevention through Environmental Design (CPTED) techniques can play a pivotal role in deterring crime! Those committed to these acts of violence want their plans to succeed. They realize that they have a short time frame to inflict as much damage as possible before law enforcement arrives. The slightest thing to throw a wrench into their plan could be enough to delay or dissuade them and prove to be a lifesaver!

CPTED, or Crime Prevention through Environmental Design, has been an accepted practice worldwide by planners, architects, security, and law enforcement in reducing the opportunities for crime to occur. Many of the ideas that we will discuss have their origin in CPTED, and to better understand this concept, I'd like to introduce you to this concept.

CPTED adjusts the environmental design of a property by using lighting, landscaping and overall design. These adjustments then make the property undesirable to opportunistic criminals. CPTED has been used to combat crimes that might occur in residences, businesses, parking lots, and common areas. These crimes include assaults, robberies, burglaries, and thefts. CPTED has been extremely successful in combating the opportunistic criminal.

The four key principles of CPTED are:

Surveillance – "See and be seen" is the overall goal when it comes to CPTED and surveillance. A person is less likely to commit a crime if they think someone will see them do it. Lighting, cameras, and landscape play an important role in surveillance.

Access Control – Access Control is more than a high block wall topped with barbed wire. CPTED utilizes walkways, fences, lighting, signage and landscaping to clearly guide people and vehicles to and from the proper entrances. The goal of this CPTED principle is to keep intruders out, but also to direct the flow of people while decreasing the opportunity for crime.

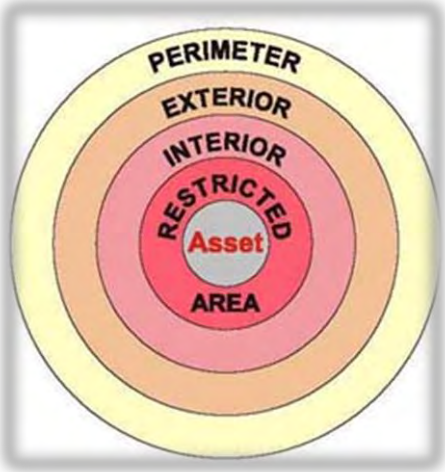
Territorial Reinforcement – The goal of Territorial Reinforcement is to create or extend a "sphere of influence" by utilizing physical designs such as pavement treatments, landscaping and signage that enable users of an area to develop a sense of proprietorship. Public areas are clearly distinguished from private ones. Potential trespassers perceive this control and are thereby discouraged.

Maintenance – CPTED and the "Broken Window Theory" suggests that one "broken window" or nuisance, if allowed to exist, will lead to others and ultimately to the decline of an entire neighborhood. Neglected and poorly maintained properties are breeding grounds for criminal activity and send the message that the owner does not care.

A risk assessment should be conducted on the property to determine the facility's security status. This assessment will identify any deficiencies or security risks and make recommendations to minimize the exposure to those risks. The assessment should be conducted by a crime prevention practitioner who is trained in the application of CPTED and also attended by a representative(s) of the facility.

Each property has layers of security, kind of like the proverbial onion and its layers of skin that protect the core. A property has layers of security that are defined as:

- Perimeter (property border)
- Exterior (building)
- Interior (students/staff)



In addition to the physical layers, there are policies and procedures that work in conjunction with keeping the students/staff and property safe and secure. These are equally as important and should be looked into along with the CPTED principles.

Perimeter

When we look at the perimeter and exterior of properties, the goal is to prevent or at the very least, slow the perpetrators ability to gain access. The use of **fences** around a school or business is a great way of demonstrating territoriality to discourage unauthorized persons from using the property. There are several types of businesses that, due to the nature of their work, have garage/service doors that are left open. This makes it difficult to limit access to the building itself, but we can certainly limit access control through a fence and gate.

Fencing comes in a variety of types and there are several factors to balance in the choice of the fence. The fence obviously should provide adequate protection, yet afford the ability for passersby to see into the area (surveillance). Oftentimes the entire property may need to be secured with a fence. If that is the case there would need to be gated access for vehicles – staff and delivery, trash removal, etc. Keep in mind that there should be some sort of convenience factor to ensure that the gate remains closed when need be. You may want to consider an electronic gate system that can open and close the gate. To allow for multiple users, the gate could be activated via a card reader or keypad.

Similar to fencing are **bollards**. Bollards are small vertical posts that are generally constructed of concrete or steel and are arranged in a path to obstruct vehicles. Oftentimes these are located in front of buildings to prevent a vehicle from striking the building or pedestrians walking. On a trail or roadway that may need emergency or maintenance access, there are removable bollards. Bollards can also be used to protect certain aspects of the building such as utilities. Instead of bollards, facilities have also used decorative landscaping to achieve the same goal.



Lighting provides another important surveillance aspect and a deterrent for would-be criminals. Any areas of use (walking trails, gathering points), parking areas, and the exterior of the building, particularly entrances/exits, should be well lit. Good lighting is one of the most effective crime deterrents! When used properly, lighting discourages criminal activity and enhances surveillance and reduces fear.

There are a couple of things to pay attention to when it comes to lighting. If you have too much light, you may cause more problems than benefits. Too much lighting will produce glare and could blind someone. Take a look at the two photos below, you can see how the light is blinding and hides the person.


Another concern with too much lighting is that it will 'trespass' onto other property. The photo to the right shows how the light is 'trespassing' into the windows of the building. Now granted, you want to light a fair amount of area, but you should remember what exactly it is that you are illuminating. In this photo shown, the light is more than likely intended for the walkway, gathering area and/or parking area – not the second floor of the building!

To address these issues of glare and trespass, a shield or cut off can be used on the light fixture. What these items do is aim or directs the light to the intended area. Many communities are requiring the use of full cut off lighting in their zoning regulations; therefore we recommend that you check with your local municipality. The photos below show the difference between the two fixtures.

So how much lighting will we need for the area? The lighting package will tell you how bright and how much the light output is. The amount of light coming from a light source is *luminous flux (lumens)* while the amount of light falling on a surface is *luminance (lux).* A general rule of thumb for a parking area is the height of the pole multiplied by 4 will give the distance the light poles should be apart. For a building, height of the light multiplied by 6 will give you the distance they should be placed apart.

Sample Lux values	
Clear night, no moon	.002 lx
Clear night, full moon	.27 – 1 lx
Living room	50 lx
Sunrise/sunset	300-500 lx
Overcast day	10000 lx
Daylight	10,000 – 25,000 lx
Direct sunlight	32,000 – 130,0000 lx

When installing lighting, plan ahead! If planting trees or other landscaping, think about what may happen when the tree begins to grow; will it block the light fixture, rendering it obsolete?

Types of Lighting

- **Incandescent**

  These are the most common lights in our homes. Incandescent lights do not have a long life span and produce quite a bit of heat.

- **Fluorescent**

  Used in both home and commercial settings. Three to four times more efficient than the incandescent and lasts up to ten times longer. Also has a low heat output.

- **Pressurized sodium**

  These are most commonly used as street lights and Exterior lights at businesses. They cut through fog well but have poor color rendition due to their "yellowish" light.

- **Metal Halide**

  These are often found in gymnasiums or warehouses. They take a bit to 'warm up' but emit a white light that is excellent for color rendition. However, they have a higher initial cost than the sodium lights.

- **LED**

  LED lights have a high initial cost but are extremely cost efficient and have a long life span. They emit a white light and do not have the warm up time that metal halide does.

