



**UNHCR**  
The UN Refugee Agency

# Security Risk Management



## Learning Module

Prepared by the UNHCR eCentre in  
collaboration with InterWorks, LLC

January 2009



# Security Risk Management

## Learning Module

Prepared by the UNHCR eCentre in  
collaboration with InterWorks, LLC

January 2009

## **About this course**

This course is based on materials and approaches developed by UNHCR's Field Safety Section for the training of UNHCR managers deploying to insecure environments. The materials have been modified by the eCentre to apply to a wide range of humanitarian and development partners. The Security Risk Assessment (SRA) model is based principally on that of the United Nations Department of Safety and Security (UNDSS). Other tools and materials have been drawn from various text, on-line, and other training resources, with due attribution to the original source wherever possible.

The aim of this course is to introduce managers of humanitarian and development programs in insecure areas to the techniques and tools of managing risk. Emphasis is placed on three principle areas of concern: security risk assessment, security plans and planning, and critical incident management. The course also provides insights into the current security environment and organizational responses, managerial accountability and due diligence, security-related relationships with other actors in the field, and management of stress in insecure field environments. The ultimate aim is to help managers to cope better with the difficult task of balancing humanitarian programmatic imperatives with the associated security risks to their staff.

The course is designed to be self-contained, allowing learners to proceed at their own pace. Questions for reflection are interspersed throughout the various chapters; we recommend taking time to answer these as they will encourage you to mentally apply the learning to your own experience. Each chapter ends with a short test, allowing for self-assessment of your understanding of the material.

## **About the authors**

Michael Dell'Amico is currently the UNHCR eCentre Coordinator. Prior to the present assignment, he served as UNHCR's Senior Training Officer for Staff Safety, where he developed much of the material in this book. He has been a Field Safety Adviser for UNHCR for eight years, conducting field assignments in over 25 duty stations. He previously served for ten years in the United States Marine Corps.

Jim Good is a partner with the disaster management consulting firm InterWorks, LLC. He has worked with UNHCR as a trainer and consultant in refugee emergency management, planning, and response for more than 18 years. He has worked with the UNHCR eCentre and the associated security courses and training programs since their inception in 2000.

## **Cover photograph**

The 2008 UN photo by Marie Frechon shows helmets and flack jackets belonging to the United Nations Peacekeeping Mission in the Democratic Republic of the Congo (MONUC) in North Kivu. Today, in many areas of the world, protective clothing of this type is being used by humanitarians as well as soldiers when undertaking activities in highly insecure areas.

---

This publication may be copied or reproduced in part or in whole, provided that UNHCR and the eCentre are credited, any other credits mentioned in the parts reproduced are duly acknowledged, and the parts reproduced are distributed free or at cost—not for profit. For any reproduction with commercial ends, permission must first be obtained from UNHCR.



## Table of Contents

Foreword	v
Welcome and Introduction	vi
<b>Chapter 1: Introduction to Security for Humanitarian Workers</b>	<b>1</b>
1.1 Security Context for International Field Workers	2
1.2 Recent Trends in Humanitarian Staff Security	3
1.3 Humanitarian Response to Security Threats	6
<b>Chapter 2: Approaches to Managing Security</b>	<b>15</b>
2.1 ICRC and the “Seven Pillars” Approach	16
2.2 NGO Common Approaches – The Security Triangle Model	18
2.3 The United Nations Response to Staff Security and UNHCR’s Culture of Security	21
2.4 Accountability for Staff Security	25
<b>Chapter 3: Overview of Security Risk Assessment</b>	<b>33</b>
3.1 Threat Assessment	34
3.2 Vulnerability Assessment	35
3.3 Program Assessment	36
3.4 Risk Analysis	37
3.5 Criticality Assessment	37
3.6 Decide and Implement Measures	38
3.7 Review and Modify	39
<b>Chapter 4: Threat Assessment</b>	<b>43</b>
4.1 Approaches to Threat Assessment	44
4.2 Historical Analysis	45
4.3 Pattern Analysis	47
4.4 Change Analysis	49
<b>Chapter 5: Vulnerability Assessment</b>	<b>55</b>
5.1 The Importance of Vulnerability Assessment in SRA	56
5.2 Key Factors to Consider in Vulnerability Assessment	57
5.3 Vulnerability “Benchmarking”	62
<b>Chapter 6: Program Assessment</b>	<b>67</b>
6.1 What is Program Assessment?	68
6.2 How Humanitarian Programs Affect Staff Security in the Field	68
6.3 Program-Related Risk Factors May Change Over Time	71
6.4 The Other Side—How Measures to Improve Staff Security Affect Humanitarian Programs	72
6.5 Doing your Own Program Assessment	73



<b>Chapter 7: Risk Assessment and the Risk Matrix</b> .....	79
7.1 Understanding Risk .....	80
7.2 Determining Impact .....	81
7.3 Determining Likelihood .....	82
7.4 The Risk Matrix .....	85
7.5 Practical Guidance on Using the Risk Matrix .....	88
7.6 Risk Assessment and Bias .....	88
<b>Chapter 8: Risk Reduction Measures</b> .....	95
8.1 Criticality Assessment .....	96
8.2 Types of Risk Reduction Measures .....	98
8.3 The Risk Reduction Toolkit .....	99
<b>Chapter 9: Security Plans and Planning</b> .....	109
9.1 Does Every Office Need a Security Plan? .....	110
9.2 The Plan .....	111
9.3 Scenario-Based Security Contingency Planning .....	116
9.4 Security Planning and Your Budget .....	116
<b>Chapter 10: Critical Incident Management</b> .....	121
10.1 Critical Incident Management and Security Planning .....	122
10.2 Stages of a Critical Incident and Response .....	122
10.3 Tools and Methods .....	125
10.4 Information Management .....	127
<b>Chapter 11: Security Relationships in the Field</b> .....	133
11.1 Security Relationships with the Host Government .....	134
11.2 Security Relationships with and among NGOs and Other Partner Agencies .....	135
11.3 Security Relationships between Humanitarian and Military Organizations .....	138
11.4 Staff Security and the Security of Beneficiaries .....	141
<b>Chapter 12: Security and Stress</b> .....	149
12.1 The Relationship between Stress and Security .....	150
12.2 Some Basic Information about Stress .....	150
12.3 Individual Adapting and Coping Strategies .....	152
12.4 Managing Staff Stress in Insecure Field Environments .....	155
12.5 Provide Support to Staff after Critical Events .....	157

## Foreword


Managers of humanitarian and development programs today need no reminder of how complex our security environment has become. From political instability in some countries to ongoing conflict in others, from the global terrorist threat to widespread criminality in some urban areas, those responsible for programs continue to face the difficult challenge of balancing operational imperatives and risks to staff. This has resulted in additional responsibilities, accountabilities and pressures being placed upon managers.

The present learning module was designed with these realities in mind. Based on the materials and learning from the eCentre's highly popular Security Risk Management Workshop, the course introduces the techniques and tools of managing risk in humanitarian operations. In the pages that follow, you will find practical and systematic approaches to assessing threats, vulnerabilities and risks, selecting appropriate mitigating measures, preparing security plans and responding to critical incidents. The module will explore challenges to accountability and will enhance the ability of managers to ensure safety. Finally, you will read about the impact of security on a range of related issues including the safety of people affected by emergency situations, partnerships, relations with the military and stress.

I would like to thank Interworks LLC, principle collaborators in the development of this learning module and one of the driving forces behind the eCentre's successful training since its inception.

Understanding how to manage risk in today's world has become an essential part of our dual responsibility to carry out our mandates while ensuring the safety and welfare of our staff. I have every hope that this Learning Module will enable you to fulfill these tasks more effectively.

I wish you good luck with your learning and safety and success in the field.



Arnauld Akodjenou  
Director,  
Division of Operational Services



## Welcome and Introduction

Welcome to this self-study learning module on Security Risk Management (SRM). It is designed for learners who have some experience with humanitarian field work and want to learn more about managing security for themselves and their co-workers in insecure field environments. While much of the guidance and protocols described in this course are based on the United Nations' and UNHCR's security guidelines in particular, the advice presented is of a general nature and should be valuable for any humanitarian or development worker in any insecure or dangerous field environment.

## Learning Objectives for this Course

After successfully completing this learning module, you should be able to:

- Better understand the global trend of insecurity facing humanitarian field workers and the general types of responses that are being taken to meet security threats in the field by UN, Red Cross Movement, and NGO partners.
- Understand, appreciate and explain the overall Security Risk Assessment (SRA) and Security Risk Management (SRM) approaches to security management for humanitarian field workers.
- Use standardized terminology and tools to assess threat patterns, analyze risk, and prioritize measures to reduce risks of different threats in your working environment.
- Develop basic security plans, Standard Operating Procedures (SOPs), and scenario-specific contingency plans for serious security incidents.
- Understand the basic strategies for responding effectively to critical security incidents in the field should they actually occur.
- Understand the relationships between different operational partners in the field concerning your security.
- Understand and deal with the relationship between stress and security for field-based staff.

## Organization of this Course

This course is divided into twelve chapters, each one based on a different aspect of managing risk in the field. The text is designed to be read from beginning to end, and in most instances a good understanding of the material presented in any chapter is required to fully appreciate the next. For the casual reader who only wants to review those chapters of most interest, however, references to important points in previous (and in some instances future) chapters are included where required for full understanding.



**Chapter 1: Introduction to Security for Humanitarians Workers** – This chapter provides an overview of the global security situation facing humanitarian aid workers today. It also explores some of the recent trends regarding threats against staff in the field.

**Chapter 2: Approaches to Managing Security** – This chapter explores the basic response strategies in use by humanitarian organizations. It explains, in simple terms, the options and strategies for security management in use by the Red Cross Movement, the UN system, and in a very general way, by the many NGOs working in insecure environments.

**Chapter 3: Overview of Security Risk Assessment** – This chapter provides a step-by-step outline of the SRA process. Each part of the cycle is discussed in detail in the following chapters of the course.

**Chapter 4: Threat Assessment** – This chapter provides guidance on practical ways to collect and analyze security threat information.

**Chapter 5: Vulnerability Assessment** – This chapter illustrates some of the key aspects of vulnerability relevant to humanitarian programs, and shows their importance in the overall SRA process.

**Chapter 6: Program Assessment** – This chapter examines ways in which the programs undertaken by humanitarian organizations can affect their security. It proposes concrete ways for managers in the field to analyze this relationship methodically.

**Chapter 7: Risk Assessment and the Risk Matrix** – This chapter discusses how Threat, Vulnerability and Program Assessment are brought together to yield an overall picture of risk. It introduces the Risk Matrix as a tool to analyze, prioritize and explain threats in terms of their impact and likelihood.

**Chapter 8: Risk Reduction Measures** – This chapter begins by discussing Criticality Assessment as a process for weighing programmatic benefits against the associated risks to staff. It then provides an overview of a range of prevention and mitigation measures – a field safety toolkit – that can be used to reduce risk to tolerable levels.

**Chapter 9: Security Plans and Planning** – This chapter describes the importance of security planning and provides the reader with both generic and specific templates that can be used to begin or improve the security planning process.

**Chapter 10: Critical Incident Management** – Even with good security planning, serious security incidents can still occur. This chapter gives some guidance on the immediate actions to take when critical security incidents happen.

**Chapter 11: Security Relationships in the Field** – Humanitarian workers are almost never alone in the field. There are many actors involved, from the host government, Red Cross, UN, Military, NGO, and local community stakeholders. All of them have an impact on and are influenced by the others. This chapter investigates some of the key security relationships between the usual players in humanitarian field situations.

**Chapter 12: Security and Stress** – Situations of high risk increase stress on field staff. High levels of stress among field staff increase risk to the team. This chapter provides some advice and guidelines on managing stress in insecure field environments.



## How to Use this Course

Self-study is more demanding than traditional classroom instruction in that learners must provide their own framework for study instead of having it imposed by the course or workshop timetable. One of the problems with self-study courses is that people begin with great enthusiasm at a pace that they cannot sustain. The best way to undertake this learning module is to plan your own study schedule over a pre-set period by thinking ahead and making your own schedule for study.

The course is designed to take approximately 20 hours to complete. This includes the time for reading, reflecting, answering the questions in the text, completing the exercises provided and filling out the evaluation form at the end. This module is provided for professional and personal development. There is no final test, exam or academic accreditation of any kind.

### *Pre-test*

The pre-test included at the beginning of this course allows you to test your general knowledge of field security issues and security risk management terminology and best practice. This test consists of 36 true/false questions. Taking this test before beginning the course should stimulate you to compare your own thoughts about managing field security to those presented in the text.

Also, the pre-test allows you to determine quickly how much you already know about the ideas presented here, and it will help you determine which parts of the course you can move through more quickly and those on which you may need to spend more time.

### *Instant Feedback: Self-Assessment Questions and Exercises*

In a self-study text like this, instant feedback from an instructor is not possible. However, to address the need for assessing your learning, each chapter has five true-false questions and five multiple-choice questions. The answers are provided at the end of each chapter. Other questions and exercises of a more reflective nature are found throughout the chapters to help you get the most from the materials. You are encouraged to take the time to actually write your answers out in the spaces provided as this will increase your mental engagement with the material and will aid in retention of new ideas presented. Each chapter concludes with a summary of key points as a review.

# Pretest

## Security Risk Management



Circle T or F to indicate whether a statement is True or False

Answer key on page xii.

### CHAPTER 1

- T  F 1. In the 1990s, the increased quantity of reported security incidents was due, at least in part, to overall greater numbers of humanitarian workers in the field.
- T  F 2. One trend that has been evident since 2000 is the increasing sophistication of terrorist weapons and attacks.
- T  F 3. In the UN, the strategy of protecting offices and compounds with high walls and gates has generally been rejected in favor of more image-friendly approaches.

### CHAPTER 2

- T  F 4. Security management response strategies ultimately rely on only one useful action – protection or “hardening the target” of field staff, vehicles, and offices.
- T  F 5. The security triangle is defined as the high-risk road travel between, and time spent at, three common points: insecure office spaces, hotels and guest houses, and highly vulnerable personal and social activities, for example at public restaurants.
- T  F 6. The ICRC does not pursue staff security as a core element of its work, since it is understood that all ICRC activities will be high risk.

### CHAPTER 3

- T  F 7. The term *threat* as used in the SRA process refers to the bad or harmful things that can happen to staff in the field, and are generally expressed as events.
- T  F 8. The term *impact* in determining risk relates to how damaging a threat will be if it happens.
- T  F 9. The term *likelihood* in risk analysis relates to the probability that a predicted threat will actually happen.

### CHAPTER 4

- T  F 10. Pattern analysis is a component of threat assessment that refers specifically to the damage patterns from bomb attacks to determine what locations are safest inside an office or residential building.
- T  F 11. Historical analysis depends on the collection and analysis of previous threat data.
- T  F 12. Change analysis is done to better understand and predict how threat patterns may change.



CHAPTER 5

- 13. Consideration of Program Impact, in terms of vulnerability assessment, implies that your vulnerability is based on more than walls, fences and guards...the perceived results of your work in the field also affects your vulnerability.
  - 14. Security problems can arise from the mistaken belief that people in the community understand the objectives of your operations.
  - 15. Staff members' interpersonal communication and negotiation skills are valuable for program development purposes but have little or no effect on security issues.
- 

CHAPTER 6

- 16. Programs that distribute relief items or services that are highly valued by the community will not increase security risks to staff.
  - 17. Programs that challenge traditional beliefs or norms may increase the risk to staff carrying out the programs.
  - 18. Projects that reduce risk to staff in the short term will always reduce risk in the longer term.
- 

CHAPTER 7

- 19. Risk is dependent on two factors: threat level and rate of change in the threat environment.
  - 20. It is generally easier to imagine and agree on the resulting level of harm from a potential threat than it is to agree on how likely it is that it will actually occur.
  - 21. Security risk analysis for an organization should only be done by experienced security officers.
- 

CHAPTER 8

- 22. Mitigation means a reduction in the impact or harm of a potential threat.
  - 23. Prevention means the reduction of likelihood that a potential threat will occur.
  - 24. A high concrete wall around an office compound might be considered a hardening option as well as deterrent.
-

**CHAPTER 9**

- T F** 25. Offices with less than 10 staff do not require a security plan.
- T F** 26. Because the security plan is a sensitive document, it should not be shared with general staff beyond the logistics, communications and security team.
- T F** 27. A national staff continuity plan, as part of the larger security plan, should include, among other things, how the remaining staff are to be paid in the absence of international staff being evacuated out of the country.
- 

**CHAPTER 10**

- T F** 28. Critical incident management and Security Risk Management basically mean the same thing.
- T F** 29. The first step to be taken after a critical incident is to get control of yourself and your own emotions.
- T F** 30. Critical incident management is limited to actions that occur within the first 24 hours after a serious security incident.
- 

**CHAPTER 11**

- T F** 31. Sharing information on security incidents and threats should be avoided since most organizations' mandates do not allow for such exchanges.
- T F** 32. According to generally recognized principles of international law, primary responsibility for the security and protection of humanitarian personnel resides with the host governments of the countries in which they work.
- T F** 33. Despite some differences in organization and operating norms, military forces and humanitarian organizations can be safely assumed to share the same overall objectives in responding to a humanitarian emergency.
- 

**CHAPTER 12**

- T F** 34. Critical incident stress—and not chronic stress—should be of concern to managers
- T F** 35. Critical incident or traumatic stress can result in “flashbacks”—intrusive mental images or memories of the traumatic experience.
- T F** 36. Nothing can be done to mitigate critical incident stress as only time will eventually soften the results.
-



**Pretest  
Answer  
Key**

- |     |   |     |   |
|-----|---|-----|---|
| 1.  | T | 19. | F |
| 2.  | T | 20. | T |
| 3.  | F | 21. | F |
| 4.  | F | 22. | T |
| 5.  | F | 23. | T |
| 6.  | F | 24. | T |
| 7.  | T | 25. | F |
| 8.  | T | 26. | F |
| 9.  | T | 27. | T |
| 10. | F | 28. | F |
| 11. | T | 29. | T |
| 12. | T | 30. | F |
| 13. | T | 31. | F |
| 14. | T | 32. | T |
| 15. | F | 33. | F |
| 16. | F | 34. | F |
| 17. | T | 15. | T |
| 18. | F | 36. | F |

# Chapter 1

## Introduction to Security for Humanitarian Workers

*United Nations members loading flag-draped metal transfer cases carrying the remains of bombing victims from the UN Office of Humanitarian Coordinator for Iraq (UNOHCI) onto an aircraft during a ceremony held at Baghdad International Airport. The bombing victims' remains were airlifted to their respective home countries for repatriation.*



Photo by MSGT Robert Hargreaves Jr., USAF, 26 Aug 2003

Humanitarian field workers from the United Nations, the Red Cross and Red Crescent Movement, and the many non-governmental organizations (NGOs) involved in conflict and post-conflict areas around the world are facing serious security threats. Those who have traditionally worked in high-risk areas such as the International Committee of the Red Cross (ICRC) and the United Nations High Commissioner for Refugees (UNHCR) have developed strategies for remaining in the field under these threats. Today, other relief and development agencies that have been accustomed to working in peaceful and safe environments are also working in increasingly insecure areas. Even those involved in activities like education and cultural exchange programs may now find themselves at heightened risk of random urban crime, being caught in the crossfire of armed conflict, or even the direct target of terrorism.



### Learning Objectives

This chapter will provide you with a basis for better understanding the risks of field work, and for undertaking this distance learning course. In particular, this chapter highlights:

- The current security context for humanitarian field workers.
- Recent trends in humanitarian staff security.
- Some of the ways that humanitarian organizations are responding to security risks in the field.



## 1.1 Security Context for International Field Workers

Humanitarian field staff are dedicated to protecting and assisting those affected by conflict and other disasters. Those staff members also have families, lives, and real fears. Managers of those dedicated staff members now recognize the need to protect their own staff in carrying out their humanitarian mandates. Throughout the world humanitarian workers are at risk of becoming the subject of the next news story as a victim rather than as a rescuer. The perception of this danger has become amplified through the news media, resulting in heightened fear of the dangers involved.



Question

*What examples of serious security incidents involving humanitarian field workers have you heard of, or experienced in the last three years?*

---

---

---

---

Today, news reports of serious security incidents involving humanitarians are common in the international media. The excerpts shown here are only a few of the hundreds of recent examples.

Security threats in the field vary depending on the country, the region, the district, and even the time of year. Although each situation is different, there are some general trends that are useful in understanding the overall security environment.

### **ICRC guard killed in Mogadishu shooting incident**

On Saturday, 13 December, 2008 a Somali security guard working with the International Committee of the Red Cross (ICRC) was killed in a shooting incident Saturday in Mogadishu, an ICRC spokeswoman said. Aid workers have repeatedly been caught in the cross-fire of Somalia's deadly conflict, which has made Mogadishu one of the most dangerous capitals in the world for relief organizations. Many have pulled out their foreign staff following a spate of killings and kidnappings this year but gunmen have since targeted Somalis working for international organizations. Armed groups currently hold two foreign aid workers from the French organization Medecins du Monde as well as four members of the Action Contre la Faim (Action Against Hunger) NGO.

Based on an AFP article from December 2008.

### **"Aid Worker Died Doing What He Loved"**

The family of a British aid worker who was killed by a landmine in Sudan yesterday paid tribute to his 'love of humanity'. Save the Children programme manager Rafe Bullick, 34, from Edinburgh, died when his vehicle drove over the explosive in the troubled Darfur region. His colleague, Sudanese water engineer Nourredine Issa Tayeb, 41, also died in the anti-tank landmine blast in the Um Barro area last Sunday.

From an article in the 13, October, 2004 Birmingham Post, England

### **Aid Worker Murdered in Batticaloa, Sri Lanka**

An aid worker with the Norwegian Refugee Council (NRC) was killed by unidentified gunmen in Batticaloa last night. A. Vigneswaran was shot and killed after the gunmen forced him from his house

according to local authorities. Vigneswaran had worked as a construction-supervisor with NRC for two years.

From a security news report dated 28/11/08



### Gunmen Kill American Aid Worker and Driver in Peshawar

Gunmen shot and killed an American aid worker and his driver in Peshawar, Pakistan on Wednesday 12 November. The men were killed near their office in the University Town area. The *NYT* has identified the murdered American as Steve Vance of the Co-operative Housing Foundation (CHF). The Tehrik-i-Taliban, also known as the Pakistani Taliban, has claimed responsibility for the murders.

From a *New York Times* report

### Gunmen kidnap foreign, Somali aid workers on airstrip

MOGADISHU, Nov 5 (Reuters) – Gunmen stormed an airstrip in central Somalia on Wednesday, kidnapping a group of foreign and local aid workers, witnesses and humanitarian sources said. Six foreigners—two Kenyans, two French, a Bulgarian and a Belgian—were among those seized, a spokesman for the European Commission said in Brussels. The kidnappings near Dusamareb town were the latest in a series of abductions of humanitarian workers this year in the lawless Horn of Africa

nation. “Heavily armed men with three battle-wagons and three small cars kidnapped the foreigners who landed a plane, and also some people waiting for them at the airstrip,” a local resident, Farah Osman, told Reuters. Aid workers have been increasingly targeted this year for assassination and kidnap in Somalia, where Islamist insurgents are fighting the government and its Ethiopian military allies.

From a news article by Abdi Sheikh and Ibrahim Mohamed – Reuters

## 1.2 Recent Trends in Humanitarian Staff Security

Organizational focus on staff security grew throughout the 1990s. Prior to that era, security was largely viewed as an administrative function left to technical experts. Increasingly since the 1990s, humanitarian organizations are viewing security management as an integral part of their operations and one of the core competencies of humanitarian managers and staff.

### Security trends in the 1990s

Humanitarian aid workers from UN organizations, NGOs and the Red Cross/Red Crescent Movement have traditionally enjoyed both international legal protection, and de facto immunity from attack by belligerent parties. However, attacks on humanitarian workers became more frequent starting in the 1990s. This is attributed to a number of factors, including the following:

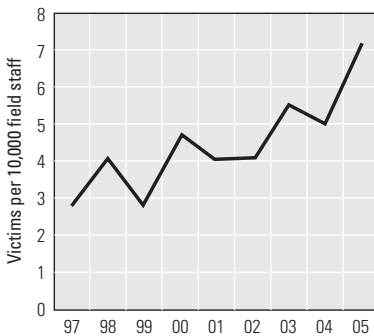
- An increasing number of humanitarian workers deployed during the period.
- Increasingly unstable working environments.
- Proliferation of irregular, non-state actors: warlords and rebel groups or armed militias, often with little discipline or respect for the norms of armed conflict.
- Increasing politicization of humanitarian work, with humanitarian agencies no longer being perceived as neutral by all parties.
- Proliferation of small arms and landmines.
- Increasing pressure on humanitarian agencies to meet beneficiary and donor expectations, even in the face of increasing security threats, due in part to advances in mass media.

Some analysts say that the increase in security incidents during this period was due to the concurrent increase in activities and number of staff in the field. One analyst at the time explained that “... the rising numbers of deaths among relief workers can probably be explained by a surge in humanitarian activities since the cold war. For example, at the height of relief operations in Rwanda and Haiti there were more than 800 non-governmental organizations operating in the respective countries. At the same time, humanitarian missions are increasingly taking place under poor security conditions, with a lack of protection normally accorded under international humanitarian law. High staff turnover and recruitment problems have also led many non-governmental organizations to employ young and inexperienced volunteers, who may face greater risks of exposure to danger.” (*Benjamin Seet, in a 3 February, 2001 British Medical Journal article, “Increased Humanitarian Deaths May Not Mean Higher Risks of Dying”.*)



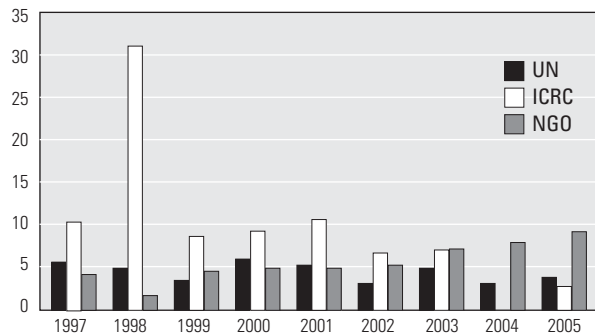
There have been some differences noted in the trends of security incidents during this period in terms of who were affected. National and international staff are apparently affected differently. The Humanitarian Policy Group (HPG) issued a report documenting that while threats against international staff stayed the same or even decreased slightly during the period from 1997-2005, the rate of incidents against national staff have increased markedly. Also, threats against NGOs have, in general, been more numerous than those against the UN and Red Cross staff in the field. Both of these trends are shown in the graphs below.

**National staff victims relative to their number in the field, 1997–2005**



*The majority of aid worker victims (78%) are nationals of the host country—a number that more than doubled over the period of the study. The incidence rate for international workers is stable or declining while it is rising for nationals, particularly in the most dangerous environments.*

**Trends in casualty rates by institution, 1997–2005**



*UN and ICRC aid workers have both seen a decrease in major violent incidents, while NGOs have endured increasing numbers of incidents in absolute, relative and proportional terms. . . . This divergence may be due to increased conservatism within the UN and the ICRC for a period after the bombings in Iraq in 2003. Another factor could be increased NGO operations in high-risk areas over the past few years.*

Recreated graphs are based on those in the HPG Briefing Paper 24 – Providing Aid in Insecure Environments: Trends in Policy and Operations (9/2006).

### Trends in humanitarian field security since 2000

The patterns of global conflict and instability that emerged in the 1990s did not decisively change with the new millennium. However, some general trends have emerged since the September 11, 2001 attacks on the US World Trade Center and Pentagon buildings. Most prominent are the raised perception of terrorism as a global threat and the further polarization of stakeholders involved in the larger conflict that has grown out of that incident. Key trends include the following:

- Modern technology has contributed to increased complexity and sophistication of threats; for example, the use of state-of-the-art explosives, the coordination of attacks using cell phone and internet technology, and the intermingling of banditry, terrorism, narcotics and human trafficking.
- Trans-national terrorism currently dominates the agenda of many nations and the headlines of the major news media. Efforts to cope with this phenomenon, described by some nations as the *War on Terror*, have had a polarizing effect, and this has eroded the perception of the United Nations’ neutrality.
- While terrorism is not a new phenomenon, recent years have seen a proliferation of new terrorist organizations and the use of more sophisticated methods to recruit, organize and conduct attacks. Terrorist attacks are now seen as commonplace and copycat attacks are multiplying. More spectacular attacks and the rise of suicide bombing as a tactic are also



continuing trends in numerous attacks in cities around the world. A recent example is the massive orchestrated attacks on private hotels and other institutions in Mumbai, India, on 28 November 2008, resulting in the deaths of some 200 people and the injury of another 300.

- The UN, Red Cross/Red Crescent Movement, NGOs, and other humanitarian actors have unequivocally been targeted by terrorist groups.

A 2005 review of humanitarian fatalities around the world noted several trends and presented the following conclusions:

- **The increasing number of deaths reflects the expansion of humanitarian activities in or near conflict zones.** The end of the Cold War brought a number of internal wars and new possibilities for collective intervention, leading to more aid operations in areas of conflict.
- **Despite growing casualties in absolute numbers, the security risk to individual humanitarian workers has probably decreased.** Humanitarian operations and workers in the field have expanded faster than the incidence of violent death among humanitarians, even when using the high death estimates for recent years.
- **The security risk is not evenly spread.** This was dramatically illustrated in 2003, when the bombing of the UN headquarters in Baghdad and violence in Afghanistan accounted for about half of the deaths of humanitarian workers in that year.
- **Most humanitarian workers who die in the line of work are intentionally killed.** Deliberate violence was recorded as the cause of 76% of deaths; plane crash, landmines, car accidents and unintentional bombing accounted for the rest.
- **More local staff are being killed than internationals.** Various factors may explain this: there may simply be more local staff than internationals, national staff may be more exposed in the field, agencies may employ more national than international staff in high-risk areas (as in Iraq), and local employees may be more vulnerable politically than expatriates.
- **Deadly violence takes different forms in different regions.** In Iraq, humanitarian workers are most likely to be killed or injured by bombs. In Afghanistan, they face ambushes and de facto executions. In Angola, they risk running across landmines.
- **Most security incidents do not end with death.** Humanitarian workers face a range of threats, including banditry, hostage taking, theft of office property and vehicles, ransacking of warehouses, hijacking of relief convoys, bomb threats and harassment of various kinds.



*Global aid worker deaths due to violence by year based on review by the Humanitarian Policy Group (HPG) Briefing Paper 24 (9/06).*

Recent statistics for UN security incidents include the following:

- Between 1 January 1992 and 1 April 2005, there were 229 malicious deaths among UN civilian staff. Of these, 49 were internationally-recruited staff and 180 were locally-recruited staff. Twenty-nine were from UNHCR.
- Of these victims, 129 died of gunshot wounds; 50 were victims of malicious acts including bombings and landmines; 47 were victims of ethnic violence in Rwanda and Burundi alone.



- Between January 1993 and July 2004, 278 UN civilian staff members were taken hostage; 191 were international staff members and 87 were national staff. There were 19 incidents of hostage-taking reported in the past year.
- The most prevalent threats to the security of United Nations staff and operations are physical attacks, threats, robbery and theft. During the period from 1 July 2004 to 30 June 2005, there were 19 incidents of hostage-taking and 19 kidnappings, as well as 5 cases of rape and 10 cases of sexual assault on United Nations personnel. A total of 119 incidents of armed robbery of significant United Nations assets were reported and 43 attacks on humanitarian convoys and operations, resulting in death or injury of United Nations personnel. This is a significant increase over the 7 such incidents recorded during the previous reporting period.

Global trends must be balanced with local realities, however. Threats and trends must be assessed on a country by country, or even a district by district basis. Afghanistan is a good example of a country in which the specific trends have been carefully documented. The Afghanistan NGO Safety Office (ANSO) provides a quarterly report on “crime and conflict related incidents” involving NGOs in Afghanistan. It also tracks “conventional and asymmetric conflict across the country” and in 2007 reported a nearly 100% increase in attacks over the previous year. Regardless of global trends, this country-specific information is obviously important for those planning to work in Afghanistan.

