IMG

INCIDENT MANAGEMENT GROUP

NOTES

EXECUTIVE PROTECTION

INTRODUCTION

Presented below is an overview of personal protection suggestions and recommendations that should be followed during any period of heightened threat.

The purpose of this overview is not to:

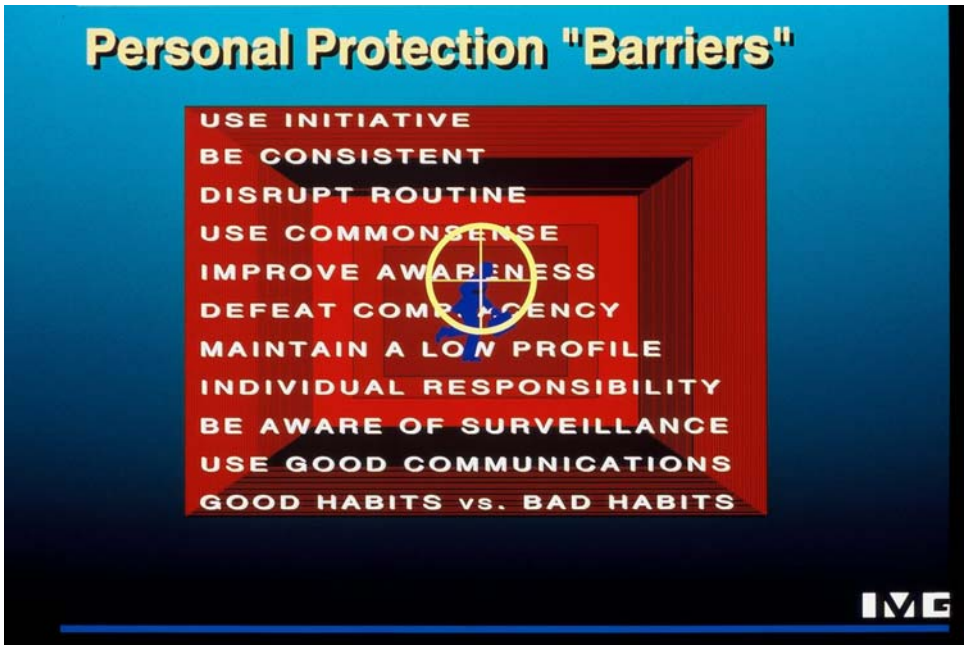
- Elevate the risk beyond actuality
- Provide anyone with sufficient expertise to repel a direct criminal or terrorist attack
- Produce an over-reaction which may limit your ability to work or function efficiently

The purpose is to:

- Acquaint you with some of the principles of personal protection, including those intended to raise awareness
- Provide a few hints for emergency situations

Below are some of the principles of personal protection:

- Pay close attention to the principles of personal protection which are: the need to be aware and suspicious, to be methodical, to avoid routine, to utilize good communications and to apply the requisites of initiative and common sense to all activities which may be the subject of threat.
- All members of your family should exercise an increased level of awareness and suspicion and should be prepared to summon police immediately in the event of pretext telephone calls, visits, or other suspicious circumstances, no matter how trivial.
- While maintaining a balanced perspective geared to the current level of threat, all your actions and those of your family should be colored by the fact that a criminal attack against you or your assets is a possibility.
- You and your family should be particularly alert to the possibility of surveillance, conducted either as a form of harassment or as a precursor to further action. In such cases, you should summon police assistance without hesitation (see below). If driving, you should be prepared to seek refuge at the nearest safe haven such as a police station or other public area. Under no circumstances should you permit your vehicle to be followed into an area which may provide an advantage to an assailant or circumstances conducive to physical assault.
- A precise, evidential log should be maintained detailing all acts of harassment, suspicious telephone calls, etc. Complete details of each incident should be included, as well as the identity of those persons available to provide corroborative evidence.



PERSONAL PROTECTION "BARRIERS"

Personal protection "barriers" are procedural barriers used in much the same way as physical and technical barriers are employed to protect a house or company facility.

