

A Primer On Managing Violence

Christopher A. Hertig

Violence, in all its varied forms, has become a greater threat in every area of the world. It commands the attention of the news media, terrorizes people and causes protection professionals to make plans, test the plans and revise them as necessary (plan, test, review). In some areas the threat of violence is from terrorist organizations. In others it is from criminal gangs. Still other areas face the lone demented individual bent on righting some perceived injustice.

What happens in one geographic area at a particular point in time is often replicated thousands of miles away years later. What happens “there” tends to come “here” at some point and some form. The point and form taken are in accordance with the area’s cultural, legal and political environment. The US did not experience suicide bombings between the 1983 Beirut truck bombing of the Marine barracks and the airline attacks of September 11th, 2001. Canada awoke in October of 2014 with attacks on soldiers and Parliament; the type of problem faced by other nations for years. Chinese knife attacks have occurred in schools and other public places. America has also seen knife attacks in schools. Knife attacks in the UK have been a concern for some time. And a knife can be a devastating weapon due to its simplicity and the relative silence of the assault.

Sometimes protective planning is really “protective reaction”. It addresses a specific type of threat scenario. In some instances those responsible for protecting others - such as security and HR professionals - tend to see only workplace violence stemming from disgruntled employees. Realistically ; we must have strategies for managing other types of active threat; be it from employees or external adversaries. Or some combination of the two. Protection professionals need to try and see all of the threats on the “battlefield”. They cannot get swept up in current media frenzy over a particular problem. They must view the “battlefield” through history, current conditions as well as what can reasonably be anticipated in the future.

Threats as they relate to Environments

One must see the total environment. One example is healthcare facilities, often with various campuses and satellite operations. Hospitals have parking, retail, restaurants. There may be hospice facilities. There are pharmacies filled with drugs and cash.

And there is the emergency room where the victims of violence are brought in; often with friends and family members who interfere with treatment. Occasionally the adversaries from the original violence may enter the ER and attempt to finish what they started.

Hospitals may also face spillover violence; particularly when they are in high crime areas. A gang shootout moves onto hospital property or a robber escapes through the hospital’s parking lot.

Due to the presence of terminally ill persons, a mercy killing of a close relative is a potential problem. The terminally ill patient may also attempt to kill themselves; becoming another suicide threat in addition to the addicted and mentally ill.

A shooter enters to vent his anger at hospital staff because of what he/she perceives to have been poor treatment of a loved one that resulted in a poor outcome. The threat of this type of violence is somewhat generic as customer disputes can arise in many types of environments. And it bolsters the argument for customer/patient/client/guest/patron service as a means of threat mitigation. Managing violence from customers may incorporate a firm foundation in customer service training with additional attention given to handling customer complaints.

Schools, office complexes and shopping centers also face violence and/or threats from disgruntled individuals; be they students, employees or customers. They may also have to deal with gang violence or attacks by terror groups. Note that “birds of a feather flock together”: violent individuals may be attracted to criminal gangs or terror groups. Group ideology is really secondary for some of the true predators. In addition, groups evolve from one to the other as well as

work together (narco-terrorism). And groups dissolve, splinter off into other groups, etc. The dynamic nature of organized crime/gangs and terrorism requires continuous intelligence assessments by those responsible for security.

Retail stores have long dealt with shop-lifters who fight. They also must confront professionals who work in teams where team members attack store personnel attempting to apprehend other gang members. Flash mobs have converged on stores and committed shoplifting en masse. Active shooters have become a concern in US retail establishments for years. A more recent trend is for active shooters to target shopping centers (malls). The US has seen this and Kenya had the horrific Westgate Mall attack in 2013. More can be expected.

Active Threat Response: "CANE "

Responding to an active threat requires proper assessment and decision making. Factors of time and distance must be taken into account. Some people have difficulty understanding these concepts. This is especially true if the learner has never experienced an assault or confronted an armed individual. The reactionary gap between seeing an assault and the time it takes to mount a defense is often misunderstood. The Force Science Institute has conducted research in this area and may be a good source of information for those developing training programs.