Color Rendition

Daylight

Low pressure sodium

LED

High pressure sodium

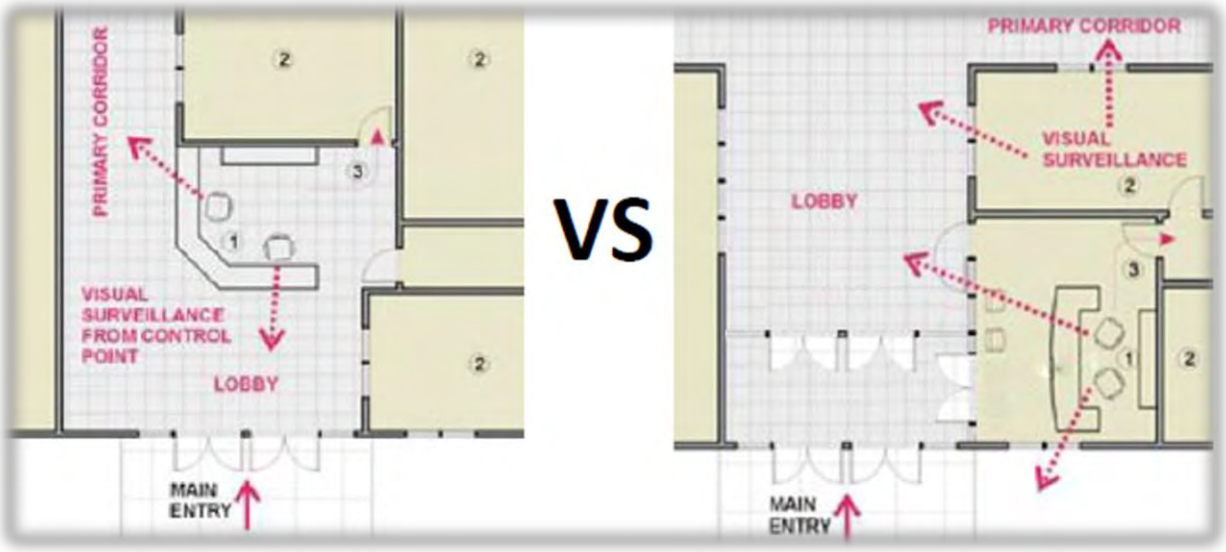
Metal Halide

Building

This is the second layer of security of a facility, and we still employ the bollards and lighting in this area, but now we look at access control more closely. How are people accessing the building? Given the nature of society, buildings are becoming less and less 'open' than in the past. For the general public, there really needs to be limited access points. Especially in a school or office setting, visitors need to be directed to a main point of entrance and greeted by someone.

We also need to make sure that our ***buildings are marked properly and give direction*** to the visitors. This is a part of the territoriality principle in CPTED. There are certain areas of the property that are off limits to visitors or reserved for staff, and we need to clearly mark that and give directions.

Schools, for example, are creating areas where the visitor is forced to go into the office prior to gaining access to the rest of the school; this is called a ***'layered approach.'*** Office buildings have a similar approach where the guest encounters a receptionist first. Ideally all other access should be secure until they are vetted by the receptionist or office staff. Examples of the two variations are shown below.



By having a single 'public' entry point helps ensure that only authorized people are getting into the building. Staffed entrances and greeters send a message to would be criminals that they are being watched. Have you ever been greeted at Walmart or said 'hi' to by a grocery store employee? Not only are those pretty good examples of customer service, but also a way of incorporating the CPTED practice of surveillance!

Invariably the ***receptionist or office staff*** is going to be part of our "front line' of defense, and we need to make them feel as comfortable as possible. Many businesses want that 'open' feel in their lobbies or reception area, so we need to find a balance between that and the level of security. A business could have a windowed office like the photo to the right. This area has a considerable amount of glass giving the open feeling and allowing surveillance, yet making it secure enough that it would be difficult for the intruder to get through and also allowing staff to exit quickly.

Another option is similar to what is seen in financial institutions with teller areas. Even though there are no full physical barriers with this, there is enough of a barrier that would make it difficult for a person to jump over or through, and at the very least, delay that intruder.

Some businesses have gone the way of eliminating a receptionist; however you can still maintain the security through the use of a phone where visitors are directed to a phone and list of extensions to call for their contact person. The employee then meets with the visitor and has them sign in and obtain a visitor badge.

As we encourage the use of one main entrance that is staffed, we need to ensure that the other entrances and access points remain secured. All too often, when law enforcement visits various buildings, we see ***doors propped open or not fully secured***. Sometimes this is done as a matter of convenience (air flow, deliveries, etc.) or there are maintenance issues that impede the door from closing completely. Correcting the issues in the photos below is relatively easy, and if the access point needs to be open for air flow, there are screened coverings that can be installed that will accomplish both air flow and security measures.

Now let's take a look at the types of access points that we have on our building. Typically these consist of ***doors and windows*** and we need to make sure that they are adequately protected to deny and delay an intruder. Doors come in a variety of types, most often in a commercial setting they are constructed of some type of metal. Exterior doors need to be of a stronger construction than interior doors. These are typically a solid construction.

Along with the type of door is the locking mechanism. Retail, office, manufacturing and so on should have commercial grade locks and hardware mostly due to the amount of use as compared to a residence. The following info boxes below show the difference between the three grades of locks.

Grades of Locks

Grade 1	Grade 2	Grade 3
-Heavy usage -Has built in features to resist manipulation and/or physical attack. -Tested for 320,000 openings.	- Commercial use -Have some resistance to physical attack and fire resistance. -Tested for 160,000 openings.	-Residential -Do not need to have physical resistance or fire resistance. -Tested for 80,000 openings.

Types of Locks

Keyed

- Uses a key to open. Locking mechanism is a either latch or deadbolt lock.
- Should maintain an inventory of who has keys.

Cipher Lock

- Uses a combination to open the door.
- Can be set to only work during certain times of the day.
- Can be changed should an employee leave.
- A downfall is that the code can be given to others

Device Locks

- Often used in machines in a factory as a safety measure.
- Can also be used to prevent the theft of items such as computers.

Electromagnetic Locks

- These are extremely powerful locks that have a holding force of 600 to 1200 lbs.
- There are two types – *fail secure* (remains locked when power is lost) and a *fail safe* (unlocked when de-energized.)

Keyless card

- Reprogrammable and often used in hotel operations.
- Locks are stand alone or networked that can log employee number, door number, and time of access.

Proximity Card

- Part of an automated and networked perimeter control system and have the capability of recording employee, door location and time of entry exit.
- Can be easily deactivated should an employee leave.

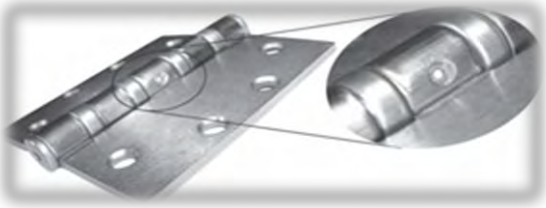
Biometric Controls

- Rely on fingerprint or biological info to open doors.

There have been occasions when a criminal will use a tool to manipulate the door latch to gain access to the building. If you have a door that may allow that to happen there are latch guards that can be obtained relatively inexpensively. You may also have a door that is an 'egress only' door, if so – consider removing any hardware on the exterior to limit the chances that it could be compromised.



In addition to the locking mechanisms, the hinges on exterior doors should have security features. If the door hinge is exposed, a would be criminal could remove that hinge pin and remove the entire door! To defeat this from happening, we recommend installing security hinges that have a set screw in the bolt preventing it's removal.



In addition to encouraging employees not to prop doors open, we need to be aware of people sneaking in or circumventing the security measures. Here are a few ways that is accomplished:

- **Piggybacking -** occurs when an authorized person gains access to a secure area and allows others to follow – by holding open a secured door.
- **Tailgating** - occurs when an unauthorized person enters a secure area by following closely behind an authorized cardholder.

Windows and glass is the next area of access points to a building. Glass affords excellent surveillance capabilities but is not as secure as metal doors. Many entries to buildings are through windows and/or glass doors. The photos below are from Sandy Hook Elementary School where the shooter gained entry to the office area of the school through the windows.


Glass originally was not designed to resist windblown debris, explosions, vandalism, forced entry or anything else that can put stress on it. When broken, this glass would produce lethal shards or fall in large pieces. To prevent this, legislation was passed in the 70's mandating the use of tempered glass. The mandates however only cover particular areas such as: floor to ceiling windows; glass doors; panes of glass next to doors; and glass areas next to heavy pedestrian traffic.

Types of Glass

Standard

- Inexpensive to produce. Weak glass and will not slow down or stop entry.
- Breaks into large and sharp pieces.

