Basic Executive Protection - Proactive Security

Part One: Threat Assessment

A new wrinkle in the fabric of executive protection emerged recently shifting emphasis from preventative measures to post-incident preparation and contingency planning. This trend towards reactive security has the ability to obscure the primary focus of executive protection in subtle ways. Kidnap insurance, for example, represents a move towards reactive security procedures designed to facilitate the safe return of the kidnap victims. Kidnap insurance protects victims from financial harm including ransom, lost wages, and losses due to operational interruptions. Some policies cost in excess of $160,000 per year, yet make the assigned individual no safer than someone without an insurance policy. While a worthy pursuit certain to benefit kidnapees, reactive security methods like these in essence approach executive protection from a defeatist perspective. It's important, even critical, to know how to react and train to react properly, but reacting properly is not enough, especially if there are measures available to help avoid danger in the first place. The proper approach to executive protection has been, and always will be, preventive, proactive steps taken to reduce the likelihood of attack.

Proactive security can best be defined as a security program designed to anticipate and avoid danger. Proactive security suggests a comprehensive approach involving protectee threat analysis, advance planning and training for these threats, logistical sophistication designed to balance the comfort level of an assigned protectee with proper security procedures, and a thorough emergency response/crisis management plan. Executive protection providers operate most effectively when they understand the risks facing their clients, prepare to reduce or avoid those risks, and have the ability to react properly while maintaining a comfort level suitable to the protectee.

Four principles guide the successful operation of any proactive security mission: Threat Analysis, Planning, Logistics, and Emergency Response. As part of our commitment to providing critical information to security practitioners, Diogenes LLC will address each element of a proactive security regime, beginning with Part One: Assessing the Risk.

Assessing the Risk: Threat Analysis

Threat assessment involves investigative and operational activities designed to identify, assess, and manage risk, including groups and individuals who may pose a threat to identifiable targets. Threat assessment also represents the first step towards a proactive security regime. Understanding the potential threats and risks executives face provides the best opportunity to avoid those risks. This fundamental concept has existed from the time of Sun Tzu, who quipped simply "know thy enemy." This basic approach to proactive security exists today at the philosophical core of the United States Secret Service. As a guiding principle, the Secret Service continually reviews its security measures and training methods to assess its vulnerabilities in response to violent incidents around the world. This naturally reactive step folds neatly into the proactive

philosophy of learning from others' mistakes to avoid making the same error. By understanding violent attacks, the Secret Service places itself in the best position to both avoid such attacks, and respond properly if they occur.

With this concept in mind, the Secret Service recently completed an Operational Study of Assassination in the United States, in which several noted academics set out to investigate the thinking and behavior patterns of all 83 persons known to have attacked or approached to attack a prominent public figure in the US. The authors poured over every conceivable shred of evidence surrounding notable attacks in the U.S. during the last 50 years in an attempt to identify the profile of a typical attacker. The Investigators reviewed each subject's demographic characteristics, and examined their movements from the formation of the idea to attack through the attack itself. While no clear attacker profile emerged, the study revealed a common theme linking each attack or near-attack to an identifiable pattern of behavior, a "discernible process of thinking and action." This conclusion reinforces the protective strategies developed by the Secret Service and similar agencies. It forces the Secret Service and other security providers to focus on identifying risk-producing patterns, not risk-producing individuals.

Approaching executive protection from this point of view, proactive security practitioners can learn to recognize patterns of behavior which are more likely than others to produce harm, and prepare against those contingencies.

Focus on Likely Sources of Harm...

How do security practitioners identify legitimate risks? First, proactive practitioners prioritize potential threat sources. As an overriding principle, those who threaten don't attack, and attackers don't threaten. The Secret Service report indicated that none of the 34 people who actually attacked a public figure in the US over the last 50 years ever communicated a threat to do so directly to the intended target. The myth that attackers threaten victims can lead to the mistaken focus on those who threaten as the primary source of danger. This kind of error can introduce vulnerability to attack from a legitimate threat. Individuals who threaten protectees should not under any circumstances be ignored, but the most serious threat facing a protectee is unlikely to come from a threatening individual.