The acronym below can be useful in training and educating people regarding the immediate response to active threats. This may include all employees; but it should start with supervisors and/or security staff initially: the assumption that someone knows something due to rank or job title must never be made. Active threats are any imminent dangers posed by weapons, explosives, fire, HAZMAT, or the human body (hands, feet, heads,teeth,etc.). The acronym provides a conceptual framework to aid in understanding the reality of an attack by an armed person or persons. It aids in making the right decisions in the right order at the right distance.

This acronym can be used in teaching people how to respond to an active threat by experienced, qualified instructors who have sufficient time and teaching resources (personnel and materials).

C – cover (shielding) and concealment (hiding). Ideally cover and concealment are used simultaneously but this may not be possible. Cover includes objects (vehicles) or structures (walls) that shield one from bullets. Cover provides protection as it stops (prevents) or slows down (mitigates) bullets.

A general rule is to get behind something, anything, as it will at least partially slow down the bullets. The caveat is to avoid getting behind glass as the glass may fragment ("spalling") and cause injury.

Cover from other types of active threats may include furniture gotten behind or placed between the assailant and defender. This works for attacks with non-projectile weapons such as clubs or knives. A chair overturned in the path of a knife wielder or getting behind the corner of a desk or table may provide quick protection.

Concealment is simply objects which one can hide behind. If the attacker cannot see their intended victim they can't attack as effectively so harm to the victim is mitigated. If they don't initiate or continue the attack due to the target being concealed, that attack has been prevented.

The old adage of "see others before they see you" is relevant to concealment and easily taught.

A – Assess. Seeing and understanding the threat is crucial to dealing with it. What is in the hands of the assailant? What type of weapon do they have? How are they dressed? How many adversaries are there?

N – Notify. Alert the right people as quickly as possible. This may take the form of yelling which alerts those nearby. The yelling could also be the employment of "hard verbals" such as "Stop!,Stop,Stop" at the attacker. These verbals serve several different purposes and are particularly useful as a defensive measure.

Notification may also include calling the right people (police, security, etc.). Note that in some active shooting cases calls were made to parents and boyfriends before police were notified. Communications should be practiced by everyone so that this type of problem does not occur. Communications training should also contain practice in describing clearly what is transpiring. This includes persons (attackers), behaviors and weapons.

E – Escape or Engage. Sneak away undetected, run or fight. Obviously sneaking away is the preferred option but it may not be a viable one. Running away may make more sense even if seen by the assailant. Engaging with or fighting an assailant may also be an option.

Whether or not to fight is a decision that must be made promptly and properly. One aspect of this is distance from an adversary. If very close to a shooting assailant; grabbing and controlling the weapon would almost certainly be necessary. As the distance from the assailant increases; the viability of engagement declines. In addition, it is difficult to hit a moving target. And it gets increasingly so the farther that target is away from the shooter. These are the issues that must be covered in training ; and they must be covered well.

Obviously protective service professionals have a greater duty to protect others, making engagement more likely for them than line employees. This option must be viewed in terms of law and policy; as well as weapons, training and ability of the protector. Finally, it is a moral decision: how a protection officer handles an active threat stays with them for the rest of their lives.

Containment or isolation of the problem is a security force function with any type of crisis. With active threats this may mean shutting off access to certain areas of the facility; locking assailants in rooms, evacuating those near the attackers/crisis point. Containment or isolation may be part of an escape or an engagement response. It is a primary consideration when developing crisis plans. Tabletop exercises and other types of scenario evaluations may help shed some light on isolation/containment as well as other aspects of response.

Avenues of approach used by adversaries need to be identified and assessed. This is part of containment. Certainly all initial and first responders need to be proficient in establishing perimeters. Training and practice in this is integral to success at doing it in a real situation.