Tempered

- Stronger than standard and breaks into small pieces.
- May slow entry but not by much.

Wired

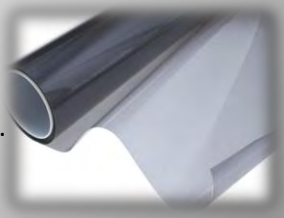
- Primarily a safety related product used in fire doors.
- Will keep glass in place but still breaks in large pieces.

Laminated

- Two layers of glass that are bonded together by an interlayer of polyvinyl.
- Often used in aircraft and automobile windshields.
- Will remain in the opening upon breakage.

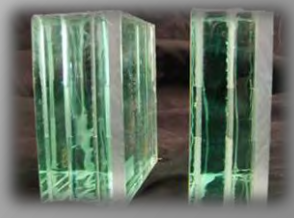
Security Film

- Film that forms a barrier which delays the penetration of the glass.
- If penetrated, the opening created is going to be the size of the device used to create it.
- If used make sure to have the film installed into the window/door frame.
- Security film also helps with heating/cooling.



Bullet Resistant

- Very costly.
- Also should have ballistic framing, bullet resistant doors and walls.



Interior

Ideally we work to prevent the access of unauthorized persons, and that is what the beginning of this chapter worked upon. However, it is what is inside of our buildings that are most important!

When it comes to prevention, the main goal is to *prevent* something from occurring. ***Alarm systems*** can serve that purpose as well as serve as a way of notifying the authorities of an intrusion or problem. There are two types of systems:

- **Monitored** - an outside agency monitors the alarm and notifies key holder and/or police of alarm. Can be silent, audible or a combination of both. This requires a monthly fee for service. Be aware that these alarm systems are often tied into your phone lines to communicate the alarm. Many phone providers now rely on computer modems for transmission. Make sure that your modem has a battery backup in the event of a power failure.

- **Non-monitored** – typically is an audible alarm that deters the criminal and also warns anyone in the immediate area.

Types of Alarm Sensors

- **Door/Window Contacts –** These are small magnetic contacts installed along the opening of either the door or window. The alarm is activated when the magnetic field is broken between the two sensors.

- **Motion Detector –** These are small alarms with a sensor that will detect any motion. Earlier versions of these alarms would activate with any type of movement – such as balloons blowing when an HVAC system kicked in. Current versions are pretty accurate and are able to distinguish the difference between an 80 pound child and 80 pound dog!

- **Glass Breakage** – As we read earlier, glass can be a pretty weak access point and enticing way for criminals to get access to our building. There are sensors that can detect the sound of breaking glass.

- **Panic Alarm -** This could be a system that is monitored or tied into an internal notification system whereby a message or alert is conveyed to someone internally. There are panic alarms that are a hard wired button system and others that are portable.

Security cameras can be used to monitor activities in and around the building. Areas for cameras could be at points of entry, hallways, parking lots, and really any area that could afford extra monitoring. Many times these cameras are used after the fact unless you have someone monitoring the cameras all of the time. Because they are used after an incident and for evidentiary and investigative purpose we want to make sure that the cameras you select are worth the investment.

The main question to answer is *what am I hoping to capture on film?* Once you have that answer, then you can work on selecting the appropriate camera and system.

Security Camera Considerations

- **Lighting –** The camera needs to be able to see what is being filmed. If you have an area that has periods of low light, you are going to need an infrared camera.

- **Quality –** We have all seen the various police television shows where they are able to zoom in and obtain a license plate or even more. The ability to enhance an image is only as good as what is originally obtained. The higher the megapixel of the camera, the better the image and the greater area that is covered.

In this example the 2.1 megapixel camera has a much greater ability to clearly zoom in on the person.

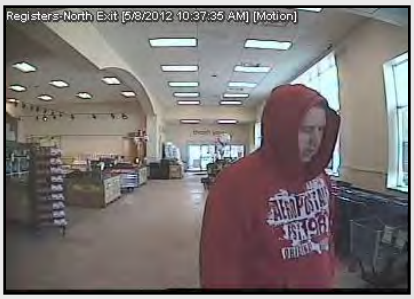
In this example the 2 megapixel camera has a much greater area of coverage that is equal to 6 analog cameras.

- **Data Storage –** The amount of storage needed is going to be dependent on the size of the image (megapixels) and how long you plan on storing the image. Give consideration to storing the data at an offsite or cloud location to prevent someone from tampering with the server. Some systems also have the capability of only recording when the camera detects motion, which may be a way to save on data storage.

Security Camera Considerations

- **Placement –** Make sure the camera is picking up what is intended. In the retail setting, we see surveillance all too often from a camera placed high in a corner. Many criminals will go to lengths to hide their appearance from cameras, and the placement of these cameras makes any footage useless.

These two photos show the difference between a high mount and one that is more at eye level.



If you choose to identify cars coming onto the property, you are going to want to limit access control and set a camera that is specific to capturing license plates, which is going to be slightly higher quality than one that captures people in a hallway.

- **Camera Types –** There are many types of cameras and housings available which are all dependent on where you are installing them.

Another camera type that has become popular in recent years is the panoramic camera. These cameras have the ability to capture an area in a 360 degree, 270 degree, or 180 degree field of view.

- **Portable Cameras -** There may be times when you are concerned about certain areas that don't necessitate the installation of a permanent camera, maybe the funding is unavailable, or it is something that you need addressed immediately. Wildlife or trail cameras have become more common in security applications.

In the event of a crisis, we need to ensure that our staff and visitors are well protected. In the next chapter we will look at the response portion of a critical incident but here are some ideas that can employed to further harden the criminals attempt to gain access to our most important assets!

- **Office Doors –** Consideration should be given to having locks on office and room doors. As we have learned, often times something as simple as a locked door will keep the threat moving on.

  It is also a good idea to have interior office doors closed and locked during non-use hours, as it limits the access to those unauthorized visitors. It also helps to expedite a search of the building by law enforcement in the event of an alarm or burglary.

- **ID Cards –** Many businesses are not open to the public therefore all visitors and staff should be readily identifiable by a ID badge. Given the large number of employees in some companies it is impossible for staff to know every other employee and the ID badge signifies that employee status to one another. It is recommended that ID badges be issued to all employees and that they wear them, in a visible spot, at all times.

  Often it is difficult to get employees buy in to wear the badges. Some companies have done unique things with the badge such as tie them into the card reader system and/or time card system or have rewarded employees with lunch if there is compliance.

  Visitors are required to sign in and obtain an ID badge. Staff should be trained to "challenge" those that do not have an ID badge. By challenge we are referring to asking that person if they need any assistance and directing them to the area that they are looking for and ensuring that they check in. These visitors should also be accompanied through the facility by a staff member.

- **Numbers on Exterior Doors -** When emergencies occur, the rapid response of emergency workers to the incident can be critical. There are some businesses that are large and have dozens of doors providing entrance and egress to their buildings. During an emergency it may be necessary for responders to gain access through the door closest to the emergency scene. Numbering external doors can have great value to the emergency responders and will also assist your students and staff in acclimating themselves to door locations in case of an emergency.

  All exterior entrances that allow access to the interior of the building should be numbered in a sequential order starting with the main entrance (office door/public entrance). The main entrance should always be #1.

  Subsequent entrances should be numbered in sequential order in a clockwise manner.

RESPOND

In the previous chapters we have discussed how to identify those potential threats and steps that we can take to detect, deter, and delay those wishing to cause harm. Unfortunately there are those instances where the threat is going to gain access to our building. That is why this chapter is critical in mitigating injuries and loss of life.

Research has shown that on average it takes law enforcement about three minutes to arrive at the scene of an active shooter. If you think about it, three minutes is pretty darn fast – it would take that long for most of us to get up and walk out to our car. However, if you are in a critical situation, those three minutes can seem like an eternity! It was what we, as citizens, do in those three minutes that could potentially be lifesaving!

Notification

When a threat presents itself, we need to notify others! There should be some sort of ***notification system*** in place to notify staff and students of an incident and lockdown. This can be done via a paging or telephone system. Don't limit the system to only being in place in the office or main part of the building. You may be faced with an emergency in other parts of the building that are a distance from the main office. Some schools and business also utilize two-way radios to communicate with other staff throughout the building. This is a cost effective method that can be implemented rather quickly. Also think about some redundancy in the system in case plan 'A' fails!

