2011

Safety & Security Planning

A HANDBOOK FOR PERSONAL AND CORPORATE SAFETY AND SECURITY PLANNING

WRITTEN BY: KERRY SAUVE

Table of Contents

I. Introduction

II. Objectives

III. Risk Assessment

IV. Personal Safety & Security Planning

I. Introduction

The world has become an increasingly dangerous and unpredictable place. In order for an organization or individual to increase their safety and security it is imperative that they plan. This planning must not be haphazard or piecemeal, and should be based on the three *"R's" (Real, Researched, Relevant).* The goal for any organization when developing a safety and security plan should be to focus on the threats and incidents most likely to occur and to spend most their time, effort and resources reducing risk in these areas. This is not to say that anomalies and singularities cannot, or will not occur. They can and should be accounted for in every plan, and this is where a thorough risk assessment will assist them in identifying probable and potential threats to the day to day operations of their organization and the people it employs and serves.

II. Objectives

A. Objectives

A safety and security plan is a document designed to decrease the level of risk for your area of operations, infrastructure, staff, clientele and data. A safety and security plan provides a pre-planned response and mitigation for natural and man-made disasters, criminal activity and violence. It is designed to assist your organization in dealing effectively with risk-associated and emergency situations that may occur during your day to day operations, or personal life.

Primary Objectives;

- To reduce risk surrounding the multiple threats to the safety and security of your organization, infrastructure, employees, and clientele.
- A safety and security plan also addresses the specialized risks that are unique to your organization, or industry.
- To provide management and staff with the critical thinking skills and tools to mitigate risks to the safety and security of the institution, clientele and themselves.
- To provide a broad spectrum of response options to both high-risk and low-risk situations and provide an environment where the concepts outlined in the safety and security plan can be implemented and practiced.

Goals;

- To learn to recognize, profile, assess and mitigate threats to the safety and security or the organization, staff, management and clientele.
- To be able to orient oneself, communicate effectively, and travel to safety when at risk.
- To learn to utilize critical thinking skills to proactively deal with threats to any safety and security threats encountered.

III. Risk Assessment

The creation of a safety and security plan is predicated on the following assumptions;

1. Environmental factors play an important role in the effectiveness and impact the ability of organizations and individuals to maintain safety and security in both low-risk and high-risk environments.
2. Proper assessment and planning are essential to coping with internal and external security threats that may be encountered during day to day operations. It is conducive to;

    - Increasing and enhancing the resilience of the organization, its staff and clientele in all domains and environments;
    - Increasing the understanding of proactive security and of the measures to be taken before, during and after a hostile contact or incident;
    - Improve safety and security by providing the organization with the skill sets necessary to assess, avoid and mitigate potentially dangerous situations.

In order to reduce risk, it is imperative that accurate information regarding the organization, and its unique threat profile are obtained. This is accomplished through the ***Risk Assessment*** process. Risk assessment can be broadly broken down into four general areas;

1. **Threat Assessment:** The determination of quantitative or qualitative estimate of risk related to a well-defined situation and a recognized threat. *Quantitative risk assessment* requires calculations of two components of risk;

    - The magnitude of the potential incident.
    - The probability that an incident will occur.
    - Acceptable risk is a risk that is understood and tolerated, usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss.

2. **Vulnerability Assessment:** The process of identifying, quantifying, and prioritizing *(or ranking)* the vulnerabilities in a system or for an organization, or individual. Vulnerability assessments have many things in common with risk assessments. Assessments are typically performed per the following steps:

- Cataloging assets and capabilities *(resources and resiliency)* within an organization's domains and environments.
- Assigning quantifiable value *(or at least rank order)* and importance to those resources
- Identifying the vulnerabilities or potential threats to each resource.
- Mitigating or eliminating the most serious vulnerabilities for the most valuable resources.

3. **Consequence Analysis:** Consequence analysis is an evaluation of the predicted outcome of an incident and how it affects the organization and the individuals that inhabit it.
   - Consequence analysis is one of the main components of the risk assessment process and can be used to optimize planning, reduce or eliminate unacceptable risk, develop an emergency preparedness plan, or assess the mitigation system.
   - Consequence analysis includes the prediction of the magnitude of potential risks that the organization, its employees and clientele will face across all domains and environments.

4. **Emergency Response and Mitigation:** Mitigation refers to measures that reduce the chance of an incident occurring, or reduce the damaging effects of unavoidable emergencies.

   - Mitigation is achieved through the risk analysis process, which generates information that provides a foundation for typical mitigation measures, and includes establishing emergency response protocols, technology requirements, and implementing barriers such as *CPED (Crime Prevention through Environmental Design)*. Effective Mitigation efforts can break the cycle of risk, and repeat trauma.