Every time a gate in a perimeter wall is left ajar, or windows are left unsecured, or the door to an inner safe haven is left open, the value and benefit of that barrier is given away.

Personal protection barriers may not be made of bricks, mortar or solid hardwood two inches thick, but they are barriers just the same. To carry the analogy further, by relinquishing those barriers, so the threat posed to an individual is increased.

So what are personal protection barriers? As an example consider the following scenario:

A senior executive is enjoying an excellent meal at a fashionable restaurant when his dining partner looks up with a strange expression on his or her face and he feels a hard, metal object placed against the side of his head. He manages to look around momentarily and notices that the object is a semi-automatic pistol held by a man standing to one side. Conversation in the restaurant is subdued.

What could this incident mean in terms of unnecessarily relinquishing barriers?

- The executive came to notice in the first place because he failed to maintain a low profile.
- He lacked awareness because, although he obviously was the subject of criminal planning including surveillance, he failed to notice it.

- He may have been aware of one or more threats, but as in the past had decided to ignore them.
- He probably operated a fixed and predictable routine and stuck to inadequate procedures.
- He failed to notice the onset of the attack until the gun was placed against his head -- again lax procedures and a lack of awareness.
- Finally, he probably took no last ditch action when the gun was pointing at him; he failed to recover from surprise and maintain the initiative. When fast, aggressive action was called for, he sat there waiting for the inevitable.

So personal protection barriers can include:

- Maintaining a low profile
- Utilizing awareness training
- Selecting a dominant and all-seeing position in the restaurant
- Avoiding fixed and predictable routines
- Using initiative and common sense
- Recovering from surprise and maintaining the initiative
- Life saving tactics

Other barriers can include using good communications, engendering a positive attitude towards the threat and security procedures, being methodical, consistent and so on.

When executives and others ponder what to do when they are driving along and find that the road is blocked by people who have it in mind to kidnap or assault them, or when someone has pointed a gun at them but they have been lucky enough to escape, at this point they have failed.

They have failed to put in place the various personal protection barriers between them and those who would cause them harm – similar to retiring at night with all the doors open in a neighborhood that has experienced home invasions.

Of course business leaders or their assistants can be trained in procedures which may just give them a chance of surviving an actual attack, for example, vehicle ramming or weapons disarmament techniques, but if the assailants have done their homework, and they usually have, the victim's chances of survival may be slim.

TRANSFERRING THE TARGET ELSEWHERE

This is a prime goal of personal protection, one that is accomplished by utilizing physical security methods and the parallel personal protection “barriers” to deflect criminal interest in an individual.

An individual who consistently deploys the appropriate protective barriers will often transfer criminal interest elsewhere. A would-be attacker will consider the benefits of targeting a number of individuals who have come to notice and will usually transfer his focus elsewhere should the target appear difficult, risky or unpredictable.

MAINTAINING A LOW PROFILE

Maintaining a low profile is another important "barrier". If this can be achieved, there is a good chance that a possible target will never be illuminated by a prospective attacker's radar.

Ways to maintain a low profile include avoiding all activities which may bring a person to notice, for example:

- Ostentatious lifestyle
- Attendance at meetings or social functions with others who may themselves be the subject of a threat or surveillance
- Involvement in labor unrest
- Exposure to media coverage, etc

Periodically, conduct your own survey in an attempt to find out how much information about you or your company can be discovered. Once this has been done, a concerted effort should be made to reduce sensitive or non-essential information that is public or easily available.

With regard to maintaining a low profile, it is as well to know a little about how attackers go about selecting their targets.

- A pre-defined goal
- An identified target
- Well-planned actions with little left to chance
- Every aspect planned
- Analysis of the target's lifestyle, habits and routines
- Collection of media articles, photographs
- Pretext calls – results
- Surveillance – results

There seems to be two stages of target selection:

- The first occurs when an individual comes to notice and is placed on a list of possible targets.