In some businesses there may be areas that are loud, some even requiring hearing protection for not only employees but visitors. With that said, a system of a voice only notification may not be entirely sufficient. In addition to the voice notification some type of flashing light or signal could be employed alerting those employees in a noisy environment to stop and listen to the message.

Keep in mind that the *appropriate* warning system be utilized. In the event of an act of violence, employees should not be using the fire alarm system as a warning mechanism because that will generate a different type of response than what should be utilized. Employees and staff are preconditioned to take a certain route and go to a certain location in a fire drill. The same applies to the type of emergency response – public safety is responding to what they perceive as a fire.

So now that you have a system in place, what exactly is it that you are communicating? For those who have been in a critical situation, you know the chaos and stress levels are extreme. That is why you need to have a clear and simple message that can be easily understood. We have found a great program called the Standard Response Protocol that was created for schools but can really be adapted to any setting.

The Standard Response Protocol is a uniform response to any type of situation such as a fire, active shooter, weather, accidents, intruders, and so on. The protocol is not based on an individual situation but rather the response to any given situation. The premise is simple, there are ***four specific actions: Lockout, Lockdown, Evacuate, and Shelter.***

Standard Response Protocol in Action

- **Lockout** is followed by the directive *"Secure the Perimeter"* and is the protocol used to safeguard students and staff within the building.
- **Lockdown** is followed by *"Locks, Lights, Out of Sight"* and is the protocol used to secure individual rooms and keep students quiet and in place.
- **Evacuate** is always followed by a location, and is used to move students and staff from one location to a different location in or out of the building. *"Evacuate to the bus zone."*
- **Shelter** is always followed by a type and a method and is the protocol for group and self protection. *"Shelter for tornado; drop, cover and hold."*

In the school setting we tend to see *lockdown and lockout* used interchangeably. There is a difference between the two. A ***lockout*** situation typically means that something is happening outside of the building such as a tactical situation nearby. In a lockout, access is tightened to the building and those inside are kept inside until the situation is resolved or an all clear is given. Business can continue as usual inside of the building. A ***lockdown*** is when you have a credible threat inside of the building. That is when normal activities stop and staff and students take precautions.

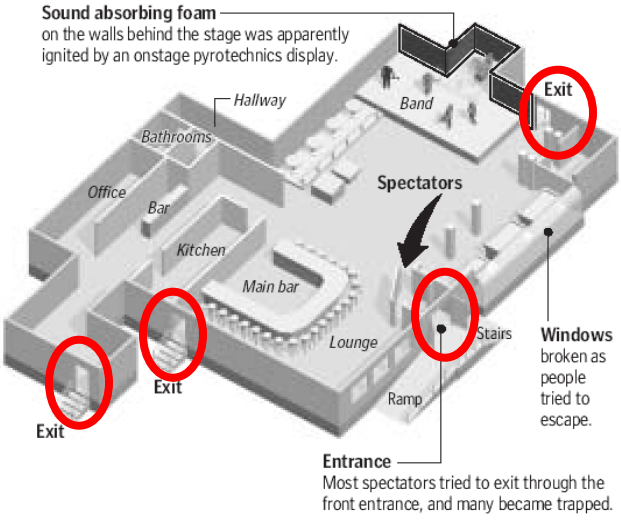
Employee Response

There has been quite a bit of research conducted on these active shooter events, and all have agreed that the shooter's intention is to cause as much harm and damage as possible. The shooters are well aware that they have a small window and know that law enforcement will be arriving in a short time. Department of Homeland Security research has shown that the active shooter incident lasts just over 12 minutes. As we look into what our response options are, we need to first look at the human psyche in a critical incident.

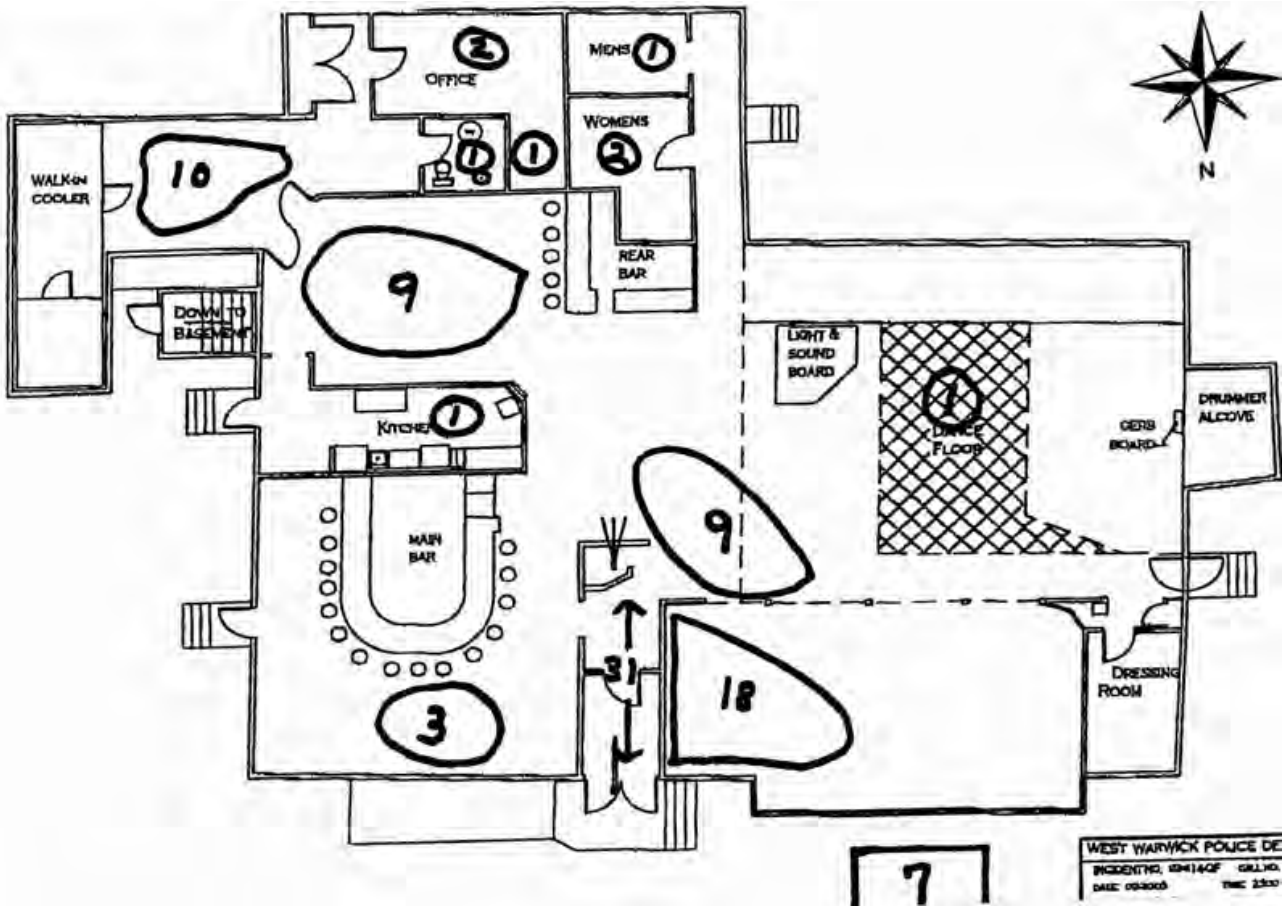
For the most part, we do not want to believe what is occurring…if we don't acknowledge it, it isn't happening. Take a gunshot for example; there are times when someone hears a gunshot, a lot of the time it is immediately dismissed as being a firework. We need to look at the situation and think for a minute if this makes sense! *Wait a minute…it is October and we are in the middle of an office or school….why would there be firecrackers going off?* The quicker we can recognize the threat, the quicker we can formulate our action step.

