CHAPTER 1

Important Personal Security Concepts

INTRODUCTION

Security is a broad discipline that embraces a wide spectrum of activities and concepts. The sphere of personal security is no exception. Personal security applies to you and, taken in a business context, the safety and the well-being of your team, colleagues, or employees. It is the portable set of wisdom that is most critical when you or your colleagues step outside of the relatively safe confines of the workplace, the familiarity of hearth and home. When you get on a plane or a train and travel outside of the developed world into the developing world, whether by design or by accident, the principles of personal security are what will distinguish those who survive and thrive from those who become victims. Like its cousins in the physical or cyber realms, personal security shares similar concepts in protection, such as layering defense against threat. Likewise, the concepts of threat, risk, and asset value are similar. There are key theoretical distinctions that must be made, however, to separate personal security from related disciplines. Examining these distinctions helps throw into sharp contrast the aspects of personal security that are unique to this category.

CONCEPT OF EFFECTIVENESS

The first concept of personal security is that of effectiveness. For example, a good physical security plan would be utterly ineffective if the layers of defense were procured and laid out but not implemented. A perimeter fence that is not erected offers no deterrence. A closed-circuit television camera (CCTV) that has not been connected offers no detection of threats. Or a duress alarm that cannot be assessed is of minimal use. While all of these measures might, on the designer's drawings, seem to be

present for the purpose of security, they are just that—security on paper, not in reality. This absurd example is used to illustrate a point regarding personal security: if the measure cannot be remembered and acted on when it is most needed, it is useless. Just as the effectiveness of physical security is measured in how well the various layers of defense are implemented, the effectiveness of personal security is measured in how well the various layers of defense are available for immediate recall from memory. Personal security is, unlike other security disciplines, much more intimate because it is principally focused on one key asset: you.

CONCEPTS OF THREAT, VULNERABILITY, AND RISK

The second set of concepts within personal security that are different are those of threat, vulnerability, and risk. These discrete elements of risk take on new meaning when considered in the personal security sphere. The terms *threat* and *risk* are often used interchangeably. In fact, these terms are not the same. It is important to have a clear understanding of what each term really means and how it applies to your personal security.

A threat, defined in the context of personal security, is an event with an undesired impact on your health and well-being. It is a supplemental ingredient to risk and should never be substituted for it. The components of a threat include the threat agent, or the actor, and the undesirable event. Threat events can be classified by type and category into intentional events that are planned and carried out or unintentional events such as accidents and natural disasters.

Vulnerabilities are weaknesses intrinsic and inherent to you that can be exploited by a threat actor or are susceptible to hazard events. In terms of personal security, these can include bad practices, such as never varying your routine or schedule, and bad habits, such as being easily distracted or inattentive, drinking too much, or being indiscreet about your location or business. Another example of bad practice is checking into a hotel, on the 40th floor beyond the reach of fire-fighting rescue ladders.

Risk is a more complex term. It is a calculus that, technically speaking, takes into measured consideration the loss potential to an asset that will likely occur if a threat is able to exploit a vulnerability. Another way of stating this is that it is the potential harm to you if a threat actor such as a kidnapper or a terrorist is able to take advantage of a weakness in your personal profile. Notice that conditional words such as *potential* and *likelihood* are included in the description of risk—these are important conditional terms that can be scaled up or down depending on the weight and the relevance of threat, vulnerability, and impact to you.

There are much more sophisticated definitions and implementations of risk evaluation—security is a broad discipline that embraces a wide spectrum of activity. However, for the purpose of developing a solid personal security program, it is sufficient to understand risk in these most basic terms.

Threats and vulnerabilities in personal security are very dynamic and multidimensional: dynamic, in the sense that there is movement through an ever-shifting risk environment, and multidimensional, in the sense that threats and vulnerabilities can be both external and internal. An integral part of a personal security plan is having an informed, internalized course of action that is capable of anticipation as well as reaction. Being able to identify a risk context as it is unfolding and identify indicators of change in the risk environment mitigates apprehension and reduces fear within the individual. Being able to correctly identify these changes does not eliminate fear, nor should it. However, a good plan of action directly addresses the vulnerability that we all have to *paralyzing* fear in the face of danger, identifying and reducing the paralysis itself without entirely removing the fear. Fear, if properly harnessed, can motivate the right reactions at the right time. As will be pointed out in later chapters, having a good sense of timing and acting on it can make the difference, for instance, between being a kidnap victim or not. Good personal security planning provides this benefit.

CONCEPT OF TIME

Time is a valuable commodity in personal security. The time that it takes to identify, react, and mitigate a potential or validated threat event as it blossoms against or around you or those for whom you are directly responsible is much shorter—generally speaking—than in other fields of security. For this reason, this book puts special emphasis on threat pattern and indicator recognition and detection of (i.e., gang signs, symbols, tattoos, graffiti) potentially threatening profiles or behavioral traits. This has consistently been useful to me over the course of my career and lifetime. Taken together, sensitivity to detail on the street provides you the anticipatory skill needed to react in a timely fashion to a potential threat event as it is developing and not after it occurs. The importance of good timing cannot be overestimated. Like physical security or cybersecurity, a good personal security program is subject to a methodical assessment and design process. However, to be resilient, effective, and of maximum use, the repository of that program cannot be sitting in a tabbed binder on the corporate security officer's shelf at headquarters. Since there is really only one principal asset—you—a significant part of the design process is having a knowledge transfer

method that embeds critical reactive elements—*good timing instincts*—into your memory.