### 1.3 Humanitarian Response to Security Threats

#### *Who is responsible for your safety in the field?*

According to generally recognized principles of public international law, primary responsibility for the security and protection of humanitarian workers lies with the host government. This flows from the government’s responsibility to provide for law and order, both for its own citizens as well as for expatriates. But what happens in countries where authorities do not have the ability to ensure your safety, or in extreme cases where there are no legitimate authorities at all? Worse still, what if the authorities are in control, but unwilling to keep you safe, or even pose a direct threat themselves to your safety?

In such cases, it becomes incumbent upon organizations sending staff into dangerous locations to take their own additional precautions. Where local capacities cannot provide adequate staff safety, the organizations and their staff members must do something to fill the gap. How do humanitarian organizations respond to increased risks?



**Question**

*What has your organization done to respond to the threats that you and your colleagues face in the field?*

---

---

---

---

---

---



### Question

*What practical options exist for humanitarian organizations for managing the risk to their staff in insecure areas?*

---



---



---



---



---



---



---

Organizational responses to security challenges in the field vary widely. They are based on the nature of the specific organizations, their mandates, policies and philosophies of service as well as their budgets. The points below give a very brief overview of some basic response strategies in practice today. The following chapters in this course will explain these in more detail and will ultimately focus on one particular strategy — the Security Risk Management (SRM) approach.

### *“Responsibilizing” authorities*

Humanitarian organizations must take additional security measures when local authorities cannot provide adequate protection for their staff. However, some caution that the push for self-protection could be short-sighted. Before rushing to substitute for existing capacities, shouldn't we first try to strengthen or fix what is already in place?

*Responsibilizing*, coined from the French word *responsibiliser* meaning to make or hold someone responsible, here means encouraging or helping authorities to fulfill their legal obligations. When Sir David Veness was appointed as first UN Undersecretary General for Safety and Security in 2004, he announced that one of his top priorities would be to foster greater responsibility among host government authorities for safety of staff.

Encouraging more effective action from those responsible for your safety can take the form of advocacy. Negotiating, convincing or even pressuring authorities to do what is needed can be an important aspect of managing field security. It can also include various forms of capacity building such as providing training and equipment to strengthen weak law enforcement agencies, rather than resorting to a private security service, for example.

There should be no illusions that every security problem in the field can be solved by such responsibilizing, at least not in the short term. At the same time, it is equally true that wherever capable and willing partners do exist, humanitarian organizations should do all they can to encourage them to play a greater role. In any event, we should never allow legitimate authorities to absolve themselves completely of their responsibilities to keep humanitarian staff safe.



## *Analysis and planning*

Many organizations have responded to the global threat environment by improving their ability to analyze the security situations they are in and to apply this improved understanding to their plans and operations to improve staff security. The ICRC, for example, held a high level conference in Glion, Switzerland in 1997 to outline the growing threats to their staff and ways to better respond to them. The meeting was “a milestone in the recent history of the ICRC. Its aim was to mobilize senior operational staff around security issues in situations where humanitarian operations are undertaken. The recent tragic events affecting the ICRC (the assassination of ten staff members in Burundi, Chechnya and Cambodia) and the murder of three members of *Médecins du Monde* as well as four United Nations human rights monitors in Rwanda have highlighted the need to reassess security and humanitarian action on behalf of conflict victims.” (Quotation is from a statement posted on the ICRC website).

The UN responded similarly with a series of studies and reports highlighting the difficult security situation facing UN staff members around the world. Like the ICRC, their response began with the cornerstone declaration that they must continue their mandate, and therefore remain at work, to the extent possible, even in difficult areas. One of the main results was the call for a heightened ability to assess and respond to security threats in a more professional way. The UN Secretary General called for such improved abilities in 2004, resulting in the creation of the UN Department of Safety and Security (DSS) in 2005. This office and its security expertise will be described further in the next chapter.

Many international NGOs have responded similarly through the expansion of their security desks and units, and through the hiring of security experts (most often from military and police backgrounds) to assist their humanitarian field staff. Improved planning and analysis are now considered a cornerstone of the humanitarian response to security threats.

## *Protective measures*

Partially as a result of the newly acquired security expertise in their organizations as described above, and partially due to the heightened perception of the threats, many organizations began to spend more money on protective measures. Today it is common to see high walls topped with razor wire, guards, and protected windows and doors in Red Cross, UN, and NGO field offices. Particularly in insecure areas where analysis has indicated that these organizations may be targeted, humanitarian offices, compounds and enclaves have become fortified. Sometimes this protection comes at the cost of taking on a militarized image, which has long been held as an unacceptable step by many in the humanitarian field.

## *Training*

Security training for staff has been among the organizational responses of nearly all large humanitarian agencies. The NGO community has launched many training initiatives for field staff to become more aware of their surroundings and to take appropriate actions when security threats actually occur. In 1995, the United States Agency for International Development's Office of Foreign Disaster Assistance (USAID/OFDA) provided the NGO consortium InterAction with a grant to develop curricula for non-governmental organization (NGO) training courses in two specific areas—health and security. The resulting security training modules formed the basis for many NGOs' ongoing security training programs. The UN has also significantly increased its budget for staff



security training. UN security training includes specific programs for managers, security officers, security management teams and individual staff. The Safe and Secure Access to Field Environments (SSAFE) program is a pre-deployment training program for staff deploying to high-risk duty stations. The UN has also made completion of an interactive computer-based training on basic security a mandatory requirement for all staff, and has further developed a companion program on advanced security for those working in particularly dangerous environments.

### ***Recruitment of professional security officers***

Before the 1990s, the term “security officer” for most humanitarian workers would probably bring to mind the image of the uniformed guards that control the entrances to buildings in major cities, and little more. In the mid-1990s the UN began recruiting specialists as Field Security Officers (or Advisers) to look specifically at measures needed to keep staff safe in the field. These FSOs or FSAs usually come with a military or police background, and in the past two decades their numbers have grown steadily. Today there are more than 1,000 UN security professionals in duty stations around the globe. Recruitment of security professionals has not been limited to the UN; large NGOs like World Vision and Mercy Corps International have sought these same types of specialists for their operations in insecure places. The Red Cross movement organizations are also increasing their security expertise. The ICRC maintains a team of headquarters-based security professionals, who make regular visits to the regions, provide training, and who can support major operations during crises. Many of the National Societies that are involved in deploying staff internationally also now have security officers, and the International Federation of Red Cross and Red Crescent Societies (IFRC) is promoting security officers for stations with a large Movement presence.

The strategy of increasing professional security staff is not without some controversy, however. On one hand, security officers have specific knowledge and skills that general humanitarian staff may not have. On the other hand, some humanitarians worry that over-reliance on security professionals can lead to complacency among the rest of staff, who may come to believe that security is something for the Security Officer alone to handle.

### ***Reduction of staff exposure to threats***

One response to security threats is simply to avoid going to places that are too dangerous. This strategy is straightforward: if you are not present where the security incident occurs, then it is not a threat to you. Partial exposure reduction strategies include limiting travel in certain areas (e.g., roads prone to ambush) or at certain times (especially nighttime); or by reducing staff numbers, thereby decreasing the number of potential targets (but also possibly the level of assistance). The complete form of exposure reduction is of course evacuation of all staff from the field. This and other means means of risk reduction are covered in more detail in *Chapter 8 – Risk Reduction Measures*.

Consider the example on the following page taken from the Somalia Monthly Cluster Report of May 2008. The full report documents the ongoing situation and this section in particular highlights the humanitarian community’s response to the deteriorating security situation in the country.



“The deteriorating security situation and constrained humanitarian access in Somalia during the month continued to challenge national and international organizations. Major obstacles faced by the humanitarian community in Somalia in May included deliberate targeting of aid workers, threats of abduction and actual kidnapping and looting of food relief. On 7 May, a WFP-contracted truck driver was killed by militiamen at an illegal checkpoint in Mudug region. Then on 17 May the head of office of the NGO Horn Relief was brutally murdered in Kismaayo. This incident brings the number of aid workers killed in Somalia so far this year to thirteen.

At the same time, the threat of abduction still continues to affect humanitarian aid workers in Somalia. On 20 May a dozen gunmen barged into the compound of an Italian aid organization in Aw Dheegle, Lower Shabelle and kidnapped two Italian nationals and their Somali colleague. These latest abductions bring the number of aid workers and other foreign nationals currently being held hostage in Somalia to seven. Also on 20 May, unidentified militiamen attempted to attack the UN compound in Mogadishu with a hand grenade, the second such attack this year. Luckily, the device did not detonate, and there were no injuries. On 2 June a UNDP National Officer was shot on the street in Baidoa, Bay region. Although he was wounded on his shoulder and upper arm, his condition was not critical and he was flown to Nairobi for treatment.

In Awdinle and Gofgadud Buure (Bay region) supplementary feeding programmes sites; food rations meant for the families with malnourished children were looted at the distribution centres.

**As a consequence of security threats and incidents, most NGOs have taken out their international staff and the UN has decided to limit international staff presence to key locations. In May, regular UN Humanitarian Air Service flights were reduced to key locations and unnecessary travel by road between many locations halted.”**

– Excerpt from the Humanitarian Response in Somalia:  
Monthly Cluster Report, May 2008, as posted on ReliefWeb

Program suspension or cancellation is, of course, the most drastic measure in terms of impact on humanitarian programs. It is, strictly speaking, not balancing programs and risks, but conceding that in certain cases no such balance is possible. This is fully consistent with the SRM approach, which emphasizes weighing programmatic needs and dangers in the environment to make responsible security decisions. When all other responsabilizing and self-protection security measures fail, humanitarian organizations are sometimes left with no other alternative than to leave.

## Summary



### Key Points

The working environment for humanitarian field workers can be dangerous, even life-threatening.

---

Perception of the threat has also increased, along with total number of incidents, so that staff security is now a key concern of field office managers.

---

During the 1990s, there were increasing numbers of humanitarian workers deployed in increasingly unstable environments. The key security trends of the time were:

- Increased numbers of security incidents reported.
  - Increased number of incidents against national staff as compared to international staff.
  - Proliferation of irregular, non-state actors with the result of loss of respect for the norms of armed conflict and respect for neutrality of Red Cross, UN, and other unaligned humanitarian field workers.
  - Increasing politicization of humanitarian work.
  - Proliferation of small arms and landmines.
  - Increasing pressure on humanitarian agencies to be active in insecure areas, due in part to advances in mass media.
- 

Since 2000, types of security threats have not dramatically changed; however, the number of them as well as the reporting of them has significantly increased. Some developing trends include:

- Improved technology has allowed many threats to increase in complexity and sophistication.
  - Trans-national terrorism and national and international responses to combat it have resulted in the polarization of stakeholders, with the result that humanitarian organizations once seen as neutral are now commonly seen as aligned to the West.
  - Terrorist organizations and acts have proliferated and suicide attacks have become more common.
  - The UN, Red Cross/Red Crescent Movement, NGOs, and other humanitarians have unequivocally been targeted by terrorist groups.
- 

*continued next page*



Security threats against humanitarian field staff are not the same everywhere. Security analysis and planning have become cornerstones of security management for humanitarian agencies.

---

In general, humanitarian organizations have responded to the security environment in a number of ways, including:

- Encouraging responsibility of authorities
- Better security analysis and planning
- Improved protective measures
- Recruiting security specialists
- Training
- Reduction of staff exposure to threats



## Chapter 1 Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

- T**  **F** 1. The total number of threats against all humanitarian field staff has actually been decreasing since 2000.
- T**  **F** 2. In the 1990s, the increased quantity of reported security incidents was due, at least in part, to overall greater numbers of humanitarian workers in the field.
- T**  **F** 3. One trend that has been evident since 2000 is the increasing sophistication of terrorist weapons and attacks.
- T**  **F** 4. In the UN, the strategy of protecting offices and compounds with high walls and gates has been generally rejected in favor of more image-friendly approaches.
- T**  **F** 5. Serious security incidents against humanitarian field workers are seldom reported in the international news media.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following are strategies that have been used in response to field security threats against humanitarian agencies?
  - A** Increase physical protective measures.
  - B** Improve security analysis and planning expertise.
  - C** Increase presence in the field of humanitarian program staff.
  - D** Decrease presence in the field of humanitarian program staff.
- 7. Which of these represent security trends of the 1990s?
  - A** Increased number of humanitarian field workers deployed.
  - B** Increased rate of attacks against national staff.
  - C** Increased proliferation of small arms and mines.
  - D** Increased respect for the neutrality of international humanitarian organizations.



**Chapter 1**

**Self-Assessment Questions** *(continued)*

8. Which of these represent the developing security trends in the field since 2000?
- A** Increased technology and ability to coordinate attacks by terrorist groups.
  - B** Increased polarization amongst stakeholders in humanitarian response, heightening tensions.
  - C** Fewer security incidents annually reported than in the previous decade.
  - D** Most security incidents result in death.
9. Which of the following are generally true about trends in training humanitarian staff in field security?
- A** Only the NGOs are providing training in this area.
  - B** Only the UN is providing training in this area.
  - C** Only the Red Cross is providing training in this area.
  - D** Almost all large humanitarian organizations are now conducting some training in field security issues.
10. Which of the following is considered a cornerstone to security risk management by most humanitarian organizations?
- A** Organizational image is the most important aspect of field security.
  - B** Similar levels of protective measures should be pursued for all offices worldwide.
  - C** Security analysis and planning should be the basis for other security-related measures.
  - D** The humanitarian mandate comes first; humanitarian field staff should never leave the field due to security threats, even when they are credible and significant.



**Chapter 1  
Answer  
Key**

- |    |   |     |         |
|----|---|-----|---------|
| 1. | F | 5.  | F       |
| 2. | T | 6.  | A, B, D |
| 3. | T | 7.  | A, B, C |
| 4. | F | 8.  | A, B    |
| 5. | F | 9.  | D       |
| 6. | F | 10. | C       |

# Chapter 2

## Approaches to Managing Security

*Recently trained Timorese National Police (PNTL) officers perform a tactical demonstration exercise during a ceremony after successful completion of their three-week training course facilitated by the United Nations Police (UNPOL) component of the United Nations Integrated Mission in Timor-Leste (UNMIT) in August 2008.*



UN Photo by Martine Perret

The responses to security threats are as widely varied as the threats themselves. Basic approaches range from making humanitarian organizations more transparent and available to the community, to building higher walls for greater protection, or even to deploying armed guards capable of returning fire in the event of violence. Which of these is best, in what circumstances? Which strategies have humanitarian organizations chosen?



### Learning Objectives

This chapter presents some of the basic approaches being used to address security concerns by different humanitarian organizations such as the United Nations, the ICRC and the Red Cross Movement, and many NGOs. Methods for determining levels of professional responsibility from the private and professional fields will be examined to provide additional insights. In particular, you will learn about:

- The ICRC *Seven Pillars of Security* model.
- The security triangle approach.
- The UN security management system and the UNHCR culture of security.
- The professional concept of due diligence as applied to security risk management.



There are many ways to respond to security threats. What works for one organization doesn't necessarily work for another. Determining an organization's overall security strategy must include consideration of its mandate, basic philosophy, and budget. As important as choosing a strategy, of course, is the review and evaluation of it to see whether or not it is actually working.

*"However beautiful the strategy, you should occasionally look at the results."*

– Sir Winston Churchill

## 2.1 ICRC and the "Seven Pillars" Approach

The ICRC's security policy is uniquely matched to its core operational philosophy and mandate as an entirely neutral organization. ICRC strives to improve the safety of its field staff through training about International Humanitarian Law and ensuring respect for its neutrality. ICRC vehicles, offices, and even staff members have easily identified and clearly marked insignia. The core strategy is to be seen as a reliable, trusted, and neutral party that should not be harmed. The next step is to become as recognizable as possible, so that ICRC staff cannot be mistaken for a potential enemy.

Another cornerstone of this security management model is the reliance on seven activities or "pillars" to provide or support reasonable security to field staff. This model highlights the fact that all seven pillars in the approach must be functioning for the system to work, i.e. that security is only as strong as the weakest pillar under the roof. It also makes clear that even when properly functioning, only reasonable security can be expected – not an absolute guarantee of safety.



**Question**

*What are the elements of the ICRC's approach to staff security, when by its own unique mandate staff are often required to work in the most dangerous areas?*

---

---

---

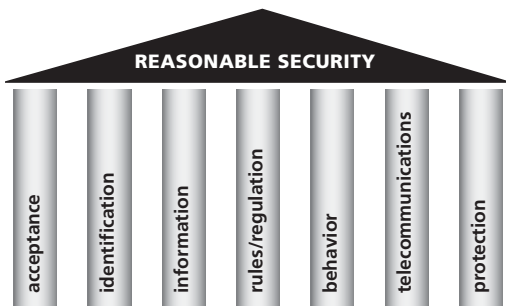
---

---

---

### Pillar 1. Acceptance

#### ICRC "Seven Pillars" Model



BASED ON ICRC TRAINING MATERIALS

Acceptance by the local community, including belligerents, is critical to the ICRC for carrying out its mandate. In achieving this, diplomacy, persuasion and influence are its primary tools. To achieve acceptance, ICRC must make its mandate widely known, and its neutrality understood. It strives to do this by maintaining a highly professional and consistent image, and through ongoing public information, community outreach and training. ICRC delegates must have a good understanding of local culture and norms and know how to work with local authorities, rebel groups, warlords, and others, to build trust and agreements to gain and maintain acceptance.



## Pillar 2. Identification

The second pillar—identification—is closely related to the first as acceptance is only useful for security purposes if people also recognize who you are. Identification has long been a hallmark of ICRC operations in the field. Flags, banners, large insignia on vehicles, and highly visible ID badges on delegates are all part of the identification pillar.

There have been some challenges to the identification pillar in recent years. Following the attack on its Baghdad Headquarters on October 27, 2003, ICRC has had to face situations where clear identification could not ensure safety, or may even have endangered staff further. In exceptional situations, ICRC has conducted operations in unmarked vehicles where doing so was deemed to be the only way to safely ensure access to beneficiaries. This low-profile approach remains extremely controversial among all humanitarian agencies, all the more so for ICRC, as identification has always been a cornerstone of its security strategy.

## Pillar 3. Information

ICRC field staff are expected to keep themselves informed of security developments around them. High priority is given to incident reporting and information sharing, especially in regard to establishing security trends or developing situations. However, due to the necessity of maintaining neutrality, particularly in active military areas, care is always taken not to collect, report, or pass on information of a military nature that might resemble activities of military espionage.

## Pillar 4. The security regulations drawn up by individual delegations

Every ICRC delegation draws up its own set of rules pertaining to security procedures and protocols, specifically related to its own operating environment. These rules are reviewed, updated to meet changing situations, and are made clear to all staff. There is a high regard for the rules and the expectation is that they will be rigorously followed.

## Pillar 5. Behavior (personality)

Acceptance in the field also depends on how individual staff members manage both their public and personal lives. Regardless of professionalism of other staff, clarity of understanding of the mandate and other factors, one poorly performing and disruptive staff member can quickly erode the community's trust in the whole organization. Individual character of staff members and their actions are important. There are strict rules regarding use of controlled substances and illicit sexual activities on the part of staff members.

## Pillar 6. Telecommunications

This pillar is related to the information pillar (Pillar 3). Information must be retrieved and disseminated quickly and clearly if it is to be useful. Staff members must be in good communication with their team and others. They are trained in standardized use of communications equipment in the field. In terms of emergency response, a robust communications system is invaluable for reporting security incidents, calling for assistance, and passing along information in support of rescue and other security-related operations.

## Pillar 7. Passive and active protective measures

Particularly in situations where the above methods do not adequately provide a reasonable level of security, ICRC also protects its assets and staff with *passive protection* responses such as walls, bomb shelters, blast-resistant film for windows, and other physical protections. These are usually the least preferred measures to be taken, and when they are used, they are as discreet as possible to avoid a military appearance. *Active protection* measures may include armed guards and escorts—used only in extreme circumstances—and even then, only with the approval of headquarters.



Another aspect of ICRC’s approach to security that is worth mentioning is mandatory pre-deployment training. In nearly all cases, delegates deploying to risky areas receive comprehensive field training lasting three to four weeks, in which personal safety risks and responses play an important part. The ICRC commitment to ensuring preparatory training is a model that is aspired to by many organizations but not always achieved.

A final factor is ICRC’s approach to enforcement of compliance. In addition to many other things, new delegates learn in their training that a breach in security policy or procedures will be tolerated only once, provided it is not too severe. If a second infraction occurs the delegate will be removed from the field. This “one-strike” policy is rigorously upheld, and cases of delegates returning early really do occur. Again, ICRC’s firm stance on breaches of rules is a distinctive point that is aspired to but not always achieved in other organizations.

**Summary: ICRC Approach to Security**

- The “seven pillars of security” approach
- Special emphasis on identity and acceptance
- Comprehensive pre-deployment training
- Firm enforcement of compliance

## 2.2 NGO Common Approaches – The Security Triangle Model

NGOs have numerous mandates and philosophies of operations. Some place a higher regard for the spirit of volunteerism than for professionalism or technical expertise, while others are extremely technical in their structured approach to staff development and drive for high quality outputs and program efficiency. Some seek to be unique and unaligned with any others, while many NGOS have found that linking with other agencies in umbrella networks can provide real benefits, including strengthening their security management resources and abilities.



**Question**

*What are the basic strategies that NGOs have at their disposal for responding to security threats in the communities in which they work?*

---



---



---



---



---

UNHCR undertook a study in 2004 looking into security approaches used by various NGOs. The goal of the study was to understand what the UN could learn from NGOs that had succeeded in conducting operations safely in high-risk areas. The report, *Maintaining a Humanitarian Presence in Periods of High Insecurity: Learning from Others*, enumerated several important points.



Some of the key themes from that study are as follows:

**There is an NGO emphasis on acceptance strategies** – As with ICRC, most NGOs see building rapport with local stakeholders as a cornerstone of their security strategy. This is not surprising for several reasons. For one thing, it accords well with the philosophy and operational approach of many NGOs, which often emphasize community outreach and relationship building as means to achieve humanitarian as well as security objectives. Moreover, the acceptance approach is decidedly less costly than “hardening” strategies that can entail resources beyond the means of small NGOs.

**Security decision-making is integrated and decentralized** – By integrated, the author of the study meant that in many NGOs, security was generally not assigned to technical experts, but rather included, or “mainstreamed” into the responsibilities of all managers and staff. By “decentralized”, he indicated that most security decision making was made at the field or provincial levels, rather than at headquarters or the capital.

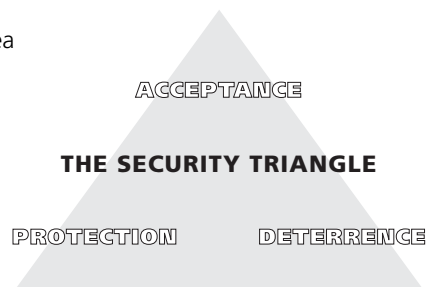
**Decision makers receive technical support** – Increasingly NGOs are making use of technical expertise to support operations in the field. This includes hiring consultants for analysis and training and in some cases the recruitment of Security Officers as regular staff members. While this may seem to contradict the point above regarding “integrated” security skills, the increased use of technical support suggests a move to balance the two approaches.

**Security partnerships support NGOs in the field** – An additional trend among many NGOs is an increased emphasis on the role of partnership in facing security threats. At the most basic level, security partnerships can include information sharing among NGOs working in the same duty station. Information to be shared can also include threats seen in the field, responses, and good security practices. Deeper partnerships can include sharing of resources as well. Recognition of the value of partnership has been mirrored by the UN, which issued a 2006 policy document “Saving Lives Together” emphasizing the benefits and responsibilities of partnerships among UN agencies and NGOs (for more on this, please see *Chapter 11– Security Relationships in the Field*). The value given to this type of partnership by an NGO, however, is very closely linked to the specific mandates and operating norms of the individual organization. While some NGOs welcome advantages of partnership, others are reluctant to collaborate closely for fear of compromising their independence or perception of their neutrality.

### *The security triangle*

One approach to security management for NGOs that is applicable to a wide variety of organizations is called the *security triangle*. Although quite simple in its design, it is descriptive of many humanitarian organizations’ security management responses. The core ideas were originally presented in the journal of the Refugee Studies Centre of the Oxford Department of International Development, the Forced Migration Review, in April 1999. The article was prepared by Randolph Martin, then the Senior Director for Operations at the International Rescue Committee in New York. For the complete article and other information about the Forced Migration Review, see their website at: <http://www.fmreview.org/>.

The International Rescue Committee (IRC) promoted the idea that each of their field offices had to adopt local security protocols that included the elements of **acceptance**, **protection** and **deterrence**, which taken together were called “the security triangle”. It was believed that effective local security responses had to review each of these components and then choose and balance them in formulating their specific response to local threats.





### ***Acceptance or “softening the threat”***

This is the same **acceptance** as described in the ICRC seven pillars model earlier. From an NGO perspective it means that when the local community accepts and supports an NGO's programs in the community, that NGO's security will be improved since people will not want to harm those NGO staff members who are now seen as friendly. Furthermore, community pressure might be brought to bear on anyone threatening the staff of that NGO since they would be considered a useful resource to the community to be protected. Some indicators of high acceptance would be:

- Belligerent parties and combatants consent to the NGO's activities.
- Community members have a stake in the programme and participate actively.
- Community members know of the NGO's activities and understand them to be beneficial and impartial as regards to differing sides in local conflicts.
- Amiable working relationships exist with local authorities such as police and military where appropriate.

### ***Protection or “hardening the target”***

**Protection measures** are the physical barriers and structures, materials and equipment used to make it harder for others to hurt you.

They include:

- Communications equipment.
- Reliable vehicles and maintenance facility.
- Perimeter security devices including walls, barbed wire and alarm systems.
- Flak jackets and helmets.

In the security triangle model, the term protection is also widened to include other organizational and policy-related activities which are not physical measures *per se*, yet still make it more difficult for others to mount an effective threat against the organization. These measures include:

- Clear financial policies and procedures including division of responsibility in accounting, and prudent cash transfer procedures.
- Curfews and no-go zones where appropriate.
- Use of a warden system or communications network for conveying emergency messages.
- Security orientation for incoming staff and routine security briefings for staff including personal security training.
- Convoy operations protocols.
- Active membership in NGO coordinating bodies.
- Collaborative field operations such as convoy operations.

### ***Deterrence or “threat of reprisal”***

The concept of deterrence in this model is based on the idea that potential attackers will be less likely to attack if there will be a reprisal, either through direct counterattack, legal justice systems, pressure from other powerful forces in the community, or the loss of program support or benefits. Deterrents then could include, among other things:

- Police guards or escorts.
- Private armed compound guards and guard dogs.
- Security cameras—with the understanding that evidence will be used to bring cases to court (in areas where courts and legal systems function).



- Diplomatic pressure from powerful forces that can bring pressure to bear on those that threaten the organization.
- Threat of temporary or complete cessation of humanitarian or development programs if staff are threatened or attacked.

### *The security triangle in practice*

The security triangle approach presented above is based on the idea that there may be an appropriate place for each element of the security triangle under any type of security threat, and that each should be considered as a legitimate part of an overall security approach in a given location and situation. Even for the same organization, different combinations of the three core elements may be needed depending on the situation at hand.

#### **Summary: NGO Approaches to Security**

- Emphasis on acceptance strategies
- Integrated and decentralized decision making
- Increasing reliance on technical expertise
- Among some NGOs, more attention to the value of partnership
- The Security Triangle

## **2.3 The United Nations Response to Staff Security and UNHCR's Culture of Security**

The primary responsibility for the security and protection of UN staff, as with other humanitarian workers, rests with the host governments of the countries in which they work. The ability to carry out this duty varies from country to country, however, and the UN also undertakes additional activities to protect its own staff, regardless of the duties of others to do so. The UN Resident Coordinator, normally responsible for achieving coordination among the overall UN presence in any country, is usually also named the Designated Official (DO) for Security and is assigned overall responsibility for the safety and security of UN staff members and their eligible dependents. In the capacity as the DO, this senior UN staff member reports to the UN Secretary General through the Under-Secretary General for Safety and Security.



UN photo

*On 19 August 2003, a truck bomb exploded outside the United Nations Headquarters in Baghdad killing the top UN envoy in Iraq, Sergio Vieira de Mello, and many others.*

While the UN has long dealt with staff security issues, the bombing of the United Nations Headquarters in Baghdad on 19 August 2003, in which 22 UN staff members were killed, had a dramatic affect on the UN security management system. A high-level investigation was carried out and a series of reports and recommendations followed, ultimately resulting in the creation of a new staff security management entity, the United Nations Department of Safety and Security (UNDSS).



**Question**

*What are your observations about the United Nations and its response to field security? List any key approaches or aspects of the UN approach that you believe direct their actions in the field.*

---

---

---

---

---

The United Nations Department of Safety and Security (UNDSS) was established in January 2005 to provide policy and facilitate security management for all UN operations worldwide. This new agency was formed by merging the former office of the United Nations Security Coordinator (UNSECOORD), the UN Security and Safety Service (SSS) and the Security Section of the UN Department of Peace-keeping Operations (DPKO). The primary role of UNDSS is to enable UN operations to continue at the field level, while giving the highest priority to the safety and security of UN staff members and their families. Sir David Veness, the first Under-Secretary General for Safety and Security, enumerated 10 priority areas to be specifically highlighted under the new UNDSS:

- 1) **Information** – The UN security management system (UNSMS) needs to develop a reliable threat and risk assessment process, based on enhanced and expanded information networks.
- 2) **Host nation support** – More advocacy is needed to persuade host country authorities to meet their obligations for security of UN staff, and to optimize support from host countries.
- 3) **Enabling operations** – UNSMS should focus on security as an enabler of UN programs and activities.
- 4) **Globalizing operations** – UNSMS needs to optimize security assets by developing a global perspective.
- 5) **Strengthening inter-agency relationships** – DSS must strengthen relationships with UN agencies, programmes and funds.
- 6) **Decentralization of security management** – DSS needs to better assist and empower Designated Officials.
- 7) **Modernization** – There is a need to modernize the UN concept of security operations and update tools, taking into consideration new global realities.
- 8) **Accelerate crisis management system** – UNSMS needs expertise, procedures and material resources to enable it to respond more rapidly to security emergencies.
- 9) **Advance training strategy** – DSS should develop a UN-wide approach to security training to ensure common standards and compatibility, while permitting individual agencies to develop security expertise in areas relevant to their own unique operations.
- 10) **Communications** – DSS has identified a need to strengthen internal and external communications within the security management system.



## *Other key elements of the UN security management system*

**The UN Inter-Agency Security Management Network (IASMN)** – IASMN includes the whole family of UN agencies, programs and funds, each of which has an organizational focal point identified for security matters. These focal points meet regularly at IASMN meetings that take place at least annually, with recent efforts to increase the frequency to biannual meetings. IASMN acts as a steering committee for policy and structural changes in the UN Security System. While UNDSS takes the lead in preparing and proposing changes, these must be agreed upon and ratified by the various members of the UN family. In this way, high-level security decision making is supported by a high degree of consensus, but it can take time to reach agreement.

**Strengthening accountability** – Attempts to define the responsibility and accountability of the various members of the UN Security Management System have been continuous for many years. In 2002, IASMN approved the UN's first Framework for Accountability, a document that enumerates the specific security tasks required of actors at both Headquarters and in the field. Efforts to update and strengthen the Framework of Accountability are currently in progress.

**Minimum Operational Safety Standards (MOSS)** – Since 2000, the UN Security System has worked to elaborate the minimum standards for reasonable safety in insecure environments. MOSS protocols require the examination of basic security needs in a range of areas: equipment and facilities, telecommunications, vehicles, plans and planning and training of staff, to name a few. These needs will vary considerably depending on the level of risk of each duty station.