The next part of the human psyche is the tendency to follow others. There was an interesting study several years ago in Great Britain where a subject was feigning to be injured or ill and was lying in a public park. The goal was to see how long it would take for someone to offer assistance. Time after time, individuals would walk past the subject – some taking a glimpse at him and others ignoring the situation. It wasn't until one person would stop to offer assistance that others would follow.

In addition to following another's lead, we need to make sure that we are aware of our surroundings or have *situational awareness.* An example of this occurred back in 2003 at what is known as the Station nightclub fire where 100 people died. In this case, the band Great White was playing a concert when a fire broke out causing people to flee the nightclub. A good majority of the crowd not only followed others but were focused on leaving the same way they entered, unaware of other potential exits.



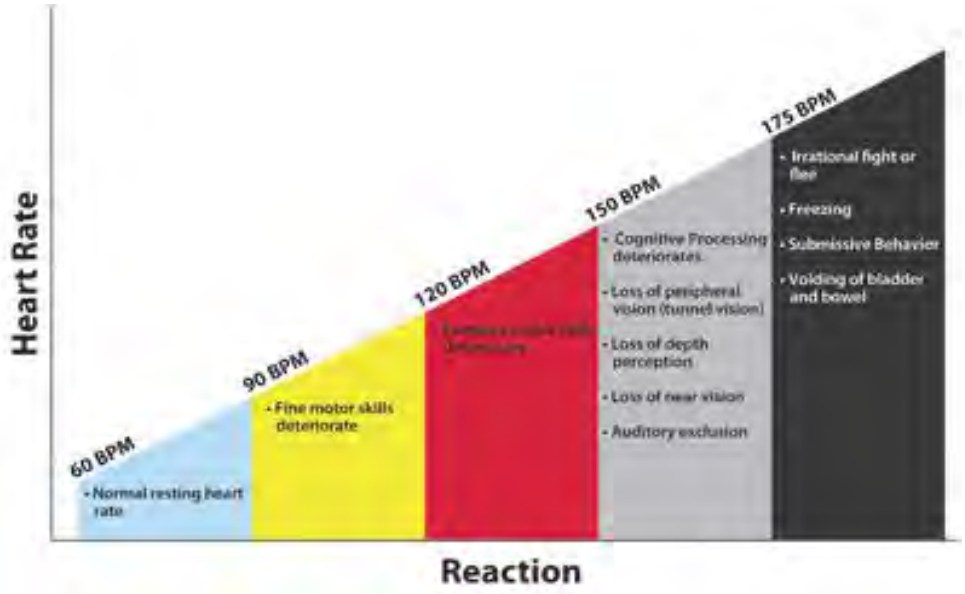
The image below is from the investigation and shows the club and where the exits were along the number of deaths in each area. Note how a majority of the fatalities were in that front entrance where the club goers arrived through.



This is a good example of having ***situational awareness.*** Wherever you are, you should be aware of your surroundings and have a plan if something goes awry. It is a relatively easy concept to employ at work in that when you return to your office or classroom, take a look around and think, "*What am I going to do if something happens?"* If you have that plan formulated in your head and have thought about it, there's a good chance that it'll go like clockwork in the event of crisis!

This is something that police officers have been trained in for the past 50 years. When a new officer is paired with a seasoned training officer, each call for service is evaluated and discussed. For example after a routine animal complaint, the training officer may ask the rookie what he/she would have done if the man had come down the stairs with a knife. Regardless of the call, officers need to be cognizant of officer safety and have an "out" formulated in their mind, regardless of the call or situation. This is a tactic that is a potential lifesaver for an officer and can certainly be for anyone else.

Speaking of tactics, an active shooter event is going to be chaotic and very stressful, quite possibly the most stressful situation you will ever encounter. Research has shown that the higher the ***stress level***, the less clear our thinking and reactions become. This is another situation that those in the military and public safety encounter and train for. The chart below shows the comparison between a person's heart rate and the effect on their reactions.



You can see that the higher the heart rate, or stress level, the diminished reactions a person has. One way to combat this is through a technique called ***combat breathing.*** Most of us are probably familiar with this, but maybe not under that terminology. How combat breathing works is when you start to notice an increase in heart rate and stress, take a moment to collect yourself and take a few deep breaths, in through the nose and out through the mouth. What this does is slow your heart rate and allow you to return back to those blue and yellow, or even red levels, where we still have most of our faculties!

So….what is our plan? That tends to be the $64,000 question from everyone. The answer is….*it depends!* There really is no fail-proof plan and it all depends on the situation and what your position is relative to the event. There are essentially three options – ***Avoid, Deny, Defend –*** and not necessarily in that order!

Avoid, Deny, Defend

- **Avoid -** Ideally, we want you to avoid the situation if you can do so carefully. So what does that mean? If there is an escape route – get out! That may mean breaking a window, but a broken window is easier to replace than a human! Remember situational awareness….*where are the exits?* Also, don't worry about your belongings – get out! This is another one of those actions that we do repetitively and tend to go on auto pilot.

- **Deny –** If you can't get out safely, you are going to need to find a place and hide. Now we don't want you to hide and pray. You are going to need to take some defensive actions and deny the person from entering. Remember that the shooter has a short amount of time to inflict as much chaos as possible so something as a locked or barricaded door is going to cause them to move on. This is again where that situational awareness comes into play and having that plan... *what am I going to do?* Make sure that you are hidden and that your phones are silenced and that you are quiet.

- **Defend** - This is in the event that you are face to face with the intruder and your life is in danger! Whether you are alone or in a group and this is what you are faced with, remember that you are in this 110% as it is a fight for your life; you need commit. Act with aggression and use some improvised weapons.

After reading the Avoid, Deny, Defend tactics there typically are some questions that arise.

What about accountability? We have young students, disabled people, etc.

Ideally accountability is great, but if you think about it, do we really have accountability all day long? Students are in different classes, meetings or bathrooms at all times during the school day. It is even worse for adults in business settings. If you recall, the shooter is going to pre plan his event at the most opportune time to strike as many victims as possible. This could be in between classes, lunch time, or during a student assembly. How are we going to maintain accountability in those events? This can give us some ideas for when we may want to have a lockdown drill!

Small children are another concern that arises. Kids are smarter than we give them credit for. The tragedy at Sandy Hook Elementary School provides us with an example of students using the *avoid* tactic and running away. Some of those students ran into the woods while others ran to friends homes in the area. It took awhile for those students to be located, but eventually they were all accounted for and all right, which is our main goal! At a recent shooting at a park in Menasha, WI, two young children whose family was shot continued to run to the family's van. The children told a Good Samaritan that their parents were shot, the park was not safe, and they wanted to go to the police department.

Invariably there may be a situation where the condition of the students or adults is not conducive to leaving and that is where the *Deny* tactic is crucial. Through situational awareness, you can have a plan in place.

What about concealed carry? My work will not allow me or anyone to have a gun!

This is a highly debated question! As a law enforcement officer, I can attest that just carrying a gun is not the"end all be all." If you are going to carry a weapon, you better be trained in its use – and not just periodically shooting at a target, you need to have some combat training! Bad guys move and do not stand still and you need to train for that. The same goes for what accessories you are carrying. Officers carry multiple magazines of bullets in case you encounter a malfunction with your weapon. By having another magazine, you can quickly overcome one of these and continue with the gun battle. The type of ammunition also has a bearing on your tactics. The National Rifle Association advocates that a good guy with a gun will stop a bad guy with a gun, and that is certainly true. However, that good guy better be adequately trained!

Training

Now that we have some idea how we are going to respond, we need to put those actions to the test. Fire drills are conducted routinely in schools and businesses across the country. These were put in place after many severe fires occurred in schools during the early 20th century. One significant fire happened in Chicago in 1958 at the Our Lady of the Angels catholic school where 92 children and three nuns perished in the blaze. Monthly fire drills were put in place in schools and businesses across the country after that, and coupled with an increase in education; deaths and injuries as a result of fires have significantly decreased.

Unfortunately in today's world, we need to start implementing the same when it comes to active threat and crisis situations. Businesses need to prepare in the event of an active threat. Schools are starting to have lockdown drills in addition to tornado and fire drills. In the business world we can start preplanning as well. Sometimes it might be difficult to conduct a drill with employees but we certainly owe it to ourselves to have discussions with employees about how to respond to this.