Bombs and Explosives

A working knowledge of explosives and bombs is an absolute necessity. It is strongly recommended that in-depth instruction on this be given to security force members by experts in the field. Supervisory personnel need this knowledge the most and should take classes in it. The brief discussion below is presented as an introduction, a starting point.

Explosives and explosive force – An explosion is a rapid chemical reaction (oxidation) where a solid or liquid becomes a gas. Force travels outward along the path of least resistance. A bomb on the ground will have most of the force traveling upward. A device placed against a wall or worn on a backpack will have most of the blast energy moving away from the wall or body. The London subway and Boston Marathon bombings were examples of this.

High explosives have a higher rate of detonation (ROD) than low explosives. They go from solid to gas much more quickly. They transmit a shattering effect that is ideal for destroying building or bridge columns; breaking up rock or mineral deposits in mining, etc. TNT (dynamite), RDX, PETN and C-4 are high explosives. High explosives shatter things, low explosives tend to push things. While ammunition and fireworks are common uses for low explosives; black powder has been used as a crude improvised explosive device (IED).

Explosive force travels in 2 waves and then a rebound or return wave when the air pressure fills the vacuum created by the explosion. This “1,2,3 punch combination” can create extensive damage to humans and property. It is important to understand this regarding the stability of structures: always remember that “1,2,3 punch combination” and the effect it

may have on a wall, floor, roof or pillar. The first wave may not destroy the structure but the second and third will do more damage. As a result, structures may not collapse immediately but are unsafe and unusable after a bomb attack. They are probably damaged more than they appear to be.

“Pancaking” of buildings can happen as a result of the explosive forces helped along by gravity. The explosion primarily pushes up and gravity pushes down. This creates a “1,2,3,4 punch combination”. As the gravitational pull is continuous, the building may collapse some time after the blast. Again, safe practices call for an engineer to assess the structure before entry attempts are made.

Under water there is an added dimension of explosive force due to water pressure. The outward blast or bubble of hot gases is quite strong. So too is the water pressure (greater than air pressure) when the shock wave contracts. An additional destructive factor may be the weight on the ends of a ship, boat or barge that pulls the vessel apart during the initial blast wave (assuming the explosive is placed in the middle of the vessel). Finally the return or rebound wave also places stress on the vessel. Bottom line: explosives placed under water are generally more destructive than those on land.

Explosive force travels outward and increases some distance from the explosion; something like a punch gaining power as the arm reaches full extension. As an example of this; the majority of the 1995 Oklahoma City casualties were across the street from the Murrah federal building where the explosives filled truck was parked. This makes shrapnel a serious threat in the surrounding area. Shrapnel is pieces of material from the container of an explosive device or other items surrounding it. Shrapnel is often added to explosives to increase casualties such as by taping nails to the outside of a bomb.

Fire is an oxidation process like explosion. The process occurs slower than in an explosion. Fire may occur with an explosion; or an explosive device may burn instead of explode. It may also precede or follow an explosion. In short, we cannot really protect against one without considering the other.

A “stacking effect” can occur with fire whereby materials high above a fire are subject to greater heat and their ignition point is reached more readily. Something that would not ordinarily burn now ignites due to the higher temperature caused by rising heat. This makes fire protection more challenging the higher the structure is or the more highly stacked the goods or materials.

Explosive force on humans often is not fatal; it throws the victim some distance. It also causes serious body cavity damage. Brain injury due to severe concussion is also common.

In an explosion or fire event there may be numerous people injured so provisions for handling mass casualties must be made. Prior assessment of nearby hospitals and triage areas are means of managing this.

Explosive or fire vulnerability should be assessed at all times. The basic questions of “What would result if an explosive was placed here?” and “What would result from a fire here?” should be asked by all protection professionals. A more definitive analysis should be determined via a professional vulnerability assessment for explosives as well as an appraisal of fire loads by a fire protection specialist.