COMMITTING A SECURITY PLAN TO MEMORY

I have never been a proponent of security plan by checklist, and this is why: checklists, although well intended, are impossible to remember unless you have a photographic memory. When you need them the most, you are likely on an airplane buckled firmly in a middle-row seat on final approach to an airport and a city that is completely unfamiliar or in the back of a darkened taxi or motor rickshaw in a monsoon rainstorm. The checklist will likely be out of reach.

Principled security planning, constructed around a simple framework, is a way of contextualizing and then internalizing in your memory your security design around layers of defense. Doing this makes it much easier to remember what needs to be done next, rather than randomly choosing from a smorgasbord of security must-do options. A principled security plan is crucial to getting street smart. This simply means that you are able to think clearly, rationally, and quickly on your feet without having to resort to a map or a global positioning system application of your smartphone or some other crutch.

There are two reasons this is an important way to develop a personal security plan. First, a structured approach to layering personal security measures via key principles is easier for training purposes—it lends itself to instructing large groups of nonsecurity professionals.

Second is the individual. The most important place for a plan of action is in one's head, not a piece of paper or a smartphone. A layered approach built around a few key concepts provides essential memory pegs on which one can hang several concepts. Knowing that you can remember what to do when it comes to all aspects of one's personal security builds confidence, a sense of clear thought, and a more deliberative way to approach the environment out there in the real world. These qualities are very important. When a crisis event happens, how you react and what you choose to do in the moment are crucial to your survival. With regard to personal security—unlike other elements of the security discipline—I pay particular attention to the importance of feelings (listening to your gut) and emotions. How you manage your emotions in any given situation is crucial. Crisis events always have their own dynamic; to the extent that you can mitigate (not eliminate) feelings of panic, fear, or confusion, you will be capable of thinking through your emotions and ultimately survive the event. You turn panic into a sense of urgency and focus, fear into action, and confusion into ordered deliberation.

THREAT AGENTS AND THREAT ACTORS

There are also important distinctions between what is considered a threat actor and a threat agent. A threat actor is an individual or a group that has the resources, the capability, and the motivation to execute an undesirable threat event. A threat agent is the causative element of what becomes a hazard event, which is a specific condition, or a set of conditions, such as a hurricane, a tornado, or an earthquake. Threat agents and consequent hazard events have follow-on catalytic properties that can evolve into cascade threat events or, simply put, unanticipated consequences.

Understanding threat agents and hazard events is relevant to the development of a personal security program, because of these threat cascade effects. An earthquake, a hurricane, or a tornado may be the initial undesirable event—but, in each instance, secondary or tertiary cascade events unfold into the rise of threat actors such as looters or thieves who take advantage of a chaotic situation to loot and assault innocent victims who get in their way.

It is important to understand threats and threat actors, because each one exhibits specific tactics, history, and characteristics as an adversary, understand who they are and where they operate, but more importantly, understand their motives and how they execute against their targets. Another way to look at it is this: on the street, it does not matter that the hooded gunman coming for you is a terrorist with political motives, a kidnapper with pecuniary motives, or a common mugger who wants your shiny new watch. What matters, at that instant, is what you do to survive the attack itself. At the end of selected chapters in this book, there will be a brief monologue focusing in on specific threat actors. This chapter is intended to put some flesh and blood behind the normally anodyne descriptions of who threat actors are. Much of this narrative is anecdotal, from my own experience and that of others in my acquaintance. In addition, later in the book, I go into some detail about the signs, the tattoos, the graffiti, and the behavior of the major international criminal gangs both in the United States and around the world. Recognition of telltale indicators of individuals who are potential gang members in an urban setting or an urban setting that clearly hosts gang activity can provide you the small but important clues needed to make quick, informed decisions about your own security.

Understanding the risk environment is important for you in terms of the tools that you select to mitigate the risk. If you are living in an earthquake zone, for instance, it is prudent to ensure that your home is built to standards that can withstand the threat of an earthquake. Similarly, if you live along the Florida coastline, your home is built to standards that can weather high winds and storm surge tides. If you are smart,

you have a generator, extra food, water, and backup communications options. You have an evacuation plan, should the storm threat rise to a very dangerous level. In fact, whether you are in a hurricane zone or an earthquake zone, many of the countermeasures that you select to mitigate your risk are very similar. These all reflect an understanding of your risk environment and the measures that you need to take to mitigate or address those risks.

As applied to international risk environments, if you travel to Tampico, Mexico, or Tripoli, Libya, for instance, it is prudent that you take measures to mitigate specific risks in those countries. In Tampico, the risk of kidnap for ransom by criminals is high. In Tripoli, Libya, the risk of hostage taking by a terrorist group is likewise high. While the threat actors may have different motives, their tactics can be roughly similar. The countermeasures that you must learn to mitigate these threats are likewise similar. Learning and developing that certain set of skills will set you apart from the average traveler and keep you and those for whom you are responsible safe and alive.