— The second occurs when a feasibility study is carried out on one more individuals to determine whether an attack against them would be logistically possible and would bring the desired results.

Adherence to a low-profile policy often prevents someone from appearing on anyone's list, but once there, further criminal assessment requires more overt action such as surveillance or pretext calls and visits. Any of these actions can be detected by an aware individual thus giving him or her advance notice of a possible attack.

To restrict gratuitous information:

— Think each time gratuitous information is asked for: Control the unnecessary release of personal information. Remove your name from the phone book, mailbox and office door. Do not mention your name in any recorded messages – those calling your number legitimately will know who they are calling.

— Conduct sensitive meetings at undisclosed locations. If these meetings need to take place on company premises, consider the use of Technical Security Countermeasures (TSCM) beforehand.

— Minimize media coverage of company activities/employees

— Travel in an inconspicuous way with no special arrangements. In high risk countries, travel as a "tourist".

— Don't take on other peoples' risks - avoid attending functions where those present may be the subject of terrorist interest (see below).

— Avoid overt security measures such as bodyguards or armored cars. It is worth mentioning that bodyguards never saved anyone. They may be a deterrent, but once criminals have assessed the situation and decided to take the target on, they invariably outgun and outwit the bodyguards.

— No special license plates, obtrusive cars or marked parking bays.

TAKING ON THE RISKS OF OTHERS

Many executives, especially in overseas environments, inadvertently assume the risks of their hosts, business acquaintances, customers, etc. An example: If the business leader who meets an arriving executive at the airport uses an armored limousine, there are usually one or two reasons: Either the in-country executive has reached a stage in life that he or she feels entitled to luxury and protection or there are genuine concerns about his or her safety. In either case, the arriving manager would be prudent to utilized less ostentatious, pre-researched transportation.

Likewise, think twice about attending social engagements that may present a risk because of the identity of the invitees, the place or the nature of the engagement. In times of heightened risk, each public appearance should be pre-examined from the security perspective.

SURVEILLANCE

Surveillance is a necessary but critical part of the would-be attacker's feasibility stage. A possible target has come to notice and further investigation is necessary to determine whether the risk/benefit equation is favorable.

If a person is being surveilled there are two possibilities: Either the attacker intends to take action against the target during the surveillance or is gathering intelligence for use in a future attack. The response is the same in both cases:

- If there is a doubt about whether surveillance is being carried out, make two or three unique turns to see if the vehicle remains behind.
- Notify the police immediately giving name, vehicle description, etc. and current location.
- Abort the route and drive to a safe haven. Immediately drive to a police station, a fire department or a public place, e.g., a shopping mall, etc.
- Do not attempt to lose the following vehicle.
- Stay on heavily-traveled main roads.
- Don't put yourself in a position in which the follower comes alongside, or engineer this situation in order to get a closer look at him or her.
- Don't drive into a deserted area or car park.
- As soon as practicable, write down the details as you remember them, including a description of the vehicle and its occupants, etc.

Surveillance is usually carefully implemented and, in the case of an important, well protected target, may last upward of a year or so.

Great care is taken to minimize the risks for those carrying out surveillance; observation periods may be limited to fifteen minutes in order to not attract attention.

Difficulties experienced at this stage—such as a target's varied routine or detection of surveillance—may well transfer criminal attention elsewhere.

Any indication that surveillance is being carried on, and this may include a pretext telephone call or visit, should be immediately reported to the police and to appropriate company colleagues. As a general rule, those who may be surveilled should adopt a positive attitude towards this possibility and engender an expectation that they will be followed, or watched, rather than the reverse. In this way, executives will be genuinely surprised when they cannot spot the observers.

Once the criminal targeting is complete and the target selected, every effort is made to carry out the operation with the minimum of risk to operatives. In many cases, plans would do credit to a

police operation order with all possible contingencies catered for, and all vulnerabilities minimized.