Because there exists no viable attacker profile, practical threat assessment focuses not on identifying types of individuals, but on thinking processes and behavior patterns, and specifically on identifying behavior patterns indicative of potential violence. To understand the process of violence, proactive security practitioners must focus on several vital questions raised in the Secret Service report: How do attackers move from the idea of an attack to actually attacking a public figure? What motivates people to act violently towards public figures? How do attackers select their targets? And finally, what planning strategies do potential attackers employ? Those who commit acts of targeted violence often engage in discrete behaviors that precede and are linked to their attacks including, thinking, planning, and logistical preparations. This part of the violence process can include: the development of an idea about an attack; early stage planning;

communication of the idea to others; following or approaching the target; and actually approaching the target in a controlled or secured setting. In addition, there are recognizable behaviors that are attack signals, even if not obvious "threats". These include: repeated attempts to contact a protectee through letters, phone calls, or other sources; repeated unwarranted presence at the office or other location where the protectee regularly visits; and attempts to approach the protectee at home. Any attempt to approach a protectee in a protected or private setting generally indicates probative efforts by the attacker to assess the target's accessibility. As the attack process unfolds, potential attackers will engage in this kind of probing activity to test the viability of different attack strategies.

Does the protectee create risk?

The second step in proactive threat assessment involves evaluating how the protectee's behavior will affect the type and number of risks that protectee likely will encounter. Some factors to consider: What countries does the client-company operate in? How much media attention does the company attract? Is the company high-profile? In a high-profile industry? How often do the company's executives travel abroad? How wealthy is the company? How well known is that wealth? Proactive security providers answer these questions while identifying potential risks primarily because they illustrate the same factors potential attackers consider while engaging in their target selection process.

Target selection will be covered in greater detail in Part Two of this article, but every proactive security practitioner needs to understand that fundamental to assessing the type and level of risk facing the protectee is understanding an attack or other violent situation from the perspective of the attacker. Kidnapping, for example, is almost never about the victim, but rather who or what the victim represents. In most cases kidnap victims represent money, or access to it. This is not to suggest that attacks are random, spontaneous events. In fact, most attacks on public figures are carefully planned over a period of months or even years. Removing the idea that a kidnap attempt centers around a personal attack can prove vital to reducing the likelihood of any such attack. Kidnappers and other attackers looking to make political or other statements are risk-averse businessmen who carefully plan and organize their activities. The best defense against kidnapping and related attacks is simply to make such attacks difficult. When viewed from the attacker's perspective, a well secured target represents high risk of failure, and most attackers will simply move on to easier prey. Armed with this knowledge, the proactive security provider eliminates significant risks simply by creating a secure barrier between the protectee and potential attackers. In other words, the safety of the protectee increases dramatically simply by having protective agents in place.

Proactive security providers must also be aware of the profile of the protectee. There exists a clear link between target interest and media exposure. The protectee's profile is most likely disseminated through the media. Press coverage generated by a merger announcement, a political statement, a company PR campaign, personal news, profit-

related news items, or other information transfers about the protectee drives the protectee's profile. Generally, the greater exposure in the media, the greater exposure to risk. Corporations have a reasonable desire for business-related media coverage. We've all heard the expression "there's no such thing as bad press". From a risk-avoidance perspective, however, there is such a thing and security conscious organizations must balance the desire and utility of press exposure against the risk created by such exposure.

Proactive security focuses on the ability to anticipate and avoid danger. Proactive security providers constantly analyze the circumstances surrounding assigned protectees in order to identify, evaluate, and control potential risk. By employing proper threat assessment methods and practices, proactive security providers take the first and most vital step towards an effective protective mission.