   - It creates safer workplaces and lifestyles by reducing exposure to situations, or individuals that may cause harm and trauma.

   - It allows the organization to minimize post-incident disruptions and recover more rapidly.

   - Each of these specific items contributes to the formation of a safety and security plan by providing information and intelligence that will be analyzed and utilized to identify, assess, and mitigate risk to the organization.

IV. Personal Safety & Security Planning Concepts

A. **Situational Awareness**

"The perception of environmental elements with respect to time or space, the comprehension of their meaning, and the projection of their status after some variable has changed, such as a predetermined event. Situational awareness is a part of a field of study tasked with understanding the environment that is critical to decision makers in complex, dynamic environments."

B. ***Objectives:***

- Accurately identify the four levels of awareness and how they relate to organizational/personal risk.
- Demonstrate awareness of the security issues associated with each level of awareness.

Awareness Cycle

1. **Unfocused Awareness**: This is a common state that we find ourselves in when we're in environments where we are comfortable and able to function semi-effectively on autopilot.
    - Think of driving in a car. Have you ever arrived at your destination only to realize you have no conscious recollection of having driven there, or if you stopped at any traffic lights etc.?

2. **Normal Functionality:** This is how we navigate the reefs and shoals of daily life.
    - We are relaxed, but still aware of what is going on around us and able to respond if a potential threat presents itself *(a car swerving into your lane or a child darting into the street)*.
    - This type of awareness is not taxing on our conscious or sub-conscious and can be maintained for extended periods of time without a noticeable change in performance or attention.

3. **Focal Awareness*:*** Focal awareness requires an enhanced degree of concentration.
    - For example, when you are attempting to complete a task with multiple steps or segments. *(i.e. completing an assignment, or writing a letter).*

4. **Fixated Awareness:** also, frequently referred to as condition black
    - This state occurs when we are in the grip of the adrenal stress response.
    - Condition black occurs once our heart rate starts to accelerate to over 145 *bpm*.
    - This creates some interesting physiological, and psychological impairments in our ability to plan, think, and act.
    - Often condition black is reached when we are not confident we have the skills, training, or ability to confront whatever we are facing. Condition black can also occur when reaction times are limited or the threat is new or unfamiliar.

A. **Target Hardening:**

"The strengthening of a building, facility, or personal security to protect the subject or reduce their exposure to attack."

B. ***Objectives***

- Demonstrate an understanding of target hardening principles and how they relate to increasing your safety and security.
- Accurately identify how each of these concepts can be utilized to increase safety and security throughout all domains and environments*.*

The goal of target hardening is to ensure that strategic or tactical assets are secured against intrusion or assault. When it comes to personal safety and security planning, target hardening simply means that procedures and precautions are put into place that make the organization, its employees and clientele less viable as a potential target for crime or violence.

The object is not to surround the organization with an impenetrable bunker. It is not realistic or possible to eliminate all risk. Having said this, the more efficient target hardening efforts become, the less likely the organization will be exposed to high-risk or unacceptable-risk situations. Some of these factors can be controlled, while others are based on dynamics and variables beyond your sphere of influence to affect. To help your organization and its people become harder targets, there are five areas that can be examined as a starting point for planning and training;

Tactical Considerations

1. **Existence of a Threat:** Who or what are the potential threats to the organization, or the assets in question.
    - This can include physical threats, threats towards infrastructure and property, asymmetrical threats, as well as threat based technology *(spyware, malware)*.

2. **Capability to Execute the Threat:** What resources, intelligence and capacity are present that would enable the individual or group to execute the threat.

3. **Historical Data:** What is the history of this type*(s)* of threat being successfully perpetrated by the individual or group in question in the past?
    - Is this ongoing pattern of behavior consistent with past behaviors?

4. **Goals and Intentions:** What goals or intentions is the threat trying to achieve or accomplish.
    - Is their motive personal, political, financial, need based *(sexual assault, drugs/alcohol)* and what is their commitment to succeed.

5. **Intelligence:** Does the threat have any intelligence that would make them a more able to carry out an attack?
    - Is the threat conducting surveillance?
    - Are they familiar with your daily routines and movements?
    - Are they aware of your vulnerabilities?

Target Hardening Principles

1. **Target Denial**: Refers to the temporary or permanent removal of potential targets for crime or violence, whether they are people, infrastructure, or property. Realistically your organization can't always accomplish this goal.
   - While you may be able to temporarily remove yourself from an area or circumstances, permanently removing yourself from becoming a potential target would be a logistical nightmare and not practical.
   - Industry utilizes this technique often when it comes to their vital IT hardware and information. Cloud computing and backup redundancy hardware has mitigated much of the damage that can be accomplished through cyber-attacks on individual hubs and organizations.