Herein lies an inherent weakness however — rigidity. Criminal or terrorist plans are not flexible because those carrying out the operation do not wish to be confronted with the unknown or unexpected; if an attack is supposed to take place at a certain road intersection because other factors there are known and have been brought under control, that is where the attack will occur.

If the plan is spotted however — even at the last moment — and action is taken to disrupt it (by stopping short of the location or reversing), chances are that the attack will be aborted. Under such circumstances, the attackers are unlikely to run down the road after their target thereby abandoning their safe and controlled environment.

DISRUPTING ROUTINE

It follows that disrupting routine is an excellent way of throwing a wrench into a criminal's attack plans and, perhaps more importantly, makes their surveillance and other planning necessary to target an individual that much more difficult and risky.

Perhaps the best advice for executives is to analysis their own habits and lifestyles to detect and vary recurring patterns. It is surprising how many individuals have made themselves easier targets by a reluctance to modify their routine. In many cases, even those at risk in public life have been hesitant to acknowledge the fact that there may be an element of danger. It's an unfortunate fact that many executives are unwilling to relinquish their past habits, even if they do jeopardize their personal safety. The following are some pointers to minimize risk:

- Try to divide departure times into a number of fifteen minute segments and select these at random together with a choice of routes.
- Use different vehicles, park in different locations, use different entrances, select different restaurants, and so on.
- It pays to remember that our homes and offices are usually the two consistent points in our schedule. This is why kidnappings and attacks are popular early in the morning or late at night when a target leaves or returns home.
- Arrivals and departures should be thought of as the most dangerous times and care should be taken to ensure that executives do not relax when they are returning home.

GOOD HABITS VERSUS BAD HABITS

Good security practices can quickly become part of an executive's set pattern of behavior. Equally, bad habits can do the same. Where there is a high level of threat, the latter can jeopardize their chances of survival.

INDIVIDUAL RESPONSIBILITY

- Don't rely on others to ensure your safety--some fail to see the risks
- Utilize intelligence from in-company and external resources, such as advice from embassies, etc
- Develop emergency and evacuation plans for overseas environments. Link these to pre-identified "trigger events"

In many cases, company personnel working in a high risk country, especially if they have been there for a number of years, fail to see or acknowledge risks which are patently there. In these cases, there seems little incentive to enforce good security practices.

When in-country personnel are told of the risks they can react in one of two ways: they either back off from their work functions and carry on their work in a more detached and less efficient manner, or they carry on in an ever more obvious manner as if confronting the problem head, as if in an attempt to discredit the information. In some cases, the individual's activities become so obtrusive that he or she will need to be relocated. Needless to say, these peoples' opinions about the prevailing security climate are suspect. U.S. based companies need to view these situations from a wider perspective.

CONSISTENCY AND COMPLACENCY

Good habits are only effective when they are consistently applied. Being consistent is easier when we accept the possibility of an attack against us.

This is not to suggest that the risk is elevated beyond reality so as to produce an over-reaction that may limit your ability to work or function efficiently. Indeed all procedures should be geared to a professional assessment of the current risk.

All security arrangements which vary an individuals habits and lifestyle can be an inconvenience, but in a low to moderate risk environment, that is all the arrangements need to be —inconvenient. And in all cases the need to vary one's habits becomes less tiresome when the new behavior becomes internalized.

Where there is an element of risk, complacency, a fatalistic approach or a laissez-faire attitude towards personal security presents a major vulnerability. The old saying, "If it's going to happen it will and there's nothing I can do to stop it" is becoming more than tiresome and executives would be surprised how endemic this opinion is even among security managers who ought to know better.

The problem is that most security procedures are unproductive; they are implemented and there is usually no feedback as to whether they have been effective or not. However there are many documented cases that suggest that would-be attackers had selected a possible target, but were deterred by what they saw.

Consistent security procedures had therefore transferred the target elsewhere; criminal operatives had considered a target but had decided that, on a risk-benefit basis, the same objectives could be achieved more safely elsewhere.

