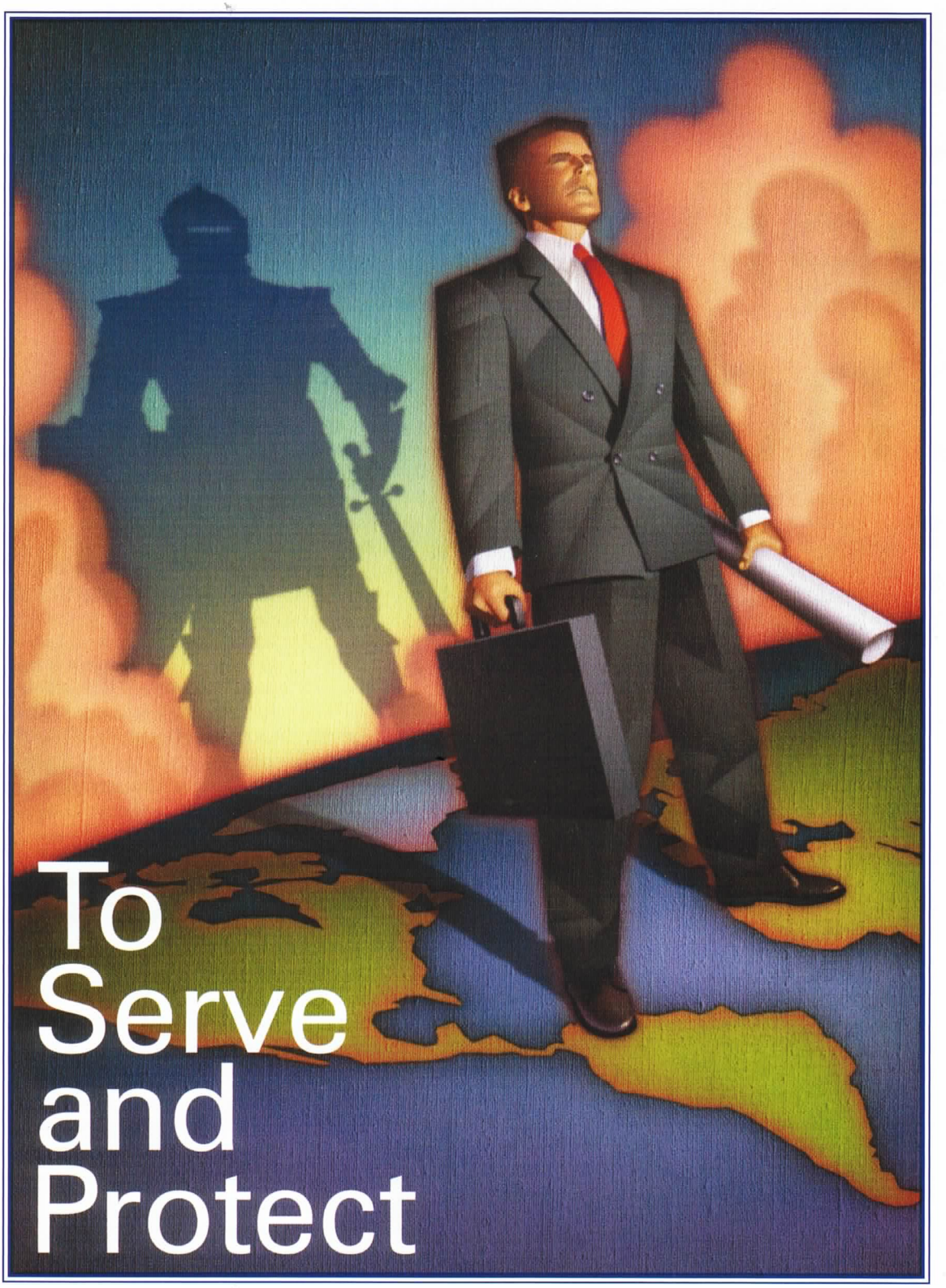
GLOBAL STRATEGIES, INC.



1600 Tysons Boulevard / 8th Floor
McLean, VA 22102
703.818.7191 / www.gsiprotection.com / info@gsiprotection.com

EXECUTIVE PROTECTION | Long before an executive plans a trip, security should have a plan for handling the executive protection component.