2. **Elimination of Means:** This technique is not only possible for organizations it is something most people probably do every single day.
   - Removing materials and access that may assist a threat in gaining access to you or your property is one of the easiest and more effective methods for elimination of means.
   - Another example would be disabling the geo-tagging function on smart phones, and not allowing location based social networking to utilize your geographic information.
   - This drastically reduces the access and opportunity needed for individuals to track your movements and identify the places you commonly frequent.
   - Elimination of means also refers to other common practices such as refraining from tagging photos and sharing personal information online.

3. **Cost Benefit Reduction:** Every predator and criminal has a motive. In many cases, your organization and its people are simply a resource for those that mean them harm, unless it's a personal issue.
   - Knowing this your organization can increase the response cost and reduce the potential gains that potential threats may have as their motive.
   - Minimizing the usefulness of potential pay offs also reduces the threats motivation for making the attempt.
   - For example, utilizing personal safety apps such as *"b-safe"* for your staff and clientele can reduce the potential pay offs for those that mean them harm as its technology connects them directly to their personal safety circle and law enforcement.

4. **Access Control:** Reducing access to vulnerable people and infrastructure can go a long way to drastically reducing if not eliminating many of the threats faced through direct access.
   - It's important to remember that access does not necessarily mean physical access.

- Your organization and its people can be placed as just as great of risk of being targeted for crime and violence through indirect access such as through the internet.

5. **Surveillance:** Surveillance works as it exposes the perpetrator to scrutiny. It increases the likelihood of the perpetrator being observed and identified. Except for government sponsored surveillance there are two types of surveillance regularly utilized that pertain directly to the formulation of a safety and security plan. *(Natural, Formal).*

   - **Natural Surveillance:** This is exactly what it sounds like. It is difficult for threats to accomplish their goals and objectives if they are observed while doing so. This is not to say that they can't access or harm you if they are being observed. It just makes it more likely they will be caught due to the increased probability of identification by those observing the incident. This may prevent the incident from occurring. Much of how we secure our homes and businesses is based on this principle. Natural surveillance is commonly used in in the business world for a variety of security reasons.
   - **Formal Surveillance:** This simply means that a lot of the common security protocols we take part in and enforce daily perform a surveillance function. For example, when I sign onto my computer at work, I'm required to provide a user name and password.

6. **Environmental Design:** Changing the design of the environment can often have a dramatic effect on reducing risk and subsequent exposure as a potential target for crime and violence. Setting up your organization to make security more manageable and effective is often inexpensive and produces immediate results.
   - It's important to note that none of these techniques is a guarantee that your organization won't become a target. As with anything in life it's about playing the odds. By increasing your odds, you decrease your risk.

7. **Laws and Rules:** We are a society of rules and laws. We put them into practice to allow us to live together in large groups with minimal problems and conflicts.
   - Here's another unfortunate truth; criminals don't follow the rules or care about the law.
   - Don't expect criminals to play by the rules. You on the other hand should use them to your advantage and know your rights and responsibilities under the law.
   - Laws and rules also provides justification and compensation if others ignore the rules and laws and you or your organization are victimized.

8. **Increased Perpetrator Risk:** Criminals and predators engage in the same sort of cost, benefit analysis as everyone else when they are deciding to access or bypass specific targets.
    - I've never met a criminal who went out of their way to look for a more difficult target. Just like the rest of us they will generally look for the easiest, least risky opportunity possible.
    - It's generally far easier to find an unaware, unprotected target than it is to attempt to access a well-fortified target.

A. **Behavioral Profiling**

The complexity surrounding the dynamics of crime and violence makes it difficult, if not impossible for the average person to predict, detect or prevent. This statement demonstrates quite aptly why appearances can be deceiving. While seemingly correct, it is also patently untrue.

People are generally reactive when dealing with threats to their safety and security. Static and dynamic security, are only part of the solution. What is needed is the ability to recognize, assess, and mitigate potential threats prior to them reaching the event horizon. Behavioural profiling is a tool that can help achieve this goal.

The term event horizon indicates the moment of contact, and when contact commences. *"An event horizon is a boundary in space time beyond which events cannot affect an outside observer."* In layman's terms it is defined as *"the point of no return."* Each instance of crime and violence is a singularity, and this has been a large part of the problem of planning how to respond pro-actively.

