



EXECUTIVE PROTECTION

EXECUTIVE PROTECTION CONSIDERATIONS

Introduction

In today's fiscally challenged business environment it may be difficult to justify providing an Executive Protection Program for an organization's key executives. However, in making this important decision one also has to consider what the cost would be to the organization's bottom line and, perhaps more importantly, to its reputation should a key member of the senior leadership team be the target of an act aimed at harming or embarrassing the individual and the organization.

Discussion

Any decision regarding enhanced personal protection measures for corporate personnel should begin with a complete understanding of the threat environment. This requires the development of a detailed understanding of the environment within which executives may find themselves – better known as the threat assessment. Detailed threat assessments allow the practitioner to see danger factors in a different light, appreciating both the contextual and progressive dynamics of a given environment. In general terms, Presidia has noted the following types of general threats faced by organizations and individuals:

- **Personal Threats:** Threats specific to the individual. These include threats from someone who may resent or have a personal issue with the Principal or the Principal's family.
- **Professional Threats:** Threats that may arise due to the Principal's specific position within his or her chosen profession or working environment.
- **Business Threats:** Threats that may be specific to an industry; in particular, those that may stem from special interest groups that may seek to cause harm or embarrassment to a Principal or the organization and bring attention to the subject's cause.
- **Geographical Threats:** Threats specific to a location that a Principal may be visiting. These threats can range from threats of violence from criminal or dissident groups to environmental threats such as weather, disease or natural disaster.

The above noted threats have been exacerbated in recent times by the increase in the use of social media. A controversial or perceived negative decision or action by a corporation or its executives can now reach an audience of hundreds of thousands of people in literally minutes. This has increased the risk of responses from individual activists, or organized groups who are willing to use extreme measures to make examples of organizations and individuals with whom they disagree.

As a result, it is extremely important for any decisions regarding executive protection measures to begin with a clear understanding of the threats, risk and vulnerabilities facing the organization and its management team. Further, these findings should be clearly documented, along with appropriate recommendations for protective measures, and communicated to members of the senior management team so that well informed decisions can be made.

Once a complete and thorough assessment has been completed and a decision has been made that one of the appropriate risk mitigation strategies is the development of an Executive Protection Program, then the next question is “how does the company go about doing that?”

A proper Executive Protection Program will be based upon the threats, risks, and vulnerabilities that were initially identified, bearing in mind that these factors will change with time and as such will require continual monitoring and updating. Although every situation will vary slightly there are key factors that exist in all Executive Protection Programs. They are:

- A robust intelligence program to ensure a clear understanding of the current threat environment
- Development of procedures for special events
- Deployment of properly trained chauffeurs
- Use of counter surveillance tactics
- Office and residential security programs
- Deployment of Executive Protection Operators

The primary aim of any Executive Protection Program is to provide the appropriate level of protection to the designated individual with the least amount of disruption to their professional and personal life. In fact, a properly developed and implemented program will enhance the life of the individual being protected. One of the big misunderstandings, often perpetuated by television and movie renditions of bodyguards is that the role of the Executive Protection Specialist is to be large and imposing. This is far from the truth. These specialists should be of low profile and unobtrusive while ensuring, through proper advanced planning, that the day-to-day activities of the principal being protected proceeds smoothly and that any potential threats have been planned for and all possible advance mitigation factors have been implemented.

Now that we understand the basic components of an Executive Protection Program and how a properly trained and experienced Executive Protection Specialist can assist the organization, we

will now take a brief look at what an organization should look for in the firms and individuals who may provide these services.

The image of the television or movie version of the large, imposing bodyguard clad in a black suit is the opposite of what is required. A professional Executive Protection Specialist's primary skill sets are intelligence, sophistication and diplomacy. These members must be able to easily blend in with the executives at professional and social events. Although the ability to react in the event of an untoward or violent occurrence is important, it is more important for the member to be able to be proactive and to identify and mitigate potential threats before they have a chance to take place.

The single biggest attribute of a proper firm or individual providing executive protection services is their ability to conduct advanced intelligence gathering and meticulous planning. In selecting a firm or individual to provide executive protection one has to consider their experience in conducting intelligence based threat and risk analysis as well as conducting background investigations on individuals and locations. The individual Executive Protection Specialist must be physically fit, professional and knowledgeable on security strategies. Often individuals are hired for these types of roles based upon their background in policing or the military, which alone does not make them appropriate for the position. An inappropriately trained and inexperienced member can quickly become more of a liability than a service.

Unfortunately, in Canada, unlike other countries such as Great Britain, there are no legislated or regulated standards for firms and individuals providing executive protection services. In all Canadian provinces and territories all that an individual has to have is a general security guard license, the exact same as anyone providing security services at malls or other such locations. That is why it is extremely important when seeking firms or individuals to provide executive protection services that a complete review of the firm and their team's training and experience is necessary. Ask for references from past clients who have received services similar to that being required by your organization, have interviews with the prospective firm or individual where you seek their response to scenario based questions. At the end of the day when the well-being of the member being protected and the reputation of your organization is at risk You do not want to enhance that risk by hiring firms or individuals who are untrained and ill prepared to provide the professional services you deserve.

About the Authors



Stephen MOORE

Stephen Moore is a police, security and emergency management professional with over thirty years of experience. He has worked with all levels of Government and with police and security agencies both domestically and internationally. Highlights of his career include leadership of the security program for the Department of National Defence and service as the Canadian Forces Provost Marshal (Chief of the Military Police) leading an organization of 2000 members delivering policing, security and criminal intelligence services both in Canada and abroad. Stephen is currently the President of Presidia Security Consulting.