To Serve and Protect

A corporate security director's phone rings at 9:10 on Monday morning. "Jim, we have a trip coming up to Sierra Leone with the CEO and the VP of business development for Africa. We're leaving on Friday and HR thought I should give you a call to see if there were any concerns you might have."

As unlikely as it may seem, these sorts of last-minute queries for security advice before a potentially dangerous trip are still fairly common after 9-11. Although security is receiving unprecedented attention in the business world, many executives perpetually think about profits before protection. It's up to the security professional within the company to make sure that the executives and others involved in arranging travel understand the importance of addressing protection issues early in the planning process.

When the possibility of a business trip to another country arises, the first step is to conduct a risk assessment to gauge whether protection is indeed necessary, and if so, how much. Security should gather information on sites to be visited, threats, and other topics to educate themselves, the protection team, and the principals. Next, whether to use in-house staff, outside contractors, or a combination of both must be considered, and training and logistics addressed.

Risk assessment. The general principles espoused in the ASIS International Risk Assessment Guideline are applicable to the executive protection risk assessment process as well. With regard to traveling executives, this includes identifying executives who will be on the trip, the historical and possible future types of risk events, and the probability of such incidents or other problems occurring while the company's executives are there. The team should determine the likely impact of such events, develop options to mitigate risks and study their feasibility, and perform a cost-benefit analysis.

One question is, who merits the protection. In some cases, it may make sense only for senior managers. However, managers or staff lower on the chain of command may merit protection as well, if the location is particularly dangerous, their itineraries are troublesome, or they are uniquely important to the successful completion of a trip. Of course, kidnappers may strike indiscriminately, knowing that any employee of a Western company is an important bargaining chip. Determining the extent of any protection for these personnel requires an analysis of the risks and costs, as discussed later.

Dossiers. If it has not already been done, security should compile dossiers of executives who will be traveling. At a minimum, these should include copies of passports, photographs, and indication of blood types and allergies, and emergency contact for family members.

[By Christopher J. Simovich]

As Seen in the October 2004 issue of
Security Management

Threats/vulnerabilities. In assessing threats and vulnerabilities and the probability of any future event, corporate security should consider the history of the site, country and region, specifically with regard to political stability and general crime and violence. It should also examine the history and future likelihood of natural disasters.

Country-specific assessments from both the State Department and private companies, such as iJet Travel Risk Management, are good sources of this information. These assessments may offer even such granular detail as rainfall averages to let companies consider the threat of storms and flooding. They are especially useful in alerting companies to evolving man-made threats, such as crime and political instability.

The right intelligence can help a company decide whether to increase security, alter travel plans, or curtail operations before a dangerous situation turns into a crisis. For example, one of the author's client companies, which had factories in Sierra Leone, at first pulled its non-native workers out of the area when civil war broke out. Ultimately, the political instability led the company to evacuate and shut down the facilities altogether. Because the company kept an eye on the situation as it progressed, it was able to change its plans and get personnel out safely before it was too late.

The security team should also assess whether the country, region, or city being visited has a history of acts of violence directed against the company, its industry, or foreign travelers and foreign companies in general. A corollary question is whether the subject company has been a more frequent target than other companies.

Some of this information can be garnered from public news reports. Security professionals should also ask their counterparts in other corporations about their in-country experiences that may not have been reported in the news.

The security team should also consider whether any new factors or issues pertaining to the region or the business make the corporation or industry a more likely target of future violence. For example, the author's firm represented a U.S.-based company operating in Belize, on the border with Guatemala. The firm used Jane's Electronic Information Services to obtain statistics and locations of political violence against various nationalities of foreigners. The intelligence showed that Guatemalan guerrillas had been entering Belize, near the client's site, to kidnap Westerners and extract ransom payments. Unfortunately, the client chose to ignore this information, and a family member of the owner was subsequently kidnapped and taken to Guatemala.

> If it has not already been done, the security team should compile dossiers of executives who will be traveling abroad.