Part Two: Planning

Proactive security can best be defined as a security program designed to anticipate and avoid danger. Proactive executive protection practitioners take a comprehensive approach to protective missions involving threat analysis, advance planning and training, logistical sophistication, and a thorough emergency response plan. Executive protection providers operate most effectively when they understand the risks facing their clients, prepare to reduce or avoid those risks, and have the ability to react properly while maintaining a comfort level suitable to the protectee.

Security today has little to do with size and strength. Rather, brainpower is a security officer's best weapon: risk assessment, advance security planning, and preparation are the proper tools of a capable security service. Proper planning often represents the critical difference between a security service that is able to perform and one that is not, and can be found at the core of every proactive security program.

Four principles guide the successful operation of any proactive security mission: Threat Analysis, Planning, Logistics, and Emergency Response. In our last section we explored Threat Analysis. Now we turn to, Planning, the development of a security program capable of dealing with those risks.

Security Mission Planning

After considering the myriad of potential risks faced by a protectee, proactive security practitioners plan first to avoid those risks and second how to react if they cannot. There are thousands of variables and contingencies that must be accounted for and factored into any security plan. The ability to comprehend these variables and incorporate them into a security plan is vital to a proactive security program. Proactive security providers know that proper planning determines whether their mission succeeds or not. Proactive security providers know what to plan for by completing systematic security advance work for each protective mission.

Advance security planning involves investigating and identifying the variables in a protective situation and developing solutions to the hazards each variable represents. In other words, what could possibly go wrong, and how can we deal with it if it does? Often a retrospective approach considering the goals of the protective mission and working backwards from those goals to the operational details necessary to accomplish them is the most effective means of developing meaningful advance procedures.

Generally, the objectives of any protective mission are to prevent unintentional injury to the protectee(s) (vehicular accidents, medical emergencies, natural disasters), avoid embarrassing situations (unwanted media attention, invasion of private life, intrusion into corporate affairs), and anticipate and avoid intentional attacks (criminal threats, hijacking, kidnapping). With these goals in mind, proactive security practitioners combine a basic plan with the provider's standard operating procedures and establish a comprehensive advance planning protocol. The emphasis is of course on the details, and proactive planners take each major component of the protective mission- itinerary, location, and transportation- and break it down piece by piece.

Security Advance: Itinerary

A majority of advance and pre-advance planning centers around the itinerary for the protective mission. Begin with the overall objective of the assignment- corporate meeting, international travel, public appearance- and make an effort to understand exactly what the protectee expects to accomplish. A review of the expected itinerary will provide the "what-where-when" basis on which to design advance protocols. From there, advance planning can be divided into three phases: the pre-advance, where the security practitioner and client make initial plans; trip advance, where the security practitioner finalizes all arrangements; and site advances, where the security practitioner physically visits each scheduled location immediately preceding the protectee's arrival. The goal in each phase is to eliminate surprises, develop thoughtful contingencies, and avoid hazards and potential vulnerabilities.

During the pre-advance, the security practitioner meets with the client to collect information. In general the security practitioner seeks information regarding the nature of the assignment, dates and times for each stage or planned aspect of the assignment, locations of each stage, key personnel involved, special protectee requirements, special medical requirements, required or preferred transportation and lodging, and any known threats. Armed with such information, the proactive planner identifies the full range of information required, and begins to make initial arrangements. The proactive planner contacts key players involved in each aspect of the assignment- local business representatives, managers for accommodations and transportation services, and local law enforcement- and both provides and gathers information pertinent to the assignment. As this initial phase unfolds, the proactive planner will begin to prioritize key elements of the assignment and formulate a procedural checklist for the next two planning phases.

Phase two of advance planning, referred to as the trip advance, involves finalization of details and arrangements made during phase one. The security practitioner contacts all agencies and personnel involved in the assignment to ensure that all logistics are present and each party involved knows exactly what is expected of them. The trip advance gives the practitioner the opportunity to hammer out the fine points of the operation, actively consider contingency preparations, and focus on how the operation will be perceived from the protectee's point of view.