The subject of profiling has gotten a lot of bad press, and in some cases rightfully so. Attempting to determine an individual's intent based upon race, or religion is a big problem. Attempting this is not only morally and ethically wrong; it is extremely ineffective and will provide a lot of false positives. Instead profiling should be based upon an individual's behaviour and an understanding how it's affected by their emotional state. Social psychologists tell us that upwards of *85%* of all communications are non-verbal. Learning how to read these non-verbal behavioural cues is the essence of all profiling.

Objectives

- Demonstrate an understanding of the basic principles associated with behavioral profiling and its function in the safety and security plan.

1. **It's vital that profiling be based on measurable datum as well as instinct and intuition:** Educating the individuals within the organization is the first step in the process.

2. **The goal of profiling is to learn to recognize patterns of behaviour that stand out as abnormal or inappropriate for the environment, and context in which they are occurring:**
    - This is vital when it comes to predicting behaviour and keeping your organization and its people safe.
    - However, the ability to consistently and accurately accomplish this is generally developed and honed by experience.
    - People can learn to develop, and utilize these skill-sets by incorporating some simple principles into how they view the world around them.

3. **What is key is to be aware of how people <u>typically</u> interact with their environment and each other.**

Areas To Profile

1. **Kinesics:** Conscious and sub-conscious body language.
2. **Biometric Cues:** Biological autonomic responses.
3. **Proxemics:** Interpersonal spatial interactions.
4. **Geographic's:** Patterns of behavior within an environment.
5. **Iconography:** Expression through symbolism.
6. **Atmospherics:** Collective attitudes that create distinct moods within an environment.

Behavioral Analysis And Profiling

1. **Learn to observe behaviour on an interpersonal level:** Pay close attention to people as they move about the areas you inhabit. Look for the natural patterns of interaction that occur in groups and between individuals. How do they affect the atmosphere of the space?

    - **Closely observe people who approach you:** Especially in areas where you are vulnerable**.** There's a big difference in the behaviour of someone walking past you in a crowded mall, and the person who recognizes you and heads towards you from across a crowded room.
    - **Pay attention to your instincts:** Not enough credit is given to instinct and gut feeling. We've all had plans to be some-place, and for whatever reason our instinct tells us not to go. Often if we ignore our instincts, something *(not necessarily crime or violence)* occurs.
    - **Actively profile individuals, groups, and places:** Every place has a mood or feeling that permeates it. You know immediately when it's going to be a bad day at the office. As soon as you arrive, the atmospherics and your interactions with others tell you things are normal, or tense.

Behavioral analysis is a tool that when practiced on a regular basis can help those in your organization become more attuned to their instincts, and provides them with an accurate method to quickly and effectively determine if an individual's behavior warrants further scrutiny. As with any skill-set profiling becomes stronger and more useful with practice and experience.

A. **Escape and Evasion**

Escape and Evasion or *(E&E)* refers to tradecraft commonly associated with military or para-military training, and is taught to soldiers to increase their chances of surviving in hostile environments. Escape and Evasion techniques are designed to help avoid capture and conflict with those that mean the you harm.

How people respond to threats is often a determining factor in survivability. Applying *E&E* concepts to a safety and security plan doesn't have to become a military exercise. They are scalable and adaptable to any environment. There are five phases associated with escape and evasion that can be modified for inclusion into everyone's safety and security plan.

B. ***Objectives***

- Understand how to utilize an escape and evasion plan to evacuate high risk situations and get to a place of safety.
- Describe how an escape and evasion plan fits into a safety and security plan

Escape & Evasion Planning

1. **Immediate Action *(Assess, Plan, Act)***
    - **Assess the situation:** What are your options for exiting the area unseen and minimizing the chances of hostile contact.
    - **Take stock of your health and well-being:** You should determine if you are injured, in shock and the best course of treatment to quickly remedy the problem.
        - Injury and exhaustion are two huge detriments to your ability to escape and evade successfully.
    - **Gather supplies and equipment:** You should have all your personal items and any survival/communications gear you may need ready to go.
    - **Evacuate the area and move to an initial safe area:** Safe areas are pre-determined locations, which can be used as a temporary base of operations while you collect yourself and prepare for the next phase of your escape and evasion plan.
    - **Initiate Call-in Procedure:** Call-in procedures are communications protocols initiated to indicate emergency situations and communicate the location and nature of the threat, or to request assistance.
    - **Sanitize:** This simply means to get rid of any clothing, documents or paraphernalia that will identify you to your pursuers.
        - Sanitizing also refers to removing clues that you were in the area. It involves showing either *No Proof of passage* or a *False proof of passage.*