One idea that is certainly worth looking into is to pay attention when these happen in the United States and ask ourselves – *what would we do here?* These incidents can be used as a reminder to 'dust off' the emergency plan and see if we are prepared and how it would be handled at our business. It'll help keep our response on the forefront of our minds and that will undoubtedly help things in the event that you are faced with it.

In addition to the periodic lockdown drills during the school day, many schools and businesses are opening their doors to work with their local law enforcement agency and conducting a more active type of drill. These tend to be much more realistic, and consideration needs to be given if you want to have students present during the drill.

The active threat training exercises normally involve officers and the use of role players and simulated firing of weapons. These are a great way to work with your local law enforcement and see what such a response entails and will afford you the opportunity to ask questions specific to your building and area!

Information and Access for Emergency Responders

The safety of our employees is our utmost concern, and we need to alert law enforcement and other emergency responders. If we heed the advice to secure access to our building, we need to ensure that those coming to help have access. Many law enforcement agencies across the United States are preplanning with schools and businesses to obtain that access and any necessary information ahead of the event. In the past there have been crisis boxes in the office that contain keys, maps, and other info.

Crisis Box Contents

- Aerial photo of campus
- Map
- Campus layout
- Blueprint of buildings
- Employee roster
- Master keys
- Fire alarm/sprinkler turnoff procedures
- Utility shut-off valve locations
- Gas/utility line layout
- Cable/telephone shut off
- Evacuation sites
- Attendance list for day
- Emergency resource list
- First aid kit locations

However, as noted, these are chaotic situations, and there may not be time or access to that crisis box. With the advent of mobile data computers (MDC) in squad cars, many agencies are obtaining floor plans and real time access to surveillance cameras and loading them into the MDCs. Some schools and businesses have also provided access to the "Knox Box," which is a fire box located on many buildings that allow firefighters access to the building's keys. Some are also providing law enforcement with an access card for those with card readers installed on doors.

Page left intentionally blank

RECOVERING

In the event that you are faced with an active shooter or crisis event at your school or business, more than likely it will be the most chaotic and traumatic event in your life. Emotions and stress levels will be high, and we need to have a plan in place to help guide us through this.

Reunification and Family Assistance

The scene is going to be extremely chaotic with a security perimeter set up, and the last thing needed is frantic loved ones trying to gain access to the area. In pre-planning and table top exercises, team members can seek out potential locations for reunification and family assistance centers. In the event of a crisis, there should be a business liaison assigned to assist the incident commander with this endeavor. This area is where many of the items in the crisis box come into play, such as employee rosters and emergency contact info.

When selecting a reunification site, to avoid any further congestion the location does not necessarily have to be onsite and could be at a different location. Families are going to be in distress and needing comfort. Ensure that there is enough staff, counselors, and resources available such as food, beverages, sitting areas, and tissues.

Psychological Trauma

These events are very traumatic and affect a wide variety of people, such as survivors, witnesses, loved ones of victims and survivors, emergency responders, neighbors, and community members. One thing to keep in mind is that there is no "one size fits all" approach to intervention – it must be tailored to the phase and nature of the incident. Certain traumatic events, such as an active shooter event, present an even greater mental health challenges than other forms of disaster. In that immediate stage, having grief workers and supporters at the reunification center is crucial. This is the place where families and loved ones are going to gravitate for information and support. Keep in mind that these areas are meant to be a private place for loved ones to grieve and should be off-limits to non-essential people and the media. Professionals to reach out and help staff can include local hospitals, mental health providers, social service organizations, employee assistance programs, etc.

The mental health response to an active shooter event is going to be an ongoing operation. There will be many different locations and phases of the healing process that need to be addressed. This obviously includes the scene and hospital immediately after the event. But this will continue as the survivors transition from hospital to home, and we certainly are going to need a support presence at vigils and funerals.

Effects of Trauma

Emotional

Whether witnessed firsthand or through the media, these incidents can cause psychological trauma. People experiencing such trauma may continually replay the event in their minds, seemingly unable to stop it. They may experience flashbacks or nightmares, particularly when similar events unfold. Victims often avoid situations that will remind them of the shooting, so they may resist returning to work and participating in activities that they associate with the event.

Physical

Psychological difficulties stemming from school shootings often manifest in physical symptoms, such as headaches, sleeping difficulties, and gastrointestinal problems. The patterns of behavior created after trauma can exacerbate physical symptoms. For instance, anxiety can lead to poor eating habits, which in turn can lead to stomach discomfort. The psychological trauma is often the underlying cause.

People experiencing psychological problems after an incident should realize they are not alone. Talking about the experience and their reactions to it may help alleviate some of the anxiety and reduce emotional and physical symptoms, but victims should not dwell on the event since overexposure may increase stress. Volunteering to help others affected by the tragedy helps empower victims. Breaking the cycle between physical and emotional symptoms is an important step toward recovery. Eating well and engaging in stress-reducing activities like moderate exercise are important. After such a traumatic incident, counselors focus on two stages of recovery: the immediate response of helping people feel safe and the long-term process of helping them cope. "Most people process the events and heal, but about 8% to 15% are likely to develop post-traumatic stress disorder (PTSD)," said Russell T. Jones, Professor of Psychology at Virginia Tech, who counseled survivors of the shootings.

After the Crisis

The actions taken after a crisis situation will have a tremendous effect on the well-being of your employees and the community at large! The following are some ideas to keep in mind following an event.

- Maintain both an information line and special call-in line for victims and their families whenever large groups are affected.
- Keep in close contact with injured victims and/or surviving family members.
- Determine the need for additional health services and resources to attend to increased physical needs of employees.
- Hold regular meetings to provide employees with information related to the crisis, eliminate rumors, advise them of next steps.
- Provide space and time for members of peer groups to meet and counsel each other.
- Designate space for "safe rooms" where, at any time, employees can receive counseling.

CRISIS COMMUNICATIONS

Communicating with Employees, Families and the Public

This may seem like the last thing that you need to worry about in a time of crisis, but it really needs to be at the top of the list. In this day of social media, cell phones, and so on, word tends to travel fast! According to a Pew Research Center study, nearly a third of the US population gets their news from Facebook!

In a recent active shooter incident in Menasha, WI the public information officer for the agency had received posts via the department's social media accounts almost simultaneously as he was getting notified by the agency of an active shooter incident. Any time there is an active incident at a business, or even a rumor of violence, it disrupts normal activities not only within the business but also throughout the community. Often these rumors or misinformation can fuel more panic than an actual event. That is why we need to "get out in front" and manage the information.

At the same time, notification needs to be made to other employees and family members. Many businesses and schools have notification lists that can send out a message a variety of ways with relative ease. Mass notification systems typically use existing data and voice networks to deliver pre-recorded or live messages that alert employees of emergencies and provide them with instructions, such as evacuating a building or going to pre-assigned rooms that serve as shelters. A comprehensive mass notification system typically allows leaders to immediately contact every employee through phone calls, text messages (also known as short message services, or SMS), instant messages, e-mails and other alerts on a wide variety of devices. These can also be set up to notify certain subsections of the business if need be.

A recent example of this use in Wisconsin was in the case of a missing 4th grade student. The boy had been missing for a few hours on a weekend, and through collaboration between a school resource officer and school district, a message was sent to every 4th grade parent; within a short time, the boy was located at a friend's home.

Working with the Media

More than likely this is the last thing you are going to want to address. However, the quicker that we can get information out, the better! As you can imagine, there will be a lot of information shared via social media and with bystanders and others speaking to the arriving media. If your business has a media relations or public information person, have them work with the law enforcement public information officer assigned through the Incident Command.

Law enforcement more than likely will take the reins on the initial few press conferences, but here are a few of the guidelines for working with the media.

Staging the media

Make sure that your location can handle an abundance of media and satellite trucks. The selected area should not interfere with the crime scene or any other work yet afford the media some good background footage. The more that you can work with and accommodate the media, the less frustrating it will be.