Immediately preceding the assignment, the proactive security practitioner completes phase three, the site advance, by physically walking through each stage of the planned itinerary as both a final check on operation protocols and an advance security sweep. At this point the security practitioner is down to specifics, looking for things that may go wrong at that particular place and time. This exercise represents a vital planning phase as the theoretical contingency planning essential to phases one and two cannot account for the last minute variances that often occur without fault or warning. With this in mind, the proactive security planner is on-site first, providing a buffer between such unforeseen events and the protectee.

Security Advance: Location

Proactive planning requires timely, accurate intelligence. This has fewer vital applications than in consideration of where the protective mission is to take place. Every security advance program should include site-surveys for each location involved or potentially involved in the assignment. Hotels, airports, meeting rooms, corporate offices, outdoor venues- any location the protectee plans to visit must first be reviewed by the security practitioner.

Initial contact at each location should be with the general manager, who can provide both the names of subsequent contacts and the authority to contact them. As in all proactive assignments, communication is essential for success. The proactive planner develops a contact list, and ensures open and accurate communication between individuals involved in the assignment. Security practitioners often find it useful to conduct face-to-face meetings with key personnel to ensure each person understands their role.

Inspection of each location must also involve an inspection of the facility, the grounds and perimeter, and the surrounding neighborhood. The proactive practitioner looks for potential liabilities related to both unintentional injury and intentional attack. Physical inspection highlights vulnerabilities and illuminates contingency options. The security practitioner should consider the layout of the location in question, how to best negotiate the grounds in a manner best suited to the mission objective, proximity of local law enforcement or emergency medical services, alternate entrances and exits, and potential "safe" room locations. Also, during the physical inspection, the proactive planner formulates operational details including check points, surveillance posts, and command center locations.

Finally, during inspection of each location, the proactive planner considers whatever special services the protectee may require, and evaluates the availability of such services. For example, if the assignment requires a hotel stay for a protectee interested in physical fitness, does the hotel have an exercise room that can be properly secured? Will the hotel cooperate with measures required to accommodate the protectee within mission parameters? Often, these questions cannot be properly answered without first visiting and physically inspecting the intended location.

Security Advance: Transportation

Without exception, every protectee values the efficient use of time, and proactive security planners must balance the need for efficiency against security demands when considering how best to move the protectee. Transportation is the area most likely to disrupt an otherwise smooth operation, and requires significant effort on the part of the security planner to work effectively. Contingency planning is a security planner's best friend in consideration of transportation- if the plane does not take off, is there a train? If the car will not start, is there a back-up? Transporting the protectee is the most difficult and dangerous aspect of any assignment, and potential problems can only be minimized by thoughtful preparation.

Proactive practitioners begin with the basics- maps, schedules, and contact information. Planners must consider multiple routes, traffic rules and conditions, local sites of interest, parking options, and scheduling options for each possible mode of transportation. Proactive planners must also have established methods of communications at departure, en route, and at arrival. The proactive security practitioner expects something to go wrong and is prepared to then deal with it when it does.

Airline travel by either private charter or public carrier requires in-depth advance planning. Proactive practitioners know how to contact both the airline and the airport administration. They know the type of plane, tail numbers and call signs, owner of the plane, and the estimated time of departure and estimated time of arrival for each scheduled flight. Proactive practitioners consider transportation to and from the airport, baggage handling, special boarding requirements, special physical security or medical emergency needs, and customs issues. It many cases, special seating arrangements may be requested in order to ensure the protectee and protective agent are in the best possible locations.

Ground transportation requires similar attention to detail. First, attention must be paid to proper vehicle selection. Proactive practitioners consider the number of people to be moved, the environment they'll be moving in, what types of cars are acceptable to the protectee, and even what color is appropriate. Planners should familiarize themselves with the vehicle, check all safety equipment, and interview the driver to ensure the driver understands his role. Often, the protective mission calls for the use of security-trained drivers. A question often overlooked regarding ground transportation is where the car should be positioned while the protectee attends the scheduled event. The vehicle often

represents the primary means of escape and protection, and must always be staged in a place providing access to this protection.