Here MOSS is linked to the UN Security Phase system, which categorizes each country (or sub-region of a country) on a scale from No Phase (i.e. reasonable safety) to Phase 5 (completely unsafe, evacuation of international staff is required). Finally, MOSS standards are specific to each country and particular sub-region, taking into account specific threats and risks found in each location. In sum, the MOSS table of security requirements for a fairly high-risk country may amount to 20-30 pages of documentation.

Setting the MOSS standards requires expertise and time dedicated to the task and meeting the standards can be resource-intensive. This may be one reason why the MOSS approach is rarely seen among smaller NGOs that lack such expertise and resources. Nevertheless, the basic principle that minimum standards of safety and security should be defined and adhered to is valid for all, and has already become a standard approach for many other aspects of humanitarian work.

**Security risk management approach** – The UN—and UNHCR in particular—is committed to taking a Risk Management Approach to balancing operational needs and dangers to staff. The essence of this approach will be further explained in the following chapters of this Learning Module.

### *UNHCR's approach to security*

As a member of the IASMN and, of course, the UN, UNHCR follows the approach to security described above for the overall UN. Additionally, because of its specific mandate which often calls for staff to work in unstable border areas, and the consequent increased exposure to risks, the organization has taken further steps to define and strengthen its own culture of security.

UNHCR's Security Policy document, first published in 2002 (updated in 2007) underscores the following five key points:

1. UNHCR is an active member of the common UN security system, complying with established guidelines, sharing information and contributing recommendations to improve overall security management.
2. UNHCR's security policy emphasizes the responsibility and accountability of managers, at Headquarters, at the level of Country Representatives and of heads of field offices,



for the security of their staff, and seeks to improve their decision making with technical field safety advice at headquarters, regionally and in the field.

3. UNHCR seeks to achieve a proactive security management system, emphasizing analysis and early warning, the early integration of security in operational planning, and training.
4. UNHCR strives to provide adequate human resources, material and training to achieve established standards of safety.
5. UNHCR's security policy underlines the responsibility of each staff member to be aware of the environment and existing guidelines, and the capacity of each person to improve his or her own safety.

In early 2004, in the wake of the bombing of the UN headquarters in Baghdad and the murder of UNHCR staff member Bettina Goislard in Afghanistan, the High Commissioner created a high-level Steering Committee chaired by the Assistant High Commissioner to conduct a thorough review of the organization's security management policies and practices. The main recommendation of the Steering Committee was that UNHCR must strengthen its culture of security as follows:

**For UNHCR, the organizational culture of security and safety means:**

- Staff members understand the risks inherent in the work of UNHCR.
- Everyone in the organisation is trained in, understands and can apply UNHCR's approach to and methodology for Security Management.
- Security and safety considerations are integrated as normal functions of UNHCR operations and activity.
- Security management is seen as everyone's job with managers at all levels of the organisation having a particular responsibility and accountability.
- UNHCR staff members at all levels are disciplined in their compliance with security rules and protocols, and non-compliance is grounds for dismissal.
- UNHCR recognizes the importance of competence in security management and prioritizes this competence in the selection and promotion of managers.
- UNHCR staff members and partners speak a common language of security in which terminology is used in a consistent manner.
- From the earliest planning of operations, security is integrated into the assessment and design process so as to maximize the delivery of protection and assistance in potentially hazardous environments without exposing staff members to an unacceptable, unnecessary or unforeseen level of risk.
- UNHCR manages its operations from a risk management perspective in which there is ongoing effort to identify, understand and mitigate risk and responsible risk taking is how UNHCR staff members carry out their work.
- Resources for security are sufficient so that the organisation does not have to compromise on measures necessary to ensure, to the fullest extent possible, the security and safety of staff members and partners.
- UNHCR actively develops an approach and methodology for managing security which takes into account the specificity of UNHCR operations and needs and builds on lessons learned and best practice.
- UNHCR is an active member of the common UN security system, complying with established guidelines, sharing information and contributing recommendations to improve overall security management.
- Staff members have full confidence in how UNHCR manages security.



On 11 December 2007, a bomb attack at the UN building in Algiers claimed the lives of 17 UN staff. The official report published in June 2008 was tellingly entitled *Toward a Culture of Security and Accountability*. The investigating team, in which UNHCR participated, concluded that reinforcing organizational security awareness and discipline had become essential now more than ever. Since then, this terminology has entered the UN-wide vocabulary for improving system-wide security.

### Summary: UN (and UNHCR) Approach to Security

- UN Department of Safety and Security (DSS) and the Inter-agency Security Management Network (IASMN)
- Continued efforts to strengthen accountability
- Elaboration of Minimum Operational Security Standards (MOSS)
- Risk Management Approach
- Efforts to strengthen a culture of security

## 2.4 Accountability for Staff Security

One of the most difficult questions of Security Risk Management concerns defining the level of responsibility and accountability of a manager for the safety of her staff. This question is more complex than it may appear at first glance. For example, we might begin by proposing simply that “the manager is responsible for the safety of her staff.” This may be true, but we also know that when organizations work in insecure areas, it is possible that even with the best analysis, preparations and countermeasures, a security incident may still occur. Ultimately, the perpetrators of deadly acts are humans and therefore their actions can never be predicted with complete certainty; this is why, as we will see in Chapter 7, we say that risk is something that can be reduced but never eliminated entirely. Recognizing this, we might modify the definition to say something like, “a manager is responsible for taking adequate measures to ensure a reasonable level of risk for staff.” But what exactly are adequate measures? And what is reasonable risk? In short, how can a manager know when she has done enough?

One approach to answering this question is the concept of due diligence. Due diligence means that an adequate level of care as required for the situation has been taken. It is commonly cited in reports and investigations following serious security incidents. Consider the following short excerpts from the UN report on the Canal Hotel Bombing of 2003:

“... At the executive level in headquarters in New York, the Steering Group on Iraq (SGI), **lacked due care or diligence** in the manner in which it dealt with the circumstances of the return to Baghdad. It should have asked some searching questions about the security aspects of the proposed return plan...

**The standard of security management as regards the Canal Hotel was seriously deficient and lacking cohesion.** This deficiency was exacerbated by the inadequate support that the Field Security Coordinator received from senior security management in New York, and from the designated Official...

... In light of the above failures [*among others in the original document, but not listed here*], the Secretary General, having reviewed the Panel’s findings and conclusions, with the assistance of his senior advisors not directly involved in the issues considered by the Panel, has decided on the following action:

- a) Refer the matter of the Chief Administrative Officer of UNOCHI and the Building Manager of UNOCHI to the Office of Human Resources Management to initiate disciplinary proceedings against the two staff members, who are being charged with misconduct;



- b) Immediate reassignment of the Field Security Coordination Officer from UNSECOORD to an appropriate post not involving any functions related to security matters;
- c) Letter of Reprimand to the Security Management Team in Iraq;
- d) Request for the immediate resignation of the humanitarian Coordinator/Designated Official from his current ASG post in the United Nations and return to his D-2 post in WFP. His future assignments will not include any responsibilities for security matters;
- e) Request for the resignation of the UN Security Coordinator from the United Nations;
- f) A letter to each head of a UN Fund of Programme who had staff in Iraq during the period 1 May – 19 August 2003, critical of their management and lack of respect for staff ceilings and security clearances (applicable in Iraq);
- g) A letter addressed to the Deputy Secretary General, in her capacity as Chairperson of the SGI, expressing his disappointment and regret with regard to the failures identified by the Panel which are attributable to the SGI. This letter would be shared with all members of the Steering Group.”

– Statement attributable to the spokesman for the Secretary-General on the Report of the Security in Iraq Accountability Panel  
New York, March 2004



**Question**

*What is meant by due diligence, and does it exist as a concept for office managers in your own agency or organization in relation to security management?*

---

---

---

---

---

---

---

---

---

---

One definition of *due diligence* from the Canadian Centre for Occupational Health and Safety follows. Note that the same concept and terminology is widely used throughout the professional world; doctors, lawyers, architects and engineers regularly use the term *due diligence* as applied to their own fields. The general concept for each profession is the same; however, the specific activities that might be listed to indicate whether or not due diligence is met will naturally vary according to the common practice and norms of each professional field.

*“Due diligence is the level of judgment, care, prudence, determination, and activity that a person would reasonably be expected to do under particular circumstances. Applied to occupational health and safety, due diligence means that employers shall take all reasonable precautions, under the particular circumstances, to prevent injuries or accidents in the workplace. This duty applies to situations that are not addressed elsewhere in the occupational health and safety legislation.”*



*“To exercise due diligence, an employer must implement a plan to identify possible workplace hazards and carry out the appropriate corrective action to prevent accidents or injuries arising from these hazards. “Due diligence” is important as a legal defense for a person charged under occupational health and safety legislation. If charged, a defendant may be found not guilty if he can prove that due diligence was exercised. In other words, the defendant must be able to prove that all precautions, reasonable under the circumstances, were taken to protect the health and safety of workers.”*

### An example of a due diligence checklist

YES	NO	
<input type="checkbox"/>	<input type="checkbox"/>	Do you know and understand your safety and health responsibilities?
<input type="checkbox"/>	<input type="checkbox"/>	Do you have definite procedures in place to identify and control hazards?
<input type="checkbox"/>	<input type="checkbox"/>	Have you integrated safety into all aspects of your work?
<input type="checkbox"/>	<input type="checkbox"/>	Do you set objectives for safety and health just as you do for quality, production, and sales?
<input type="checkbox"/>	<input type="checkbox"/>	Have you committed appropriate resources to safety and health?
<input type="checkbox"/>	<input type="checkbox"/>	Have you explained safety and health responsibilities to all employees and made sure that they understand it?
<input type="checkbox"/>	<input type="checkbox"/>	Have employees been trained to work safely and use proper protective equipment?
<input type="checkbox"/>	<input type="checkbox"/>	Is there a hazard reporting procedure in place that encourages employees to report all unsafe conditions and unsafe practices to their supervisors?
<input type="checkbox"/>	<input type="checkbox"/>	Are managers, supervisors, and workers held accountable for safety and health just as they are held accountable for quality?
<input type="checkbox"/>	<input type="checkbox"/>	Is safety a factor when acquiring new equipment or changing a process?
<input type="checkbox"/>	<input type="checkbox"/>	Do you keep records of your program activities and improvements?
<input type="checkbox"/>	<input type="checkbox"/>	Do you keep records of the training each employee has received?
<input type="checkbox"/>	<input type="checkbox"/>	Do your records show that you take disciplinary action when an employee violates safety procedures?
<input type="checkbox"/>	<input type="checkbox"/>	Do you review your OSH program at least once a year and make improvements as needed?

*from: Canadian Centre for Occupational Health and Safety see <http://www.ccohs.ca/oshanswers/legisl/diligence.html>*



**Exercise**

**Design your own checklist**

Use the space below to draft a **Security Management Due Diligence Checklist** for your own office. Take care to consider the practicality of your list in terms of what can actually be achieved, as well as how clearly the checklist statements can be applied and measured objectively in the office. You should write this in pencil so that you can return to review and revise your checklist as more points are raised in the following chapters.

YES      NO

1)

---

2)

---

3)

---

4)

---

5)

---

6)

---

7)

---

8)

---

9)

---

10)

---

## Summary



### Key Points

Just as security threats are different in different places, the possible strategies for managing them also vary widely. Every organization has its own mandate and identity; it follows that each may have different security needs and different responses.

---

**The ICRC approach to security** places a very high importance on identify and acceptance in the community, and further relies on both a high level of pre-deployment training and a firm enforcement of compliance with its security measures and protocols. The “seven pillars of security” model identifies the key elements of the strategy. The seven pillars are:

- Acceptance
- Identification
- Information
- Rules and regulations
- Behavior (personality)
- Telecommunications
- Passive and active protective measures

---

**The NGO approach to security** is more difficult to define as NGOs vary widely from one to another. Some general points common to many NGO approaches to security are:

- Emphasis on acceptance strategies.
- Integrated and decentralized decision-making on security issues.
- Increasing reliance on technical security expertise.
- Attention being given to the importance of partnerships for improved security, for some NGOs.
- Use of the *security triangle* approach and its three elements:
  - Acceptance
  - Protection
  - Deterrence

---

**The UN approach to security** has been formalized through several key bodies and policies, including:

- The UN Department of Safety and Security (DSS) and the Inter-Agency Security Management Network.



- The UNDSS's 10 priority areas of focus for improving staff safety and security were identified in 2005 as:
  - 1) Information
  - 2) Host nation support
  - 3) Enabling operations
  - 4) Globalizing operations
  - 5) Strengthening inter-agency relationships
  - 6) Decentralization of security management
  - 7) Modernization
  - 8) Accelerate crisis management system
  - 9) Advance training strategy
  - 10) Communications
- Attempts to strengthen accountability.
- Elaboration of Minimum Operational Security Standards (MOSS).
- Adoption of the Risk Management Approach.
- Efforts to strengthen a culture of security. UNHCR, in particular, has made an organization-wide push to make staff security a core aspect of everyday operations.

---

**Due diligence** is the level of judgment, care, prudence, determination, and activity that a person would reasonably be expected to take under particular circumstances. The concept of due diligence is common in the professional field, and can be practically applied to security risk management for humanitarian agencies.

---



## Chapter 2

### Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

1. Security management response strategies ultimately rely on only one useful action—protection or “hardening” of field staff, vehicles, and offices.
2. The security triangle is defined as the high-risk road travel between, and time spent at three common points: insecure office spaces, hotels and guest houses, and highly vulnerable personal and social activities (e.g., public restaurants).
3. ICRC does not pursue staff security as a core element of its work since it is understood that all ICRC activities will face high risk.
4. UNHCR’s culture of security includes the idea that all staff should understand the risk of the environments in which they are working and be able to apply risk management principles to their work and daily activities.
5. Due diligence, in general, means the required level of care that a reasonable person should take given a particular set of circumstances.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

6. Which of the following are pillars in the ICRC seven pillars of security?
- A Access
  - B Protection
  - C Telecommunications
  - D Behavior
7. As described in the security triangle model, which of the following would be considered to be **protection** measures?
- A Building higher walls around the office compound.
  - B Coordination of several organization’s security and communications protocols concerning convoy movement.
  - C Armed police guards outside the main gates of the office.
  - D A public awareness campaign about the good work the organization is doing in the community.



**Chapter 2**

**Self-Assessment Questions** *(continued)*

8. Who is officially the primary responsible party for the security of UN staff working in a high-risk area?
- A UN DSS
  - B UNHCR
  - C The UN System
  - D The Host Government
9. Which of the following are goals of UNHCR's culture of security initiative?
- A Everyone in the organization is a security expert.
  - B Everyone in the organization understands and can use a commonly shared security risk management approach.
  - C Field offices have enough funds to be able to meet security needs that are based on local assessment.
  - D Security considerations are integrated into the assessment and design process so that staff can carry out their mandated work in potentially hazardous environments without exposing staff members to an unacceptable, unnecessary or unforeseen level of risk.
10. The full title of the UN Designated Official (DO) is the UN Designated Official for what?
- A Safety
  - B Security
  - C Staff
  - D Systems



**Chapter 2  
Answer  
Key**

- |            |      |
|------------|------|
| 10. B      | 5. T |
| 9. B, C, D | 4. T |
| 8. D       | 3. F |
| 7. A, B    | 2. F |
| 6. B, C, D | 1. F |

## Overview of Security Risk Assessment

*A group of newly arrived Somali refugees waits at the gate of the UNHCR compound to be admitted to Dadaab refugee camp, Kenya, October 2008.*



Will the peaceful early morning crowd outside the Dadaab office still be there later in the day? Could it grow to become an angry and unruly mob? How can the possibility of this threat be predicted or assessed? What might be done to prevent this from occurring? Or, if it does happen, what steps should be taken to manage the situation and reduce the risk of harm to staff?

Security Risk Assessment is a practical tool aimed at helping managers answer questions like these. It is a systematic approach to organizing and analyzing a complicated array of information in order to better understand the risks being faced and the response measures needed. It does not seek to eliminate subjectivity nor does it purport to offer guaranteed “right and wrong” answers. However, by taking an orderly and comprehensive approach it can lead to more thoughtful and effective decision making. It is a critical step in the Security Risk Management process.



### Learning Objectives

This chapter presents an outline of the Security Risk Assessment process. Each step in the process will be explained in greater detail in subsequent chapters, but this chapter will help you get an overview of the process and see the relationship of the steps to one another. In particular, this chapter will explain the meaning and relationships among the following activities:

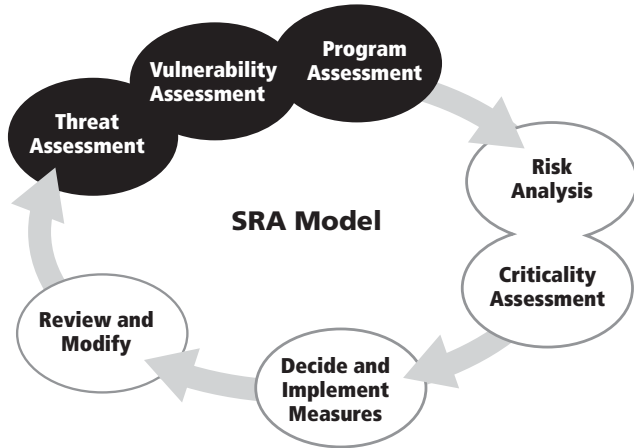
- Threat assessment
- Vulnerability assessment
- Program assessment
- Risk analysis
- Criticality assessment
- Decision and implementation of risk reduction measures
- Review and modification of assessment



### 3.1 Threat Assessment

As in any kind of ongoing process, you have to start someplace. The SRA process is iterative, which means that once you have taken the steps outlined in the process, you will need to start the cycle again since some of the steps you have taken have likely changed your security risk situation. To understand your new situation, you begin again. For this training course we will begin with the step of **threat assessment** as a starting point.

Threats are defined as potential dangers in your working environment. They are normally expressed as specific events such as robbery, kidnapping or harassment, for example. It can be useful at this point to subdivide threats to your staff into different types, in order to gain a more comprehensive overall picture, and to help organize your thinking about how to respond to or prepare for each type. There are four basic types of threat to consider:



- 1 – **Direct threats** which specifically target you, your staff, or office.
- 2 – **Indirect threats** which do not specifically target you, but can still harm you simply for being “in the wrong place at the wrong time” or “caught in the crossfire.”
- 3 – **Criminality and banditry** which typically targets your money or possessions, but which may result in other harm to you beyond the loss of your property.
- 4 – **Miscellaneous threats** include everything else, for example, illnesses, natural disasters, vehicle accidents and stress.



**Exercise**

Using an example of an insecure field situation that you are familiar with, categorize the threats you can imagine using the table below. Try to think of at least one threat that belongs in each category.

Your country or location	Direct Threats	Indirect Threats	Criminality and Banditry	Miscellaneous Threats
Threat example				
Threat example				
Threat example				
Threat example				
Threat example				



Threat assessment can be described as the assessment you make looking out at the field environment from inside your organization. The situation implied is that of an agency or organization that has entered an environment in which there are pre-existing threats. The table shown below provides a variety of threats categorized by their type. It is only an example and does not mean that these particular threats are those that you may encounter in your country or work assignment. Each area's threats will be different, but considering them and recording them in a similar way will give your organization the useful benefit of being able to compare threats in different offices or areas of operation in a meaningful way.



Answer

	EXAMPLE				
	<b>Insecure location</b>	Direct Threats	Indirect Threats	Criminality and Banditry	Miscellaneous Threats
Threat example	<b>Small arms attack on office</b>	<b>Armed conflict in the operating area "getting caught in the crossfire"</b>	<b>Carjacking</b>	<b>Traffic/vehicle accident</b>	
Threat example	<b>Roadside bomb blast (IED) against office vehicle</b>	<b>Landmine strike on antipersonnel mine by field monitor</b>	<b>Robbery</b>	<b>Illness/disease</b> (List specifics)	
Threat example	<b>Rape of staff member</b>	<b>General aerial bombing/shelling of program area</b>	<b>Pickpocketing and petty theft</b>	<b>Natural disasters</b> (List specifics)	

While doing this kind of threat assessment is a cornerstone of SRA, and may yield useful information very quickly, it is important to remember that your very presence in the environment may also change the nature of the threat. This dynamic is further discussed under program assessment below. A fuller description of threat assessment along with some of the techniques and tools used for carrying it out are provided in *Chapter 4 – Threat Assessment*.

## 3.2 Vulnerability Assessment

Vulnerability assessment looks inward at an organization's own weaknesses and how these can affect the security of its staff, premises, and equipment. It is an assessment of factors that are specific to the organization and its operations rather than the environment. Some specific vulnerability factors for humanitarian organizations include the following:

**Location** – An organization working in an area with significant threats and many security incidents will face higher risk. Similarly, working in a remote area where medical facilities and transportation systems are inadequate may make the impact of certain threats greater as timely measures to stabilize the situation after the incident cannot be assured. This too has the effect of increasing overall risk.

**Exposure of staff and property** – Organizations working in the same general location may face different levels of risk due to increased opportunities for contact with potential threats, e.g., due to higher staff numbers or frequent field missions to more dangerous locations.

**Value of property** – Organizations with more valuable property may be more likely to be selected as targets.

**Impact of programs** – Organizations whose programs have an impact on different groups or are seen to benefit one of the parties to a conflict may be more vulnerable than others.



**Security measures** – Organizations that adopt appropriate measures are usually less vulnerable than those that do not.

**Compliance** – Even if an organization adopts appropriate security measures, vulnerability is still dependent upon the staff’s consistent compliance with them.

**Staff interpersonal skills** – Poor personal behavior and communication skills can affect your vulnerability by increasing the chance of personal interactions turning into conflict or even developing into security incidents. Good interpersonal skills help staff members to avoid incidents and mitigate the impact if they occur.

**Image** – Vulnerability can also be dependent on the image of your organization. For example, a field office of an organization that has an image of wealth, and little tolerance for community conflict, may be a more likely target for theft than other offices.

These vulnerability factors and some of the methods used to evaluate them are described in more detail in *Chapter 5 – Vulnerability Assessment*.

### 3.3 Program Assessment

Program assessment is the third type of assessment considered in SRA. It includes consideration of how your program activities influence your vulnerability and how your activities influence the threats toward you. Program activities may decrease the likelihood of a threat, for example by providing greater stability, prosperity or self-sufficiency to a crime-prone community; however, they may also increase threats, for example, when they are perceived to support some beneficiaries preferentially over others or when they introduce controversial changes to local customs or traditions. Program activities that require staff to travel long distances in insecure areas for monitoring purposes will tend to increase vulnerability through greater exposure of the vehicles and staff to local threats.

It is useful to consider the effects of your program activities in the short, medium and long-term as well. For example, programs aimed at promoting long-term stability may have short-term effects that cause immediate increase in tensions.



**Question**

*From your own experience, can you think of an example where the programs you were undertaking had an effect on your security, for better or worse?*

---

---

---

---

---

---

---

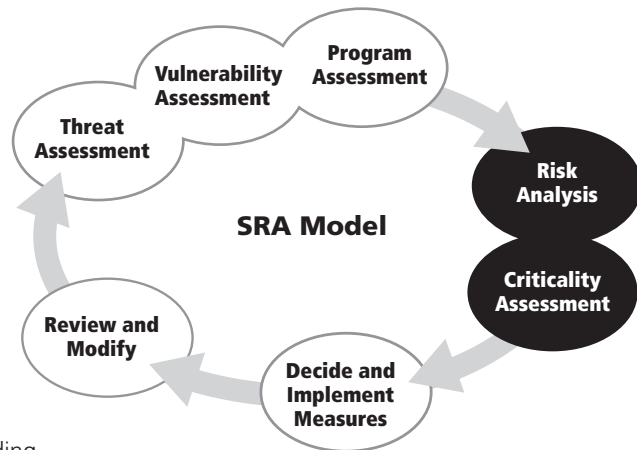
---

Ways that programs can affect risk, and how to analyze the relationship, are the subject of *Chapter 6 – Program Assessment*.



### 3.4 Risk Analysis

Threats are generally considered to be part of the overall security environment. A list of possible threats might be considered to be the same for all organizations operating in that environment. Vulnerability, on the other hand, will differ for each organization, and can be influenced directly from within each organization. Considered together, external threat and internal vulnerability can provide the basis for understanding an organization's overall risk.



A theoretical formula for thinking about risk is:

$$\text{Threat} \times \text{Vulnerability} = \text{Risk}$$

This simple equation means that risk is based both on the actual threats you face as well as your vulnerability to those threats. Consider the threat of being hit by a thrown stone while driving down a rural road. If the road is on an uninhabited island, and there is no one to throw rocks at you, the threat is zero, and even if your vulnerability is high (for example you drive very slowly, with the windows open, radio going, while laughing and joking about the poor skills of the local marksmen) you still have no risk of being hit. On the other hand, imagine that there is indeed a troublemaker waiting in ambush with a rock, but this time you have decided to drive in a fully armored military tank. In this case your risk is still zero, because even if the rock is thrown it cannot hurt you in your well protected vehicle. In other words, your vulnerability is now zero, so again your risk is zero.

Once the local threats and your vulnerability to them have been identified, the next step in the threat assessment process is to evaluate both their **impact** and **likelihood**.

**Impact** is the measure or estimate of how much damage you will suffer if the potential threat were actually to occur.

**Likelihood** is the measure or estimate of how probable it is that the event will happen.

Once an assessment has been made regarding the impact and likelihood of the threats you face, these two factors can be graphed together to gain a useful understanding of the threats that will then allow you to prioritize the actions you can take to reduce your risk arising from these threats. This process and the tools for plotting and analyzing risk using impact and likelihood are described in greater detail in *Chapter 7 – Risk Assessment and the Risk Matrix*.

### 3.5 Criticality Assessment

Program criticality assessment considers the importance or urgency of the programmed activity, and weighs the benefits (usually to the beneficiaries of the programs) against the risks (usually to you or your staff). It can be thought of as a kind of cost-benefit analysis. The process starts with looking at the situation faced by the beneficiaries and the consequences for them of implementing

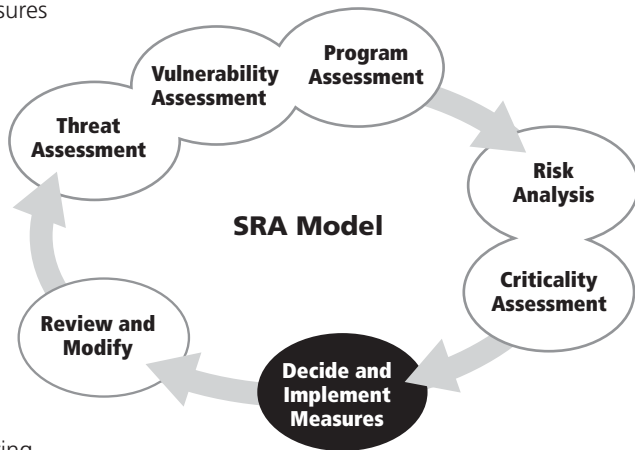


or canceling the planned programs. Is the program urgent and life-saving, or simply desirable? This assessment is then weighed against the risk to staff, as assessed previously through threat and vulnerability analyses.

Criticality assessment can yield three possible outcomes. The first possibility is that the benefits clearly outweigh the risks; in which case implementing the program falls in the category of reasonable risk. The second possibility is that the risks clearly outweigh the benefits; in which case the activity entails unacceptable risk. The third possibility is that the risk can be made acceptable, but only with additional mitigating measures. In this case the manager must select and implement appropriate measures designed to eliminate unnecessary and unacceptable risk.

### 3.6 Decide and Implement Measures

Most responses to threats may be thought of as either **prevention** or **mitigation** measures (or both). Preventive measures are aimed at reducing the likelihood that an event will occur; for example, by declaring an area off limits or seeking to raise image and acceptance among a sensitive population. Mitigating measures seek to reduce the impact of the event; for example, equipping a vehicle with anti-mine ballistic blankets, first aid kits and proper communications equipment probably will not decrease the probability of encountering a mine, but they may lessen its effects. Some measures can both prevent and mitigate; training is an example.



**Question**

*What kinds of measures might you take to reduce your risks from the threats that you listed in the threat assessment chart earlier in this chapter?*

---



---



---



---



---



---



---



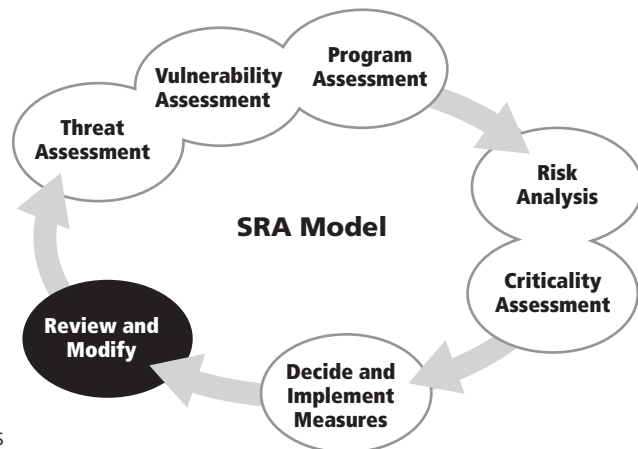
Different security response measures can be grouped into several generic categories. It is important to remember that a well-conceived response to security threats will normally require a mix of the alternatives below. In certain cases however, specific choices may be mutually exclusive, as is sometimes the case with specific protection and acceptance measures. In such cases, managers must balance the advantages and disadvantages of each possible measure in the context of their specific situation and the operation as a whole.

- **Planning** for security protocols and responses in readiness for response to potential threats.
- **Coordination**, both internally among staff and organizational units, and externally with other organizations.
- **Hardening** measures such as walls and strong gates and doors.
- **Deterrence** measures such as guards and police.
- **Image- and acceptance**-improving measures such as public outreach campaigns and immediate organizational recognition measures like flags and large decals for buildings and vehicles.
- **Communications** equipment and readiness for use by all staff members.
- **Vehicles**, their drivers and the associated equipment and procedures for using them.
- **Risk transference** strategies, such as insurance policies and hiring others to undertake dangerous tasks.
- **Staff knowledge and skills** that guide them in avoiding unnecessary risks and prepare them for emergency response if need be.
- **Reducing exposure** by reducing staff in the field, the amount of time that they are in harm's way, or the areas in which they work and travel.

The criticality assessment process, and the range of preventive and mitigating measures available to a manager, are discussed in *Chapter 8 – Risk Reduction Measures*.

### 3.7 Review and Modify

Security Risk Assessments must be reviewed and updated on an ongoing basis. This is in part because the threats (and humanitarian programs) change and evolve constantly. It is equally necessary because the actions and decisions that you make as a part of the SRA process will, in themselves, have an impact on the threat environment. They may decrease your vulnerability to a threat and reduce its likelihood or impact, but they also expose you to new, unforeseen or previously negligible risks. For these reasons, the process of reviewing effects of decisions, updating analyses and making modifications as needed, are integral parts of the overall SRA process. It should be noted that this process can require considerable effort and time; office managers must ensure that adequate attention is given to this task so that security assessments do not simply gather dust on the shelf as the security situation evolves.



## Summary



### Key Points

**Security Risk Assessment** is a systematic approach to analyzing information in order to better understand risks and make better decisions regarding how to respond to them. A complete assessment of risk for humanitarian field workers should include all of the steps listed below.

---

**Threat assessment** provides an understanding of the potential dangers in your environment. Threats in this assessment are usually presented as events such as kidnapping, road ambush, sniper shooting, etc.

---

**Vulnerability assessment** is an internal analysis of an organization's own weaknesses. Typical aspects of an organization or office's vulnerability include:

Location • Exposure • Value of property • Program impact  
Security measures • Compliance • Staff interpersonal skills • Image

---

**Program assessment** is related to threat and vulnerability assessment but looks specifically at the results of the activities or programs of the organization in the field and the ways that these programs influence the risk to staff, either positively or negatively.