Vehicles pose threats! Some involve explosives and some do not. Vehicle borne improvised explosive devices (VBIED's) can be parked nearby a target or driven through gates, fences or doors. Vehicles can be used as battering rams, personnel carriers with adversaries inside or loaded with explosives (in addition to the gasoline in the tank). Note that

vehicle attacks may also be directed at people in a crowd. They may also be non-violent; simply driving through doors or walls as a means of burglarizing a building. Appropriate vehicle control measures need to be in place at all facilities.

Response to an explosive event must be cautious. There may be secondary devices planted, ambushes or HAZMAT threats from toxic fumes. Building or road collapse may occur. Responders should stay low to avoid shrapnel. Staying low also provides some measure of protection from heat and fumes. They also approach from behind available cover and communicate with the command post.

Once on scene they should systematically assess it as they would a crime or accident scene. They must provide essential life protection functions such as rendering first aid, removing victims or other actions to mitigate and minimize the danger.

And they should photograph the scene quickly as it is subject to rapid change. In the case of unexploded devices or suspicious objects; these should be photographed for investigative purposes. "Protect, preserve, make notes" is what needs to be done at any crisis scene.

Once immediate safety concerns and initial photos have been taken a search of the scene must be conducted. This can be a priority search where the most obvious or critical areas are assessed first. It can be a spiral pattern moving inward to insure maximum safety. Additional search patterns such as an outward spiral may be conducted. The key point is to search the entire area so that all hazards and evidence has been located.

If a suspected device is found it can be vented to minimize the explosive force. Allow it to dissipate by opening windows, doors, etc. Other means of blast mitigation are to remove combustibles and explosives. This may include chemicals as well as vehicles. Shutting off utilities which would create substantial damage if a blast were to occur such as water, gas and electricity is also recommended.

It may be advisable to channel or direct the blast away from personnel or vital assets. Direct the blast with barriers such as sandbags, bomb blankets or explosive containers. Having some of these assets on hand may be prudent. As sandbags can be used to aid in redirecting water as well as blast; a stronger case can be made for having them accessible.

Power outages may occur due to utility shut downs, fire or blast effects. Adversaries may also cut off power and communications prior to an attack. Being ready to work without power and to quickly and efficiently respond to sudden losses of power is something all protection forces should be adept at. This is but one reason why officers should have a flashlight on their person at all times.

Suicide Prevention

Suicide is a concern for security forces in that it is a form of violence. As such it must be prevented and protection staff at high rise offices, hotels, casinos and hospitals have to be concerned about it in its own right. Crisis prevention includes suicide prevention and crisis intervention includes suicide intervention. Suicide of patrons, guests, patients and employees must be prevented as much as possible by protection officers. So too must the suicides of their brothers in arms such as fellow security officers, police, EMS and military personnel.

Suicide attacks have been part of warfare at various points in history. The Moros of the Phillipine Insurrection and the Japanese Kamikaze pilots of World War II are well known examples. Terror groups such as the Tamil Tigers and various Islamic Fundamentalist terror groups have also employed suicide attacks. Primary targets have been personnel: crowds of people, specific individuals in assassination attacks, trains and airliners.

Suicide bombers may attack in various ways from using Vehicle-Borne Improvised Explosive Devices (VBIED's) to wearing explosives laden vests or even having explosives hidden internally. Suicide bomb attacks are a serious concern and certainly deserving of concerted study. Some basic protective concepts for dealing with them are to extend the perimeter of a facility outward so that bombers are further away from their intended targets. Another is to control the hands of someone attempting to detonate an explosive – and assuming the risk of being charged with a battery if the individual is not a suicide bomber. Better still is apprehension of the bomber before they strike. This can be early in the plot before they get near the target or immediately after they arrive at the target.

While we generally think of suicide bombings as they are common at the present time; other forms of suicide attacks have been used in the past. During the Philippine Insurrection in the early 20th century, it was common for Moro tribesmen to attack American soldiers with swords while wrapping their bodies tightly with white cloth to restrict bleeding. While their targets were personnel like those of contemporary suicide bombers; the Moros nonetheless demonstrated that there are various forms of suicide attack.