The person was held captive for three weeks, during which time the client had to call on the military and other forces for assistance. While the family, in this case, was able to save their relative by paying out a high ransom, everyone involved suffered considerable stress that could have been avoided. The client now

Leveraging Technology

The Internet, the ultimate information resource, provides a wealth of resources for gathering background material. Up-to-date studies on countries around the world are available through online government agencies such as the U.S. State Department. The Overseas Security Advisory Council (OSAC) provides timely and recurring information through daily briefings and updates that are e-mailed automatically and cover the country profiles of one's choosing.

Country fact books abound on government sites, such as that of the CIA. These detailed resources provide information ranging from the amount of rainfall and executive might expect to the biographies of current government ministers.

Many security departments use these resources to create their own "country reports" incorporating information and maps from the risk assessment. These documents should be used not just as an information tool for executives traveling in high-risk areas but also as an opportunity to educate the executive on why a protection program is necessary and how the threat profile was developed. To increase the likelihood that busy top executive will really read this information, security professionals should boil down the reports to a two or three page executive summary.

The free government information can be supplemented by various private sources, which charge a fee but generally update their information more often than the government. These companies provide data on political violence, terrorism, and natural disasters, and they often make the information available through telecommunication devices such as global positioning systems or satellite phones, so that it can be accessed from any location while the team travels. Such systems typically work well, but satellite reception can be spotty in cities.

Some companies rent telecommunication devices on a per-trip basis, which may be more cost-effective option than purchasing them outright, depending on how much and where executives travel. These devices can be used to give the traveling executives relevant up-to-date information via text messaging. The updates allow executives to make informed decisions as to their own safety and security. But devices should be tested by security in real-life situations as part of the advance before they are given out for field use.

Another caveat is that some governments forbid foreigners from bringing such equipment into their country. For example, Middle Eastern and some Southeast Asian countries make it difficult to carry in such devices. In those cases, the team will have to stay current through more traditional means.

uses executive protection regularly, and this scenario is used as a case study by the author's firm to educate other clients.

With regard to historical incidents, the security team should identify who was behind them, how they were carried out, and other information that might be instructional. Security should also ask whether overseas personnel are required to maintain residences within a "Green Zone" or other protected area. This type of housing arrangement signals a more dangerous environment. If this is the case, security should also ask how protection is coordinated in and out of secured areas.

Options. If corporate executives absolutely must do business within a high-threat region, they should be presented with several options that will reduce their vulnerability to the risk of going to that location. One choice is to relocate to a nearby safer site. For example, a business meeting to be attended by a CEO and high-level staff on improving the Iraqi infrastructure, slated to take place in Baghdad in early 2004, was diverted to a safer haven in the nearby Persian Gulf island nation of Bahrain. This alternative enabled corporate executives to show that they were committed to their business endeavors with their foreign partners while keeping executives out of a de facto war zone.

Another option is for several companies with the same needs to pool their efforts to help make security cost-effective. Even members of competing corporations have pooled resources when operating in a high-risk environment, as in the case where two large oil corporations operating from the Northern Moroccan coast purchased and secured a ten-room villa and estate for use by their senior executives while conducting business on trips to the region. The villa was part of a compound of Western residences and buildings protected by U.S., British, and French security forces.

Logistics. Because an executive is typically on the move when being protected, logistics are a major consideration. Most logistical planning can be taken care of with a U.S. Secret Service-style 11-point advance, which should be overseen by the security manager. Much of this can be considered a "pre-advance", which should be overseen by the security manager because it doesn't require the security manager to set foot in the foreign country. Other elements, however, do require being in-country.

These duties include arranging points of contact, motorcade arrival and departure points, protectee's movements and schedule, rooms and housing. This work must also address the placement and posting of agents, emergency procedures, technical security considerations, identification insignia for protective team members, transportation, and procedures for agents to file reports to the lead agent.

One challenge for security during this stage will be to ensure that as the company develops the executive's travel itinerary, it considers the security implications of the choices. For example, companies are increasingly using Internet travel services to get the cheapest fares, but doing so often removes control of the travel route from the company. It may be cheaper to get to Baghdad through Kuwait than it is through Syria, for example, but it will also put the executive on a much more dangerous surface route to that city.