---

**Risk analysis** combines the results of threat analysis and vulnerability analysis and then examines the threats in terms of both their likelihood and possible impact to determine the actual risk for the organization.

---

**Criticality assessment** weighs risks of carrying out program activities to staff against possible benefits of program activities to the beneficiaries of the programs.

---

**Decision and implementation** entails selecting appropriate measures to reduce risk. These may be preventive measures, aimed at reducing the likelihood of a harmful event occurring, or mitigating measures, designed to lower the impact of the event if it happens.

---

**Review and modification** of assessment is necessary because security situations are fluid and constantly changing. Moreover, your actions may change the environment you face; therefore, you will need to review and revise your SRA continually as long as your staff are in the field.



### Chapter 3 Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

1. The term *threat* as used in the SRA process simply means the bad or harmful things that can happen to staff in the field, and are generally expressed as events.
2. The term *impact* in determining risk relates to how damaging a threat will be if it happens.
3. The term *likelihood* in risk analysis relates to the probability that a predicted threat will actually happen.
4. The term *vulnerability* in SRA relates to an organization's internal weakness or the opportunities it presents to be harmed by threats.
5. The term *exposure* as a factor of vulnerability means the organization's ability and experience in doing the kinds of programs they undertake.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

6. Which of the following is a logical expression of risk?
- A** threat x risk = vulnerability
- B** threat x vulnerability = risk
- C** impact x vulnerability = likelihood
- D** threat x likelihood = vulnerability
7. Which of the following shows elements of the SRA cycle in correct sequence?
- A** threat assessment, risk analysis, criticality assessment, decide and implement measures
- B** threat assessment, criticality assessment, vulnerability assessment, risk analysis
- C** threat assessment, risk analysis, vulnerability assessment, criticality assessment
- D** vulnerability assessment, risk analysis, threat assessment, criticality assessment



8. Which of the following are elements or factors that influence an organization's vulnerability in the field?
- A** Value of property and equipment.
  - B** Security measures in place.
  - C** Compliance with those security measures and protocols.
  - D** Staff interpersonal and communication skills.
9. Reasons for reviewing and modifying an organization's SRA include which of the following?
- A** Threats sometimes change over time.
  - B** Taking measures to improve staff security may change the risks.
  - C** Successive reviews of the SRA cycle will take very little effort or time so should be done often since the effort required is minimal.
  - D** Usually real improvements in security only occur after several reviews or cycles of the SRA methodology.
10. Which of the following statements are correct regarding mitigation and prevention activities?
- A** Mitigation activities reduce the likelihood that a threat event will occur.
  - B** Prevention activities reduce the likelihood that a threat event will occur.
  - C** Mitigation activities reduce the impact or damage of a threat event if it occurs.
  - D** Prevention activities reduce the impact or damage of a threat event if it occurs.



**Chapter 3  
Answer  
Key**

- |    |   |     |            |
|----|---|-----|------------|
| 5. | F | 10. | B, C       |
| 4. | T | 9.  | A, B       |
| 3. | T | 8.  | A, B, C, D |
| 2. | T | 7.  | A          |
| 1. | T | 6.  | B          |

# Chapter 4

## Threat Assessment

NATO  
Secretary  
General,  
Jaap de Hoop  
Scheffer,  
talking to  
Kosovar police  
officers on the  
Austerlitz Bridge  
in Mitrovica,  
May 2005.



***“... the UN security system failed to adequately analyze and utilize information made available to the system on threats against UN staff and premises.”***

– From the *Ahtissari Report* of the Independent Panel on Safety and Security of UN Personnel in Iraq, 20 October 2003, following the bombing of the UN Headquarters Compound at the Canal Hotel in Baghdad on 19 August 2003.

***“... we haven’t paid enough attention, at the individual level and at the collective level, to the warnings that have been issued by ourselves and by others concerning the changing environment of security that is there.”***

– From the report of investigation, *Toward a Culture of Security and Accountability*, after the bombing of UN Building in Algiers, 11 December 2007.

In the investigative reports that follow major security incidents, the finding of failure of assessment is a common theme. Information that was available was not gathered; facts that were known were not properly analyzed; and what was analyzed was not acted upon. How can managers ensure that they obtain needed information about threats in their environment and evaluate its validity? How can they avoid discovering that a security incident was imminent only after it has happened?



### Learning Objectives

Threat assessment is a process of gathering and analyzing information to gain a clear picture of the dangers in your environment. This chapter will present some of the basic techniques for collecting and assessing information in a systematic way, including:

- Historical analysis
- Pattern analysis
- Change analysis



**Threat assessment is a forward-looking process** that is undertaken to make long- and short-term predictions about the types and levels of threat in the working environment. While its purpose is to predict ongoing or future threats, it also looks *backwards at what has already happened* in recent and longer-term history. By looking at news reports, various patterns, and rate at which they occur, we can make useful, if imperfect, predictions about threats that face us each day.

**Security threats** are the potential dangers to you, your staff, and equipment in your working environment. As you learned in Chapter 3, they are normally expressed as events such as robbery, kidnapping or harassment. Conceptually, threats can be divided into four basic categories:

- **Direct threats** – you or your staff are the intended target.
- **Indirect threats** – you or your staff are not the target but could be endangered by being “in the wrong place at the wrong time” or “caught in the crossfire”.
- **Criminality and banditry** – your money or possessions are the target.
- **Other miscellaneous threats** – illnesses, natural disasters, vehicle accidents and stress.

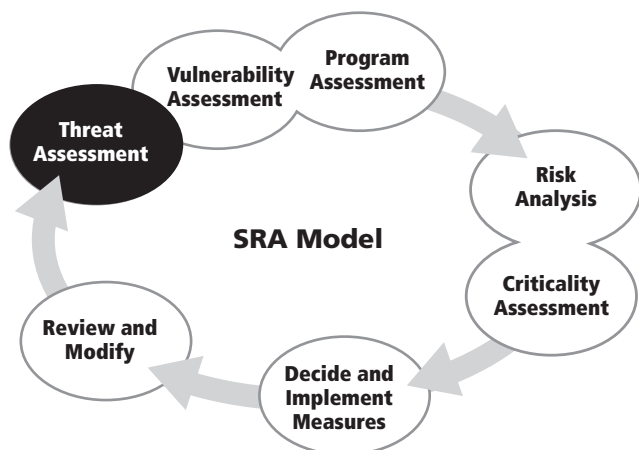
In conducting threat assessment it is useful to consider each type of threat that your organization may face in the field. For example, threats arising from natural disasters such as floods, earthquakes, storms, and tsunami, strike everyone and everything in their path without regard to nationality, ethnic group or political affiliation. For this class of threat, assessment can be done simply by looking at the history of the place and the patterns of occurrence of the threat. Cyclones tend to come at the same season each year, and intensity or severity can easily be mapped and presented as “scientific” data.

For example, in some areas, severe cyclones may occur approximately once every 5 years. Even though that information is correct and very useful as part of your threat analysis, it still will not tell whether or not you will face such a storm *this year*. Similarly, indirect threats of violence from ongoing warfare, insurrection, or terrorism in the community are also assessed by noting the numbers of events, and any patterns or trends in the data, in order to project what may happen in the future. Crime, banditry and other threats are assessed in the same general way; over time certain areas are known as “high crime areas” and others are regarded as safe.

Of course, how you behave in the field and what security measures you and your organization take can change the likelihood that an actual incident will happen to you, or possibly reduce the harm to you if it does happen. These important decision-making and risk-reduction measures will be discussed in more detail in coming chapters. The focus of this chapter is limited to threat assessment, as a logical foundation on which to build a reasonable risk-management approach.

## 4.1 Approaches to Threat Assessment

While it can be difficult to separate threat assessment distinctly from vulnerability assessment and program assessment due to the considerable overlap between these activities, it is still useful to try to distinguish the difference between them. We will, therefore, devote a chapter to developing the full details of each of these activities in this course.





The process of identifying and evaluating threats requires information about what is happening and what has happened, and a forward-looking analysis of what this information means for the future. Three useful analytical techniques are historical analysis, pattern analysis and change analysis. We will discuss each one in turn below.

## 4.2 Historical Analysis

Historical analysis consists of collecting information on past security trends and events over the longer term. It stands to reason that if something has happened before, it may happen again. If it has happened often, it will probably continue to happen often. The two basic ways of collecting this kind of information are through reading security reports and other information sources, and from targeted interviews with people who know the history of such events.

In general, the goal should be to develop as many information sources as possible. Different people have access to different sources of information. Equally, information sources each have their own special insights as well as their own individual biases. Varying your sources will allow you to hear about threats and threat levels from different perspectives, hopefully enabling you to reach a consensus, but at least exposing the divergences. This can be critical in helping you gain a more realistic picture of the threat environment.

Although each situation is different, and there may be unique information sources in some specific cases, the following are typical sources of security information in the field:

- Staff (especially local staff)
- Partner agencies and NGOs
- Law enforcement agencies (police, military, gendarmerie, border police, other)
- Other government interlocutors
- Other community leaders
- Local and international media
- Embassies/diplomatic community (including website advisories)
- Beneficiaries of your programs

### *Assessing the validity of information*

Consider the example of collecting crime reports from a local police station. It is a straightforward exercise to ask for a list of the reported crimes in a certain town for the last six months as part of your historical analysis, and it may appear that information collected is accurate, since it is from “those who should know”. There may be several ways, however, that various pressures, or perceptions on the part of the perpetrators, the victims, and even the local police interfere with your ability to draw a complete and true conclusion from the recorded crime reports.



#### **Question**

*What issues or pressures might influence the quality of local police crime report records?*

---



---



---



---



---



There are many reasons why security threat information of this type may be incorrect. Knowing the ways that information may be biased, limited, or simply incomplete may not help you in improving the recorded information, but at least your knowledge will help you to understand that there may be more to the story than meets the eye. Crime reports collected by local police may be:

- Under-recorded if the police force is understaffed, overworked, or simply poorly trained; some incidents simply go unreported, making the recorded situation look safer than it actually was.
- Under-reported when victims are afraid or unwilling to report to the local police. This can happen for many different reasons such as:
  - The police themselves can sometimes pose a threat to the local community, and many people do not want to interact with them, even to report a crime.
  - Some types of crime, such as rape, may be felt to be too shameful to report by the victim.
  - Criminals may threaten victims not to report under threat of further violence or even death.
- Over-reported for some types of victims, such as foreigners who may have a high expectation of what services are offered by the local police.
- Under-reported by illegal aliens, displaced persons from other districts, or refugees who may be afraid to go to the police.
- Under-reported if government pressure is brought to bear on the police to show an improving security situation.

Much of threat assessment is based on talking to partners, co-workers, other staff, drivers, community leaders, and those being supported by your programs such as disaster victims, refugees, and other displaced people. Are the sources credible? Is there any truth to second- or third-hand rumors circulating in the border camp? It is important that you have some way to validate the information you receive from such interviews.

### Information accuracy checklist

Remember that the usefulness of your threat assessment will ultimately be based on how current, and how correct, your information is. Consider your sources, and your own perspectives or biases when you are collecting information on which to base your analysis. The checklist below provides a basic, but useful, starting point for understanding the accuracy or bias of information you receive.



Tools

#### Information Accuracy Checklist

	YES	SOMEWHAT	NO
<b>Key questions about the person(s) providing the information</b>			
– Does he/she have direct access to the information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– Has information he/she has reported in the past been reliable?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Questions on the information</b>			
– It makes sense given what you know about the broader situation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– You have other information consistent with it.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– You have no information that contradicts it.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Questions on the person providing the information</b>			
– Probably believes that you could (and would) verify the information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– Relies upon you for employment.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– Will <i>not</i> benefit from your reaction to the information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– Expects to have a continuing relationship with you.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
– You have known him/her for some time.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

From: Threat Assessment Training Module for NGOs Operating in Conflict Zones and High-Crime Areas. Produced for the OFDA/InterAction PVO Security Task Force by Jonathan T. Dworken



### 4.3 Pattern Analysis

Pattern analysis involves reviewing past threat events to identify meaningful patterns or trends in the data.



#### Question

*What types of patterns can you think of that might be useful in predicting threats for your security threat analysis?*

---



---



---



---



---

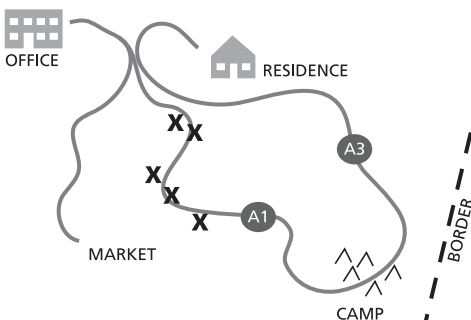
Generally, important patterns may be discerned by looking at several different dimensions or aspects of past or ongoing threats. These include the *location* of event (threat mapping), *time* of occurrence (of day, week, month or year), and the *type of target or victim*.

**Location of event** – Consider *Example 1* below. Each X on the map represents a security incident, such as an armed attack or attempted attack recorded over the past year. What conclusion could be reached from the data shown? Given that five attacks have occurred along Highway A1 and none has occurred on Highway A3, a manager might decide that Highway A3 is safer and staff should use it for movement between the office and the camp.

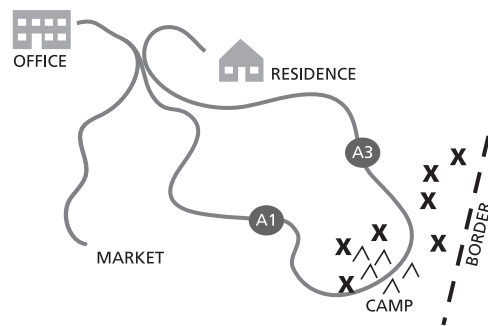
Another common pattern for UNHCR and other organizations working with refugee camps in dangerous border areas is shown in *Example 2* below.

What conclusion could be reached from the data shown now? One possibility is that the camp is located too close to the border; humanitarian staff might urge government authorities to move the camp further into the interior of the country to ensure safety.

#### Threat pattern analysis by mapping



*Example 1 – Location of Security Incidents*



*Example 2 – Location of Security Incidents*



**Question**

*What further patterns might be useful in analyzing the threats over the past year in the examples above?*

---

---

---

---

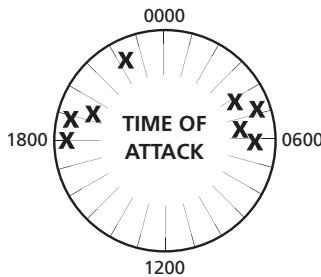
---

**Time of occurrence** – One useful aspect to look for the presence of a pattern is the time of day at which attacks have occurred. The 24-hour clock shown below is a good way to graphically display the information to reveal any pattern that may exist among the many attacks over the past year. The diagram is made by researching and then recording the time of day that road attacks have occurred. The result shown in the example is that generally attacks occur early in the morning, and late in the day (dawn and dusk). The pattern is very useful for security risk management as it implies that vehicles may still use this road with a reasonable risk, but perhaps not at dawn or dusk, and travel curfews and protocols should be put in place limiting travel at those higher risk times.

**Threat pattern analysis by time of day**

Attacks on vehicles over the past year are analyzed by their time of day and shown on a 24-hour clock.

*What are the most dangerous times of day in this example?*



*Example – Road ambushes on Highway 1A, by time of day*

Note that analyzing time of occurrence for patterns should also include longer time periods than 24 hours. Do the events occur on specific days of the week or month? Is there a pattern of threat events increasing on holidays, weekly religious days for prayer, just before paydays (people short of money have more motive for theft) or after paydays (people with money to burn may go out and cause trouble)? Is the event influenced by the seasons (as many kinds of military operations are)? Plainly, for these larger time frames, calendars rather than clocks are used to show recurrent patterns.

**Type of target** – Pattern analysis by target requires analyzing the available data with the specific focus on determining who was targeted. For example, consider the data in the pie chart below, which depicts the number of hostage-taking incidents among UN national and international staff between the years 1993 and 2004.

Does this information indicate a pattern? Before you answer, an additional detail may be useful: international staff constituted only 20% of the UN staff population globally at the time of the study. Based on this ratio, we might expect that of 278 hostage incidents, international staff should be involved in about 55. The fact that nearly four times as many were kidnapped probably indicates a global pattern, perhaps because international staff members are

**Threat pattern analysis by target**

Consider percentage of attacks against national versus international staff.

Total = 278



*Source: UNSECOORD (UNDSS)*

*Example – UN staff hostage incidents 1993 to 2004*



deemed useful as hostages as they generate more media coverage or ransom. There are at least three other points, however, that should be noted in this example:

- 1) Hostage statistics vary greatly from country to country, and patterns in a given duty station may or may not mirror the global trend.
- 2) While international staff are taken hostage more often, national staff members figure more often in statistics of deadly attacks.
- 3) Recent years have seen an increase in the number of UN national staff taken hostage—perhaps in response to increased measures protecting international staff.

The key point is that people may be at greater or lesser risk of being selected as a target due to a number of demographic factors: nationality, ethnic group (or appearance of belonging to a particular nationality or group), profession, employer and of course gender. Careful consideration of target selection patterns is an important part of pattern analysis.

### *Identifying patterns and trends*

Whatever patterns you choose to investigate, you will still need to gather the basic information first. An understanding of some of the possible patterns described above will be helpful in formulating questions or for asking for specific details that may be useful in your analysis. The tips below will help you to organize yourself for the assessment and give you some useful advice on how to start.



#### Tools

#### Pattern Analysis Tips

- Compile data on past incidents** — date, time, location, type, situation, and likely cause. As with interviews, NGOs are often a good source of data. For criminal threats, data from other expatriate organizations (especially UN agencies) may also be helpful.
- Display the data in a way that makes it easy to analyze**, such as a simple list.
- If it is difficult to identify patterns or trends with a list. **Use an uncluttered map and color-coded pins, stickers, or markers** (over plastic acetate). To identify patterns, mark all of one incident type first, look for patterns, and then add another type. To identify trends, mark incidents in order of occurrence (identifying how the map changes over time) or divide the time frame in half, and do two maps.
- To analyze the information, try to **identify clusters of incidents of similar types**; for example, car-jacking on a specific road.
- If you are concerned about indirect threats (being caught in the crossfire) because the conflict has no clear battle lines, **identify patterns and trends related to the conflict** that may indicate dangerous areas (e.g., skirmishes, ambushes, and massacres).

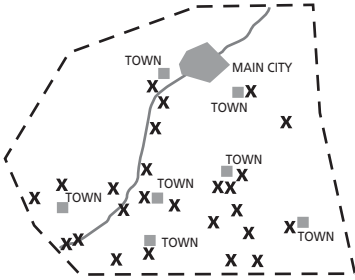
## 4.4 Change Analysis

Change analysis considers factors that could cause the threat environment to become different from the way it is now. In particular, it focuses on things that might make existing threats more frequent, damaging, more likely to target you directly; or that might cause entirely new threats to emerge. Change analysis involves both historical analysis (because it is necessary to look at what has happened in the past), and pattern analysis (because it is searching for trends), but unlike those two, it also involves actively projecting possibilities that have not yet occurred. In doing this, it addresses

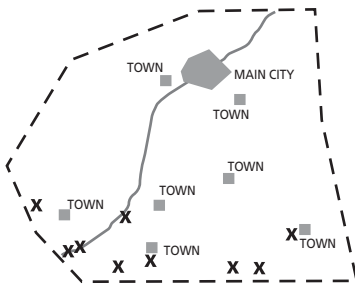


### Threat pattern analysis by location

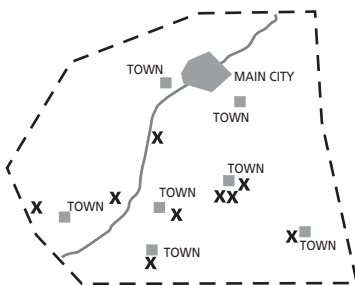
Attacks over the past 3 years



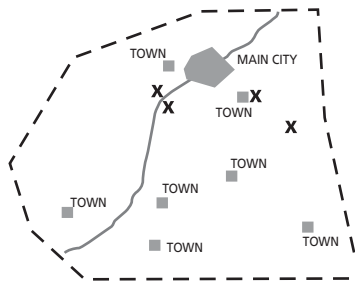
Attacks 3 years ago



Attacks 2 years ago



Attacks last year



a critical limitation of both history and pattern analysis: in both these forms of analysis, data can only be analyzed *once the event has occurred*. If this were the full extent of our analysis, we might be condemned to discover new threats only after we have become the victim of them for the first time. Security managers need a way to actively predict from known information how the threat environment is changing, and when something completely new may be likely or even imminent. Change analysis is the answer.

Consider the first example of change analysis in the small conflict-affected country at left. The capital is called Main City; dashed lines represent the national borders.

**Data:** While there have been about 15 violent incidents of attacks from rebel forces in the south of the country in the past three years, there has never been a bombing of buildings or vehicles within the capital, Main City.

**Conclusion:** Based on this, a humanitarian agency operating in Main City concludes that it is safe as long as staff remain within the city limits.

Do you agree with this agency's finding? Based on the data provided, they have assumed that Main City is safe. Why? *Because an incident has never happened there before.*

Now, the same data presented in a slightly different way.

**Data:** Three years ago several incidents occurred 200 km south of Main City. Two years ago several incidents occurred within 100 km of the city, mainly in the south of the country. Last year, several bombing events occurred in the suburban areas just south of Main City, and in some nearby towns just outside of the city limits.

**Conclusion:** The implication of this presentation of the same data should give you reasonable cause for concern. We can now see a clear trend toward attacks moving further northward across the country over the last three years. Looking at the data as presented, it is not difficult to imagine that something new may be heading our way—that the map for "This Year" may include attacks in Main City itself. Different ways of presenting the data convey very different messages. When looked at from the perspective of what is changing, or may change, those responsible for security in Main City will certainly want to take measures to prepare for threats, even though they have never occurred in Main City before.

One place where change analysis can be particularly useful is in helping humanitarian agencies assess the possibility of new patterns of attack that might directly target them. In many conflict areas around the world, humanitarian agencies work in close proximity to groups conducting hostile acts. The prevailing analysis is often: "Armed groups are fighting each other but fortunately they are not targeting us." The impact



of such an attack aimed at your staff would of course be critical—it would probably be deadly—but its likelihood may be assessed by those in the organization as very low. Why? *Because it has never happened before.* If this were your situation, would you be content with the assumption that you will never become a target?

After seeing the example of change analysis from the country above, you should be skeptical. But what do you do about it? To be of practical use for SRM, change analysis should be closely linked to the development of *warnings* or *indicators* to signal that the predicted change may be happening, so that you and your organization can respond in time; before the change in the security threat pattern catches you by surprise.

The first step is to ask: “*What could happen that would cause the situation to change, i.e., what would cause hostile groups to start targeting us?*” This should be linked to the following question: “*What indicators or warning signs might alert us that this was happening?*” The questions can be put in a table as in the example below, which shows some typical (but not all-inclusive) responses.



Tools

Threat Change Indicator and Action Table

What factors could cause the threat situation to change?	What warning signs/indicators would signal a possible change?	What concrete actions need to be taken?
<ul style="list-style-type: none"> <li>• Change in rebel tactics or alliances</li> <li>• Events that increase a belligerent’s need for resources (e.g., budget constraints, a new offensive)</li> <li>• Unpopular policy change by UN or your agency</li> <li>• Staff misbehavior</li> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Change in leadership</li> <li>• Overt threatening statements or gestures from rebel leadership</li> <li>• Attacks on targets with similar profile</li> <li>• Other</li> </ul>	<ul style="list-style-type: none"> <li>• Reduce staff movements to project sites</li> <li>• Consider requesting police escort</li> <li>• Other</li> </ul>

In order to facilitate action as well as analysis, the indicators should be accompanied by actions or measures to be taken if and when the warning signs occur. In this way, indicators become useful tools not only for analyzing future threats, but for designing immediate actions or contingencies to be taken based on the warning signs. The sample Threat Change Indicator Table above shows how it can be converted into an action chart. *Chapter 8 – Risk Reduction Measures* and *Chapter 9 – Security Plans and Planning*, will explore more concretely what kinds of measures might be taken.

The proactive and habitual search for security threat change indicators is sometimes called **Situational Awareness**. In high risk areas, keeping aware of small indicators can be a life-saving habit. Maintain your situational awareness by continuously looking for any recent changes that may affect the risks you face. This is primarily a matter of vigilance (constantly looking for changes) and discipline (remembering to ask yourself whether anything has changed, either at the end of every day or week). While an important habit to develop, in some cases long-term field workers can become so accustomed to insecure environments, they actually pay less attention to these details and may become overconfident.

Often, the local population and security forces will have more warning of impending confrontations (military battles, terrorist attacks, or riots, for example) than expatriate field staff. You should be aware of changes in their daily routines or activities and, at a minimum, ask why these changes are taking place.

## Summary



### Key Points

**Threat assessment** is closely related to vulnerability and program assessment and at least some of the data collection required for any of these three activities will likely be of use in the others.

---

Taken on its own, **threat assessment** is the collection and analysis of information about past and ongoing threats in the environment in order to make assumptions or predictions about current and future threats.

---

**Historical analysis** is the study of past security events and consideration of the possible implications for your current and future activities. Historical analysis may be carried out using different factors in order to determine patterns in the data.

---

**Pattern analysis** may take several forms such as consideration of the patterns in the **types** of threats, **locations** of threats, **time** of day, week or month, for the **likely targets** of threats. One of the key aspects of pattern analysis is the recognition that while many patterns will continue in ways that facilitate security planning, we must be aware that sometimes the patterns do change, requiring planners and managers to look for indicators that change may be happening.

---

**Change analysis** is a logical extension of threat analysis as it identifies indicators that change may occur, so that measures can be taken to avoid harm before the changing threat pattern takes you by surprise.

---

No matter which of the techniques above are used, security threat assessment relies on information from people. Since all people have different information sources, biases and interests, **information collected should be validated to the extent possible**, either by comparison of several sources, or through use of the information accuracy checklist or a similar guide to help you rate reliability.



## Chapter 4 Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

- T**  **F** 1. Threat assessment is a stand-alone activity and completely unrelated to programme or vulnerability assessment.
- T**  **F** 2. Pattern analysis is a component of threat assessment that refers specifically to the damage patterns from bomb attacks to determine what locations are safest inside an office or residential building.
- T**  **F** 3. Historical analysis depends on the collection and analysis of previous incidents.
- T**  **F** 4. Change analysis is done to better understand and predict how threat patterns may change.
- T**  **F** 5. There are so many sources of unreliable security information available in the field that the only useful information that you should consider in your threat assessment is what you have directly observed yourself.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following statements are correct about historical analysis?
  - A** Written reports from local police or other officials will always be accurate since the local police have the best information.
  - B** The timeframe over which past threats are reported has little effect on the resulting analysis of the data.
  - C** Historical analysis can be a useful part of your overall threat assessment.
  - D** Historical analysis is of little use in threat assessment since threats change so frequently.
- 7. Which of the following are examples of pattern analysis?
  - A** Recording the times of day that threats occurred on a 24-hour clock.
  - B** Recording data about who (i.e. expatriates, locally hired national staff, program, administrative, and temporary staff) was involved in security incidents and presenting the data as a ratio or pie chart.
  - C** Recording threat events on a map with different colored pins to represent different types of threats.
  - D** Recording threat events on a map with different colored pins to represent different months in which the events happened.



Self Test

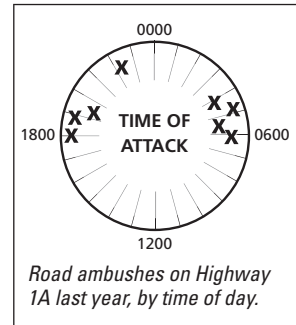
Chapter 4

Self-Assessment Questions (continued)

8. Situation awareness means:
- A** Knowledge of the history and roots of the conflict or security environment.
  - B** Paying attention to details and changes in the environment that might signal changing or imminent threats.
  - C** Understanding the relative differences in security threats amongst different countries or regions.
  - D** Proactively researching details about the motivations behind those that are likely to pose threats.

9. What conclusions could reasonably be drawn from the pattern of roadside ambushes against vehicles shown at the right?

- A** Most attacks occur around mid morning.
- B** Most attacks occur late at night.
- C** Most attacks occur near midnight and noon.
- D** Most attacks occur near dawn and dusk.



10. Which of the following might be useful indicators for use in security change analysis?
- A** New work/repair of military positions.
  - B** Sudden appearance of military convoys on the road.
  - C** New checkpoints or checkpoints starting to be manned by soldiers instead of police.
  - D** Departures from area of local families.



Chapter 4 Answer Key

- 1. F
- 2. F
- 3. T
- 4. T
- 5. F
- 6. C
- 7. A, B, C, D
- 8. B
- 9. D
- 10. A, B, C, D

# Chapter 5

## Vulnerability Assessment

*View of a UN office compound entry access gate and fence taken by a security officer while conducting a vulnerability assessment of a field office.*

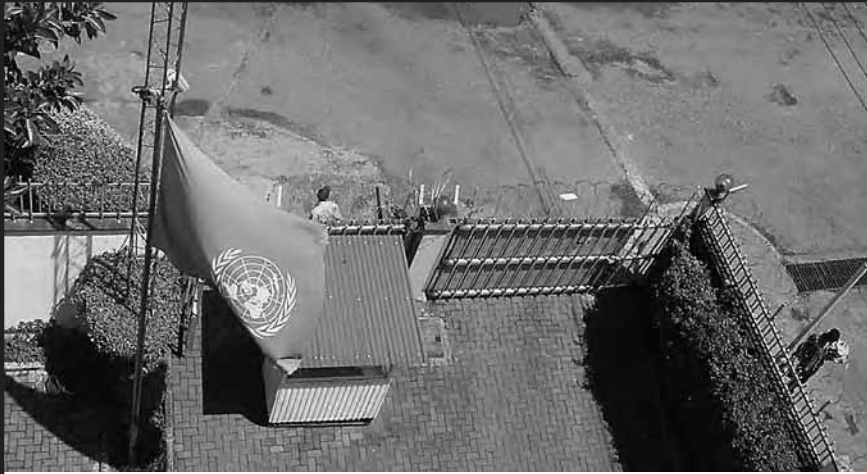


Photo by Kjell Lauwik, UNHCR

Threat assessment as discussed in the last chapter looks in detail at the outside environment in which an organization works. It is focused on the bad things that can happen to you which are considered to be part of the working environment and generally beyond your ability to control. **Vulnerability assessment**, on the other hand, looks inward at the organization itself. Its intent is to investigate weaknesses that make you or your staff more likely to be attacked, or more severely harmed if you are attacked.



### Learning Objectives

In this chapter you will learn about:

- The importance of vulnerability assessment in the SRM approach.
- Key vulnerability factors to consider in your assessment such as:
  - Location
  - Exposure
  - Value
  - Interpersonal skills
  - Adoption of, and compliance with, security measures
  - Program impacts
  - Organizational image
- Benchmarking your own organization's vulnerabilities against those of others in the same working environment.



## 5.1 The Importance of Vulnerability Assessment in SRA

We saw in previous chapters that *threat assessment* and *vulnerability assessment*, while different, are inseparably linked. Any investigation into how damaging a particular threat will be will depend on your own vulnerability to such a threat. In the same way, it is difficult to assess vulnerability without first asking the question, “vulnerable to what?” For this reason, threat and vulnerability can be thought of as equally important elements in the SRA process. There is probably no prescriptive sequence for doing threat and vulnerability assessment (and program assessment, to come in the next chapter), although some security professionals have their own individual preferences. The important points are that: 1) all are essential to the SRA process, 2) a valid risk assessment cannot be made without considering all three of them in their entirety, and 3) data and conclusions from each type of assessment must inform the others in a continual feedback loop.