Preparing the message

Work with other media relations/information persons to develop talking points and make sure that all understand what can and cannot be conveyed to the media. These comments should be short and easy to understand. Anticipate potential questions from reporters and have prepared responses.

Delivering the message

There are going to be A LOT of cameras and microphones. Stay on task and be careful not to "over talk." Be hesitant to answer questions if you do not have the answer. Respond, "We do not know the answer at this time," or "Once we have more information, we will let you know."

NEVER say "No Comment!" That implies that you have something to hide. Instead you can say, "We are still assessing the situation," or "This is a fluid moving case, and I can't answer that with certainty at this time." Highlight actions and plans that went well during the response. Be careful with non-verbal communication. Do not wear sunglasses or chew gum. You should be appropriately attired (not wearing shorts, t-shirt, etc.). Have eye contact with the crowd and be mindful of your expressions (i.e. smiling or laughing).

BUSINESS CONTINUITY PLAN

The purpose of a plan is to define the recovery process developed to restore your company's critical business functions. The plan components detail your company's procedures for responding to an emergency situation, which affects your ability to deliver core services to our customers or our ability to meet investors, legal or regulatory requirements. There are different facets of the plan depending on what the situation is. We are going to focus on an active threat scenario.

Continuity Plan Objectives

- Facilitate timely recovery of core business functions
- Protect the well being of our employees, their families and customers
- Minimize loss of revenue/customers
- Maintain public image and reputation
- Minimize loss of data
- Minimize the critical decisions to be made in a time of crisis

There are several points that need to be considered.

Access to the building

Often leaders fail to realize that when they are evacuated from a building they may not have *access to that building* for *days, if not weeks depending on the nature of the situation.* If shots were fired in the building or not, the building becomes a crime scene and appropriate protocols must be followed.

Critical operations

In the case of functions such as information technology, facility heating and cooling operations, etc. and those other operations that cannot be interrupted do you have a plan to maintain those?

Access to computer

If employees are advised they can do work via remote access, what happens if their *laptops that are required to access the virtual private network (VPN)* remain in the facility and they don't have access?

Psychological impacts

We spoke of this earlier, but it certainly needs to be addressed in the plan. Hopefully there is not a loss of life or injuries, but what if the stressors are such that employees are having a difficult time to make it to work? Human resources and employee assistance managers must take this into account. Post-traumatic stress disorder (PTSD) is not uncommon and must be planned for in advance.

Page left intentionally blank

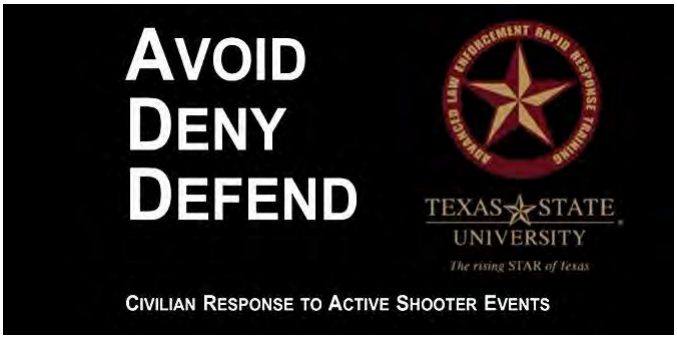
RESOURCES

Ever since the tragedy at Columbine High School in Colorado, there has been a push to raise awareness of these incidents and educate the general public on how to detect, prevent and respond to active threat events. Researchers take a look at each of these active threat incidents and compile an after-action report on what went right and what could be improved upon. We tend to learn from our past, and this is where we get our information to pass along in trainings and books.

Over the past two decades, several programs have arisen to deal with and prepare for active threat events. All of these programs are well-intentioned and have great ideas. What we have tried to do with this training and workbook is provide ideas from each of these following programs and encourage people to make a decision on their own and potentially take bits and pieces of each program to create a hybrid version that works well for their facility.

Avoid, Deny, Defend

Since 2002, the Advanced Law Enforcement Rapid Response Training (ALERRT) Program at Texas State University has been used to train law enforcement officers across the nation in how to rapidly respond to dangerous active threat situations. Over the years, we've seen response times shorten and the capabilities of law enforcement increase. As a result of increased public awareness, many citizens have asked what individuals can do to protect themselves and reduce the dangers faced during one of these events. **Avoid, Deny, Defend** has been developed as an easy to remember method for individuals to follow. As we've seen, hiding and hoping isn't a very effective strategy.



The program is based on the following concepts: Avoid, Deny, Defend. It is a civilian response plan containing three options:

Avoid. This is the preferred option and begins with situational awareness of one's environment prior to any active, hostile act occurring. It also includes having a plan ahead of time regarding what you would do in the event of an active shooter and knowing escape routes. Avoid Danger.

Deny. If avoidance isn't possible, find ways to prevent the attacker from having access to you and others around you. (Close and lock doors, barricade doorways with furniture, etc.). Deny Access.

Defend. Take action! As a last resort you have a right to defend yourself if you believe your life is in imminent danger. Defend Yourself.

For more information, visit www.avoiddenydefend.org

Standard Response Protocol

A critical ingredient in the safe school recipe is the uniform classroom response to any incident. Weather events, fires, accidents, intruders and other threats to student safety are scenarios that are planned and trained for by school and district administration and staff. Historically, schools have taken this scenario-based approach to respond to hazards and threats. It's not uncommon to find a stapled sheaf of papers or even a tabbed binder in a teacher's desk that describes a variety of things that might happen and the specific response to each event.

The Standard Response Protocol (SRP) is based not on individual scenarios, but on the response to any given situation. Like the Incident Command System (ICS), SRP demands a specific vocabulary but also allows for great flexibility. The premise is simple; there are four specific actions that can be performed during an incident. When communicating these directives, the action is labeled with a "Term of Art" and is then followed by a "Directive." Execution of the action is performed by active participants, including students, staff, teachers and first responders.

For more information, visit www.iloveyouguys.org

Ready.gov

Businesses can do much to prepare for the impact of the many hazards they face in today's world including natural hazards like floods, hurricanes, tornadoes, earthquakes and widespread serious illness such as the H1N1 flu virus pandemic. Human-caused hazards include accidents, acts of violence by people and acts of terrorism. Examples of technology-related hazards are the failure or malfunction of systems, equipment or software.

Ready Business will assist businesses in developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards. This website and its tools utilize an "all hazards approach" and follows the program elements within National Fire Protection Association 1600, Standard on Disaster/Emergency Management and Business Continuity Programs. NFPA 1600 is an American National Standard and has been adopted by the U.S. Department of Homeland Security.

The five steps in developing a preparedness program are: Program Management, Planning, Implementation, Testing and Exercises, and Program Improvement.

For more information, visit www.ready.gov/business

SECURITY SURVEYS

Providing ways to improve security is an excellent way to interact with the community on a positive and proactive note. Many of the tips provided in this manual can be shared by patrol officers in the course of investigating a theft or burglary complaint. There are too many times that we may overhear a conversation from a resident who was a victim of a property crime complaining that the *officer came out and took a report and I never heard anything more.* This obviously does not bode well for law enforcement or your agency. Now think about if that officer, while investigating a theft, tells the victim about solar powered motion lights or even better a trail cam. Now this person may be overheard praising the officer and agency for providing a little known tip!

Some agencies are taking that a step further and offering more detailed and in-depth security surveys. These can be time consuming and certainly need to be planned out in advance. There are agencies across the United States that will partner with one another to complete these surveys. This is a great way to work with one another and also affords the crime prevention officers and the business for that matter a few 'sets of eyes and ears' looking at the property. Often times you may have officers with varying areas of expertise such as: tactical, school resource officer, investigations, etc. that ends up complimenting one another.

The following few pages offers a checklist that can be used for a security survey of a business. Keep in mind that for different properties (churches, multi family, schools, etc) there will be different checklists. When you conduct a survey, bring a camera (smart phone cameras work well) and take photos so that you can include those in your final report.

Take some time when you complete the final report. This is your opportunity to shine and make wrap up the survey with a bang! Contact the author for other checklists and examples of completed surveys.

Business Security Survey Checklist

Use this as a guide when completing the security survey.