Once in the country of destination, an advance team must check out the environment and locations where the executive plans to be during the trip. Ideally, an on-site advance will match the length of the executive's stay; that is, a five-day trip should get a five-day advance. Few companies are willing to devote resources so liberally to an advance, however. Advance teams rarely get more than two days to do their work.

Advance agents should visit every location where the executive is likely to go. They should also ask each site detailed questions about security procedures and observe them if possible.

During the advance, routes should be mapped out to match the executive's itineraries, with attention paid to any dangers that might be encountered on these routes. The team should note the location of hospitals, U.S. embassies and "safe zones" and their relationship to where the executive will be at various points in time. Alternative routes should be planned and discussed among the protections team.

An emergency egress plan should be arranged if the executive and protection team will visit countries involved in conflicts or located in extremely high-risk environments. The egress plan should include possible recovery points, border crossing points, and communication procedures. It should also identify vendors (such as negotiators, medevac services, and airlift firms) that could be used if the evacuation plan had to be initiated. Some companies pay a periodic fee to such companies to ensure that their assets or services will be available during a crisis.

Licenses. The security manager must ensure that the protection team has obtained the necessary licensing or government permission to operate in the host nation. A protection team entering a host nation armed but without the proper licensing or permission will only endanger the executives they are meant to protect. For example, they may end up being detained on arrival and separated from the principal, causing the principal to remain in the public, largely uncontrolled environment of the airport for longer than necessary.

The security manager should apply well in advance for such licenses for proprietary staff and should ensure that the contactor has the necessary licenses as well.

Regional Security Officers. When an employee encounters trouble in an unfamiliar environment, nothing beats seeing a friendly face. Security managers should thus work on cultivating overseas contacts that can come to the aid of staff. Some of the best resources are U.S. government employees working in-country, such as the Regional Security Officers (RSOs) of the U.S. State Department, stationed at consulates and embassies around the world. RSOs are a fount of information and insight on the regional, political, economic, social, and security situation. It is important to coordinate with RSOs in advance of a trip and tell them where executives will be, when, and for how long. It is also critical to establish contact between the lead protection agent and the RSO, since they will be working together on site.

In the author's experience, RSOs offer exceptional cooperation and interest. While traveling on a high-risk protection assignment in the Middle East, for instance, the company's contact and coordination with RSO paid off hand-

somely. The RSO called to warn us of a 20,000-strong anti-American protest, where gunplay was expected, at a site executives were planning to tour that same afternoon. We were able to alter our agenda to avoid the trouble spot.

Other useful contacts. Security managers should also coordinate their professional counterparts in the same region. Many corporations assign country managers with the role of protecting visiting executives. Establishing a solid relationship with the country manager before executives travel to that country will make it much easier to gain the manager's support when the time comes for executives to make a trip. Ideally, the lead protection agent will have built a rapport with these country managers as well. A hasty effort to contact a country manager at the last minute may not be sufficient.

Proprietary vs. Outsourcing. When it comes to the actual advance and protection work for a specific executive protection job, security professionals can use internal staff or hire outside expertise. Maintaining a dedicated executive protection team isn't feasible for smaller companies, but some large corporations have developed an internal team and have avoided the costs and hassles involved with outsourcing. One telephone company, for example, has developed a superb in-house executive protection program since 9-11.

Some security directors find that adding executive protection to the services provided by their department enhances their team's overall value to management. These security directors often take the role of "lead protection agent" - where they accompany the executives during travel to high-risk areas--but that's usually not a good idea. While there is a natural inclination for security managers to control the environment of their executives, a protective detail in a high-risk environment is not the time or place to do this. However, if the security director has executive protection skills, he or she might serve as the in-house liaison (see below).

Corporate security directors might profitably join an executive's traveling party if allowed to do so and should even offer advice to the protection team. But these directors must trust the protection agents, allow them free rein over their operation, and stay out of the "protective perimeter" while executives are moving from point to point.

Another consideration is how much to rely on in-country (field) resources. The best approach is to maintain broad corporate control but to take advantage of field resources.

If the company is using contract executive protection services, it should request that one of the provider's agents come from a company office in the home country of the executive to increase the executive's comfort level with that one agent; other agents should hail from the country being visited.