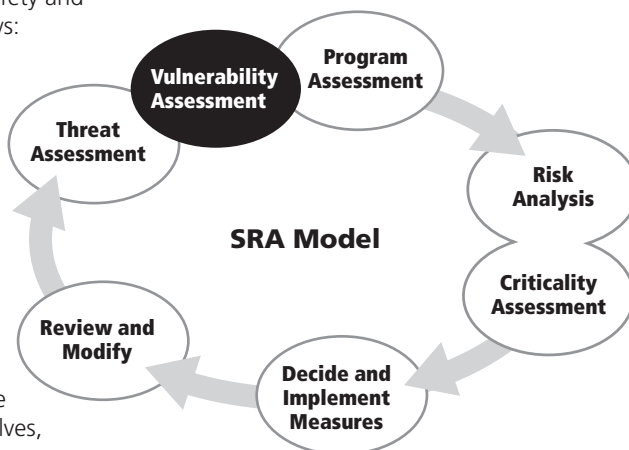
The United Nations Department of Safety and Security defines vulnerability as follows:

*Any weakness that can be exploited by a belligerent to gain access to an asset. Vulnerabilities can result from, but are not limited to: building characteristics, equipment properties, personal behavior, locations of people, equipment and buildings or operational and personnel practices.*

This course expands the definition of vulnerability slightly to include the study of certain factors that, while not necessarily weaknesses in themselves, may impact the likelihood of your being selected as a target. In all events, vulnerability assessment should be thought of as a process of examining your agency's or office's own unique profile in your particular environment.

Determination of weakness requires an “on the ground” assessment of the physical premises of the office, guest houses, or apartments where staff live, and associated compounds, vehicles and other equipment. This usually includes assessment of access points, walls, gates, doors and windows. But vulnerability is more complex than the physical structures alone; it must also include investigation into readiness and training of protection staff and guards, local police and other response forces. If an ambulance is needed from the local hospital, how reliable is it? How long does it usually take to arrive? These kinds of systemic questions also contribute to a thorough vulnerability assessment.

In conducting a vulnerability assessment, it is also important to consider factors that can reduce your vulnerability. Appropriate plans and equipment, readiness of staff, first aid training, and field communications protocols are all strengths that should be noted. If any of these is lacking, it may be a vulnerability. Will this require your immediate attention? Part of the answer to this question will depend on the results of your threat assessment: does the deficiency create a weakness that could increase the likelihood of an identified threat occurring, or could make its effect more severe if it happens? Here again, the inter-relationship of threat and vulnerability assessment should be apparent, and security managers must know how to analyze both their external environment and their own organization's strengths and weaknesses.





### Question

*What issues or factors can you think of that contribute to your vulnerability in the field?*

---



---



---



---



---



---



---



---



---



---

The factors you listed above most likely relate to your own experience and situation. While every situation is different, several factors should always be considered. The next section will detail several of these factors that play a role in vulnerability and will provide some guidance in how to assess vulnerability in relation to each factor.

## 5.2 Key Factors to Consider in Vulnerability Assessment

Many factors affect vulnerability. In *Vulnerability Assessment: Training Module for NGOs Operating in Conflict Zones and High-Crime Areas*, Jonathen Dworken identified eight factors of particular importance. This section is based on that source, but has been updated in several areas and amended to adhere to the terminology in use by the UN system.

The basic factors listed below all impact your vulnerability, but their specific applicability to your situation will vary depending on your specific organization and the threats (as well as the underlying motivation for those threats) you are facing. Some of the factors affect your vulnerability in all situations, such as the location of your staff and property. Other factors have an impact only in certain types of situations; the value of your property, for example, matters when faced with a crime/banditry threat, but not with an indirect one (e.g., getting caught in the crossfire, artillery barrage, or mined areas). The eight factors considered here are:

- 1) Location
- 2) Exposure of staff and property
- 3) Value of property
- 4) Adoption of appropriate safety measures
- 5) Staff compliance with safety measures
- 6) Staff interpersonal skills
- 7) Program impacts
- 8) Image of the organization



### *Location*

Your vulnerability may differ from that of other organizations due to the specific locations of your staff and property. Questions to ask when considering the vulnerability of your location include the following:

- Are you in a specific location (province, city, or district) that is safer or more dangerous than other comparable organizations?
- Are you in a location that is remote, difficult to reach and/or poorly serviced by critical response needs (law enforcement and fire response, emergency medical response and hospitals, etc)? Remember that the ability to respond effectively to a threat (or lack of it) will play a large part in your assessment of how potentially harmful or damaging that threat is to you.
- Are belligerents, criminals or other actors able to move easily and quickly from dangerous areas into safer ones (e.g., roaming gangs or bandits, bombing raids)?
- Is there a likelihood of the threat situation changing quickly, making relatively safe locations more dangerous on short-notice or without warning?

### *Exposure of staff and property*

Two organizations in the same location may face significantly different levels of exposure due to:

- **The number of staff and amount of valuable property** – An organization with 100 staff members in a dangerous location has greater exposure than one with 10 employees in the same place.
- **The degree to which activities require staff members to travel in particularly high-risk areas** – For example, traveling to or through remote field areas on assessments and monitoring missions. The amount of time staff and property are in vehicles or convoys, which tend to be more vulnerable than fixed sites, should be considered. Exposure explains why an organization that frequently sends staff to the “deep field” probably has greater vulnerability than one that works only in the capital city, although the two might be housed in the same office building (i.e., their location is the same).
- **Exposure can also be influenced greatly by the adoption of appropriate security measures and compliance with those security measures** – These are discussed as separate vulnerability factors below. This is another example of where the elements of SRA are inter-related and cannot be considered in isolation.

### *Value of property*

Organizations with valuable property may present attractive targets to criminals. While having valuable property is not a “weakness” *per se*, it may increase the likelihood of being selected as a target, and is therefore worth consideration in your vulnerability assessment. International organizations usually have valuable property—cash, equipment, vehicles, personal property, and relief aid. In any situation, these items are a potential target of criminals. Remember also that value is relative. Even though some items or equipment may seem of low value to you, they may have a high perceived value to those wanting to take them, especially if they will be used for other purposes; for example:

- In a conflict zone belligerents may target property to support their military efforts.
- Some property has military value (e.g., four-wheel drive vehicles, radios, fuel).
- Stolen cash can be used to purchase military equipment and supplies (e.g., weapons, ammunition, vehicles, fuel, radios, food).
- Some property can be sold or bartered (e.g., four-wheel drive vehicles, radios, medicine, valuable foodstuffs).



## *Adoption of appropriate security measures*

Organizations that adopt appropriate security measures are usually less vulnerable than those that do not. Appropriate measures include all of the following:

- Appropriate facilities (starting with selection of the site, its location and quality of construction, and including perimeter walls, barriers and other structures).
- Appropriate security equipment (alarms, lighting, shatter-resistant film, radios, vehicles, ballistic jackets and helmets, first-aid kits, fire extinguishers, etc.).
- Appropriate guards (number, equipment and training).
- Appropriate protocols and procedures (radio checks, pre-mission preparations, reporting of security information, etc.).
- Appropriate security plans and planning, including procedures, contingency plans, and supporting information (contact numbers for staff and emergency responders, etc.).
- Appropriate training for staff, including security briefing upon arrival and regular situational updates thereafter, and understanding of the security plan.
- SRA updated regularly; results used to update plans and shared with staff as appropriate.

*Chapter 8 – Risk Reduction Measures*, and *Chapter 9 – Security Plans and Planning*, will discuss these areas more fully.

## *Staff compliance with security measures*

Even if your organization adopts the appropriate security measures, actual vulnerability is still dependent upon whether the staff consistently comply with them. Organizations usually adopt a wide variety of measures, from broad policies (such as prohibiting soldiers or armed persons to ride in vehicles) to minute procedures (how to call for help using a radio). Assuming these measures are appropriate, your organization is more vulnerable than others if your staff members do not comply with the measures (see section above). Key factors for consideration include the following:

- Are security measures in place made clear to all, in briefings and in writing?  
Is the Security Plan (or appropriate parts of it) disseminated to all staff?  
Are new employees briefed and encouraged to review it?
- Do staff members understand use of security-related equipment (e.g., radios, GPS, satellite telephones, and fire extinguishers)?
- Do staff members comply with security instructions (e.g., travel clearance procedures, radio checks, curfews, and no-go areas)? What happens in cases of non-compliance?
- Is implementation of the security plan supported (or undermined) by other aspects of your organization such as orientation, education, training, equipment, funds, time, and organizational culture (e.g., risk-taking propensity)?

## *Staff interpersonal skills*

The interpersonal skills of your staff can affect your vulnerability by helping you avoid incidents and mitigate their impact if they occur. Such skills affect security in important ways:

- Interpersonal skills may determine whether a community is likely to share information and otherwise provide help and advice that can help plan for and avoid security incidents before they occur.



- Interpersonal skills can mitigate the impact of incidents by allowing you to react appropriately. When confronted with an incident (e.g., roadblock, angry mob), your behavior can either escalate the incident or reduce it, depending in part on your skills in dealing with a stressful situation and negotiating effectively.
- Skills and behavior within the team itself can be critical in preventing or dealing with security incidents. Sharing information appropriately, and ensuring staff acceptance of security measures will, in many cases, mitigate the impact of incidents through mutual support of team members.

### *Program impacts*

The impact of your programs on other actors in your environment can have an effect on your safety, both positively and negatively. Being aware of how your activities affect others helps you better understand your vulnerability.

Programs may create or increase the likelihood of threats by:

- Requiring staff to stay or travel in high-risk areas.
- Creating obvious temptations for bandits or criminals.
- Benefiting, or being perceived to benefit, some groups and not others.
- Giving the perception that benefits are spread unevenly.
- Creating competition for employment opportunities.
- Promoting dependence with aid and potential violence when aid comes to an end.
- Challenging customs, traditions or beliefs.
- Providing inadequate information which can lead to misunderstandings and misperceptions.

Some ways in which programs can reduce likelihood of threats include:

- Programs may reduce tensions in the community by providing lifesaving assistance.
- Programs may support long-term peace, stability and development.
- Programs may enhance the credibility, image and acceptance of your organization.

Experience has shown that for humanitarian and development workers in insecure areas, the impact of programs is of particular importance in assessing an organization's vulnerability and ultimately risk. For this reason, in *Chapter 6 – Program Assessment*, we will take a deeper look at the relationship between these two factors, and explore what program assessment means in the SRA context.

### *Image of the organization*

Finally, your vulnerability is partially dependent on the image of your organization within the local community. Every organization has a public image—the perception of the local population, authorities, and belligerents toward your staff and programs. What you say and do, how you appear, and the scope and impact of your programs influences the opinions of the local population. Will they accept your presence and roles, or be resentful toward you?



### Question

*Give two examples of situations where a positive image has (or could have) increased safety and security of humanitarian field staff.*

---



---



---

*Give two examples of situations where a negative image has (or could have) decreased safety or led to increased threats against humanitarian field staff.*

---



---



---

While image may not be the sole cause of significant security incidents, acceptance or resentment of your staff and programs can influence security in these important ways:

- It increases or decreases the predisposition of criminals and belligerents to target you.
- It makes the local population more or less likely to help ensure that you do not face security incidents (e.g., extending societal constraints on criminal activities to you, forewarning you of danger).
- It makes the local population more or less likely to help you when you are faced with security incidents (e.g., helping you recover stolen property).

Image problems are often founded on the mistaken belief that people understand the objectives of your operations. Often verbal messages are less important than non-verbal ones that an agency may be unaware it is sending. To help understand whether you are vulnerable because of image problems, consider the following:

**Appearance and behavior** – Does your staff's appearance and behavior lead people to believe the staff members are wealthy? Morally corrupt? Do your discussions with officials and others lead people to conclude you are naive and ignorant of the history and situation, and thus easily manipulated?

**Staff composition** – Is your staff comprised of an appropriate mix of national, ethnic, political, religious, class, rural-urban, and gender groups—in both numbers and seniority—from the perspective of being respected and seen as impartial?

**Programs** – Are your programs perceived as helping one particular ethnic group or belligerent party, aiding only some sectors of society (e.g., assisting refugees but not the local population or internally displaced persons), changing the ways in which groups have access to resources (e.g., supporting education only for girls), or altering power structures (e.g., using merchants and suppliers aligned with one group)? The issue of how your programs are perceived is different from whether they actually have an impact on the conflict.



**Headquarters** – Does the location of your headquarters portray implicit support for one side in a conflict, or association with some agencies?

**History** – Do people misinterpret repeated assessments as broken promises? Did they resent your withdrawing from the area when the security situation worsened in the past? Remember that history, and often collective memories, are long; factors predating your organization’s arrival, such as geopolitical rivalries and former colonial legacies can impact how your agency is perceived.

Another way of assessing vulnerability due to image problems is to look for evidence of how you are portrayed in the press or local discussions—as agents of western imperialism, intelligence agents, cultural imperialists, proselytizers, enemy sympathizers, or smugglers.

Remember, however, that trying to change your organization’s image may have only a limited effect on your vulnerability. Despite your best efforts, you may be unable to differentiate your staff and programs from other organizations; the local population or a certain group may simply view all similar organizations as the same.

- Belligerents may be targeting a particular population which your agency is seeking to aid, or trying to deprive it of assistance, in which case you may become a target despite all efforts to increase your image.
- Belligerents may be seeking to discredit the government and create an appearance of inefficiency and disorder, in which case targeting your agency may be expedient regardless of your image.
- Resources may be vital to the war efforts of belligerents, in which case you may be targeted no matter what they believe.

### 5.3 Vulnerability “Benchmarking”

How can you use the eight vulnerability factors listed above to assess the vulnerability of your own organization? One way might be to rank your own organization or office in each category. For example, you could use a standard set of descriptors from “Highly Vulnerable” to “Not Vulnerable” and then rate yourself in each category.

Alternatively, you might use a comparative or “benchmarking” approach. The idea is to compare your level of vulnerability using the factors presented above with that of other organizations operating in the same environment. Choose four or five (or more) organizations facing the same threat environment as you, and list your organization beside them. Next, for each vulnerability factor, rank the organizations in comparison to one another, including your own office. Assign the strongest or safest organization for each factor the number 1. Assign the weakest or most vulnerable organization number 6 (or 5 etc., depending on the number of targets being examined). Of course, you will not have complete information, but estimate as best you can (it may be useful to conduct this process with partners to compare perceptions). A generic example is filled out in full in the matrix below.



## Tools

## Vulnerability Comparison Matrix

	Safest location	Least exposure	Least value of assets	Positive program impacts	Appropriate security measures	Staff compliance	Staff interpersonal skills	Positive image
<i>Your Organization</i>	<b>5</b>	<b>6</b>	<b>2</b>	<b>2</b>	<b>6</b>	<b>5</b>	<b>6</b>	<b>3</b>
<i>UN Office</i>	<b>3</b>	<b>4</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>2</b>	<b>4</b>	<b>4</b>
<i>Foreign Embassy</i>	<b>2</b>	<b>1</b>	<b>3</b>	<b>6</b>	<b>2</b>	<b>1</b>	<b>5</b>	<b>6</b>
<i>Foreign Embassy</i>	<b>1</b>	<b>2</b>	<b>1</b>	<b>1</b>	<b>5</b>	<b>3</b>	<b>2</b>	<b>1</b>
<i>Major NGO Office</i>	<b>6</b>	<b>5</b>	<b>5</b>	<b>4</b>	<b>4</b>	<b>6</b>	<b>3</b>	<b>2</b>
<i>Major Hotel</i>	<b>4</b>	<b>3</b>	<b>6</b>	<b>5</b>	<b>3</b>	<b>4</b>	<b>1</b>	<b>5</b>

The advantage of this approach is that it approximates the thought process of many criminals (including terrorists) who target their victims by looking for “the weakest in the herd” or the “softest target.” If your organization is at the bottom compared to other nearby organizations in several vulnerability factors, it may indicate that threats may be directed at you rather than others, since you represent a “softer target”. This format is also very useful in presenting the findings of your vulnerability analysis to senior officers and budget offices to graphically explain why you are asking for funds to reduce vulnerability!

Finally, remember that to be of value, the data generated from the assessment of the different vulnerability factors must be correlated with each other, and with data from your threat assessment. For example, say that your assessment reveals that you have the most valuable property of any similar potential target in your immediate environment. If so, your next question might be, how great a threat is theft in this area? To answer this you will return to the results of your threat assessment (do not forget to include change analysis). Is the threat high? If so, then you certainly will not want to be among the bottom of the rankings for appropriate security measures, among several other relevant factors.

If your assessment indicates that you are comparatively weak in a number of vulnerability factors that relate to a threat that you have evaluated as high, this should be cause for concern—you will have to do something about it. You are now on your way to making an informed assessment of overall risk in your environment.

## Summary



### Key Points

**Vulnerability assessment** is a critical activity in the SRM approach. The field level activities done to carry out this work will usually also involve threat assessment as discussed in the previous chapter and program assessment as will be discussed in the next.

---

The eight key factors to consider in conducting your vulnerability assessment are:

- 1) **Location** of your office and activities in the field – Organizations located in dangerous and remote areas are more vulnerable than ones that are not.
- 2) **Exposure** is related to location, but also includes number of staff and time spent traveling between project sites.
- 3) **Value of program equipment and assets** – Valuable property may present an attractive target to criminals.
- 4) **Adoption of security measures** – Organizations that adopt appropriate security measures are usually less vulnerable than those that do not.
- 5) **Staff compliance** – Even with appropriate security measures, actual vulnerability is still dependent upon whether staff consistently comply with them.
- 6) **Interpersonal skills** can impact vulnerability by helping staff avoid security incidents and mitigating their effects when they occur.
- 7) **Program impacts** – The nature of your programs can influence your security in many ways, both increasing and decreasing risk.
- 8) **Organizational image** – How your organization is perceived by the local community will affect your likelihood of being targeted, or of receiving assistance if you are in an incident.

---

Use these vulnerability factors by benchmarking your own organization's vulnerabilities against those of others in the same working environment. This kind of comparison can quickly guide you in areas that may need improvement. Using the logic of the lion on the hunt, you do not want to be seen as the weakest animal in the herd.

---

Use this information to correlate vulnerabilities and threats. Are you particularly vulnerable in areas that create opportunities for a specific kind of threat? If so, you will need to take additional measures.

**Self Test**

## Chapter 5 Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

- T**  **F** 1. Vulnerability assessment is a stand-alone activity and completely unrelated to program or threat assessment.
- T**  **F** 2. The eight vulnerability factors described in this chapter are all equally relevant and important for all types of threats.
- T**  **F** 3. Consideration of program impact, in terms of vulnerability assessment, implies that your vulnerability is based on more than walls, fences and guards—the perceived results of your work in the field also affects your vulnerability.
- T**  **F** 4. Image problems are often founded on the mistaken belief that people in the community understand the objectives of your operations.
- T**  **F** 5. Staff members' interpersonal communication and negotiation skills are valuable for program development purposes but have little or no actual effect on security issues.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following can be factors in determining your level of *exposure* in your vulnerability assessment?
  - A** Number of staff and amount of valuable property in dangerous locations.
  - B** Amount of time staff and property are in vehicles or convoys.
  - C** The value of your equipment and assets.
  - D** Staff interpersonal skills.
- 7. Which of the following are examples of questions that should be asked to determine levels of compliance with organizational security procedures and protocols?
  - A** Does the staff adhere to curfews and avoid designated no-go areas?
  - B** Are new employees briefed on the security plan and encouraged to review it?
  - C** Do staff members understand how to use essential security equipment?
  - D** Have staff members memorized all important contact numbers for staff and emergency responders?



Self Test

Chapter 5

Self-Assessment Questions *(continued)*

8. Which of the following factors are involved in understanding issues regarding an organization's image in the community?
  - A Staff composition
  - B Type of programs implemented
  - C Location of headquarters
  - D Perception of organizational mandate or intent
  
9. Which of the factors below are considered among the eight factors affecting vulnerability?
  - A Location
  - B Likelihood of threat
  - C Security measures taken
  - D Magnitude of threat
  
10. The primary reason for "benchmarking" your own office's or organization's vulnerability against others in the same working environment is that:
  - A The least vulnerable office is more likely to be attacked.
  - B The image projected by an organization to the local community is the most important aspect of vulnerability assessment.
  - C The most vulnerable office is more likely to be attacked.
  - D Neither the most vulnerable and least vulnerable offices are likely to be attacked, the most dangerous situation is to be in the middle range of vulnerability in the field.



Chapter 5  
Answer  
Key

- |    |   |     |            |
|----|---|-----|------------|
| 5. | F | 10. | C          |
| 4. | T | 9.  | A, C       |
| 3. | T | 8.  | A, B, C, D |
| 2. | F | 7.  | B, C       |
| 1. | F | 6.  | A, B       |

# Chapter 6

## Program Assessment

*Internally displaced people receive emergency food aid in Agok, Sudan in May 2008. Women carry their ration of food, after fleeing their homes in the village of Abyei, engulfed by heavy fighting between the Sudan Armed Forces and the Sudan Peoples Liberation Army. Humanitarian programs provide donated food and other vital supplies to help these people survive.*



UN Photo by Tim McKulka

In Chapter 5 you saw that the activities you undertake in the field influence your organization's level of vulnerability and risk. This relationship is of particular importance for organizations conducting humanitarian and development programs in insecure areas. For this reason, when the Office of the UN Security Coordinator (UNSECOORD, now DSS) introduced its first system-wide SRA model in 2004, it promoted the idea that program assessment should be considered as more than just a sub-set of vulnerability assessment. Because of the strong influence of program activities on security for humanitarian agencies, program assessment should be considered as a separate area of assessment in its own right. This course follows the same approach, and in this chapter we will take a closer look at what program assessment means in the SRA context and how to go about it.



### Learning Objectives

In this chapter you will learn:

- The definition of program assessment and its relationship to the overall SRA approach.
- The ways that some program activities can increase or decrease your risk as a humanitarian aid worker.
- The ways that your program-related risk may change over the short- to longer term.
- How security measures to reduce risk may affect your programs.
- A process for conducting your own program assessment as part of your SRA.



## 6.1 What is Program Assessment?

Program assessment is a systematic way of asking the question: “how could the humanitarian activities that I want to do affect threats in my working environment, my vulnerability, and overall risk?” Could they create more danger for staff (increase risk)? Could they make staff safer (decrease risk)? Could some activities increase (or decrease) risk in the short term but then decrease (or increase) it in the long run?



**Question**

*Have you seen (or can you imagine) a case where your organization’s programs created (could create) increased or entirely new risks?*

---

---

---

---

*Have you seen (or can you imagine) a case where your organization’s programs made it safer for you to operate?*

---

---

---

---

## 6.2 How Humanitarian Programs Affect Staff Security in the Field



**Exercise**

Consider the following short case scenarios adapted from actual humanitarian operations. In each instance, how could the proposed programs impact the safety of staff in the organization? Could the activities increase risk? Could they make staff safer? Could they have multiple effects, e.g., in the short and the long term? Use the space below each scenario to record your answers.



**Case 1: Darfur, Sudan** Ongoing war in Sudan’s western region has been accompanied by allegations of widespread atrocities and abuses against civilians. Your human rights-based organization has been assigned to monitor and report on the situation there.

*How could your monitoring activities affect staff safety in Darfur?*

---

---

---

---



**Case 2: Sri Lanka** Near the town of Mannar, your humanitarian relief agency has established a program to support the return of displaced people to their original homes, through rebuilding infrastructure, irrigation, vocational training and community development. The beneficiaries of the program are predominantly ethnic Tamils displaced by the war. Meanwhile, the Tamil 'Tigers' continue to wage a war against the Sri Lankan government for a separate homeland.

*How could your housing and infrastructure programs impact your staff safety in Sri Lanka?*

---



---



---



**Case 3: Afghanistan** Noting the longstanding disparity in education opportunities for boys and girls, your humanitarian/development agency intends to build a series of model all-girl secondary schools. The first school will be built near the city of Kandahar, a conservative area where the rate of secondary school completion among girls is among the lowest in the country.

*How could your school building programs impact your staff safety in Afghanistan?*

---



---



---



**Case 4: South Sudan** Your development agency plans to begin a major infrastructure renovation project in the town of Yambio in Southern Equatoria. Yambio's population is split almost evenly between rival Dinka and Zande ethnic groups, and violent clashes have occurred. The UNDP project is eagerly awaited in Yambio as it is expected to generate employment opportunities for the town where unemployment is estimated to be as high as 50%.

*How could your renovation and employment programs impact staff safety in Yambio?*

---



---



---



**Case 5: Sri Lanka** You work for the development agency of a wealthy donor country. Your country has selected a village in southeast Sri Lanka to be a model “Friendship Village.” As such, it will receive generous funding for housing and other infrastructure development from your agency.

*How could your well-funded “friendship village” project impact staff safety in Sri Lanka?*

---

---

---

---

### *Ways that programs affect safety*

Humanitarian and development programs can affect risk in a number of ways. In some cases risk is reduced, in others risk is increased. Compare your answers above to the common situations described below. How many of these relationships did you mention in your answer?

Ways that humanitarian and development programs sometimes *increase risk*:

- **Programs may require staff to travel into high-risk areas** – This is perhaps the most predictable relationship for those working in insecure areas. It is certainly evident in Case 1 above, and to some extent all the others as well. Helping people affected by conflict usually requires staff to go to conflict-affected areas; this can impact your security directly by putting staff in harm’s way.
- **Programs may benefit (or be perceived to benefit) some groups and not others** – This is a danger faced especially by agencies that are mandated to help a specific category of beneficiary, such as UNHCR (refugees and other displaced persons). It may affect other organizations as well depending on how programs are conducted, explained, and perceived. The agency described in Case 2, and possibly that in Case 5, face this situation.
- **Benefits may be perceived to be spread unevenly** – Even if the problem is not perceived to be intentional, the feeling that others are getting benefits that some are not can be a source of tension in the community. This is the most likely security-related aspect of the program described in Case 5.
- **Programs may create temptations for bandits or criminals** – Often criminality increases, or indeed new forms of crime emerge, in the wake of a large influx of humanitarian and development agencies. This was the case in Burundi in 2004, following a ceasefire agreement and arrival of the United Nations Mission in Burundi (ONUB). The massive influx of relief, peace-building and development workers was accompanied by an upsurge of crime in and around the capital Bujumbura, as wealthy foreigners (UN and international NGOs) presented attractive targets for criminals.
- **Employment, contracts and other issues with financial implications can increase tensions** – In areas afflicted by poverty and unemployment, these can be the case of intense, sometimes lethal competition. This was the case for agencies entering South Sudan shortly after the cease-fire agreement of 2004, as in the situation described in Case 4.
- **Program aid may find its way to belligerents** – Resources intended for humanitarian purposes may be stolen from civilians; or civilians may be compelled to provide it; or civilians may give it willingly if they sympathize with one of the parties in the conflict. Equally, aid may be diverted by belligerents (including a government) to purposes other than those intended by the donor.



- **Programs may challenge customs, traditions or beliefs** – This danger was faced by agencies involved in the school-building program in Case 3.
- **Programs may be misperceived or not fully understood** – This may be closely related to the point above. What a program is believed to be about can be as important for your safety as what it really is, or what you intend it to be. This factor may play a role in all the cases above.
- **Aid may encourage dependence** – In this case, the ultimate cessation of aid can then lead to violence. This could apply in all cases as well, depending on how the programs are conceived and implemented.

Ways that humanitarian and development programs sometimes *decrease risk*:

- Programs may reduce tensions by providing lifesaving assistance.
- Programs may reduce risk over the longer term by supporting long-term peace, stability and development initiatives.
- Programs may enhance the credibility, image and acceptance of your organization. Knowledgeable, honest, and polite staff members, that are seen to genuinely help the local community, from the community's own perspective, may be encouraged and even protected from harm by the local community.

### 6.3 Program-Related Risk Factors May Change Over Time

It may be useful to consider the effects of your program activities in the short, medium and long term, since your risks may change dramatically over time. For example, programs aimed at promoting long-term stability, and therefore a more secure safety environment, may have short-term effects that cause an immediate increase in tensions.



#### Question

*Can you think of a case where programs brought increased risks in the short run, but decreased risks over the long run?*

---



---



---



---

*Describe a situation where the reverse was true – program activities reduced risks in the short term, but set the stage for greater risks in the long term.*

---



---



---



---



One example of this long-term versus short-term dynamic is the building of schools for girls in Afghanistan described above. Building girls' schools in some rural communities has been specifically programmed to bring greater prosperity to local communities in the longer term. This same project, however, may immediately inflame tensions between traditionalists who are against such schools and reformers or advocates who want them. Many humanitarian field staff members involved in such projects have been threatened, kidnapped, or even killed over such disputes.

For another example, consider the following account from a UNHCR staff member working in Cairo, Egypt in December 2005. It describes the days following an operation by Egyptian riot police to clear a park being occupied by Sudanese refugees and asylum seekers. In the melee that ensued, 26 Sudanese were killed and many more were wounded.

<p>The Police cleared the park, it was a bitter struggle, and people were killed. The Sudanese refugee community was convinced that UNHCR had a hand in calling for the action. There was a lot of anger against us, threats against staff. We knew we needed to rebuild relationships with the refugees, now of all times they needed our assistance. But in the short term we also knew it could be dangerous; some refugees felt we had betrayed them and wanted revenge. The weeks after the park</p>	<p>clearing by the police were tense; we had to analyze the level of risk on a day-to-day basis: was it safe to go to the mosque to deliver medicine today? Should we go to the 'old town' to check on the injured? It was 'touch and go' for a while, missions were called back at the last minute. But without these steps we couldn't have succeeded in rebuilding trust with the Sudanese community and laying the foundation for a more stable long-term relationship.</p>
---	---

Equally, it is possible that steps that seem to increase safety in the short term may prove dangerous in the long run. One common example of this is hastily prepared, but ill-considered, assistance packages provided in the early stages of some emergencies. Initially, everyone is quite happy about the freely distributed aid, but when this proves unsustainable over time, disappointment is inevitable. Managing expectations is often a common element in cases where a program's dangers can increase over the long term.

### 6.4 The Other Side – How Measures to Improve Staff Security Affect Humanitarian Programs

The security measures that your organization adopts to protect field staff can also have an impact on your humanitarian programs.



**Question**

*Can you think of examples where the security measures your organization adopted had an impact on the humanitarian or development programs you were undertaking?*

---



---



---



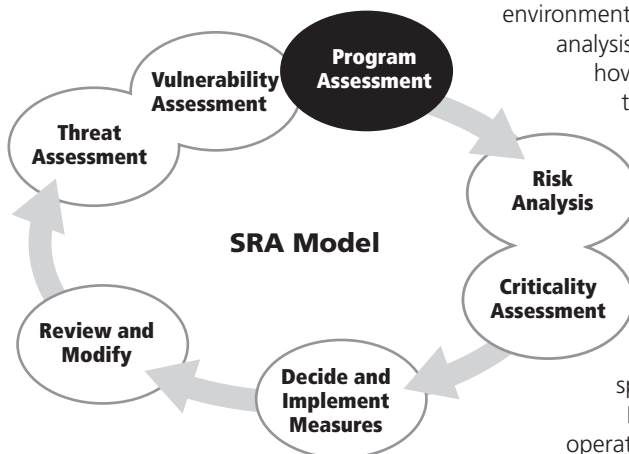
---



The most common situation in which security measures affect programs occurs when rules or procedures restrict or prohibit an agency from carrying out intended programs. Of course, if the risk assessment indicates that the danger is real, and there are no alternative measures that can prevent or mitigate the risk, then programmatic restrictions or even cancellation are legitimate choices for humanitarians. However, suspension of a program can sometimes bring security consequences of its own. For example, an agency that temporarily withdraws from the community may face even greater anger and resentment from beneficiaries if and when it eventually does return. This is something that must be considered in the criticality analysis part of your SRA, explained in more detail in Chapter 8. What should be remembered is that humanitarian programs and staff security must never be considered in isolation, but rather should be analyzed comprehensively in terms of their impacts on one another.