Security Advance: Review

Executive protection should be invisible. Perhaps the highest compliment a security practitioner can receive is one where the protectee mentions that they never noticed the protective agents. Performance at this highest level can only come through meticulous preparation, attention to detail, and commitment to follow-through with the plan. Of course, other security concerns affect proper security planning than can be explored here. Proper security advance work requires consideration of security team assembly, command post logistics, and relevant legal issues. However, the preceding should provide an outline for the basics involved in planning a proactive executive protective mission. If for no other reason, proactive security practitioners should plan each phase of their security operation because those who would attempt to penetrate that security clearly will.

Part Three: Logistics

Proactive security describes a security program designed to anticipate and avoid danger. Proactive executive protection practitioners employ this philosophy daily, knowing they operate most effectively when they understand the risks facing their clients, prepare to reduce or avoid those risks, and have the ability to react properly while maintaining a comfort level suitable to the protectee.

In our last section, we explored Planning as the second phase of a proactive security operation. Proper logistics are the natural extension of a carefully planned protective mission. While planning represents the critical difference between a security service that is able to perform and one that is not, logistical sophistication represents the critical difference between a security service that will survive and one that will not. Efficiency exists at the core of any logistically sound operation, lack of efficiency eats away at the bottom line.

Four principles guide the successful operation of any proactive security mission: Threat Analysis, Planning, Logistics, and Emergency Response. Having explored Threat Analysis and Planning, we now turn to Logistics, the development of an efficient security program.

Logistics

If you ask most security practitioners what logistics means to them, they'll likely indicate that logistics means getting what I need, where I need it, when I need it. That's correct, to an extent. However, logistics is more properly defined in terms of efficiency. What separates solid logistical planning from poor logistical planning is the ability to get what you need, where you need it, when you need it in the most efficient manner. Think of it as getting everything in the right place at the right time cost-effectively. Proactive

practitioners know that efficiency means the difference between profit and loss, especially in a tightly-competitive industry like security. Redundancy and cost-overruns that result from poor logistical planning don't come out of a client's pocket, they come out of your bottom line.

The Council of Logistics Management has adopted this definition of logistics: "Logistics is that part of the supply chain process that plans, implements, and controls the efficient, effective flow and storage of goods, services, and related information from the point of origin to the point of consumption in order to meet customers' requirements."

Federal protective agencies have dedicated logistics officers whose sole responsibility is to make sure operatives are properly equipped. Private practitioners often do not typically have that luxury, and must rely on their protective agents to develop their own logistical sophistication. Logistics is an often overlooked skill requiring training and practice. While private practitioners don't have access to dedicated logistics agents, they can help offset this disadvantage by incorporating logistics training into their professional agent development program.

Several factors contribute to a successful logistics operation. Those playing the largest roles include:

A cohesive information infrastructure. The fluid nature of protective operations requires flexibility born out of the ability to communicate effectively. Communications protocols allowing the entire chain of command to transmit, receive and process data should be a part of each operation. The read-and-react element of proactive security is only effective in an environment capable of adapting to meet challenges as they develop. Each operation, then, must provide a superior communications-technology infrastructure to ensure the practitioner's ability to react to last minute changes. Increasingly the emphasis lies on technology, with the best suited practitioners often being the ones who take advantage of communications technology to stay ahead of the competition.

Similarly, vendors, suppliers, and third party practitioners (drivers or contract agents, for example) must be a part of the communications infrastructure, and selection of these groups should be based in part on their ability to respond and contribute to the protective mission. Competent third party partners bring to the table the ability to be fully integrated into the required communications infrastructure.

Strong integration capabilities. Proactive security practitioners know that having a fully integrated operation requires agents, vendors, suppliers and third party practitioners to work together to provide for the safety of the client in a manner suitable to the needs of the client. This can be trickier than it sounds. Getting any group of people to work together can be difficult- getting security practitioners and related vendors to work together can be, well, a nightmare. Often the personality of the logistics agent plays a critical role in successfully integrating all key elements of the protective mission. Repetition is another valuable tool-- integrating third party providers into the protective

mission is best approached as a partnering process designed to build a relationship over time.