A reasonable assumption is that new forms of suicide attack will be used in the future. For this reason suicide should be studied. Another reason is the relationship of suicide to active threat events. In many cases the active shooter kills themselves after wreaking carnage on others. Additionally, suicide awareness and prevention training is fairly simple to develop – at least in a rudimentary format. And finally, preventing suicide is preserving life: precisely what protection professionals should be doing.

Emerging Trends

All too often protective planning gravitates to simplistic approaches like always evacuate, zero tolerance, etc. Later on more reasoned, appropriate countermeasures are selected. An international perspective to identify what others have done can aid in diminishing this tendency of overreaction. So too can an interdisciplinary approach. Historical research is also helpful as “the only thing new is the history we don't know”: similar events have happened in the past and we can learn something from them. Protection professionals will need to read history papers, texts and after action reports. “Ignorance of the law is no excuse”; neither is ignorance of history.

As we get more adept at understanding the crucial element of time our responses to violence will improve. The “initial responders,” such as security officers will be better understood. Those doing the immediate, necessary actions will be recognized and trained. Active shooters aren't stopped by tactical units nearly as often as they are by someone nearby. Response time is one issue; reactionary time by humans is another. A “lessons learned” approach can be used here so that time factors can be better understood. Studying the medical and military communities is an excellent starting point.

Untrained and unarmed security forces are of no use when violence erupts. Routine activity theory postulates that crime occurs with the presence of an attractive target, a motivated offender and the absence of a capable guardian. This is relevant to violent attacks as well. There must be a capable guardian in the form of a professional security force.

Some facilities have groups of armed, trained security or police officers onsite. Hospitals and college campuses seem to take this approach more than other industry segments (verticals). Across the board at most facilities there is a gradual increase in the training given to security officers to meet the threat of violence.

This will continue as more protection forces practice tactical exercises. Particularly in the school vertical where there has been an increase in both training of school employees as well as the conducting of exercises with police and local emergency responders. Unfortunately this is incremental. The degree and type of training necessary is not given in many cases. A sea change in public attitudes towards security officers will be necessary for protection forces to be seen as they really are: crucial agents of management who maintain order, respond to crisis and ensure safety.

Increased use of contract security by celebrities for personal protection has grown and will continue to do so. Personal Protection Specialists (PPS) as domestic violence countermeasures is another angle on this. PPS continues to grow and

evolve. There will be different types of principals who use PPS either on a regular or as necessary basis. While this was predicted by the author's branch manager in the late 1970's; it will be interesting to see what the future brings.

Security service firms are increasingly providing coverage at special events. While providing more cost-effective protection than in-house security forces; unity of command is essential in an emergency. Complicating the organizational structure by having a hybrid where the contract force must interact with proprietary personnel increases the complexity – and time – for an effective response. This may mitigate the growth of contract security in some sectors, although superior service providers will likely prosper.

Service providers continue to expand their menu of violence management offerings. Consultation, training, violence risk assessments, etc. are being offered by some firms. There may, however be deficiencies in the physical security planning aspects of these services. Advice on physical security must be the result of an assessment by a professional, not an add-on service. ASIS and other professional associations should increase their visibility to the consumers of security consulting services. They will need to ensure that their professional certification processes are well known and respected.

Suicide bombers have attacked concentrations of people in the past. In the future they may go after communications networks, computer rooms or other critical infrastructure points in an attempt to shut down an adversary. Standard bombing, arson or sniping attacks by deranged individuals against key facilities may also occur; absent any political/social/religious motivation. Sniping attacks against transformers has occurred; perhaps other critical, non-human targets will be selected in the future. Sniping may well become more prominent for various reasons. Militarily trained and experienced snipers may "go bad". Amateurs may snipe using hunting rifles with scopes which are readily available in many areas. There are numerous books and videos on the sniping; some of which is instructional with other material glorifying snipers. These factors combine to make copycat snipers a high probability.