## 6.5 Doing Your Own Program Assessment

It is clear that your programs directly affect your risk, but how do you go about analyzing this relationship? A good place to start is your threat assessment. Remember that during that stage



of your analysis, you identified threats in your environment based on historical data, pattern analysis and change analysis. In considering how your programs will relate to these threats, it will be useful to consider these threats by their sources. In other words, who are the organizations, groups or individual people in your environment who might be willing and able to do you harm?

Begin by listing these groups or sub-groups of people, being as specific and particular as possible.

For example, if rebel groups are operating in your area, don't just write "rebel groups"; list them by name. If there

are multiple groups, list them each separately. They may have distinctly different capabilities and intentions toward you and your programs. The examples and names below are fictional, but the specifics are given to indicate the level of detailed information you will want to collect.

Next, list the activities that you propose to undertake. Again, be as specific and particular as you can. If a program consists of several distinct sub-activities list them all.

### Possible source of threats

- Mardonian Armed Forces
- Mardonian Freedom Front (MFF—an anti-government rebel group)
- Mardonian community
- Suremian refugee community

### Planned program activities

- Monitor arrival of new refugees at Mardon-Suremia border
- Distribute non-food items at Tatopani Refugee Camp
- Conduct Women's Empowerment/Income Development Project in Camp



Because you will want to consider how each threat source (community or rebel group) might react to each activity, a useful format is a table or matrix like the one shown below. The table's two axes allow you to graphically correlate threat sources with program activities and to think about their relationships and impacts on one another.



**Tools**

**Program Assessment Correlation Table**

Examining information in table form can help systematize your thinking and expose relationships between your programs and risk. For each box, return to the list of ways that humanitarian and development programs sometimes affect risk (as well as any factors that you may have added). Consider whether any of these apply to your situation. What are the implications for your safety? What steps will you need to take?

A further step may be useful. After listing your threat sources (community and rebel groups in this example), add a column to the table that identifies the specific threats that each group might undertake against your staff. Your table should then look something like the one below.

POTENTIAL THREAT SOURCES	PROGRAM ACTIVITIES			THREATS
	Monitor new arrivals at border	Distribute non-food items at Tatopani Camp	Women's Empowerment Project	
Mardonian Armed Forces	Potentially requires transit through conflict areas Warring parties aware of/accept our presence? Adequate marking and visibility? Adequate information prior to departure?	None	None	Small arms/cross fire Aerial or artillery shelling/bombardment
MFF	Same as above		May challenge traditional Mardonian gender roles Information program Community outreach and education?	Small arms/crossfire Direct (targeted) armed attack Kidnapping
Mardonian Community		May perceive that refugees get preferential treatment—need to monitor this Mass information program Find out which agencies are helping local community	As above	Banditry and theft Individual attack
Suremian Refugee Community		Tension may arise if supplies insufficient or distribution not carefully planned		Crowd/mob violence Individual threats against staff members



Why is this additional detail important for us? Look at the example activity of Women's Empowerment Project. Notice that this activity has approximately the same potential effect on MFF Rebels as on the local Mardonian community. But now look at the specific threats (against your staff) that each is capable of carrying out. Which threat would be of more concern to you? The effect of a given program might be the same for different groups, but taking into account the group's capabilities and inclinations, the actual impact on your risk could be very different.

The immediate goal of program assessment is to identify areas where your programs may impact your risk. The next step will be to do something about it. In the table above you can already see some indication of the kind of measures that might be needed to reduce your risk. *Chapter 8 – Risk Reduction Measures* will cover preventive and mitigating measures in more detail.

## Summary



### Key Points

**Program assessment** is the systematic approach to determining the relationship between planned or ongoing humanitarian activities and the threats, vulnerability, and overall risk the organization will face in carrying out those activities.

---

Humanitarian and development programs sometimes *increase* risk when:

- Programs require staff to travel into high-risk areas.
- Programs benefit—are perceived to benefit—some groups and not others.
- Benefits are perceived to be spread unevenly.
- Programs create temptations for bandits or criminals.
- Employment, contracts and other issues with financial implications increase tensions.
- Program aid finds its way to belligerents.
- Programs challenge customs or traditions or beliefs.
- Programs are misperceived or not fully understood.
- Programs encourage aid dependence.

---

Humanitarian and development programs sometimes decrease risk when:

- Programs provide lifesaving assistance.
- Programs support long-term peace, stability and development.
- Programs enhance the credibility, image and acceptance of your organization in the field.

---

The timeframe for considering risk associated with program activities should also be considered. Programs aimed at promoting long-term stability, and therefore a more secure safety environment, may have short-term effects that cause immediate increase in tensions and reduce staff safety.

---

A simple tool and process for carrying out program assessment is the correlation of program activities and sources of threats (usually groups or sub-groups in the community) using the *Program Assessment Correlation Table*.



## Chapter 6

### Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*.

- T**  **F** 1. The fact that programs are humanitarian in nature does not automatically mean that these programs will be low-risk activities for humanitarian field staff.
- T**  **F** 2. Programs that distribute relief items or services that are highly valued by the community will not increase security risks to staff.
- T**  **F** 3. Programs that challenge traditional beliefs or norms may increase the risk to staff carrying out the programs.
- T**  **F** 4. Projects that reduce risk to staff in the short term will always reduce risk in the longer term.
- T**  **F** 5. Criticality assessment answers the question: "What humanitarian activities are most important today?"

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following humanitarian programs would tend to result in increased risk to program staff?
  - A** Programs that require staff to travel into high-risk areas.
  - B** Programs that benefit some groups but not others.
  - C** Programs that are perceived to spread benefits unevenly.
  - D** Programs that create temptations for bandits or criminals.
- 7. Which of the following are good illustrations of the importance of considering the timeframe (short- and long-term) of risks associated with your project?
  - A** Building girls' schools that challenge traditional norms, may lead to long-term security while increasing risk to project staff in the short term.
  - B** Building girls' schools in a way that provides income to the locally unemployed may lead to short-term security, while increasing risks to staff when the project is ultimately ended and workers are to be laid off.
  - C** Building schools that benefit some groups and not others (e.g., a certain ethnic group).
  - D** Building schools to suit local norms and practices.



Self Test

Chapter 6

Self-Assessment Questions (continued)

8. Which of the following are steps required for setting up a basic program assessment correlation table?
  - A** List the vulnerabilities of your own organization.
  - B** List the historical threats against your own organization.
  - C** List the groups or sources of threats against you in the community or area.
  - D** List the program activities that you plan to undertake.
  
9. Which of the following steps is proposed in the text to further improve your program assessment correlation table to be more useful to your overall SRA?
  - A** Add a column with explanation of source information for your assumptions.
  - B** Add a column with the specific threats you could expect from each group or source in relation to the effects of each planned activity.
  - C** Add a row with specific vulnerabilities of each group or source of threat.
  - D** Add a row with specific quantities of humanitarian goods or services to be delivered.
  
10. Which of the following programs would be expected to reduce risk to your staff (in either the short or long term)?
  - A** Programs that clearly provide lifesaving assistance to the community.
  - B** Programs that support long-term peace, stability and development initiatives.
  - C** Programs that enhance the credibility, image and acceptance of your organization.
  - D** Programs that bring modern changes to outdated community norms.



Chapter 6  
Answer  
Key

- |    |   |     |            |
|----|---|-----|------------|
| 5. | F | 10. | A, B, C    |
| 4. | F | 9.  | B          |
| 3. | T | 8.  | C, D       |
| 2. | F | 7.  | A, B       |
| 1. | T | 6.  | A, B, C, D |

# Chapter 7

## Risk Assessment and the Risk Matrix

*Japanese NGO representative working with team to develop a risk matrix for their operations in Southern Sudan, in a UNHCR eCentre SRM workshop held in Tokyo, Japan in 2008.*



N. Shimazaki, UNHCR eCentre

In the preceding three chapters we looked in detail at the elements that make up Threat, Vulnerability and Program Assessment. With these in place, we are now ready to construct an overall picture of your organization's risk.



### Learning Objectives

The goal of risk assessment is to help you better prioritize and adequately plan for the variety of threats you may face in the field. In this chapter you will learn a basic process for analyzing risk based on your threat, vulnerability, and program assessments. In particular, you will learn:

- The concept of the "Risk Equation" and its key components; **risk, likelihood, and impact.**
- A standard set of definitions for describing impact and likelihood.
- A method for using these elements to prioritize areas for risk reduction using the **risk matrix.**
- Some practical guidance on developing and updating your risk matrix.
- Some common forms of bias that can occur when analyzing risk.



## 7.1 Understanding Risk

The term **risk** implies uncertainty. Every action we undertake entails some risk; *we can never eliminate risk completely*. For example, imagine that because of a fear of flying in airplanes, you were to resort to driving to a distant city instead. That option entails risks as well. The actual chances of being seriously injured or killed in a road accident are greater than the chances of being in an airplane crash. You might then decide to just stick to walking, but would still face some degree of risk, e.g., encountering a mugger. In the end, you might be tempted to think that locking your door and never leaving your bed would eliminate risk, but even that could not guarantee your safety from, say, an earthquake. Finally, if you never left your bed you would ultimately suffer from atrophied muscles and related illnesses that would considerably reduce your lifespan (to say nothing of quality of living). In the long run this would be a much riskier strategy than simply boarding the airplane and flying.

While it is impossible to completely eliminate risk, the goal of risk management is to reduce it to tolerable levels. Generally, this includes removing any **unnecessary** risk—by not doing things that are plainly foolish, reckless or otherwise disproportionately dangerous relative to the potential benefits; and managing residual risk; i.e., by taking appropriate mitigating measures. But first we must find a way of assessing the degree of risk that we are facing.

### Assessing risk

We have seen that an organization’s risk is affected by both the threats it may encounter and its own vulnerability to those threats (including in the latter the weaknesses or strengths resulting from the programs that it implements). We expressed this relationship with the formula, **threat x vulnerability = risk**. For example, if an organization is located in a country where the threat of bomb attack is high, but all staff of the organization live and work within a highly fortified compound, then the risk of staff being injured by a bomb attack might be relatively low (high threat but low vulnerability). Alternatively, if staff members work in an office that is weakly protected, but where bombings rarely or never occur, then overall risk might be similarly low (high vulnerability but low likelihood of threat as well). However, if an office is vulnerable and is located in an area with a real threat of bombings, the office may face a high level of risk.

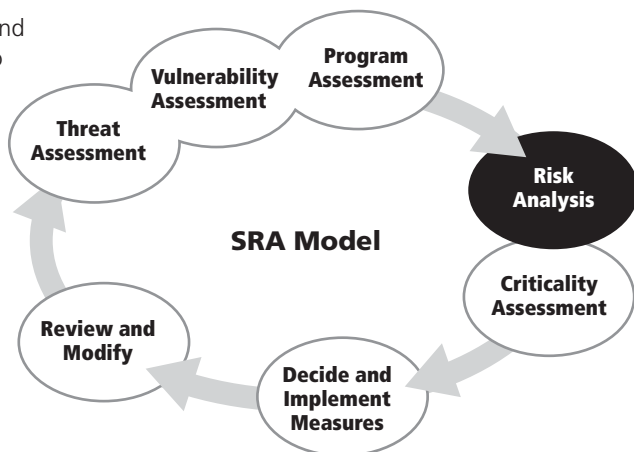
Now we look at risk in a slightly different way by asking two fundamental questions:

- What are the chances that something bad will happen?
- How bad will the result be if it does happen?

These two aspects of risk are simply referred to as **likelihood** and **impact**. Consider the definitions below from the Conference Room Paper 3 of the United Nations Security Management System Network Steering Group, (Prepared by DSS), Geneva, Switzerland 12-14 November 2008:

**Risk** The combination of the **impact** and **likelihood** for harm, loss or damage to the United Nations system from the exposure to threats. Risks are categorized in levels from **very low** to **very high** for their prioritization.

**Risk assessment** The process of identifying the threats which could affect UN personnel, assets or operations and the UN’s vulnerability to them, assessing risks to the UN in terms of likelihood and impact, prioritizing the risks and identifying mitigation strategies and measures.





It is clear from these definitions that a true understanding of risk must be based on an understanding of the threats in the working environment and their likelihood. This underlines the importance of threat assessment, and the historical and pattern analyses presented earlier. Similarly, vulnerability analysis is required to understand how much damage might be done if a particular threat event does occur. *Program Assessment* informs both of the other two activities and so all three taken together prepare the working platform for *Risk Analysis*.

In order to make some sense out of the various threats and our vulnerabilities to them, we need to assign some levels or values in order to relate them to one another. This will allow us to prioritize threats in our planning and identify key areas where we need to reduce our vulnerability.

## 7.2 Determining Impact

**To determine impact** you ask the question: “how bad would it be if the event happened?”

How much damage to your staff and property would result? How would your operation be affected? These questions are, to a certain extent, subjective, and different people will respond in different ways. This is because people have different information, and also because people do not always perceive the impact of an event in the same way. These differences are not necessarily bad; insights gained from discussion of the divergences can be enlightening. Nevertheless, we should seek to reduce problems caused by simple differences in interpretation of the question or terminology. To do this, it helps to have a common language of shared terms with agreed meanings when talking about risk. For example, the UN Security Management System has adopted a system that describes impact using the five one-word descriptors shown below.

DESCRIPTOR	DEFINITIONS
<b>Negligible</b>	The consequences may result in <i>minor disruption</i> to the organization’s activities.
<b>Minor</b>	The consequences may result in some <i>minor injuries</i> to staff, <i>possible damage or some loss of equipment</i> and facilities and/or limited delays to activities.
<b>Moderate</b>	The consequences may result in <i>injury to staff, some loss of equipment and facilities, and/or delays to activities</i> .
<b>Severe</b>	The consequences result in <i>severe injury to staff, significant loss of equipment and facilities</i> , and/or <i>major delays</i> and possible cancellation of activities.
<b>Critical</b>	The consequences are <i>catastrophic, resulting in death and severe injury to staff, major loss of equipment and facilities, and/or cancellation of activities</i> .

Even with these standard definitions, there is room for subjective assumptions about the results of any given threat and the relative vulnerability of your office and staff to that threat. Nevertheless, the terms above provide a common language that is especially useful if several staff members in an office, or partners in an area, are undertaking the assessment together.

Several things to note when you determine impact:

- The descriptors above show possible impacts on staff, property and programs. As a rule, you should **classify an event at the highest level of impact that applies to any one of these three categories**; e.g., a form of theft that is assessed to have a moderate effect on property and operations, but no particular effect on staff’s physical safety, would be classified as having overall moderate impact.
- In considering the impact of a given event, you should **take into consideration any mitigating measures currently in place**. For example, the impact of a bomb outside your office might be assessed as moderate or even minor if you have appropriate protective



measures—distance or perimeter walls. However, do not include any measures that you expect to undertake in the future. A risk assessment is a snapshot in time, and the moment that you are “photographing” is right now.

- You may come to a situation where opinions diverge sharply over likely impact, because more than one distinct scenario can be imagined. For example, “traffic accident” could mean a small urban “fender bender” where heavy city traffic prevents speeds capable of causing major damage; or it could mean a high-speed collision on a six-lane superhighway. In such cases you probably need to **break down your scenarios into distinct threats**: e.g., “urban traffic accident” and “highway traffic accident,” and consider each separately.



For this exercise imagine a small field office in a rural area with very limited medical facilities or other immediate assistance providers. Using the descriptors for impact from the chart on the previous page, match each of the short descriptions of possible threats with the best-fitting descriptor. Read each scenario, making any further assumptions that you need to make your decision, and fill in the descriptor of impact that you feel best reflects each one.

POSSIBLE THREAT Scenario	Impact DESCRIPTOR
1) A suicide bomber walks into the waiting room of your office and successfully detonates a bomb, killing several people and destroying the office.	
2) An unarmed child soldier appears at the doorway of your office and demands money and food from the office secretary.	
3) A checkpoint guard on the road to the project site detains your staff and their vehicle for thirty minutes before letting them proceed to the site.	
4) A road accident in the middle of town results in crumpled fenders and an argument with local townspeople.	
5) A high-speed road accident on the main highway results in several broken bones and lacerations to your Program Officer’s head and hands.	
6) An un-armored car traveling on the main road comes under small arms fire from a lone gunman.	
7) An armored car traveling on the main road comes under small arms fire from a lone gunman.	
8) An angry mob riots outside the office and breaks the windows, threatens the staff, and refuses to leave the office compound until their demands are heard.	
9) An angry mob riots outside the office and burns it to the ground, killing three staff members.	
10) Pickpockets in the local market steal the twenty dollars from the pocket of your Procurement Officer, who becomes nervous and a little embarrassed.	

### 7.3 Determining Likelihood

To determine likelihood you ask how probable it is that a threat event will occur. Most practitioners find that agreeing upon likelihood is usually more difficult than determining impact. While you may be able to visualize clearly the result of an event, assigning a likelihood value requires many assumptions. As you can imagine, a good assessment of likelihood also depends greatly on the quality of your information (historical, pattern and change analysis are all important here).



Ultimately, however, potential perpetrators of bad acts think and act on their own terms and reasons, or even whims. Predicting the likelihood of other's actions can never be 100% accurate.

As in the case of impact, it is useful to have standardized terminology for assessing likelihood. Below are the five likelihood descriptors used by the UN Security Management System, and their definitions. The likelihood descriptors still leave room for subjectivity, which is not necessarily bad if it leads to discussion of differing information and perspectives. Use of these descriptors will also help in providing a common language to facilitate the process of clarifying risk.

DESCRIPTOR	DEFINITIONS
<b>Very unlikely</b>	The consequences may result in minor disruption to the organization's activities. This event has a very low probability of happening to the target group under the prevailing conditions. Normal precautions and monitoring the situation for changes are warranted.
<b>Unlikely</b>	This event is considered to have a low but reasonable probability of happening to the target group under the prevailing conditions. Effort should be made to reduce this probability and/or mitigate the impact of the event.
<b>Moderately likely</b>	This event is considered to have a significant probability of happening to the target group under the prevailing conditions. Significant effort is required to reduce this probability and/or mitigate the impact of the event.
<b>Likely</b>	This event is considered to have a high probability of happening to the target group under the prevailing conditions. High priority should be given to efforts to reduce this probability and/or mitigate the impact of the event.
<b>Very likely/ imminent</b>	This event is considered to be imminent and will occur. The organization must take immediate and extreme measures to protect itself, e.g., evacuate to a safer location if the impact of the event warrants it.

In considering likelihood, it is very important to **define the target group of your analysis carefully and correctly**. In other words, it is likely that the event will happen *to whom?* Normally, the answer will be to your office and staff, or possibly to your office and staff plus immediate partners. For example, imagine that you work near a conflict area and are considering the possibility of being exposed to shelling. The likelihood of it occurring in the near future may be almost certain, but this does not mean it will directly affect you or your staff. The question you should ask is "what is the likelihood of this event (shelling) happening to my staff?"

As mentioned, the target group may be expanded to include partner agencies. **Remember that the wider your group, the less exact your results will be.** This is because different groups may have significantly different vulnerability profiles, and considering them together will only tell you an average likelihood, which may not be particularly descriptive of any one group. Note that for this reason we do not recommend including your beneficiary population in the analysis group of your staff risk analysis. This is not because we value the lives of the people we are seeking to help less than those of our staff; indeed in later chapters we will discuss how SRA techniques may be used as tools to analyze their needs as well. The simple fact is that affected populations usually present a significantly different vulnerability profile from humanitarian staff, and mixing the two together in your analysis will not yield useful results for either.

As with impact, **consider likelihood in light of all preventive and mitigating measures currently in place.** For example, if you maintain regular contact with officials and carefully avoid areas designated as unsafe, this will probably reduce the likelihood of staff being exposed to shelling, and should be reflected in your likelihood analysis.



Using the descriptors for **likelihood** from the previous table, match the short descriptions of **possible threats** with the best descriptor. This is the same situation described in the previous exercise—a small field office in a rural area with very limited medical facilities or other immediate assistance providers. For each possible scenario, make any assumptions that are needed to make your decision about the relative likelihood of each event. Write in the impact descriptor you feel best reflects each one.

POSSIBLE THREAT Scenario	LIKELIHOOD Descriptor
1) A suicide bomber walks into the waiting room of your office and successfully detonates a bomb, killing several people and destroying the office.	
2) An unarmed child soldier appears at the doorway of your office and demands money and food from the office secretary.	
3) A checkpoint guard on the road to the project site detains your staff and their vehicle for thirty minutes before letting them proceed to the site.	
4) A road accident in the middle of town results in crumpled fenders and an argument with local townspeople.	
5) A high speed road accident on the main highway results in several broken bones and lacerations to your Program Officer's head and hands.	
6) An un-armored car traveling on the main road comes under small arms fire from a lone gunman.	
7) An armored car traveling on the main road comes under small arms fire from a lone gunman.	
8) An angry mob riots outside the office and breaks the windows, threatens the staff, and refuses to leave the office compound until their demands are heard.	
9) An angry mob riots outside the office and burns it to the ground, killing three staff members.	
10) Pickpockets in the local market steal the twenty dollars from the pocket of your Procurement Officer, who becomes nervous and a little embarrassed.	

This was probably a much harder exercise to complete than the previous one concerning impact. The likelihood of such threat events actually happening obviously depends on where you are, what time of year it is, local political events, and the general situation. Your threat pattern analyses (described in Chapter 4) provide one way to undertake this part of risk analysis. This is true for all types of threats. For example, if you work in the Caribbean Sea region, you might say the likelihood of a dangerous hurricane is *likely* in August, but *unlikely* in January. The patterns of hurricane formation in this region are clearly understood.

There may be similar patterns for other non-natural threats as well. Do guerillas become active in the spring to make new incursions into government-held areas? Has the pattern been that theft (and violence) rises at the end of winter as the population consumes the end of their annual food stocks? Are you more likely to be taken hostage in Japan or Somalia? In every instance, the local situation dictates the answer, and this analysis must be made with those who are well-informed and familiar with the day-to-day realities and threat patterns in the local areas concerned. There is no one right answer to this kind of exercise without providing the detailed specifics of the security context—it all depends on the underlying threat assessment.



## 7.4 The Risk Matrix

After identifying the threats you face and ranking them for *likelihood* and *impact*, you are ready to deal with *risk assessment*. What is needed is to present both aspects of risk—the likelihood of the threat occurring and the resulting impact—at once. You can do this by indexing them against each other in a matrix. Begin by listing the threats generated from your threat assessment.



### Example

#### Threat list with *likelihood* and *impact* rankings

This example lists the threats that were encountered at one duty station and the level of impact and probability that staff assigned to each. This is only an example. The rankings are not the “right” answers for all situations and will vary according to time and place.

THREAT	Assumptions or reasons for rankings	IMPACT Level	LIKELIHOOD Level
A) Theft of office supplies	Office staff have noted this is an almost daily, ongoing problem, therefore, likelihood is ranked certain. So far, only small items have been taken.	Negligible	Very likely
B) Accidental fire in the office	Office maintenance staff member demanded that this be put on the list of threats. He says the kerosene heater is dangerous, that expatriate staff members always add too much fuel and are careless.	Minor	Moderately likely
C) Large political demonstration at the office	These events have occurred before, often with severe damage to buildings and vehicles, although no one has been killed in the past. With a major election next month, national staff expect at least one big demonstration. Your office is just opposite the park where these demonstrations often occur, and they feel it could become a target.	Severe	Certain/imminent
D) Riot at the food distribution center	Programme staff say that the ongoing food distributions may be delayed this month due to shortage reports coming from your procurement officer. Last year in a similar situation, there was a riot, in which two national staff members sustained minor injuries.	Moderate	Very likely
E) Attack on staff member by angry beneficiary	Some field staff say the policy of removing beneficiaries from the distribution lists after 12 months is making them angry. There have been threats, and field staff say they are afraid they may be carried out once people are actually dropped from the lists next week.	Moderate	Likely
F) Stone throwing by children	Children in the town often throw stones at cars as they pass by. These are small children and they are simply misbehaving says the Community Welfare officer. Nevertheless, someone could get hurt.	Minor	Likely
G) Multi vehicle accident in town	These accidents are frequent; most organizations in the town have had at least one traffic incident in this town of notoriously bad drivers. In some cases there have been broken bones, and sometimes threats from those involved.	Moderate	Very likely
H) Hostage taking	Two European staff from a partner NGO were kidnapped last year. Though released after several weeks, there were threats to kill both.	Critical	Moderately likely
I) Kerosene theft from drums in office compound	This threat still exists since fuel was stolen last year and a general fuel shortage persists; however, spring is coming soon and there will be less need for kerosene. Furthermore, a guard has now been assigned to watch, so it is unlikely that someone would try again.	Negligible	Unlikely
J) Landmine strike	There are mined areas in the project area, and local people have been seriously wounded, and in some cases killed; however, sites are well marked, and after last month's landmine awareness training, staff know to avoid these areas completely. Though unlikely, a strike could still happen.	Critical	Unlikely



Displaying your analysis in a list format as above can be useful, but it is still difficult to prioritize risk among the various threats in this format. Now look at the example risk matrix presented in the exercise below. The same descriptors from the list above are presented along the two axes of the matrix. The five descriptors for impact are shown along the vertical axis and the five descriptors for likelihood across the horizontal axis. This lets us record both the degree of likelihood and probable impact within a single framework for a more complete understanding of overall risk. These threats should now be placed on the matrix based on their rankings for both likelihood and impact.



Use the sample risk matrix below to plot each threat listed above in its appropriate place in the grid. Write in the letter and a few key words to identify each threat (A-J) on the matrix below. The correct answer is shown at the end of this chapter. *Note: These threats are illustrative and do not necessarily represent any particular area or operation.*

<b>THREATS</b>	<b>Unlikely</b>	<b>Moderately Likely</b>	<b>Likely</b>	<b>Very Likely</b>	<b>Certain/ Imminent</b>
<b>Critical</b>					
<b>Severe</b>					
<b>Moderate</b>					
<b>Minor</b>					
<b>Negligible</b>					



**Question**

*In which part of the matrix do you find the highest-risk threats?  
Which threats would you prioritize as requiring immediate attention?  
Why?*

---



---



---



---



---



---



## Determination of risk level using the risk matrix

When risk analysts use the risk matrix, they usually look to the upper-right area to identify their highest priorities. This is because these threats represent the greatest combined value of impact and likelihood and, therefore, have the greatest overall risk. These threats are usually considered *very high* or *high* risk. Greatest priority should be given to finding ways to prevent or mitigate them.

Which threats would you prioritize next? Opinions among professional security officers differ on this. Some look to the top-left, saying that a *very high-impact* but *low-likelihood* threat should be dealt with next as the result would be catastrophic should they occur. Others look at the bottom-right section, saying that *high-likelihood* but *low-impact* threats, if not dealt with, will eventually have a cumulative effect that could be as bad as a single dramatic incident. What is clear, however, is that these areas represent the next area of focus—*medium risk threats*—and should be dealt with after considering the very high and high-risk threats.



### Tools

The guideline below can be used to assign a risk level to each threat on your risk matrix. Once again the point of such a system or tool is to begin using a standardized language and approach so that different threats can be compared and ranked for prioritization in your overall risk management task.

RISK ANALYSIS TABLE		LIKELIHOOD				
		Unlikely	Moderately Likely	Likely	Very Likely	Certain/Imminent
IMPACT	Critical	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
	Severe	LOW	MEDIUM	HIGH	HIGH	VERY HIGH
	Moderate	VERY LOW	LOW	MEDIUM	HIGH	HIGH
	Minor	VERY LOW	LOW	LOW	MEDIUM	MEDIUM
	Negligible	VERY LOW	VERY LOW	VERY LOW	LOW	LOW



### Exercise

#### Risk Level for Identified Threats

Now compare the risk matrix that you completed in the exercise above to this guideline. What is the risk level for each threat on the matrix? Write in the appropriate risk-level descriptor from the above guideline after each threat (A-J).

Threat	Risk Level
A – Theft of office supplies	
B – Accidental fire in the office	
C – Large political demonstration at the office	
D – Riot at the food distribution center	
E – Attack on staff member by angry beneficiary	
F – Stone throwing by children	
G – Multi-vehicle accident in town	
H – Hostage Taking	
I – Theft of kerosene from the drums stored in the office compound	
J – Landmine strike	

The answers for this exercise are at the end of this chapter.



## 7.5 Practical Guidance on Using the Risk Matrix

You have now learned the steps required for setting up a systematic and graphic way to assess the risk of various threats in your working environment and to communicate your analysis to others. The idea is simple, but, several practical measures should be taken in using this analysis in the field.

### *Some practical tips on drawing up your own risk matrix*

- The risk matrix is an especially useful tool when used with other staff or partners. Conducting this analysis with a group of people with different expertise or backgrounds can bring new information and helps overcome individual biases.
- The Risk Matrix is a flexible tool that can be used at different scopes and scales. National-level managers may need to do the exercise at the country level to set overall program budgets and to plan appropriately. Smaller offices in remote districts may be more concerned with their day-to-day operations and will only need to analyze threats within the scope of their own local situation.
- If you are in a fairly dangerous area, and you are trying to determine how best to carry out your operations under local threats, you should focus specifically on the area(s) in which you work. However, remember the principle of change analysis discussed in Chapter 4. If threats are moving your way from other areas, you want to know about them—**before they start involving your staff**. The only way to accomplish this is to include the areas on the periphery of your own immediate working area in your analysis.
- Try to conduct the exercise on a large sheet of paper on the wall so everyone can see it and express their views. Cards, tape and “Post-It” sticky notes are ideal for listing the threats and placing them on the matrix, so that they can be repositioned easily if needed.
- When people begin to place the various threats on the matrix, they frequently change their determination of the likelihood or impact descriptors once they begin to think of them in relative terms on the matrix. This is not a problem, and should be encouraged, as long as the final assessment is reasonable and the stakeholders generally agree.
- Remember that the goal of the risk analysis step of the SRA process is to identify and clarify the threats that require your immediate attention. The risk matrix is first and foremost a managerial tool to help you visualize and prioritize the threats you are facing. Ultimately, your aim will be to manage each threat—either, make it less likely by moving it to the left on your matrix—and/or less “impactful” by moving it down on the matrix. How to do this will be the subject of the next chapter.
- Regular revisiting of the matrix and updating will help show you trends in the overall security environment and help you evaluate if you are really reducing or mitigating your risk in any significant ways.

## 7.6 Risk Assessment and Bias

As mentioned in the beginning of this chapter, we live in a world of uncertainty, and can never eliminate risk entirely. However, people often perceive risk in dramatically different ways. This is not always a bad thing, as it can expose new information or different perceptions of impact or likelihood of a threat. However, divergences can also result from systematic errors or omissions in the way we analyze the facts.

The word for such systematic error, from a statistical viewpoint is *bias*. Such bias is perfectly normal; all human beings exhibit biases of some sort. However, this does not mean that we should simply accept bias as inevitable; we must do our best to reduce or neutralize it, and the best way to do this



is to first become aware of the bias. The following points explain some of the more common forms of bias that often appear when people analyze risk.

**Recency bias** – Similar events to those that have occurred recently may seem more likely to repeat than they really are. When a devastating earthquake occurs, for example, people often become hyper-aware of the threat of earthquakes over the risk of other threats even though seismic activity in the region may be prone to happen cyclically over a period of hundreds or thousands of years.

**Media bias** – Spectacular events are likely to receive substantial media coverage and may seem more likely than they really are. This applies to most violent crime, including terrorism. In most countries, the chances of dying in a road accident are much higher than of being killed maliciously. Various diseases are more likely still; however, these mundane dangers are unlikely to appear often in the news, and therefore may not be appreciated in their true proportion to overall risk.

**Control bias** – Events that we can control may seem less risky to us than ones beyond our control. A common example of this is the difference in perceptions of flying and driving. Flying is statistically much safer than driving, but when we are behind the wheel of our car we have the illusion of control, believing that if the situation demands it, we will be able to avoid an imminent accident. Here media bias may also play a role, as large-scale plane crashes, however uncommon, make for more dramatic news coverage, distorting the real likelihood of becoming a victim of such an event.