AWARENESS AND SUSPICION

Awareness is not a natural state of mind in a busy world; apart from times when traffic conditions threaten us, we drive along and notice or remember little of the journey. Instead we think about what needs to be done today in the office, about the current project, about personal problems and a myriad of other more important details.

Likewise with suspicion. Very few of us are naturally suspicious unless we have learned to be this way due to an unfortunate past experience. We all want to believe that everyone will treat us as we treat them.

To be forced to consider otherwise, to be forced to believe that there are individuals out there who intend us harm is both depressing and stressful.

One way to deflect any possible harm is to develop both awareness and intuitive suspicion. The latter means that individuals should exercise a certain amount of reasonable suspicion that will provide them an intuitive feel for possible danger or pretext incidents.

To become aware requires exercising self-discipline; the self discipline necessary to put other considerations off until individuals are ready to think about them; to devote some time to identifying and interpreting everything that is going on around them.

How many times have we all been standing next to someone we know well and have not noticed them? How many times have they seen us before we have seen them? How many times have we narrowly avoided an accident because we have let our vehicle get into a situation which could have been avoided with a little forethought and concentration?

On the plus side, there is a satisfaction in being aware of all that is going on around us; at first it requires effort, concentration and practice, but later it becomes almost automatic with oddities and possibly suspicious circumstances intervening to sound the alarm.

This basic degree of awareness can be built on by imagining "what if" situations that present a danger: what do we do when in slow-moving traffic and to our disbelief, the man walking towards our car and looking at us reaches inside his jacket and pulls out a handgun? What happens next if we drive round a curve and find the road blocked by an truck? And so on.

We will be more able to deal effectively with the gun situation if personal protection procedures have been correctly implemented. For example, we will be aware of the following:

— We overcame surprise because we are aware of the man’s actions.

- Our car is not armored and will provide little, if any, protection against a handgun bullet.
- An accurate shot from a handgun will be that much more difficult if evasive action is taken.
- Our windows are open no more than 2 inches and the doors are locked.
- The use of our horn or a siren fitted to the vehicle will possibly deter an attack.
- We left sufficient space between our vehicle and those next to us to permit some maneuvering.
- Our vehicle can be a lethal weapon if the threat makes this necessary.
- Our natural aversion to striking another vehicle will be overcome by the threat of graver consequences.
- We have previously thought about “ramming” techniques and the best way to clear a path without disabling our vehicle.
- Our seat belt is on and will help to restrain us in the event of a collision.
- We have practiced emergency vehicle tactics ourselves during defensive driving courses.

Intuitive suspicion can be characterized as a "gut feeling". The feeling is all the more relevant if it is based on a threat assessment and from awareness of what is going on around us. Unfortunately, we all have a tendency to disbelieve the unusual or suspicious when it confronts us directly.

We read about the unfortunate victims of a hijacking, but are comforted by the fact that we are never going to suffer a similar traumatic incident ourselves. We refuse to believe something bad is happening to us unless we are presented with irrefutable proof.

The same attitude applies to how we conduct our everyday lives. We witness subconsciously or otherwise a series of suspicious or unusual events and yet continue into a scenario in an effort to prove to ourselves that it was just a coincidence or that we were foolish to be worried. Even though we know that a criminal’s planning is usually rigid and that any an unforeseen interruption to the plan can abort the attack, there is still a tendency to drive up to a roadblock, or leave the residence when a car is suspiciously parked nearby, or to allow a someone to follow us into a remote area or virtually unoccupied car park.

What do we lose by refusing to go into a possible dangerous situation? A little time perhaps or the prospect of minor ridicule from our less security-conscious passengers, or our own embarrassment if our suspicions turn out to be unfounded. But who cares. We are safe.

NARRATION

Narration is a learning tool used to train advanced police drivers. The concept is particularly helpful because it forces a driver to increase his or her awareness of traffic situations and operate the vehicle accordingly. Narration can also be used by executives as a valuable tool to elevate their awareness. The training involves describing aloud everything the driver notices, is doing or intends to do. The process quickly becomes internalized and continues without the need to describe actions aloud.