The successful logistics agent has the ability to partner with several third party providers, making them feel like part of a professional unit. Proactive agents maintain a network of key suppliers and reliable vendors that are aware of the agent's expectations and confident in their ability to meet them. Caution is warranted, however, as discretion requires that security practitioners maintain confidentiality. But involving third party providers in the details of the operation allows those providers to work with the security team to the greatest extent possible, as opposed to just working for the security provider. Finding a proper balance between "need to know" and "would be useful to know" is the logistics agent responsibility, and, once accomplished, results in a sophisticated, professional operation.

Process-improvement expertise. Proactive security practitioners learn from their mistakes. Developing logistical sophistication is an ongoing process that demands constant attention and improvement. Proactive agents own the ability to carry lessons from past mistakes into future operations, eliminating waste and maximizing efficiency. It might seem like common sense, but too often similar mistakes plague consecutive missions. Logistical sophistication will flow naturally from the ability to monitor operations and suggest ongoing improvements. While the tenets of proactive security may not be open to constant innovation, the development of an efficient security service certainly is. By exploring and refining new ways to manage personnel and equipment, security providers can improve the bottom line.

Control. Lack of control can erode profits, and end client relationships. Logistics agents must maintain control over all aspects of the operation, including the security of sensitive material. The same tools that can make an operation successful--communication, integration, review and development are the same avenues through which an unforgivable information leak can escape. Given the likely profile of a typical protectee, security is an important consideration. Again, the logistics agent is charged with balancing the client's demand for confidentiality against the pure business sense of efficiency tools like open communication, integration, and process review and improvement.

A logistically sound operation is an efficient operation.

The goal of a logistics agent is to maximize the efficient use of personnel, vehicles, and equipment. Logistics agents must look for opportunities to maximize efficient use and minimize waste, especially in the context of private security, where waste can cause profit margins to disappear completely. The idea sounds simple enough, but can prove daunting in practice. Here are a few tips from the field:

Cut the fat, but cut the right fat. The single most important guiding principle in cost-reduction decisions is what impact such decisions will have on the client. The client's safety is the proactive agent's foremost thought. The client's happiness should be a

close second. Every decision in the planning and logistics stage potentially impacts the client's impression of your performance. Slight miscues can end client relationships. Therefore, logistical sophistication entails the ability to make cost-cutting decisions that will not negatively impact the client's happiness. Failure to meet customer demands is a surefire step towards long-term insolvency.

Yet some practitioners operate on a locust-like mentality squeezing what profit they can out of each client at minimal expense before moving on. Any competent professional will tell you that this is not a successful business model. The proper approach is to appreciate the client's needs, and develop techniques for meeting those needs without redundancy or wasted resources.

Don't reinvent the wheel. Competition within the security industry is fierce, and not always contained to inter-company battles. Add to that the heightened sense of urgency surrounding client confidentiality, and the result is wasted intra-company resources. Security practitioners often own vast amounts of detailed operations information that is so highly sectioned that agents within the same organization repeat the same resource-planning steps mission to mission. Bearing in mind confidentiality concerns, most security practitioners can benefit from centralizing mission planning information to promote efficiency.

Equipment Bundles. In order to help visualize the total equipment demands of a particular operation, it may be useful to consider "equipment bundles". Instead of drawing out a list of every item needed for a particular mission, and then figuring out how to move each piece of equipment, consider the basic equipment each agent needs as an equipment bundle, then figure out how to move the bundles. For example, let's say your next assignment requires 10 flashlights, 10 first aid kits, 5 bullet proof vests, 10 radios, 3 laptop computers, 4 vehicles, 2 sets of debugging equipment, and 5 handguns. Instead of worrying about whether or not each individual piece of equipment is accounted for at every mission venue, reduce the equipment list to a bundle, and track each bundle. Here, one bundle could consist of 2 flashlights, 2 first aid kits, one bullet proof vest, 2 radios, one laptop computer, and one handgun. Assign each bundle to an agent, then figure out how to move the agent and his or her bundle. Simplifying the number of items to move and account for will reduce error, waste, and frustration.