**Acceptance bias** – Risks that we willingly accept often seem less dangerous than ones that are thrust upon us. Smoking, investing in stocks, or applying for a dangerous field assignment may feel less risky than having to breathe second-hand smoke, having your money stolen, or being sent on a dangerous assignment without your consent.

**Impact-likelihood blurring bias** – Events that are very high-impact may seem more likely, and events that are very likely may seem to have a higher impact than they actually do. The critical impact of murder, for example, may lead us to rank it as moderately likely or even likely when it is in fact very unlikely. We may feel that since the event is “extreme,” both impact and likelihood should be high, when in fact only one factor (impact) is high. Likewise, repeated minor car accidents may lead some to incorrectly inflate the impact, thinking that “the effect of so many accidents must surely add up to a high impact!” While the idea of a cumulative effect is correct, this effect is already captured in your risk analysis by its high likelihood ranking, so considering it again on the impact side incorrectly inflates the real risk.

**Confirmation bias** – Once we hold a belief, we tend to be very reluctant to change it. This can lead us to filter out any information that would contradict our usual way of thinking and to only consider facts that corroborate our pre-conceived notions. This bias often plays a role in prejudicial assessment of other ethnic, political, or religious groups, for example. Once we hold such a bias, we will immediately seize upon facts that support our prejudiced notions while not noticing or disregarding those that contradict them. To sum it up, we tend to see only the information that supports what we already believe to be true.

Biases are normal and inevitable for all of us, but when analyzing risk, they can cause significant errors. For this reason it is important for risk managers to try to understand and overcome their own biases when making assessments. One of the best ways to do this is to conduct risk assessment with others, allowing the group process to test and expose biases when they occur.

## Summary



### Key Points

*Your risk = threat x vulnerability*

The **risk equation** and its key components, *risk*, *likelihood* and *impact*, provide the basic approach to determining and prioritizing risk of various security threats faced by an organization. The meaning of this simple equation is that risk is determined both by how vulnerable you are to each threat (and therefore how much impact it will have on you) and how likely it is that the specific threat will actually occur.

---

The UN system has *a standard set of definitions for describing impact* in order to further standardize risk analysis. In order of increasing harm, they are:

**Negligible • Minor • Moderate • Severe • Critical**

---

To further standardize risk analysis, *a standard set of definitions for describing likelihood* in order of increasing odds of the event occurring are:

**Very unlikely • Unlikely • Moderately Likely • Likely • Very likely/Imminent**

---

A useful method for analyzing risk using the descriptors above is called the Risk Matrix. This analytical tool allows users to graphically index the two risk factors into a single analysis. The results of plotting possible threats on the matrix shows clearly the ranking order of threats on the basis of their risk to the organization, and thereby provides managers a guide by which to prioritize risk reduction activities.

---

Even though the process is straightforward, responsible use of the Risk Matrix requires more than simply filling in threats on a chart. Some practical guidance on developing and updating your risk matrix is required:

- Conduct the process with a group of stakeholders who are well-informed of the security threats in the area, but who may have different perspectives and/or sources of information in order to avoid important gaps in your assessment information.
- Conduct the process in an open and flexible way that facilitates discussion and changing of the location of the threats on the matrix as required.
- Update the Risk Matrix periodically and as required by any indicators of significant change in the threat environment.

---

Biases, or systematic errors, that apply to the assessment of risk include: recency bias, media bias, control bias, acceptance bias, impact-likelihood blurring and confirmation bias. Biases are extremely prevalent, and can cause significant errors when analyzing risk. For this reason it is important for risk managers to try to understand and overcome biases when making risk assessments.

**Self Test**

## Chapter 7 Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

1. Risk is dependent on two factors; threat level and rate of change in the threat environment.
2. It is generally easier to imagine and agree on the resulting level of harm from a potential threat than it is to agree on how likely it is that it will actually occur.
3. Security risk analysis for an organization should only be done by experienced security officers.
4. The Risk Matrix should be revised every 4 years.
5. Both vulnerability to a threat and the probability that the threat will actually occur are to be considered in determining risk.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

6. Which of the following is a correct formula for risk?
- A** risk = likelihood of a threat x accuracy of the assessment data
- B** risk = likelihood of vulnerability x actual vulnerability to a threat
- C** risk = likelihood of impact x threat
- D** risk = likelihood of a threat x impact of the threat
7. Which of these descriptors are related to impact?
- A** Negligible
- B** Likely
- C** Moderate
- D** Very Unlikely



Self Test

Chapter 7

Self-Assessment Questions (continued)

- 8. Which of these descriptors are related to likelihood?
  - A Minor
  - B Moderately Likely
  - C Severe
  - D Very Unlikely
  
- 9. What is the **risk level designation** given to a threat that is plotted on a Risk Matrix with the descriptors "Critical" and "Likely"?
  - A Low
  - B Medium
  - C High
  - D Very High
  
- 10. Which of the following are true about assessment bias?
  - A Biases are systematic errors; all human beings exhibit them to some extent.
  - B Only racially prejudiced people have biases.
  - C Recency bias, media bias and control bias are examples of ways that bias can affect risk analysis.
  - D Ways to overcome bias include understanding your own biases and conducting your analysis with others.



Chapter 7  
Answer  
Key

- 5. T
- 4. F
- 3. F
- 2. T
- 1. F
  
- 10. A, C, D
- 9. D
- 8. B, D
- 7. A, C
- 6. D



## Chapter 7

### Self-Study Exercise Answers

Proposed answers to the exercise on page 84. Possible choice of impact descriptors for each threat listed along with assumptions or reasons (right column) which may differ from yours.

THREAT SCENARIO	POSSIBLE IMPACT DESCRIPTOR	ASSUMPTIONS & REASONING
1) A suicide bomber walks into the waiting room of your office and detonates a bomb, killing several people and destroying the office.	Critical	Clearly the results are catastrophic, death and severe injury with major loss of equipment and facilities. This one is clear in any context or environment.
2) An unarmed child soldier appears at the doorway of your office and demands money and food from the office secretary.	Negligible to Moderate	If the child is unarmed, this situation can probably be resolved without difficulty and the impact is negligible. If the child were armed the impact level would rise.
3) A checkpoint guard on the road to the project site detains your staff and their vehicle for thirty minutes before letting them proceed to the site.	Negligible	Assuming that there were no threats or use of violence the primary impact is loss of time. If use of violence is a possibility then impact will be higher.
4) A road accident in the middle of town results in crumpled fenders and an argument with local townspeople.	Minor to Moderate	This is a common occurrence in many cities, and routinely solved by paying for damage or by working through the local police office. If minor incidents can result in crowds forming and violence against those perceived as being at fault, then impact may be higher.
5) A high speed road accident on the main highway results in several broken bones and lacerations to your Program Officer's head and hands.	Moderate to Critical	Broken bones and significant loss of blood can lead to death, making it critical in the worst case. Most would probably rate this potential scenario as severe.
6) An un-armored car traveling on the main road comes under small arms fire from a lone gunman.	Critical	Bullet wounds and significant loss of blood can lead to death.
7) An armored car traveling on the main road comes under small arms fire from a lone gunman.	Moderate or Severe	This case is similar to #6, but due to mitigating measures (armored vehicle), you are less vulnerable. This should lower your impact, but, take note that most armored vehicles cannot guarantee stopping all projectiles in all cases or all events. Being shot at is serious, making the impact at least moderate, and probably severe.
8) An angry mob riots outside the office and breaks the windows, threatens the staff, and refuses to leave the office compound until their demands are heard.	Minor to Severe	This depends very much on patterns of previous similar events. If instantaneous disruptions often flare up and then fade without serious harm, this might constitute minor impact to the staff. If previous examples indicate that real violence could erupt against staff, this could be severe.
9) An angry mob riots outside the office and burns it to the ground, killing three staff members.	Critical	This is plainly a critical possibility. Major loss of life, facilities, and equipment are all involved.
10) Pickpockets in the local market steal \$20 from the pocket of your Procurement Officer, who becomes nervous and a little embarrassed.	Negligible	No one is hurt, and the only delay is in replacing the staff member's documents and asking for more money, or making budget cuts for the money lost.



**Chapter 7**  
**Self-Study Exercise Answers**

Correct placement of threats on the Risk Matrix for the exercise on page 86.

<i>THREATS are only illustrative</i>	<b>Unlikely</b>	<b>Moderately Likely</b>	<b>Likely</b>	<b>Very Likely</b>	<b>Certain/ Imminent</b>
<b>Critical</b>	J) Landmine strike				
<b>Severe</b>					C) Large political demonstration at office
<b>Moderate</b>			E) Knife/club attack on staff from angry individual	D) Riot at the distribution center G) Multi-vehicle accident in town	
<b>Minor</b>	A) Theft of office supplies	B) Accidental fire at the office	F) Stone throwing by children		H) Hostage taking
<b>Negligible</b>	I) Theft of fuel from compound depot				

**Risk Level for Identified Threats – Answer Key – page 87**

<b>Threat</b>	<b>Risk Level</b>
A – Theft of office supplies	Very low
B – Accidental fire in the office	Low
C – Large political demonstration at the office	Very high
D – Riot at the food distribution center	High
E – Attack on staff member by angry beneficiary	Medium
F – Stone throwing by children	Low
G – Multi-vehicle accident in town	High
H – Hostage Taking	Medium
I – Theft of kerosene from the drums stored in the office compound	Very low
J – Landmine strike	High

# Chapter 8

## Risk Reduction Measures

*UN team wearing protective body armor and helmets in preparation for a helicopter flight in Baghdad, Iraq, in October of 2008.*



We have spent considerable time analyzing threats, vulnerability, programs and risk. Security Risk Management (SRM), however, is not just an academic exercise designed to produce an elegant analysis. The ultimate aim of SRM is to help clarify the risks faced in the field so something can be done about them, enabling important humanitarian work to go on safely. This requires deciding whether your programs can continue in light of identified dangers and then implementing appropriate measures to reduce risk to a tolerable level.



### Learning Objectives

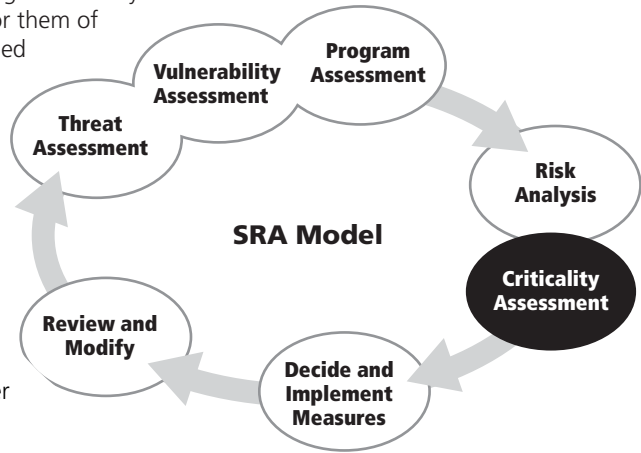
In this chapter you will learn about:

- Criticality Assessment – deciding when programs or activities are simply too risky to undertake for the resulting benefits.
- Two basic types of risk reduction measures:
  - Prevention measures
  - Mitigation measures
- The “Risk Reduction Toolkit” or set of activities and means for reducing risk in the field. This toolkit of options includes:
  - Planning
  - Coordination
  - Hardening measures
  - Deterrence measures
  - Image and acceptance
  - Communications
  - Vehicle equipment and procedures
  - Risk-transference strategies
  - Staff knowledge and skills
  - Exposure reduction



## 8.1 Criticality Assessment

**Criticality assessment** considers the importance or urgency of a planned activity, and weighs this against the risks to staff in carrying out the activity. It can be thought of as a kind of cost-benefit analysis. It starts by looking at the dangers faced by the beneficiaries and the consequences for them of either doing or not doing the envisioned program. Is the program urgent, important, and life-saving, or simply desirable? This assessment is then weighed against the risks to your own staff, as assessed previously through your SRA process.



Consider the statements below made by those who have been directly involved in such decisions. The first quote is from an evaluation of an incident in which a staff member was killed—raising the concern that criticality assessment was not done.

*“...the security of staff cannot be divorced from that of refugees and from the provision of assistance. When programme activities have already been seriously decreased by a reduction of funds and insecurity, the situation must be closely monitored in order to ensure that staff are not left in situations of potential danger where the risks outweigh the benefits to refugees.”*

– Summary Report of the Inquiry into the Death of One UNHCR Staff Member and the Abduction of Another in Macenta, Guinea on 17 September, 2000

The next quote is from the UNHCR High Commissioner, explaining his removal of international staff from the field in a different instance, in essence, by citing a criticality assessment.

*“UNHCR’s recent experience in Iraq provides a good example of the need to find the right balance. In this case, I felt I had no option but to remove all of my international staff from the country. This was a difficult decision, but in the end I came to the conclusion that UNHCR’s programmes in Iraq were indeed not life-saving and that the risks involved for my staff were too great. I also had to take into consideration the views of the Iraqi national staff, who in [the] current situation have made it known that they feel safer without the presence of internationals and who have been doing an excellent job.”*

– Letter from Ruud Lubbers to Louise Frechette, UN Deputy Secretary –General, 5 November 2003

As seen in these examples, criticality can involve life or death questions—for both staff and the people you are helping. Careful and dispassionate consideration of all the facts and good judgment are especially important at this stage of your SRA.

Broadly speaking, your criticality assessment can yield three possible outcomes.

- 1) Benefits clearly outweigh the risks; undertaking the program falls in the category of reasonable risk.
- 2) Risks clearly outweigh the benefits; the activity entails unacceptable risk.
- 3) The risk may be acceptable, but only with additional mitigating measures. In this case the manager must select and implement appropriate measures designed to eliminate unnecessary risk and manage any residual risk.



For an example of the first outcome (benefits clearly outweigh risks), consider crossing the street for a cup of coffee in a normal, well policed city. It really doesn't matter that a hot beverage is a non-essential luxury (for most at least), there is simply no (security) reason preventing you from undertaking the activity. This is clearly a "go" scenario, as are most humanitarian and development activities in peaceful countries with sufficient law and order.

For an example of the reverse (risks clearly outweigh benefits), consider the case of walking into a live minefield. There is simply no program that justifies taking this risk. Even in the extreme instance where another person is trapped in the minefield, possibly even injured, mine experts counsel that the only way to help is to call for assistance and wait for trained experts to clear a path to the victim. To cite an axiom used by firefighters, "don't bring more victims to the fire." For aid workers in conflict-affected areas, providing assistance in a location where combat is actually ongoing is usually another example of a clear "no-go" scenario: as urgent as the needs may be, you simply have to wait until the shooting stops.

If the world only consisted of scenarios like the ones above, the humanitarian manager's security risk management responsibility would be relatively simple and clear cut. Unfortunately, cases also occur where risk and program benefits must be more carefully weighed against one another. Consider the following example: it is dark, stormy and foggy outside; roads are covered with ice and visibility is close to zero. You have a sore throat and would like to go to the pharmacy to buy cough drops. Should you go? You might reasonably determine that weather conditions make the roads too dangerous, and cough drops are not absolutely essential—the criticality of your proposed activity does not outweigh the risks. You decide to stay home and drink some tea with honey and lemon instead.

Now, imagine that the weather conditions are exactly as in the situation above, but this time you have a colleague whose appendix has ruptured. If she does not receive immediate medical attention she may die. What will you decide in this case? Perhaps in this instance you will determine that the urgency of the situation now justifies the risk, and drive your friend to the hospital; however, in doing so, you also determine that you will *not* make a side-trip along the way to the pharmacy for cough drops (eliminate unnecessary risk), and will use only major, well-lit roads, wear seatbelts and drive not faster than 30 kilometers per hour (manage residual risk).

It must be underscored here that *criticality assessment is not a license to justify actions that clearly entail unacceptable risk*; as with the examples of minefields and combat zones above, there are cases where no degree of urgency can justify the program. In these cases the security risk management approach urges managers to take the steps that are necessary to ensure the safety of their staff, including stopping the program and evacuating to a safer area.

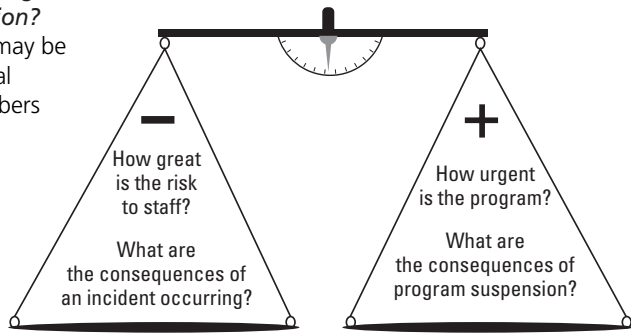
### ***How to do your criticality assessment***

Criticality assessment encourages managers to ask the following questions:

- ***How great is the risk to staff?*** What conclusions do you draw from your threat and vulnerability assessments? What is the likelihood and probable impact of an unwanted event occurring? The key to answering these questions, of course, is your risk analysis and risk matrix.
- ***How urgent are the activities envisioned?*** Here, you will be considering the nature of your programs, which you have most likely considered in detail in non-security contexts. Are they life-saving, very important, or only desirable? If you have not thought of this question before now, you may want to consider using the tools you have learned to conduct a risk assessment from the beneficiaries' points of view. This can help clarify the urgency of the needs and criticality of programs designed to address those dangers.



- *What are the short, medium and long-term consequences of program suspension?* Remember that one of the results may be increased risk to staff upon eventual return if the local community members feel they were abandoned.
- *What are the programmatic consequences of a security incident occurring?* Often an incident will cause the area to be declared "off limits" indefinitely, or until further detailed assessments and/or assurances from the host government are forthcoming.



**Are there other ways of meeting the needs that entail less risk?**

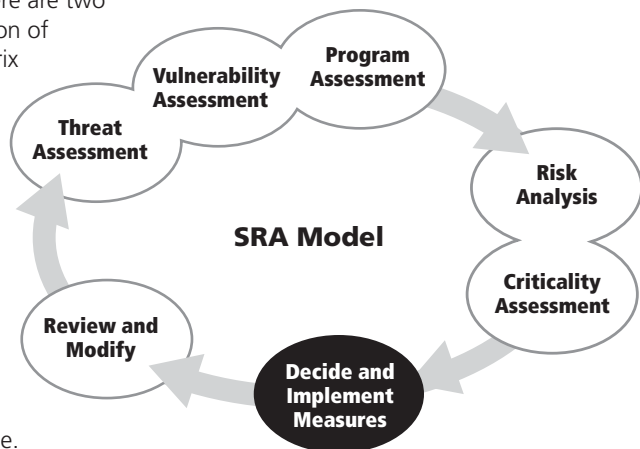
In summary, criticality analysis is a process of weighing the benefits of programs against their risks. It does not produce absolute, right-or-wrong answers, and it cannot be used to provide justification where risk is clearly unacceptable; however, it can help clarify thinking, expose strengths and weaknesses in an argument, and provide support for a decision entailing reasonable risk once it is taken. Criticality analysis is an important step in the due diligence of a humanitarian manager.

## 8.2 Types of Risk Reduction Measures

If you have made the decision that the importance of your program outweighs the dangers, additional measures are likely needed to bring risk to within tolerable levels. How will you do this? What measures and options are at your disposal?

When we think of ways to protect ourselves from possible harm in the field, we may immediately think of high walls, gates, barricades, armored cars and jackets like the ones shown in the photo at the beginning of this chapter. The SRM approach however, is designed to match appropriate risk reduction measures to the actual threats, vulnerabilities, and program aspects that you have analyzed as part of this overall process. The now-familiar diagram of the SRM cycle below shows the dependence of deciding on, and implementing risk reduction measures on the previously accomplished assessments and analysis.

As discussed in the previous chapter, there are two components involved in the determination of risk: impact and likelihood. The risk matrix tool graphically shows the relationship of these two components for all threats considered in your threat assessment. Threats with higher risk are shown in the upper-right corner of the matrix, i.e., where the descriptors for the highest impact and the highest likelihood intersect. The security risk manager's job is to find effective and achievable ways to move threats with unacceptable levels of risk to a point on the matrix where the risk level is tolerable.





This can be done in three ways as described below.

- 1) **Reduce the likelihood** that a particular threat will occur, pushing the threat to the left on the matrix. Measures to accomplish this are generally called **prevention measures**. While they generally do not absolutely prevent all possibility of a particular threat occurring (except, for example, in the case of total evacuation from the field), they are designed to significantly reduce the likelihood that they will occur, making the risk lower and therefore more acceptable. A good example of this is clearly marking (in most situations) vehicles as being humanitarian in nature. In situations where there is general acceptance of your organization, for example, flags and large decals make it clear who you are, thereby reducing the likelihood that a combatant will mistake you for an enemy and fire at you. The flags and decals do nothing to reduce the impact if shooting starts; they only serve to reduce the chance that someone will shoot at you.

- 2) **Reduce the impact** or harm that is done if the threat actually occurs, thereby pushing the threat lower on the matrix. Measures that are designed to reduce the impact of a threat are generally called **mitigation measures**. A good example of this is the use of seatbelts in vehicles. While seatbelts do not reduce the likelihood of an accident, they are designed to keep you safer should an accident occur.

RISK MATRIX		LIKELIHOOD				
		Unlikely	Moderately Likely	Likely	Very Likely	Certain/Imminent
IMPACT	Critical		Prevented THREAT	← PREVENTION		THREAT
	Severe					↓ MITIGATION
	Moderate					
	Minor					Mitigated THREAT
	Negligible					

- 3) **Reduce both the likelihood and the impact of potential threats.** In reality, many measures that can be taken have both mitigating and prevention aspects. A high strong wall around the office is a good example. The wall will reduce harm to those inside if shooting occurs outside, and the fact that there is a wall may well dissuade potential attackers from shooting at the office at all. Such measures have both mitigation and prevention components and are effective at reducing risk since they will move the threat both down and to the left on the matrix.

### 8.3 The Risk Reduction Toolkit

There are many different activities and measures than can be taken to reduce risk. Which one you choose depends on many factors including the findings from your threat, vulnerability, and program analyses, your budget, and your overall organizational security strategy. Some organizations may decide upon a core strategy of maximum prevention activities. For example, the ICRC and many of the Red Cross National Societies often forgo protective vehicles and helmets, even in dangerous areas, and rely largely on community acceptance and plain identification of themselves in the field. Other organizations, which for pragmatic or political reasons, may feel that they are already a target and that prevention strategies will not work for them, at least in the short term. They will necessarily have to depend on more protective and mitigation-based strategies.



**Exercise**

*In the spaces below, list at least two examples each of realistic prevention and mitigation measures you could implement (or already have implemented) in your own office or operation.*

**Prevention measures**

**Mitigation measures**


The *Risk Reduction Toolkit* is simply a catalogue of measures found to be useful in many areas around the world for many organizations. As you read through them, compare the measures to the answers you wrote above. While the list is not exhaustive, and other creative ideas can be identified, these ten measures are the basic tools for risk reduction:

- |                         |                                     |
|-------------------------|-------------------------------------|
| 1) Planning             | 6) Communications                   |
| 2) Coordination         | 7) Vehicle equipment and procedures |
| 3) Hardening            | 8) Risk transference                |
| 4) Deterrence           | 9) Staff knowledge and skills       |
| 5) Image and Acceptance | 10) Exposure reduction              |

The brief descriptions that follow comprise your risk reduction options or toolkit. Your organization may not have the ability to apply all of these measures, nor may it need to. What is important is that you consider your actual situation in the field and then **survey all of the possible tools at your disposal**. You will only need to use as many as are required to reduce your risk to an acceptable level. Note that the list below is not a sequence, nor are the “tools” shown in any particular priority. A comprehensive response to most high security risk situations will often entail a mix of some or all of the ten tools described below.

- 1) Planning** is basically intended to help you foresee potential security threats and problems and reduce emergency response time. When security planning is done jointly with partners, it can facilitate a concerted response (see coordination below).
- An **office security plan** contains basic information such as identification of key people with security responsibilities, analysis of the situation and threats, and basic steps to be taken in the event of a security incident. Updated staff lists are usually included as an annex. *Every office, no matter how small, should have a security plan*, although the amount of detail can vary according to the needs of the office.
  - Specific security **scenario-based contingency plans** explain how the office will respond to scenarios that have been identified as being particularly important in the risk analysis process. They can be included as annexes in the overall security plan.

The American General Dwight D. Eisenhower once said “Plans are nothing; planning is everything.” What he meant was that the value gained from the planning process itself—meeting with partners, identifying problems, brainstorming options—is often more important than the document that results from the process. Knowing who your partners are and how they will react in case of a serious security event can be critical to your own safety and security as well. More detailed information on security planning is presented in *Chapter 9 – Security Plans and Planning*.



**2) Coordination** with other actors in the field serves two important security functions. It can help you obtain important information that affects your security before it is too late, and it can facilitate quicker, more concerted emergency response/rescue in the event of an incident.

Coordination measures can be both external and internal:

- **External coordination** includes critical partners such as *host government counterparts, other humanitarian or development agencies, local community leaders, and your program beneficiaries*. Do you have linkages in place to ensure that critical security information gets to you in time from these sources?
- **Internal coordination** includes establishing a *warden system*, or information tree, to ensure that all staff can be contacted immediately in the event of an emergency and know what to do. Remember to test the system regularly once it is in place. An outdated staffing list can actually slow down response time and introduce chaos into your emergency response.

**3) Hardening** usually comes to mind first when thinking about security measures. Hardening (or protective) measures are intended to make it more difficult for an attacker to harm you (hopefully preventing them from even trying) or to mitigate the effect of an attack if it occurs.

A few common hardening measures include:

- A strong perimeter enclosure—wall or sturdy fence.
- A sturdy gate and lock.
- Strong building materials (concrete or brick) with sturdy locking doors.
- Shatter-resistant film on exterior glass windows.
- Steel bars on external windows.
- A bunker or safe room inside the office or compound provisioned with emergency supplies.

Hardening measures may also have disadvantages:

- They may be equipment-intensive and therefore expensive.
- They may work in opposition to image and acceptance strategies (see below).

Still, some hardening measures are almost always part of a comprehensive security strategy.

**4) Deterrence** suggests that not only will it be hard for attackers to harm you, but that there will be some reprisal in response. For example, ballistic blankets and bullet-proof glass in a vehicle are considered hardening measures, but a police escort for the vehicle is a deterrent. If attacked, the police will fight back. What kinds of deterrence do humanitarian agencies have at their disposal?

- **Guards** may be appropriate or necessary and can include any of the following:
  - Unarmed guards, either recruited locally or provided by a reputable security firm.
  - Armed guards, provided by a reputable security firm.
  - Guards specially provided by the host government.
  - Local police.
  - Police or military escorts for road movements.
  - Host government military forces.
  - International military forces (e.g., UN Peacekeeping Forces).
  - In certain cases, other military forces (e.g., forces of a specific faction controlling the ground where you are operating, or a national armed force operating in your area).

Note that using guards involves important considerations such as the level of training and awareness of guards, the impact on your mission and mandate and the impact of your cooperation on perceptions of impartiality and neutrality.

- **Program suspension** or sometimes just the threat of suspending your program (or pulling out altogether) can be a form of deterrence to threatening behavior. It can also be an influential bargaining point in negotiating support with local authorities for improved protection. But remember, in cases where perpetrators are hoping their acts will force you to leave, program suspension is not a deterrent at all.



**5) Image and acceptance** strategies are purely preventive and aim to decrease the likelihood of an attack by reducing the potential attacker's desire to do harm to you or to your agency. Note that the term "acceptance" has a double meaning in the risk management context: among humanitarian agencies it has come to mean the receptivity of a population to the agency's staff and programs. However, in the professional risk management industry, it is sometimes used to refer to a person's "risk tolerance"; that is, the degree of risk that they are willing to accept. For this reason the term "hostility avoidance" is also used to refer to generic strategies aimed at reducing ill will toward aid workers. Common strategies include:

- A clear and proactive public information campaign to explain the agency's programs.
- Regular and positive interaction with the local population.
- Programs that benefit the population and that distribute benefits fairly and transparently.
- Staff behavior that respects cultural norms.

As noted, image and acceptance strategies may sometimes be considered to be in opposition to hardening strategies. In such cases, managers must balance the advantages and disadvantages of each measure in the context of their specific situation and the operation as a whole.

**6) Communications equipment and procedures** give you the ability to communicate quickly and clearly — a cornerstone of field security. This is so critical for humanitarians working in dangerous field environments that it merits special attention. Important questions to ask include:

- Do I have an assured means of *communicating with all my staff* in an emergency, and can they reach me?
- Do I have a way of communicating with *critical partners* and *headquarters*?
- Do staff members working in *areas at risk* have a means of communication with each other?
- Do I have reliable communications with staff members during *road travel*, where they are often at particular risk?
- For all of the above, is there a *backup means of communication*? In areas of particularly high risk this may be a minimum standard.
- Is communication equipment well maintained? *Do all staff members know how to operate it?*
- Are there appropriate communications *protocols/procedures* in place, and does staff know and comply with them?

You should consult a telecommunications and/or security officer for more detailed advice in this highly technical area. Some common communications solutions include:

- Landline telephones (Is the network reliable in your area?)
- Mobile/cellular telephones (Remember, the network is likely to become overloaded and may collapse during a large-scale crisis!)
- VHF and HF Radios (Are you familiar with the range/terrain limitations? Are additional base stations or repeaters needed?)
- Satellite telephones (Is there appropriate satellite coverage in your area?)
- Various data transmission systems

**7) Vehicle equipment and procedures** – Like communications equipment, vehicles deserve special attention due to the generally recognized high vulnerability of staff during road travel in dangerous areas. Key questions to ask (the answer should be "yes" in each case):

- Are your vehicles appropriately chosen and equipped for the threats in your area?
- Are they appropriate for the terrain and natural hazards?
- Are there appropriate procedures in place, such as a mission tracking system?
- Do staff members know what emergency actions are to be taken in the event of an incident?
- Do drivers have appropriate training?



**8) Risk transference** refers to measures designed to shift risk to another party. The example of risk transference that is most familiar to most of us is the use of insurance; in exchange for a monthly fee or premium, we transfer liability for a potentially costly event to the insurer. In humanitarian activities risk transference is used when you hire a trucking company to transport food into dangerous areas or seek the intervention of security forces to handle a potentially violent situation. In these cases the risk does not go away, but someone else has to face it.

Risk transference strategies have advantages and cautions. They may be appropriate when:

- The party to whom you are transferring risk is mandated or better equipped to deal with the risk (as in the case with law enforcement above).
- Your transfer of risk distributes it among many, thus reducing it to acceptable levels for all.
- A number of parties are sharing in the benefits of a particular program where it may be appropriate for them to share the risks equally.



**Question**

*Why not transfer all risk to other partners? Can you list any reasons why you would not want to transfer your risk to others if the humanitarian objective of your mission could still be achieved?*

---



---



---

Risk transference has obvious benefits for the transferring organization that thereby lowers its risk. However, there may be political, managerial and ethical considerations as well:

- Risk transference may result in loss of control and quality of the work or program.
- It may result in transference of some of the benefits, e.g., from positive publicity of the program.
- There may be significant issues of responsibility and accountability for the well-being of those assigned to do the work, both morally and, in many instances, legally.

**9) Staff knowledge and skills** – Staff who are knowledgeable and alert about security risks and procedures are more likely to avoid security incidents, or to handle them effectively when they occur. What specific knowledge or skills are most important for security management?



**Question**

*List the specific knowledge and skills that field staff need to know in order to reduce their risk in a dangerous field environment.*

**Risk reduction knowledge**

**Risk reduction skills**

<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>



**Risk reduction knowledge**

**Risk reduction skills**

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Your answers may include topics and locally appropriate skills (e.g., local language skills) associated with your specific location or field security environment. Better informed and more skillful staff will be safer staff. The more they understand and are equipped to respond to their security environment, the less risk they will face. Increasing this understanding and improving the response skills required are important parts of a comprehensive risk reduction strategy. Some important knowledge and skill areas include:

- Briefing and understanding of the general environment, its threats and risks.
- Knowledge of the specific local security plan.
- Knowledge of generic responses and procedures for specific contingencies. (e.g., general landmine awareness training).
- Knowledge of specific procedures to follow in event of particular contingencies (i.e., standard procedures determined in your contingency planning).
- Security risk assessment and management skills (e.g., this course).
- First aid training.
- Communications equipment familiarity and use.
- Cultural awareness.
- Language training.