ROUTE PLANNING

Route planning has been briefly mentioned before and becomes more effective, security-wise, by paying attention to the following requirements:

- Plot possible routes beforehand
- Be aware that the shortest route is not necessarily the safest route.
- Note possible vulnerable points and safe havens en route. Include:
  - roadwork
  - heavy traffic
  - a checkpoint
  - a tree blocking the road
  - an unusual street detour sign
  - a disabled vehicle blocking the road
  - unpopulated or heavily forested areas, etc
- Know the locations of medical facilities en route
- Ensure that the journey disrupts routine
- Ensure good communications during the journey
- Notify departure and arrival times to security personnel or a trusted individual. Agree beforehand on procedures in the event of non-notification
- Distribute details of your journey strictly on a need-to-know basis
- Travel at the maximum safe speed
- Exercise awareness and anti-surveillance procedures

USE OF INITIATIVE AND COMMON SENSE.

The use of initiative depends on a number of factors:

- An awareness of a change in circumstances
- The ability to comprehend a change in circumstances
- Recovery from surprise
- Quickly assessing the safest course of action
- Seeing that action through in a positive and determined manner

Much depends of course on us as individuals. We each know how we are likely to react to emergencies; are we flustered or immobilized by the unusual or are we cool, calm and collected until after the event?

Training in dealing with difficult circumstances often helps because it raises our threshold to the onset of panic because of knowledge and familiarity.

But not all of us get the benefit of training although in the field of defensive driving there are many excellent courses available that improve our ability to effectively control a vehicle under adverse and dangerous conditions.

As mentioned before, an effective way of self-training is to practice "what-if" situations.

All personal protection advice is based on commonsense measures and an analysis of past incidents. The recommended actions may not work on the day, but are considerably better than doing nothing. Unfortunately, people tend to ignore commonsense measures in an emergency.

Good personal security is a matter of methodically and consistently carrying out procedures which we have reason to believe may deflect an attack or may at the least indicate that something is going wrong.

The following are a few suggestions for use during a period of extra vigilance:

VISITORS IN THE WORKPLACE

During periods of heightened risk, consider the following points:

- Additional emphasis may need to be placed on access controls during any period of heightened threat.
- Pay additional attention to visitors in the workplace. To the extent possible, visitors should be by appointment only.

- Ensure that the recipient of the visit is informed before the visitor is allowed entry to the secure part of the building.
- Visitors should be escorted into and out of the building.
- Ensure that employee, contractor and visitor ID procedures are rigidly applied.
- Carry out a closer scrutiny of contractors. Ensure that changes in personnel are notified by the vendor in advance.
- Maintain a “clean desks” policy and keep executive offices locked when unoccupied.
- Configure each office with a duress button and rehearse its use.
- Implement a duress procedure to covertly request help in an emergency.
- Implement a notification/relocation/lock-down process if building security believes that unauthorized persons may have gained access to the building.
- Implement and think through bomb threat control procedures, including those applicable to handling mail.

RESIDENTIAL SECURITY

- Make full use of existing security measures such as the gated community or lobby guard, your intrusion alarm system, good quality locks, etc.
- Ensure that any residential security force is aware that there is a possibility that unauthorized personnel may try to gain access to the area, either surreptitiously or by pretext. Seek their help and advice.
- Remove vegetation close to your building that may provide concealment for an attacker.
- Make sure that the exterior is adequately lit at night.
- Don’t open a door to unexpected visitors until their identity has been confirmed.
- Verify a caller’s identity by means of an external camera, intercom or peephole. Keep interior lights in the entry way off and exterior lights on.
- Satisfy yourself that the bona fide visitor if not being held under duress by someone else.
- At night, obscure a view of the interior of the residence with blinds or drapes.
- Adhere to the rules regarding possible suspect mail.
- Document phone hang-ups, etc. Utilize caller ID and an answer machine to initially screen calls. Report threats immediately to the police and corporate personnel.
- If there is a discussion with a threatening caller, keep him/her on the line as long as possible. Try to determine the caller’s motivation and what he or she intends to do. For example, if the caller threatens to blow up the company’s premises, suggest that this may cost innocent lives – such a reply has sometimes elicited comments such as, “Yes, but I’ll do it when they’re not around” etc. Such responses may validate the threat.