W.H. (Bud) Garrick

W.H. (Bud) Garrick has more than 30 years of experience in the realm of police and security operations both domestically and internationally. He served with the Canadian Forces Military Police for 27 years, retiring as a Lieutenant Colonel and Commanding Officer of the Canadian Forces National Investigation Service, upon retirement he assumed the position of Deputy Director General for Criminal Intelligence Service Canada. He is currently the Vice President of Presidia Security Consulting.

Additional Articles from Presidia Security¹

Ask the Question – What is Your Security Strategy?

Security is often thought of as a tactical issue that should remain at the “gates and guards” level. While these tactical security pieces may be important they are most effective as part of a security strategy that is designed to mitigate the threats and risks to your company and its operations. True security strategy is integrated into a company’s “C Suite” and is seen as an enabler. The questions and discussion that follow outline the framework for a company security strategy.

Assessing and Tracking Threats - Protecting Your Employees and Your Company

Recent incidents of violence in the workplace in Canada tragically illustrate what happens when threats materialize into actions; they serve as a stark reminder to businesses across the country of their responsibility to protect their employees in the spirit of “due diligence” and “due care and attention.” Rarely, if ever, do these violent situations manifest themselves without some sort of prior indicators. This underscores the importance of having proper procedures in place to track and assess threats to your employees. Take the time to review the following recommendations to determine whether your company is prepared to address threats to employees.

Due Diligence Investigations

If asked, many companies would say that they have “due diligence investigation” processes in place; however, these processes are often designed to review the financial and operational affairs of a particular company and fail to closely inspect the background of the main principals or executives of the company. In addition, many companies do nothing more than cursory checks on individuals they are about to hire. The lack of a robust background investigation can result in wasted time and can cause legal and financial problems. There is an abundance of legal findings across Canada, as well as internationally, that clearly articulate the liability facing companies who do not carry out appropriate due diligence investigations. In order to inspect this issue closer one must first begin with a definition and understanding of what “due diligence” consists of.

Take a Moment to Celebrate Success

Take a moment today to think about the successes you have had and the team that got you there. It is well worth it.

¹ Available online at our website: www.presidiasecurity.com/library.html

A Solid Foundation for Administrative Investigations

"Is it time for the implementation of standards, including proper training and oversight, as it pertains to the conduct of "administrative investigations"? It could be argued that administrative investigations are purely "administrative" in nature and as such there is no requirement for an enhanced capability. However, it can also just as easily be argued that these types of investigations can have a very negative impact on the lives of those being investigated, including the potential loss of their livelihood. They also bring with them a large degree of "personal and institutional liability" on the part of those individuals conducting the investigations and the "organizations for which they are employed."

Marine Port Security - Published in FrontLine Magazine

"Since 9/11, marine port security has been the subject of increased scrutiny as it is clear that contraband flows - undetected and uninterrupted - through access and egress points of both Canada and the United States. Numerous reviews initiated by the United States Government Accountability Office (GAO) and the Canadian Standing Senate Committee on National Security and Defence have clearly articulated that ports are a haven for criminal activity and organized crime, as well as targets for potential terrorist activity. Both these reviews demand an increase in the level of intelligence sharing among partner agencies focused on policing and security of marine port operations."

Setting up an Intelligence Hub - Published in FrontLine Magazine

Intelligence in some form is in use today across a broad spectrum. No longer just the purview of Government entities, business intelligence is a common term and practice among corporations. Today, in the internet age, there is an abundance of readily accessible information about any given topic, organization or person. The immense growth of social networking in recent years has added to a rich information bank that is readily accessible to anyone with an internet connection. The challenge today is to sift through vast quantities of information to uncover and piece together the information you require into an intelligence picture that supports your operations. The value of your own information can increase exponentially when combined with open source research and information from other entities with whom you are willing to share.

Security Policy

"Policy writing: next to cleaning the coffee break area, doing personnel assessments or wrestling a hungry grizzly bear, it is probably one of the least desirable tasks in any organization. Its mere mention can send employees scrambling over desks and seeking cover in the hopes of being spared the mind---numbing drudgery of documenting the company's rules, procedures and practices. There is a good reason for this: writing is hard work – and writing clearly, concisely and meaningfully is even harder still. When it comes to communicating an effective security policy, capturing that policy on paper (or, in today's digital environment, electronically) is only the first – albeit most critical – step. Disseminating the policy and ensuring compliance are close second and third priorities, followed by periodic reviews to ensure the aforementioned policy continues to meet your organization's requirements. "

Travel Security

"Media reports continue to include stories about company executives, oil field workers and regular travellers who have been the victims of kidnappings, armed robberies and murder while visiting foreign countries. Recent events have seen a Canadian woman kidnapped in northern Nigeria and her captors demanding \$136,000 for her release. This woman was a financial advisor who was in Nigeria with other Canadians as part of an exchange program and she was kidnapped as she was entering a house after attending a social event. There are also ongoing reports of oil workers being kidnapped by rebels in South America and Africa; it would appear that these types of incidents are increasing rather becoming a thing of the past. "

Duty of Care

"The dynamic threat environment that persists in today's business climate demand constant vigilance and discipline. Under the Canadian Criminal Code, companies owe a duty of care to their employees. This means businesses must take "reasonable steps" to protect workers, whether they are in Canada or working internationally. If companies do not meet this duty of care, they can be found criminally and financially liable under the Criminal Code. In the most extreme cases, the company can face hefty fines and the executives can be prosecuted and potentially jailed. In addition to the criminal prosecution, individuals can also face personal civil litigation. "