In-house liaison. To add corporate control into the environment, corporate security should assign an in-house staff person with executive protection skills and training to the protection detail. The in-house person should be the primary contact or liaison between the executive and the rest of the team, communicating concerns both ways.

Training. Whether members of the protection team are in-house or contract personnel, they must be properly trained for the job. General security training is not sufficient.

Personnel tasked with protective services must receive specific training in both solo and team-based protection methods. They should be proficient with both firearms and non-lethal devices, such as pepper spray (OC) and batons (ASPs), pertinent to protective operations. They must have at least minimum proficiency in first aid with certification as a First Responder and follow-on training in trauma injuries.

If the protection agent is expected to serve as a driver, he or she should also be a graduate of a reputable school that specializes in protective driving. Martial art skills are useful, but it is the more subtle maneuvers that are relevant to this type of work, not the flashy moves seen in the movies. Executive protection agents are expected to be discreet, and quiet techniques, such as applying pressure to an adversary's pressure points, are best suited for the task.

Also important are annual follow-up training as well as training specific to carrying out operations in a high-risk environment. These specialized training topics should include protective intelligence, emergency medicine, advanced firearms, legal compliance, and radio/satellite communications, to name a few.

Training should include scenario-based exercises using real-world models. These exercises should test an agent's ability to respond to attacks on principals and medical emergencies in high-risk environments while under stress or under fire.

Many contract companies require their agents to receive 80 hours of in-service training per year, plus updated medical training to maintain First Responder certifications. Companies should ask contract providers specifically about the training and experience levels of the agents who will be assigned to them.

Cost-benefit analysis. While having an information security specialist on staff full-time is commonplace, having an in-house professional source solely for protective services is a tough sell come budget time, even in a post-9-11 world. And although executives are more receptive today than in the past to having a protective team join them on travel, here too, budget justification may be demanded.

One effective way to show the bottom-line benefit of a protective detail is to go beyond the security it provides, highlighting how it can boost the executive's productivity. Here's how it works: First, determine the total annual compensation package for executives. For our purposes, the May 10, 2004 issue of Forbes magazine listed the salaries of the top executive in each of the Fortune 500 companies. The top ten executives averaged an annual total compensation package of $58.5 million per year. Assuming the executive works the average CEO week of 65

hours, he or she earns $17,308 per hour.

The median annual compensation of Standard and Poor's 500 CEOs is about $4.6 million. In a 65-hour work week, that adds up to about $1,360 an hour.

One of the goals of a protection team is to facilitate and speed movement, such as through the customs process, because the faster principals are moved from one safe environment to another, the less threat exposure they face. But this minimization of wasted time also maximizes an executive's available work time. Showing how an executive protection team can maximize the use of an executive's time, drives home the security function's return on investment (ROI).

One Japanese financial institution uses protective services for just this reason. Besides protecting its rainmakers, this company has found that, on average, it saves the executive 25 hours per day because of the protection agent's ability to speed his charge through checkpoints and immigration stops. Based on the just-mentioned averages (the actual compensation amount isn't public), this translates into a minimum $3,400 in savings per day per executive.

Of course, the far more important value is that of securing the company's most important human assets. Although the value of an executive would seem self-evident, security managers may want to drive home the reality of the risk and the true cost of ignoring it by citing actual cases in which companies have lost a senior manager to an act of violence, kidnapping, or natural disaster and how that affected the company financially.

Security should also get figures on how much the company is paying yearly for Kidnap, Ransom & Extortion (KR&E) and travel insurance. There are typically substantial drops in premiums for companies that maintain protective details for their executives, have KR&E contractors in place, and have arranged extraction plans for their executives abroad.

The greatest sell of a protection plan to executives is through education. By providing executives with pertinent information on the environment in which they intend to operate - in particular, the specifics risks-the security manager will be better able to influence their stance on protective services.

Some of the best vacations are spontaneous, but that's almost never true of a business trip. Business trips benefit from painstaking planning and attention to detail, and the executive protection element is no exception. ■

Christopher J. Simovich is the president at Global Strategies, Inc. He is the author of numerous articles and books on Executive Protection and Security Consulting. He is a member of ASIS International.