Leapfrogging. When a protectee will visit multiple venues, personnel and equipment bundles can be coordinated to stay one step ahead of the protectee. The Secret Service long ago developed a "leapfrogging" technique, whereby agent teams move to several spots in coordination and ahead of the President's schedule, effectively cutting resource needs in half. To illustrate, say the President's schedule calls for an 8:00am arrival at the airport, a 9:00am breakfast meeting, a 10:30 golf outing, a 2:00 power lunch, a 3:30 fund raiser, and a 5:15 departure time. Each venue does not require its own agent team. Rather, one team can be assigned to handle airport arrival and departure. A second team handles the breakfast meeting and the power lunch. A third team tackles the golf outing and the fund raiser. At each location then, the agent team is in place in

advance of the President, can stay for the duration of the visit, then can move to the next venue in orderly fashion without slowing the President's movements.

Obviously, private practitioners do not have access to the same resources as the Secret Service. But the idea of leapfrogging personnel and equipment bundles on protective assignments can still maximize efficiency and minimize waste, and provide a smooth operation destined to keep clients happy.

A well planned operation requires logistical sophistication to work properly, and proactive security practitioners survive on well planned operations. Developing sound logistics is a skill like any other, requiring years of practice to master. The rewards for mastery include long-term survival in the security industry, just as failure to develop the skill usually spells defeat. Part Four: Emergency Response

Proactive Security Part Four: Emergency Response

Part One - Threat Assessment studied investigative and operational techniques designed to identify, assess, and manage risk. In Part Two - Planning, we discovered that security today has little to do with size and strength. Rather, brainpower is a security officer's best weapon advance security planning and preparation are the proper tools of a capable security service. Proper planning often represents the critical difference between a security service that is able to perform and one that is not, and can be found at the core of every proactive security program. In Part Three - Logistics, we explored operational logistics as the natural extension of a carefully planned protective mission. While planning represents the critical difference between a security service that is able to perform and one that is not, logistical sophistication represents the critical difference between a security service that will survive and one that will not.

In this, the last section, we explore the final element of a proactive security program, Emergency Response. Threat Assessment, Planning, and Logistics represent purely proactive elements, while Emergency Response focuses on a proper response to an attack or other emergency situation. Through each proactive step, security practitioners prepare for the reactive step in a security operation- emergency response. Though an inherently reactive measure, proper emergency responses are achieved through planning and training and thus are inherently proactive concepts.

Emergency Response

The most visible members of a security team are the last line of defense, to be used only if the advance planning fails to anticipate and reduce risk. Most everyone is familiar with the image of dark-suited Secret Service agents surrounding the President of the United States or jogging alongside the Presidential Limousine. Highly trained Secret Service agents maintain positions around a protected person in order to deter or stop an assault. These agents are prepared to stop an assailant or shield the protectee from harm. They represent a conspicuous and observable barrier between the protectee and a possible attacker. They also represent the less-observable advance team and behind-

the-scenes coordination designed to limit lethal access to the protectee. As we discussed in previous issues, advance work, planning, and logistical coordination represent the building blocks of a proactive security program. These steps lay the foundation on which to base the final element of a proactive program emergency response.

Ironically, emergency response actually represents a reactive element of a proactive security program, and a critical element at that. Just as the ability to respond to a crisis is insufficient without threat analysis and advance planning, all the preparation in the world is useless unless the responsible agents react properly at the critical moment. It's important, even critical to know how to react, and to train to react properly in a crisis situation. One lesson taken from the Secret Service makes clear the only way to ensure that protective agents will react properly when called upon is in-depth, consistent training.