2. **Getting Out**

- **When it is safe to do so you should begin moving in the direction of safety*:*** It's important to note that most successful escapes and evasion take place during the first few minutes.
    - This is when you are likely closer to familiar areas and your pursuers still in a state of confusion.
    - The goal is to quickly get outside of the area of operations.
    - Most of the time searches are focused *"inward"* from a perimeter. If you are hiding inside the perimeter, there is a good chance you will be found.
- **Move away from the area of operations:** Moving uphill outside will provide better situational awareness and may slow pursuers down as they often search lower lying areas first.
    - Inside buildings, move to ground floor levels to avoid becoming trapped.
    - Remember the law of angles. This refers to the fact that every time you turn a corner to elude a pursuer you are losing time and ground. Instead take a direct route *(through alleys, buildings, etc.)* to quickly remove yourself from the pursuers line of sight.
    - Moving erratically further confuses pursuers and makes them work harder to find proof of passage.

- **Use terrain and concealment to your advantage:** Hiding or sheltering in place should be your last resort *(it reduces their likelihood of escape and is essentially tantamount to your belief in luck).*
    - Move in the shadows, avoiding running or other sudden suspicious movements that will attract the attention of a pursuer.
    - This is easier to accomplish at night as it limits the searchers ability to track you.
    - What typically gives people away when moving at night is; *(Shape, Shine, Silhouette, and Movement).*
    - People are predators by nature and our eyes have been conditioned to look for the distinct human shape, as well as the shine of our eyes, the oils on our skin and our teeth.

- **Maintain Light Discipline and Noise Discipline:** Do not turn on flashlights, light lighters or frequent light sources.
    - Any significant light source takes away your night vision for 5-7 minutes.
    - Any pursuer's eyes will also automatically be drawn to light sources and may provide them with clues to your location.
    - Cover items such as watches, glasses and jewelry that may reflect light. Likewise keep sources of noise to a minimum.

    - Loose change, zippers, jewelry, etc. should all be checked and either silenced or removed to avoid attracting the attention of your pursuers.
    - Turn off phones, alarms and all non-essential electronics.

3. **Evacuate to a Safe Area**
    - A safe area can be defined as a *"secret place for sanctuary or suitable to hide a person from hostile actions or actors, or from retribution or perceived forms of danger."*
        - It should serve as both cover and concealment, and be a suitable distance away from the potential threat.
        - It should offer numerous avenues of escape, and can be used as a communications post.
        - Safe areas should ideally be stocked with the supplies and equipment needed to call for help and keep the subject provisioned until help arrives, or you can ex-filtrate yourself.
        - Minimally safe areas should contain food/water, communications equipment, and first aid supplies.

4. **Utilize Stealthy Movement**
    - **Travel slowly and deliberately:** Remember that haste draws attention and causes people to make mistakes.
        - The goal is to elude a pursuer, and in most instances, they will not be highly trained hunters or trackers.
        - Remember that people catch people, and by simply avoiding detection escape and evasion is almost guaranteed.
    - **Be flexible; profile actively:** These micro-plans will enable you to fine tune your escape and evasion plan on the fly.
    - **Stop, look, listen, and smell:** Tobacco, scented deodorants, colognes, perfumes can give away a pursuer, just as easily as it can help to locate you.
    - **Avoid Common Use Areas:** This will greatly increase your chances of successfully escaping your pursuers.
    - **Use cover and concealment to move from point to point:** Time movements to appear normal and natural.
        - Avoid sudden, jerky movement as it attracts the eye.
        - Move on angles and use peripheral vision to more effectively pick up movement at night.
    - **Leave no proof of passage:** Avoid disturbing vegetation, running and erratic movements when travelling.
        - Avoid littering; discarded items can easily point pursuers in your direction and will often reveal the identity of the litter bug.
    - **Employ counter-tracking techniques:** Some of these include not moving towards a logical or known location *(home, vehicle, friends, and known hang outs)*.
        - Avoid areas where it would make sense for pursuers to search.

    - You may be able to throw trackers off your trail by setting false proof of passage for pursuers to find indicating that they are travelling towards a different location.
- **Attempt to move towards *"friendly"* locations"** *(police, business, government):* Avoid high rise buildings and market places they can easily become traps.
- **Have a pre-arranged area for pick up and recovery**: Find the best time and place to communicate that you are safe, or to request a pick up.
- **Ensure that you have a *"Plan B"* if your primary recovery site is compromised:** Be prepared for unconventional recovery options.
- **Observe and report any movement by pursuers or other potential hostiles in the area:** This can impact the subject's ability to be safely ex-filtrated.
- **Secure all equipment and remain concealed until the subject is picked up, or until they can get to a place of safety.**