Biohazard attacks have been somewhat limited in the past but this could change. The last decade or so has seen a tremendous evolution in the sophistication regarding IED's. It is certainly not inconceivable that organized terrorist groups could develop similar expertise with biological agents. Sophistication at this level would almost certainly require governmental sponsorship. Some terror groups have long had such support. Other groups such as ISIS and Boko Haram aspire to having an Islamic state, a caliphate. Control over an existing state or the developed portions of one could provide terrorists with CBR capabilities. Either external government support or the conquest of existing laboratory facilities would be a major game changer if germ warfare resulted from it.

Coordinated attacks of varied types such as armed assaults or civil disobedience actions will likely increase. The terrorist assault at Mumbai, India employed ten attackers divided into two- person teams that killed approximately 170 people using bombs and small arms. A small number of attackers at the Westgate Mall in Kenya killed 67 people and wounded 200 more. Al Qaida has used coordinated attacks for some time.

Coordinated instances of civil disobedience/protest will also grow in frequency. Civil disturbances with different groups acting in concert with one another are nothing new. Radicalized group members may shift from non-violence and a-violence (targeting property) to human targets (violence). Flash mobs have evolved and will continue to do so. The destructive capabilities of these groups will likely take new forms beyond protest, robbery and shoplifting.

Drone usage is exploding in both military and commercial sectors. It is similarly expanding in private applications such as photography by an individual. This has obvious ramifications for surveillance and countersurveillance, not to mention disinformation and propaganda. It also opens up a whole new avenue of attack where drones could be fitted with CBRNE devices or agents.

Cyber attacks will grow in both frequency and criticality; forcing organizations to adopt additional protective measures. Cyber attacks are integrated within the military along with artillery, air power and infantry. Terrorist groups and

perhaps even individual lone wolves will likely follow suit. Radical environmental groups have long used various forms of cyber attacks; these will also continue and probably morph into more virulent forms which endanger humans.

Increased government regulation and standards adoption will be drivers for security industry growth: more officers, more training and more technology. This has been occurring and will continue, but it will be in fits and spurts. As there are more laws passed and standards adopted, there will be a positive effect upon the growth of the security industry on the personnel side of the house.

Technological advances are another driver in security industry growth. Detection equipment such as x-ray machines at access points has been growing and moving into new market sectors. In the US, metal detection first appeared in courthouses and nuclear plants. Later it moved into nightclubs and schools. Surveillance gunshot detection and communications systems are being bought by cities and will likely be acquired by organizations that never had them before such as shopping centers and office parks.

Attacks on critical infrastructure sites are a favored target for terrorist groups, for good reason. They offer what is seen by the terrorist as a soft target offering maximum effect with minimal chance of interdiction. The potential effects in terms of damage, the hugely detrimental economic impact, disruption of normal daily life and resulting publicity, can far outweigh the terrorist organizations' commitment in both manpower and risk.

At the same time; symbolic targets such as companies that engage in animal processing or houses of worship are targets for extremists. Continuous monitoring of an organization's public profile is a necessity. Commercial services, proprietary security departments and external agency liaison all play a role in this. With the speed and widespread internet exposure currently available; this is a growing challenge. Intelligence professionals and service providers will increase in number.

Climate change has also seen more extreme weather patterns, creating additional hazardous, unseasonal and unpredictable conditions resulting in a severe strain on infrastructure. People without food, water or sanitation get agitated and can be readily led down the path to violence by the right leader. Natural disasters significantly enhance the stature of charismatic leaders. The charisma factor is especially acute when religion is in the recipe. Some of these leaders choose terror or organized criminal activity (black markets, robbery, extortion, looting) for their followers. Extreme weather conditions can in some cases be a causal factor in violence.

An allied factor is refugees from either natural disaster or war. There have been massive numbers of refugees in Syria and other places. Refugees from disaster areas or war zones are an incubator for civil unrest and sometimes terrorism. The Taliban grew in refugee camps. Other such groups are sure to follow.