Business Information

Contact Name:	
Name of Business:	
Physical Address:	
Street name/number:	
City/Town/Zip:	

How many full time staff are employed?	
How many part-time/volunteer staff are employed?	
What year was the building built?	
What year(s) were structural additions made to the building?	
What is the approximate acreage of the property?	
What is the purpose of the business?	

What are the operating hours of the business?		
Weekdays	**Saturday**	**Sunday**

RECENT INCIDENTS OF CONCERN

Check out past police activity. Anytime you can 'localize' and make the presentation 'personal' it tends to strike home. It gets rid of the 'it doesn't happen here' mentality.

EMERGENCY OPERATION PLAN

Does the business have an emergency operation plan?	
What year was the emergency response plan last update?	

Does the Emergency Response Plan include						
Section	**Yes**	**No**		**Section**	**Yes**	**No**
Lockdown Procedure				**Communication**		
Lockout Procedure				**Reunification**		
Shelter in Place Procedure				**Behavioral Health**		
Avoid, Deny, Defend Procedure				**Security**		
Evacuation Procedure				**Workplace Violence**		
Active Shooter				**Natural Emergencies**		
Fire Emergencies				**Medical Emergencies**		

Does the facility have an emergency response team?	
Does the business provide training for the emergency planning team that includes workshops and refreshers?	
Have floor plans of the business been supplied to local emergency responders?	
Are the emergency contacts up to date?	
Does the business have any type of security staff?	
Do emergency response organizations (police, fire, emergency medical, emergency management) tour the building on an annual basis other than annual fire department inspections?	
Is there a plan for reunification in the event of an emergency?	

Does the business have personnel who are familiar with the lifesaving procedures to stop massive bleeding, applying tourniquets and/or to open a closed airway?			
Number CPR Trained		**Number First Aid Trained**	

RISK ASSESSMENT CHECKLIST

BUILDING EXTERIOR

Type of building?	
Is the address clearly posted?	
Number of floors?	
Open or secured by fence?	
Does fence have gates? Are they secured?	
Does the landscaping hinder surveillance?	
Any materials stored outside of the building?	
Are all entrances marked by a number?	
Are all exterior doors of solid construction?	
Do all doors allow to look out prior to exiting?	
What type of glass is used on the exterior?	
Is the building, entrances and exterior utilities protected from vehicles (bollards)?	
Can the roof be accessed?	

PARKING AREAS

Is there employee parking within the perimeter?	
Are cars parked adjacent to the fences?	
Are cars parked adjacent to the building?	
Are cars parked near loading docks/areas?	
Do the employee's vehicles have permits?	
Is visitor parking segregated from employee parking?	
Are their signs directing visitors?	
Is the parking lot posted for employee/customer parking only?	
Is the parking lot lit?	

LIGHTING

Is the perimeter lit?	
Is the perimeter lighting adequate for the task?	
Is there an emergency lighting system?	
Are all doorways sufficiently illuminated?	
What hours is lighting in use?	
Is the parking lot are illuminated?	
How often is the lighting checked?	
Is the interior lighting suitable for nighttime surveillance?	

ACCESS CONTROL - PROCEDURES

How many unlocked access control points are there?	
Are there signs directing visitors?	
Is there a reception area?	
Does that reception area allow uncontrolled access to rest of building?	
Does the receptionist have the ability to notify others in the event of an emergency?	
Is there a visitor sign in sheet?	
Are visitors provided with an ID tag?	
Are visitors escorted?	
Do employees have an ID tag?	
Do they wear it and is that enforced?	
Are employees encouraged to 'challenge' unescorted visitors in the building?	
Are public restroom entrances able to be observed by staff?	

ACCESS CONTROL - PHYSICAL

Are interior doors secured after hours?	
Do the exterior doors have security hinges?	
Do spring latches have exterior latch guards?	
What types of locks are in use?	
Are keys centrally held?	
Is a record of keys, key changes, and faults maintained?	
How are keys secured when not in use?	
Is there a master key system?	
How many master keys are issued?	
How frequently are key inventories conducted?	
Are locks changed when there are lost keys?	
How many combination/cipher locks?	
Is a record kept as to who has access to those combinations?	
How frequently are the combinations changed?	
Is there a record kept of those changes?	
Are combinations changed when an employee leaves or is terminated?	

ALARM SYSTEMS

Does the facility have an alarm system?	
Is the alarm audible, silent or both?	
Is the alarm system monitored?	
How are the alarms activated?	
Are all external doors covered by the alarms?	
Are all ground floor windows covered by the alarms?	
Are any internal doors covered by alarms?	
What is the procedure for reacting to alarms?	
Is the alarm system connected to emergency power backup?	
Are the employees trained in alarm procedures?	

SURVEILLANCE CAMERAS

Does the facility use surveillance cameras?	
Are they inside/outside or both?	
Are the access control points covered?	
Do the cameras have infrared capability for nighttime and low light situations?	
What is the megapixel of the cameras?	
Is the recording system closed circuit or an IP based?	
Is the recording continuous or motion activated?	
How long is the footage archived?	
Are the cameras positioned properly? Do they capture what is intended?	

SHIPPING/RECEIVING CONTROLS

Is there a dedicated area for receiving goods?	
How is access controlled?	
How are the goods received (rail, vehicle)?	
Are deliveries received during work hours?	
What about deliveries arriving after hours?	
Is there a segregated area for delivery drivers?	
Is a record of access maintained?	
Is a record of goods received maintained?	

MONEY HANDLING AND RETAIL ISSUES

Is there limits to cash being held onsite (business hours vs. after hours)?	
How is cash stored?	
Who has access to the cash?	
Is there surveillance coverage of cash handling?	
Are there security provisions for deposits?	
Are checkout areas located in the front of the store and able to be seen from outside?	
Is there surveillance through the outside windows?	
Does the clerk have visibility of the store?	
Are there expensive/tempting items near exits?	
Are 'dummy' boxes used for display?	
Are storage/stock rooms secured when not in use?	

SECURITY PROCEDURES

Are employees subjected to background checks?	
Are ongoing checks conducted?	
Staff is required to use passwords and unique login information to access electronic files.	
Security plans for computer and information systems are established.	
These computer and information system security systems include both hardware and software.	
Faculty and staff are trained in safe and secure computer use.	
Video security system is adequately protected against hackers.	
Is there a reporting mechanism for employees to report suspicious and/or harassing behavior?	
Are there opening/closing procedures?	
Are employees provided security training?	
Are exit interviews conducted of employees who leave?	
What is the process for recovering company property when an employee leaves?	
What process is in place for employees facing disciplinary action?	
Is there a 'neutral' room for conducting disciplinary or fact finding interviews?	

Page left intentionally blank

Acknowledgements

Author/Editor **Jason Weber**

Jason has worked in law enforcement since 1990 and has been assigned in various positions such as patrol, investigations, and community policing. Jason also serves as the Vice President of the WI Crime Prevention Practitioners Association and as a consultant/instructor to the WI Safe and Healthy Schools organization and the National Criminal Justice Training Center.

Proofreader **Taylor Maccoux**

Editors **WI Crime Prevention Practitioners Association**

WI Safe and Healthy Schools

Sources

A Study of Active Shooter Incidents, 2000 - 2013. Federal Bureau of Investigation (2014)

Active Shooter Recommendations and Analysis for Risk Mitigation. New York City Police Department (2012)

Report of the National School Shield Task Force. The National School Shield (2013)

Safe School Initiative Report, United States Secret Service and Department of Education, (2002)

Standing Up for School Safety, Los Angeles County Sheriff's Department (2013)

The School Shooter: A Threat Assessment Perspective, CIRG/NCAVC, (1999)

www.alicetraining.com

www.avoiddenydefend.org

www.iloveyouguys.org

www.nasponline.org

Images courtesy of FreeDigitalPhotos.net; Images by Hawkeye; MusikAnimal; Federal Bureau of Investigation; US Dept. of Education; State of Colorado; West Warwick (RI) PD; National Rifle Association; National Crime Prevention Council; Getty Images; Roundy's Foods; Village of Fox Crossing; Author