Training

Security training is a process like any other it requires constant reinforcement to maintain effectiveness. Protective agents, especially, require constant reinforcement of protective techniques. "Cover and evacuate" is not instinctual, but it's the right move when faced with an attack on a protectee. Proactive agents must train constantly so that "cover and evacuate" becomes instinct. In attack situation, agents have seconds, or fractions of seconds, to react and they must be able to respond without thinking. To a proactive agent, "cover and evacuate" must come as naturally as breathing.

Training exercises must be realistic in order to be effective. Attack situations involve savage emotional impact because of the speed with which they normally develop. The sudden change from status quo to chaos is enough to freeze most individuals. But protective agents must react properly in those first few seconds of chaos. Properly trained agents overcome the shock of the attack situation by remaining composed and reacting instinctively because they are "comfortable" in the attack situation. Proactive agents are literally "cool under fire."

Realistic scenario training involves repetition exercises similar to the very same operation techniques employed by the agent, with the occasional attack on the protectee. Training sessions should involve more exercises without attack than those with in order to best simulate real-life attacks. Attacks on principals are in fact very rare. Training must simulate tedium, if the impact of the simulated-attack is to be effective.

The Secret Service rotates agents through training sessions every 6 weeks. Private practitioners may not have the resources to move agents through training on such a rigorous schedule, but must not ignore their responsibility to maintain regular training sessions– even for experienced agents.

Proactive Reaction?

Properly trained proactive agents react properly. Sounds odd, but it's true. The proactive nature of security operations, threat assessment and planning, pre-determines the appropriate reaction in attack scenarios. The "appropriate response" in any situation depends on several factors. Proactive security practitioners are able to identify each of the relevant factors and plan accordingly. As a result, proactive agents do in fact react properly. Based on a combination of training, experience, and preparation, a proactive agent faced with an attack reacts immediately to protect the principal, and remove the principal from harm.

Medical Training

Part of a protective agent's training regime should involve medical training. In the unlikely event of a successful attack on the protectee or some other medical emergency, the protective agent's immediate treatment may spell the difference between life and death. Seconds after John Hinkley shot President Reagan, Secret Service Agent Jerry Parr performed an on-site assessment of Reagan's medical condition. Despite lack of visible wound, Parr determined that Reagan needed immediate medical attention. Parr noticed frothy red blood coming out of the President's mouth, and because of his medical training knew that oxygenated blood indicated a possible wound in the President's lungs. Parr re-directed the evacuation team to nearest hospital, and in so doing saved the President's life.

Proactive agents are capable of emergency triage. The ability to assess an injured person's medical status and make critical decisions based on that information. Through proper planning and with proper logistical support, proactive agents are aware of emergency treatment options at all times and have the ability to reach them. But neither of these capabilities does much for an injured person if the agent's cannot accurately determine which of those options is appropriate.

A proactive agent's trauma response training such include the following skills:

Ability to provide treatment, stabilization and care of those injured at the scene;

Ability to recognize and provide appropriate transportation;

Access to an ability to use emergency medical equipment;

Ability to establish effective triage points and systems and determine the priority evacuation needs of those injured;

Ability to communicate effectively with trained medical personnel; and

Ability to maintain emergency cover throughout the trauma incident and stabilize protection.

Medical training is such an important element of a proactive agent's emergency response training because agents are far more likely to encounter a medical emergency than they are an actual assault on the protectee.

Conclusion

Protective agents must react properly in emergency situations. Agents cannot so react without proper identification of possible threats and pre-determined responses to each threat accompanied with the ability to carry-out each planned response. In essence then, the proactive elements of a proactive security program depend for their validity on the sole reactive element– emergency response. Similarly, proper reactions to emergency situations come about only through proactive threat assessment, planning, and logistics. Though seemingly circular, the entire concept subsumes the very nature of proactive security: identify and plan for every possible misstep, be prepared to counter any threat to the protectee, ensure your ability to handle any emergency, and thereby reduce your need to do so.