If refugees become citizens of a new country and are marginalized and discriminated against; they may adopt extremist ideology. This often occurs with first-generation immigrants. Although not refugees per se, they feel alienated and may join extremist groups or lash out on their own as lone wolves. The cycle of disaster/war, refugees and violence continues in the new generation.

The violent actions of lone individuals who are mentally unstable and/or radicalized by terror groups will continue to be a concern. "Workplace avengers", the traditional perpetrators of workplace violence; will increasingly consist of persons holding extreme beliefs. Internet influence will be a larger factor in this. Influence over teenagers and children who are particularly vulnerable to extremist views will increase. Geographic distance will mean less and less. Radicalized persons "here" will become so via the internet from "there". And the virulent nature of some radical Islamic fundamentalists indicates that a very long and nasty period of conflict lies ahead.

The quest for notoriety is a major driver in violent attacks. Organized terrorists as well as the mentally unstable seek publicity. As our society becomes more media focused, the desire for fame may exert more influence on those already predisposed to commit sensational acts of violence. The copycat phenomena will undoubtedly increase.

References

Arnold, J.R.(2011) . THE MORO WAR: How America Battled A Muslim Insurgency In The Philippine Jungle, 1902-1913.Bloomsbury; New York, NY.

Chapa, L. (2014). An Emotional Response Plan. SECURITY MANAGEMENT. Oct. pp18-22.

Are Schools Focusing Too Much on the Active Shooter Scenario?

Jim McKay | July 9, 2014

<http://www.emergencymgmt.com/training/Are-Schools-Focusing-Too-Much-Active-Shooter.html?page=2> (Retrieved August 20,2014)

Active Shooter: Is Having a Plan Enough?

Wednesday, 14 May 2014 10:52

<http://portal.com/solution-providers/retail-news/item/3050-active-shooter-is-having-a-plan-enough.html> (Retrieved August 20,2014)

ShareFacebookTwitter.Boko Haram crisis: Nigeria's female bombers strike By Farouk Chothia

5 August 2014

<http://www.bbc.com/news/world-africa-28657085> (Retrieved August 16,2014)

Lessons Learned from 2011 Joplin Tornado Show the Importance of Social Media in Disaster Preparedness and Response

<http://nacchopreparedness.org/?p=2679> (Retrieved August 29,2014)

Canfield, A. School security solution takes 'holistic approach'Penn. school district pleased with multifaceted program Friday, August 29, 2014 <http://www.securitydirectornews.com/schools/school-security-solution-takes-holistic-approach> (Retrieved September 2,2014)

Protective Intelligence and

Threat Assessment Investigations:

A Guide for State and

Local Law Enforcement Officials

by Robert A. Fein and Bryan Vossekuil

July 1998

(<http://c.ymcdn.com/sites/www.atapworldwide.org/resource/resmgr/imported/documents/protectiveintelligence.pdf>. Retrieved September 15,2014).

Lasky, S.

Mitigating Risk, Ensuring Staff Safety are Key Healthcare Security Concerns

Created: February 27, 2014

<http://www.securityinfowatch.com/article/11320054/healthcare-security-leaders-share-insights-on-changing-landscape> (Retrieved March 28,2014)

10 Ways to Prevent Workplace Violence Escalation

By Felix P. Nater

February 12, 2013

<http://www.securitymagazine.com/articles/84013-ways-to-prevent-workplace-violence-escalation> (Retrieved September 18,2014)

Workplace Violence Prevention: A Training Management Commitment

By Felix P Nater

October 1, 2010

<http://www.securitymagazine.com/articles/81408-workplace-violence-prevention-a-training-management-commitment-1>

(Retrieved October 27,2014)

School Security Task Force Final Report

New Jersey School Boards Association

October 22, 2014

<http://www.njsba.org/news/security-task-force/>

(Retrieved November 8,2014)

Hassig, Lee (1991) COMMANDO OPERATIONS: The New Face of War

Time-Life Books

Alexandria, VA