VEHICLE SECURITY

The main points are:

- Vary routes between home and work.
- Identify safe havens along each route.
- Identify dangerous areas or “choke points”.
- Keep vehicle doors locked, windows closed and seatbelt on.
- Don’t stop too close behind other vehicles – leave room to maneuver.
- To the extent possible, avoid traffic jams or congested intersections. Choose a route on which there is likely to be continued movement.
- If you have car trouble, raise the hood, turn on hazard flashers and wait inside the vehicle with the doors and windows locked.
- Do not get out of the car to help a “distressed motorist”.
- Do not pick up hitchhikers or offer rides.
- Vehicles used by the family should be locked, kept clean and with alarm systems activated.
- Family vehicles should be garaged when parked at the residence. If there are signs that either a vehicle or the garage has been forcibly entered, refrain from touching the vehicle prior to obtaining professional advice.
- When family vehicles are taken out of your immediate control, for example during servicing, etc. they should be subject to a thorough and complete search prior to being taken back into general use.

The following general points apply to the day-to-day use of vehicles:

- Disrupt routine; apply time and route variance and use alternate vehicles such as those belonging the company/colleagues on occasion. Bear in mind that the shortest route is not necessarily the safest route.
- Prior to all journeys, think about the route or consult good quality route maps in order to determine the location of safe havens, hospitals, etc.
- Practice awareness and route narration as well as simulating the ramifications of hostile situations and formulating likely responses. (Note: If you are not fully conversant with these terms, don’t hesitate to ask for an explanation).
- Keep vehicle doors locked at all times during transit. Windows should kept closed if possible, but if they are to be opened, limit the gap to no more than two inches.

— Be aware that arrivals and departures are the most vulnerable parts of any journey. You should be prepared to drive past your destination and summon police assistance should suspicions be aroused.

— Be prepared to drive off as soon as passengers have safely entered the vehicle. Care should be taken not to sit in a stationary vehicle except when unavoidably detained by legitimate traffic conditions.

— Be aware of possible vulnerable points en route such as high-crime or unlit areas, curves, tree-lined areas bordering the road, road junctions, tunnels and bridges, high banks, narrow or deserted roads, the presence of combustibles, thick vegetation, overlooking features, heavy traffic and, above all, arrival and departure points.

— Establish communications using your phone en route. Route details and estimated arrival times should be provided to a designated company employee and/or family members. Reasons for delay should be notified to these individuals. The fact that arrival is not notified, together with route details, should be reported for investigation.

— Disclose the dates and times of proposed visits only on a need-to-know basis and never to unauthorized personnel.

— Equip your vehicles with a comprehensive medical kit (details available on request), a powerful flashlight, a fire extinguisher, vehicle tools, a tow rope, a crow bar and complete map documentation covering areas likely to be visited.

RESPONDING TO EMERGENCIES

Responding to emergencies is easier if:

— You notice the impending attack.

— If in a vehicle, there is room to maneuver. Remember a vehicle is a lethal weapon, but there is a psychological barrier to colliding with someone else. Always position your vehicle so that you are able to take evasive action. Seek guidance to familiarize yourself with anti-ambush and vehicle ramming techniques, the best way to recover from surprise, etc.

If in a vehicle, the preferred sequence of events (in diminishing order of preference) is:

— Drive through

— Reverse out

— Remain at the scene.

“Action at the scene” is the least preferable scenario. As mentioned above, if the first that is seen of the attacker is when he attacks, we have failed.

— All actions should be fast, aggressive, but controlled.

USE OF PERSONAL WEAPONS

The following comments apply to the use of a personal weapon:

— Persons in possession of a weapon should acquaint themselves with Federal and State laws governing the use of firearms such as licensing, a permit and the fact that the weapon should only used when the user’s life is in danger. The legal and other consequences of use of your use of a weapon should be closely considered.

— Those with access to the weapon must realize that situations may occur where it is necessary to shoot someone during an encounter. For this reason, they should be psychologically prepared for this contingency prior to carrying the weapon. Any hesitancy in this respect can result in the weapon being used against its owner. A weapon should never be produced to threaten or intimidate anyone.

— The purchased weapon should be appropriate to its proposed purpose. A revolver, such as S&W model 36 is an example of a simple and easy to use weapon.

— Children or minors should not be permitted access to the weapon.

— The firearm should be kept loaded with appropriate ammunition.

— Those likely to make use of the weapon during an emergency should be regularly and thoroughly trained in its use. Small arms training should be provided sufficient to demonstrate consistent, effective use of a lethal weapon. An assessment during training should indicate the likely response of the trainee to threat situations. Firearms refresher training should be regularly provided and periods between training should not exceed two months.

CAR BOMBS

An explosive device placed on or in a vehicle provides an effective method of targeting senior officials or company personnel. Such a device may well be hurriedly placed in position and a purely superficial search of the vehicle will be sufficient to alert the driver. Once armed, car bombs like many other types of improvised explosive devices (IED's) may have more than one method of initiating detonation and should not be touched. Effective deterrents to a car bomb include the following:

- A thorough search of the underside of a vehicle including wheel arches, body pan, beneath front and rear body sills, underside of the fuel tank and underside of the engine.
- A thorough inspection of the exterior of a clean car for signs of fingerprints and other indications that the vehicle has been tampered with.
- Equipping the vehicle with an effective car alarm system that will activate if anything has been added to the vehicle.
- Keeping the vehicle locked at all times when unattended and restricting access whenever possible by means of a locked garage or fence.
- Paying particular attention to searching the vehicle whenever it has been outside the driver's control, for example, after garage servicing, etc.

POSTAL BOMBS

Letter bombs are specially designed devices, small enough to be shipped through the mail, and usually set off by the act of opening. They can take the form of envelopes, boxes or other packages. Letter bombs are frequently meant to terrorize and although such devices are rarely fatal, they can inflict severe burning, can blind or result in the loss of a limb.

Letter bombs require the same three essential elements of other bombs: power source, initiator and charge. Tiny hearing aid batteries, squib-sized blasting caps and flexible sheet explosive are often used. Although relatively safe until interfered with, an untrained person is likely to trigger detonation irrespective of how the package is opened. With careful scrutiny, however, these devices can be detected -- or at the very least, suspicions can be aroused.

Look out for the following characteristics of letter bombs:

- Unusual postmarks or places of origin and excessive postage
- Incorrect addresses or titles of recipients -- particularly handwritten
- Signs of excess handling, wrapping, taping and inappropriate bulkiness
- A double label or one which may show signs of having been substituted or otherwise interfered with.

- Signs of excess handling or greasy-looking spots or areas
- Excess weight, springiness, stiffness, bulges or uneven balance or feel
- An odor of almonds or a chemical odor
- Pinholes from which a safety pin arming device may have been withdrawn
- The rattling sound or feel of small objects within the item

If a doubt persists relative to a particular package, do not open it. If suspicions seem to be confirmed, the suspected device should be placed away from personnel and law enforcement notified immediately.

SUMMARY -- REQUISITES OF PERSONAL PROTECTION:

For your continued safety, pay close attention close attention to the principles of personal protection which are again summarized as follows:

- Maintain a low profile
- Be aware and suspicious
- Develop good habits
- Be methodical
- Disrupt routine
- Remember your individual responsibility
- Utilize good communications
- Be consistent and avoid complacency