**10) Exposure reduction** is sometimes referred to as “reducing the operational tempo” which means reducing the size of the target presented to potential threats. In general these are:

- Reduction of geographic exposure: by limiting or curtailing operations in certain high-risk zones, declaring no-go areas, etc.
- Reduction of the amount of time (or specific times) that you or your staff are exposed to threats: by limiting hours of operation in sensitive locations, limiting time of travel to daylight hours only, establishing staff curfews etc.
- Reduction of total number of staff exposed by setting staffing ceilings or reducing certain categories of staff (due to sensitive nationality, gender, national/international status etc).

The most extreme form of exposure reduction, of course, is program suspension and ultimately, program or mission cancellation.

The risk reduction toolkit of options described above is not intended to be all-inclusive—the ways to reduce risk and enable program success are limited only by your creativity and imagination. The important points to remember are that, as a manager, you have a broad range of options at your disposal, and a balanced and comprehensive security strategy will usually include a range of these different measures.

## Summary



### Key Points

**Criticality assessment** considers the importance or urgency of the program activity, and weighs this against the risks to staff in carrying out the activity. Generally speaking, it can yield three possible outcomes:

- Benefits clearly outweigh the risks; undertaking the program falls in the category of reasonable risk.
- Risks clearly outweigh the benefits; the activity entails unacceptable risk.
- The risk may be acceptable, but only with additional mitigating measures. In this case the manager must select and implement appropriate measures designed to eliminate unnecessary risk and manage residual risk.

---

Criticality analysis cannot produce absolute, right or wrong answers and cannot be used to provide justification where risk is clearly unacceptable; however, it can help to clarify thinking, expose strengths and weaknesses in an argument, and provide support for a decision entailing reasonable risk once it is taken.

---

The SRA process should lead to practical measures designed to deal with risk. The two basic types of risk reduction measures are:

- **Prevention measures** that reduce the likelihood that potential threats will occur.
- **Mitigation measures** that reduce the damaging impact of potential threats when they do occur.

---

The “Risk Reduction Toolkit” is a generic set of activities and means for reducing risk in the field. This toolkit of risk reduction measures includes:

- **Planning** for security protocols and responses in readiness for response to potential threats.
- **Coordination**, both internally among staff and organizational units, and externally with other organizations.
- **Hardening** measures such as walls and strong gates and doors.
- **Deterrence** measures such as guards and police.
- **Image- and acceptance**-improving measures such as public outreach campaigns and immediate organizational recognition measures like flags and large decals for buildings and vehicles.
- **Communications** equipment and readiness for use by all staff members.
- **Vehicles**, their drivers and the associated equipment and procedures for using them.
- **Risk transference** strategies, such as insurance policies and hiring others to undertake dangerous tasks.
- **Staff knowledge and skills** that guide them in avoiding unnecessary risks and prepare them for emergency response if need be.
- **Reducing exposure** by reducing staff in the field, the amount of time that they are in harm’s way, or the areas in which they work and travel.



Chapter 8  
Self-Assessment Questions

Check T or F to indicate whether a statement is True or False

- T  F 1. Mitigation means a reduction in the impact or harm of a potential threat.
- T  F 2. Prevention means the reduction of likelihood that a potential threat will occur.
- T  F 3. Every office, no matter how small, should have a security plan.
- T  F 4. A high concrete wall around an office compound might be considered a hardening option as well as deterrent.
- T  F 5. Criticality assessment answers the question "Which humanitarian activities are most important today?"

Before answering the multiple choice questions on the next page, review the diagram below which was drawn up by the office manager and her team in a small field office in a high-risk conflict area. The three threats shown in the circles with the solid lines are in their relative risk positions on the matrix under the current situation and conditions. The circles with dashed lines show the reduced risk locations on the matrix for these same threats if the manager's planned risk reduction measures are put into place. The three potential threats considered are:

- 1) A riot outside the office due to expected negative response to the scheduled announcement that relief distributions will be suspended next month.
- 2) A serious road accident on the mountainous roads leading to the capital city. There are frequent accidents reported weekly, often resulting in broken limbs, and occasionally deaths from high speed collisions, and run-offs.
- 3) Threat assessment has shown that other similar offices have suffered bomb attacks in the past, usually by small trucks or other vehicles carrying the bombs to the entryways or front doors of international aid offices, often resulting in significant damage and deaths.

FIELD OFFICE RISK MATRIX		LIKELIHOOD				
		Unlikely	Moderately Likely	Likely	Very Likely	Certain/Imminent
IMPACT	Critical	3B Vehicle borne bomb at office	←	3 Vehicle borne bomb at office		
	Severe			3A vehicle borne bomb at office		1 Riot outside office
	Moderate	2A Road accident	←	2 Road accident		↓
	Minor					1A Riot outside office
	Negligible	2B Road accident				



## Chapter 8

### Self-Assessment Questions *(continued)*

*Multiple choice. To answer these questions, please refer to the diagram on the previous page. Mark ALL correct statements—more than one may apply.*

6. Which of the following statements could reasonably be implied by the two locations of the threat of a riot before (position 1) and after risk-reduction measures are taken (position 1A)?
- A** The management team concluded that the riot, or at least a large demonstration, was probably unavoidable, and therefore decided to focus on mitigation measures.
  - B** The management team concluded that significant damage resulting from a riot would be unavoidable if it were to happen, and therefore decided to focus on prevention measures.
  - C** The team's primary recommendations probably included hardening measures.
  - D** The team probably recommended flying a large organizational flag as an image and acceptance measure.
7. Which of the following measures could have realistically changed the road accident threat at risk position 2 on the matrix to the new reduced risk position at 2A?
- A** Exposure reduction by allowing fewer road missions to travel.
  - B** Knowledge and skills by requiring safe-driving training.
  - C** Exposure reduction to this threat by instructing the drivers to take the long way around the mountains to avoid the most unsafe roads.
  - D** Vehicle equipment and procedures by requiring all passengers to wear their seatbelts in the cars at all times.
8. Further measures are also to be taken along with those chosen above to make road travel safer. Which of the following measures might realistically move the threat of a serious road accident from position 2A to 2B?
- A** Improved knowledge and skills, such as first aid training for the staff.
  - B** Improved communications abilities such as backup means to be able to reach medical assistance if needed.
  - C** Exposure reduction to this threat by instructing the drivers to take the long way around the mountains to avoid the most unsafe roads.
  - D** Vehicle equipment and procedures by requiring all passengers to wear their seatbelts in the cars at all times.



Self Test

Chapter 8  
Self-Assessment Questions (continued)

9. What measures could the management team have reasonably proposed to move the threat of a vehicle-borne bomb in at their office from position 3 to 3A on the risk matrix?
- A Hardening, by placing blast film on the windows.
  - B Hardening, by building strong perimeter walls to keep vehicles from approaching too near to the building.
  - C Knowledge and skills by training staff in emergency response procedures and first aid.
  - D Image and acceptance, by plainly marking the building gates with the organizational emblem.
10. Which of the following statements could reasonably be said about the manager's proposal to move the threat of the vehicle-borne bomb from position 3 to 3B?
- A It could be an image and acceptance strategy.
  - B It could be a deterrent strategy, such as heavy showing of armed guards or police outside the office compound.
  - C It could be a hardening strategy such as a strong, tall perimeter wall that does not allow vehicular access close to the building.
  - D It could be a knowledge and skills measure like first aid training.



Chapter 8  
Answer  
Key

- |    |   |     |         |
|----|---|-----|---------|
| 5. | F | 10. | A, B, C |
| 4. | T | 9.  | A, B, C |
| 3. | T | 8.  | A, B, D |
| 2. | T | 7.  | A, B, C |
| 1. | T | 6.  | A, C    |

# Chapter 9

## Security Plans and Planning

UNHCR staff in Chad put their evacuation plan into effect in February 2008 and board a UN plane bound for Cameroon. Nearly all UNHCR staff were evacuated from N'Djamena amid fighting in and around the city.



UNHCR photo by A. Rehr

*"Dig the well before you are thirsty."*

– Chinese Proverb

*"A goal without a plan is just a wish."*

– Antoine de Saint-Exupery

*"In preparing for battle I have always found that plans are useless, but planning is indispensable."*

– Dwight D. Eisenhower

These quotations illustrate the fact that planning is basically a process of thinking ahead. Planning has long been an important part of humanitarian work. Emergency operations planning, logistics planning, and food needs planning are among many examples familiar to aid workers. More recently, security planning has also been added to the list of core competencies of humanitarian field managers. Careful forethought regarding actions to take when confronted with likely security threats can mean the difference between life or death. In particular, planning for how to extricate staff in the event of a serious deterioration of the situation, or evacuation planning, has become a minimum standard for safe operations in insecure environments.



### Learning Objectives

This chapter will illustrate the importance of security planning and provide you with some guidelines and practical advice on how to structure and manage your security plans. In particular, you will learn:

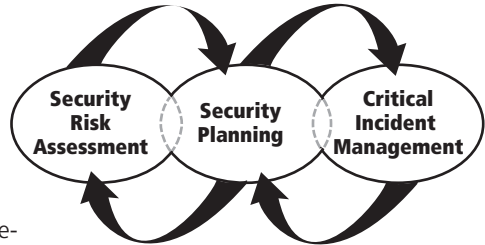
- The relationship between security plans and planning and the SRA process.
- How to determine the level of planning needed by your office.
- The basic contents and structure of a comprehensive field security plan.
- The specific design and use of scenario-based security contingency plans as components of the overall security plan.
- How to relate your planning to your budget.



### The relationship between security plans and Security Risk Assessment

How do security plans and planning fit in with the SRA model shown in the preceding chapters? In Chapter 8 we already saw one way in which planning figures in SRA. As a key part of the risk reduction toolkit, security planning is an important preventive and mitigating measure to be taken during the decision and implementation part of SRA.

This diagram illustrates another way to view the relationship—presenting security planning as overlapping yet separate from SRA. This is because you must do your SRA first in order to know what to plan for; then, using your analysis of the threats, vulnerabilities and risks, you can plan accordingly.



A third overlapping activity—Critical Incident Management—is included in the diagram because an accurate assessment and well-prepared plans will increase your ability to respond to a critical security incident more effectively, should it occur. This activity will be discussed in detail in the next chapter.

Finally, you will notice that the arrows on the diagram above link activities forward as well as backward. This is because an incident, should it occur, hopefully produces new insights and lessons learned; and these should be used to update your SRA and revise plans accordingly in a constant feedback loop. Security Risk Assessment, Security Plans and Planning and Critical Incident Management constitute the principle tools of Security Risk Management.

## 9.1 Does Every Office Need a Security Plan?

Yes. Every office should have some form of security plan; however, what is required for your particular office's security plan will vary considerably depending on your location and situation. For example, your organization may occupy an office alongside partner agencies in a building which already has an adequate building-wide security plan. In this case you might only need to maintain a copy of the plan on hand and ensure that staff are kept informed and aware of the parts that concern them.

This principle holds true for organizations working in the field sharing common security protocols (e.g., UN agencies under the UN security management system or NGOs operating in accordance with shared guidelines). Where a system-wide plan exists, it would be pointless to create a separate plan; however, your office's plan should address agency-specific contingencies (such as incidents involving refugees in the case of UNHCR), as well as particular information about how the office would integrate into the overall plan. In a very small field activity, such as a satellite office, security plans might consist of 2-3 pages of key information (means and location of evacuation, concentration and assembly areas) along with updated staff lists and information on key communications to maintain in the event of an emergency. In short, each office should go through the security planning process, but the resulting plan should be unique and tailored to the realities of that office.



**Question**

*Who should prepare the security plan?*

---

---

---



In many offices, a security specialist (field security officer or field safety adviser) takes the lead in drafting the security plan. However, the plan must be approved by the responsible manager, and the manager must have detailed familiarity with its contents. Ideally, the manager should have direct involvement in the planning and preparation process as well. If you do not have an assigned security specialist working in your office, this does not mean that you do not need a security plan. In the absence of such specialists, office managers are encouraged to seek assistance from their headquarters, partners in their area and other avenues to undertake the process themselves. To sum up: not having a security officer is no excuse for not having a security plan.



### Question

*Is the security plan a “sensitive document”? If so, what, if any of it, should be shared with staff?*

---



---



---



---

Yes, the security plan is usually a sensitive document. In some duty stations, your summary of the situation and possible risks may be politically sensitive. In high-crime duty stations, open access to complete staff lists may be perceived as exposing people to targeted crime. In other cases it may be deemed necessary to limit knowledge of security plans or intentions in the event of an emergency. For these reasons, the complete security plan should generally be kept locked in a secure place.

However, it is important that staff members are aware of the basic elements of the plan, and what will be required of them in certain contingencies. For example, they must know how to evacuate the building in the event of a fire, where to assemble, where to concentrate in an evacuation, and who their zone wardens are. Moreover, staff members should have the right to know that there is a plan and, barring exceptional circumstances, to see it and ask questions about it if they desire.

In certain duty stations, where the security plan is relatively concise and there are no special sensitivities, the plan may simply be made available to all. In other duty stations, the best solution may be to condense the information that all staff must know into a brief (1-3 page) document for general distribution. In such instances, staff members should still have the right to view the full plan (but not take a copy for themselves) unless exceptional circumstances prohibit this. In all cases, critical information should be the subject of regular briefings, and ideally, rehearsals.

**In many duty stations, summarizing key, “must-know” points from the security plan into a brief 1-3 page document for all staff is an effective solution to balance the sensitivity of the overall plan and the need to keep all staff informed.**

## 9.2 The Plan

The outline below is a useful template for a complete security plan. However, bear in mind that this is a sample plan only; the specifics of your particular office may preclude the need for certain details and necessitate the inclusion of others. As with everything else in field security, your plans must above all make sense for you in your unique situation.



There are certain elements that are common to all good security plans. Consider your own office's security plan and ask yourself whether it adequately addresses the following essential points:

- **Situation overview and assessment of key contingencies** – Begin your security plan with a summary of the current situation and your assessment of the principal threats that you must plan for. In this way the security plan ties in directly to the security risk assessment process.
- **Identification of key personnel in the security management system** – Be sure to include contact information, the responsible manager, security officer (if any), office security focal point and/or host nation law enforcement and first-response emergency points of contact.
- **Updated staff lists** – Should include work, home and mobile phone numbers and addresses.
- **A communications plan** – Should list radio frequencies in use, call signs, satellite telephone numbers and special procedures applicable in emergency situations.
- **Evacuation plans and procedures** – Strictly speaking, evacuation is one type of contingency. Its importance is such that it should be considered an indispensable part of any security plan. There are several things that the evacuation plan must address:
  - **The evacuation destination** and a primary evacuation route, and at least one alternate, should be identified.
  - **Means of evacuation** (e.g., UN vehicles, chartered aircraft, partnership arrangements). Again, there should ideally be a primary and alternate means established.
  - **Location of Emergency Coordination Center** which may be in a designated room of a local UN, Red Cross or Red Crescent, NGO office, or the office of a partner agency. It should normally be in a well-protected location and equipped with supplies including computers, telecommunications equipment, extra food, water and medical supplies.
  - **Concentration point(s)**, or safe areas, where staff will assemble in preparation for movement to the evacuation point.
  - **Safe points** in the city where staff members are instructed to go in the event of major disturbances such as rioting or attack may be further identified in the plan; they may be the same as concentration points.
- **National staff continuity plan** – For humanitarian agencies working in dangerous areas (UN, NGOs and others), national staff are only evacuated from the country in exceptional cases, but they may be relocated to safer areas inside the country. Therefore, the security plan must foresee steps to safeguard local staff in the event of an evacuation of international staff and, where applicable, continue operations. Specific considerations include:
  - Identification of a national staff **Officer in Charge (OIC)** and chain of command.
  - **Specific instructions** for the national OIC.
  - **Plan for necessary signature authorizations** and provision of authorized entitlements (e.g., salary advance).
  - **Plans for local relocation of national staff**, identifying staff to be relocated, locations, and logistic requirements to effect the movement.
  - **Identification of which programs are essential** and how they are to be conducted in the absence of international staff.
- **Medical evacuation (MEDEVAC)** – Offices should have a plan for how an injured or sick staff member can be safely and rapidly evacuated. Ideally this should include an agreement in writing with the provider of emergency medical and transportation services.
- **Procedures for other contingencies** – Specific information and actions should be included for the major contingencies identified in the security plan; these may include armed attack, violent demonstrations, intruders, fire, natural disasters and others.



- **Maps** – Security plans should include appropriate maps of the country or region, showing evacuation routes, and the town or city, showing the location of UN and other critical offices, airports, ports, and hospital facilities among other features. A city map showing the location of staff residences and security warden zones should also be included.



### Question

*How often should I update my security plan?*

---



---



---

*“It is a bad plan that admits of no modification.”*

– Publilius Syrus (~100 BC)

A general rule is that security plans should be reviewed and updated at least annually in areas that are relatively stable (UN Security Phases 0-2), and semiannually in areas that are more volatile (UN Security Phases 3-5). However, this general rule must be adapted to the local circumstances. Perhaps you have closed or opened additional offices or are now using different frequencies or call signs. Key security personnel may have changed. Fighting in a neighboring country may render evacuation to that country as no longer feasible. In such situations, more frequent review and update of plans are required.

Remember that staff need to be kept informed of changes that affect them; identifying a new concentration point or assembly area will not help if staff are not aware of them. The review and updating process should be followed by a staff briefing, and ideally a rehearsal.



### Exercise

*What goes into a good security plan? Use the spaces below to write an outline or headings for a security plan that you feel would be adequate for your own duty station or working environment.*

---



---



---



---



---



---



---



---



---



---



Below is an outline of a generic UN security plan to use as a tool in creating your own security plan. The body of the plan is kept to a bare minimum, with most of the specific details included in annexes. This will facilitate ease and speed of access to critical information in an emergency. Also, note that this is a notional plan only; the specifics of your particular office and situation may not require certain details and may call for the inclusion of others not listed here. No template has all the solutions or can eliminate the need for careful, situation-specific thinking. Remember that while using templates from other security plans can save time and serve as useful checklists, your plans must be appropriate for you in your unique situation. *Don't follow prepared templates blindly.*



### Tools

#### Template 1. General UN Security Plan Format

- I. Introduction
  - A. Purpose of the plan
  - B. Security situation
    1. General description
    2. Identification of principal contingencies of concern
- II. Identification of key actors in the country security system (Designated Official, Deputy Designated Official, line manager, field safety adviser, field security coordination officer, security focal point(s), and host nation law enforcement and first-response emergency points of contact)
- III. Emergency and evacuation
  - A. Locations of safe haven(s)
  - B. Means of movement there (alternate and backup)
  - C. Location of Emergency Coordination Center
  - D. Location of Concentration Point(s)

#### Annexes

- A. Security Management Team contact list: Name/Off & Home Telephone, Cellular & Fax numbers
- B. ESS/FSS and DSS contact lists: Name/Off & Home Telephone, Cellular & Fax numbers
- C. Area Coordinator List: Name/Off & Home Telephone, Cellular & Fax numbers
- D. Warden List by Zone: Name/Off & Home Telephone, Cellular & Fax numbers
- E. Safe haven Points of Contact: Name/Off & Home Telephone, Cellular & Fax numbers
- F. Communications
  1. List of frequencies in use (regional and national; HF, VHF, UHF)
  2. Duty Station Call Sign List
  3. Satellite Telephone Numbers: Designated Official, other Agencies
- G. List of vehicles at duty station
- H. Continuity plan
  1. National staff OIC and chain of command
  2. National staff relocation plan
- I. Hostage incident management plan
- J. Safe Haven response plan
- K. Medevac plan
- L. Natural Disaster Plan (as required)
- M. Other specific contingency plans (as identified in I.B.2. above)
- N. Sub- or field-office security plans (or specific details of plans, as applicable and necessary)
  1. Sub-office A
  2. Sub-office B
- O. Staff Lists: national and international staff
- P. Maps
  1. Country: identify UN Offices, airports, ports
  2. City: identify UN offices, airports, ports, hospitals
  3. UN Staff: identify warden zones



## Template 2. A Generic NGO Security Plan

There are many good examples of security plans to use as tools or templates for developing your own plans. Make use of your own organizational plans and guides where you can, and do not be shy to ask for partner agency assistance in providing templates or existing plans as guides for creating your own. The detailed example below was drafted in 2006 by Joel McNamara. An electronic security plan template is available for free non-commercial use and modification at the website [aidworkers.net](http://aidworkers.net). As in the preceding example, remember that no tool or template is right for every situation. Use them to get started and to generate ideas but don't feel that you have to replicate all of this content in your own security plan.

### 1. OVERVIEW

- 1.1 Introduction
- 1.2 Safety and Security Responsibility
- 1.3 Safety and Security Focal Person
- 1.4 Safety and Security Committee
- 1.5 Safety and Security Plan
- 1.6 Current Threats
- 1.7 Current Risk Rating
- 1.8 Safety and Security Planning Assessment

### 2. CRISIS MANAGEMENT

- 2.1 Crisis Management Team
  - 2.1.1 Training
- 2.2 Death or Serious Injury of Staff Member
- 2.3 Staff Member Abduction
- 2.4 Staff Member Assault
- 2.5 Staff Member Arrest or Detention
- 2.6 Vehicle Accident (Death or Serious Injury of Non-Staff Member)
- 2.7 Evacuation/Relocation/Hibernation
- 2.8 Medical Evacuation
- 2.9 Natural Disasters
- 2.10 Theft, Fraud or Embezzlement (Significant Amounts)
- 2.11 Continuity of Operations
- 2.12 Civil Unrest

### 3. FACILITIES

- 3.1 Your Office Facilities
- 3.2 Facilities Security and Access
  - 3.2.1 Key Policy
  - 3.2.2 Staff After Hours Policy
  - 3.2.3 Visitor Policy
  - 3.2.4 Changing Locks and Access Codes
  - 3.2.5 Alarm Systems
- 3.3 Facilities Safety
  - 3.3.1 Your Office Evacuation Plan
  - 3.3.2 Telephone Bomb Threats
- 3.4 Fire and Electrical Safety
  - 3.4.1 Fire extinguishers
  - 3.4.2 Smoke detectors
  - 3.4.3 Smoking areas
  - 3.4.4 Space heaters
  - 3.4.5 Electrical safety
  - 3.4.6 Fire and Electrical Safety Inspections
- 3.5 Facility Medical Emergencies
  - 3.5.1 Response
  - 3.5.2 First Aid Kits
- 3.6 Facility Site Selection
- 3.7 Facility Safety and Security Assessment

### 4. TRANSPORTATION

- 4.1 Your Office Vehicles
- 4.2 Vehicle Use Policies
- 4.3 Passenger Policies
- 4.4 Seat Belt Policy
- 4.5 Vehicle Maintenance and Inspection Schedule
- 4.6 Minimum Vehicle Equipment
- 4.7 Accident Procedures
- 4.8 Insurance

### 5. COMMUNICATION

- 5.1 Types of Communication Systems
- 5.2 Warden System/Phone Tree
- 5.3 Communications Assessment

### 6. INFORMATION

- 6.1 Information
  - 6.1.1 Information Classification
  - 6.1.2 Information Storage
  - 6.1.3 Information Security
- 6.2 Incident Reporting
- 6.3 Computers and Networks
- 6.4 Information Assessment

### 7. PERSONNEL

- 7.1 Key Staff Contact List
- 7.2 Safety and Security Briefings
- 7.3 Staff Health
  - 7.3.1 Vaccinations
  - 7.3.2 Insurance/Healthcare
  - 7.3.3 Flu Pandemic
  - 7.3.4 Training
  - 7.3.5 Stress Management
- 7.4 Staff Safety and Security Training
- 7.5 Record of Emergency Data (RED)
- 7.6 Hiring and Termination Policies
- 7.7 Alcohol and Drug Policy
- 7.8 Staff Movement
- 7.9 Visiting Staff or Consultants
- 7.10 Guards
- 7.11 Personnel Assessment

#### Appendix A – Current Threats

#### Appendix B – Risk Ratings

#### Appendix C – Evacuation/Relocation/Hibernation Plans

#### Appendix D – Medical Evacuation Plan



### 9.3 Scenario-Based Security Contingency Planning

Contingency planning can be defined as a forward planning *process* in a state of uncertainty in which *scenarios* and objectives are *agreed*, and potential response systems put in place to *respond* to an emergency. Most offices routinely conduct contingency planning for humanitarian emergencies, such as mass influx, spontaneous repatriation and outbreak of disease. The same processes can and should be applied to planning for security-related contingencies. General considerations include:

- **Contingency planning begins with the question, “what if?”** In the case of security-related contingency planning, it usually focuses on the three or four events identified by your SRA as entailing the highest risk (that is, greatest impact, likelihood, or combination of the two), e.g. armed attack, violent demonstrations, bombing, intruders, fire, natural disasters and others.
- **The next step is to ask “what then?”** What consequences would this event pose for your office or program if it actually happened? Specific questions to ask:
  - What actions would have to be taken? Try to identify standard procedures to follow if it occurred. Can any steps be taken now to reduce response time in an emergency?
  - “Who will do what? Assign likely roles/responsibilities; identify coordination mechanisms.
  - “What are we missing?” Identify shortfalls in equipment or other categories (people, training) to accomplish these steps.
- **Involve likely partners in the process.** Doing so can facilitate a common understanding of the problem, reduce duplication and gaps, increase efficiency by pooling resources, and improve coordination and response time in a crisis.
- **Follow up.** This includes preparing a written plan and sharing it with all who need to know its contents. Briefing and training are ways to accomplish this but live rehearsals of plans are best. Remember that the plan is a “living document” and situations evolve continuously; plan for regular review and update of your contingency plans and make modifications as needed.

### 9.4 Security Planning and Your Budget

For humanitarian organizations working in insecure areas, security-related expenses have become part of the cost of doing business. Planning operations without adequate consideration of how the security situation will affect your budget is unrealistic and potentially dangerous. UNHCR’s Security Policy emphasizes that managers are responsible for ensuring that safety is a core component of all programs, and that adequate funding should be provided to ensure this. For this to happen, *security must be a core component of operational planning from the outset.*

Most humanitarian organizations have a budgetary planning cycle that begins at least one year before the year being planned. In UNHCR, the standard tool of medium-term operational planning is the Country Operations Plan (COP), which is prepared in March of the previous year. Planning documents like the COP must have thoughtful and substantial consideration of security-related issues. Your security risk analysis and contingency planning processes should be used to highlight the measures and resources needed to ensure safe operating standards. A security officer should be a key member of the planning process. Their advice and expertise can help managers be aware of all options and help adapt programs and procedures to changes in the threat environment. If a security officer is not present, the requirement to fully reflect security needs remains the same.

Remember that changes in the operating environment may require changes in your planned security measures. For the UN, security measures made mandatory by Minimum Operational Security Standards (MOSS) may also be affected. UN standards normally require such measures to be implemented within 60 days of endorsement by the UN Security Management Team. Given the financial implications of MOSS to the operation, and the normal timeline of budgetary processes, proper pre-planning is of the utmost importance to avoid delays in implementing operations.

## Summary



### Key Points

*Security plans and planning* relate to SRA, in that the threats, vulnerabilities and risks that you analyze should tell you what you need to plan for.

---

*Planning is a basic part of humanitarian field work.* Security planning is now considered an essential core competency for office managers and must be carried out whether or not there is a dedicated security professional assigned to this task.

---

*All offices, regardless of size, require a security plan;* however, the complexity of the plan will vary widely according to the size and scale of the operation and the particular security threats and other concerns identified in your SRA.

---

*Security plans may contain sensitive information* that should be restricted from wide circulation, however, *all staff members must be aware of those portions of the plan* that depend on their knowledge of the plan's protocol and proposed responses.

---

While the precise format and content of security plans will vary widely from office to office and from situation to situation, the following points should normally be considered in most moderate- to high- risk field situations:

- Overview of the situation and assessment of key contingencies.
  - Identification of key personnel in the security management system.
  - Updated staff lists.
  - A communications plan.
  - Evacuation plans and procedures.
  - Medical evacuation (MEDEVAC).
  - Procedures for other contingencies.
  - Maps.
- 

*Scenario-based contingency planning* for incorporation into the overall security plan usually focuses on the three or four threats identified by your SRA as entailing the highest risk to your staff.



**Chapter 9**  
**Self-Assessment Questions**

*Check T or F to indicate whether a statement is True or False*

- T**  **F** 1. Offices with less than 10 staff do not require a security plan.
- T**  **F** 2. Because the security plan is a sensitive document, it should not be shared with the general staff beyond the logistics, communications and security team.
- T**  **F** 3. A national staff continuity plan, as part of the larger security plan, should include, among other things, how the remaining staff are to be paid in the absence of international staff being evacuated out of the country.
- T**  **F** 4. Maps should be included in most security plans.
- T**  **F** 5. The basic plan format should be simple, with critical lists, documents, and supporting information in well-marked annexes for ease and speed of use in an emergency.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following statements are true concerning security scenario-based contingency planning?
  - A** Only the highest risk threat should be included for this type of planning.
  - B** A few of the key threats in terms of risk to staff should be included.
  - C** Low-risk threats should be included.
  - D** Specific contingency plans should be included for all threats identified in the SRA.
- 7. As part of a security plan, a concentration point is:
  - A** A key element of the plan that requires focused attention of all staff.
  - B** An area inside the office where staff are told to take cover in the event of an attack.
  - C** A person responsible for all security-related planning details.
  - D** A location where staff are supposed to gather together after an incident, or upon order, for organizing an evacuation or other movement.

**Self Test****Chapter 9****Self-Assessment Questions** *(continued)*

8. Which of the following elements would be expected in a security plan for a medium sized office in a high risk field situation?
- A** Overview of the situation and assessment of key contingencies.
  - B** Updated staff lists.
  - C** A communications plan.
  - D** Evacuation plans and procedures.
9. Which of the following provide good advice for planning your overall budget for field operations in dangerous environments?
- A** Always include security-related costs from the beginning of the budgeting process.
  - B** Always inflate the costs for security-related items as you will never receive the full amount you need.
  - C** Smart managers add in the cost of security-related items only after operations are up and running.
  - D** Security planners and operations planners are two separate entities, neither of the two should be concerned with the operations of the other.
10. Which of the following provide good advice for those preparing to use another organization's (or office's) security plan as a tool or template for developing their own?
- A** One plan is as good as another, copy whatever you can.
  - B** Using a template can save time, but use only the parts that are applicable to your situation.
  - C** Using a template can serve as a good checklist of things to consider for your own plan.
  - D** Never use another organization's plan as a template for your own, security situations are too different for the plans of others to be of any use to you.



**Chapter 9  
Answer  
Key**

- |    |   |     |            |
|----|---|-----|------------|
| 1. | F | 5.  | T          |
| 2. | F | 6.  | B          |
| 3. | T | 7.  | D          |
| 4. | T | 8.  | A, B, C, D |
| 5. | T | 9.  | A          |
| 6. | B | 10. | B, C       |

# Chapter 10

## Critical Incident Management

*A building damaged by the 11 December 2007 terrorist attack on the UN Headquarters complex in Algiers. Starting at about 9:30 a.m. local time, two car bombs exploded 10 minutes apart. The bombing claimed the lives of 17 United Nations workers.*



Even the best threat and vulnerability assessment and the most thorough planning cannot eliminate the possibility of a serious security event occurring. When it does, lives may depend on the actions that are taken in the first few moments. Prompt and appropriate response depends on preparations made beforehand. This chapter examines critical incident management as one specific aspect of risk management. It will focus on the support systems, sequence of events, and “tools” required for responding to a critical incident.

This chapter’s goal is to increase your awareness of the steps to take before and during a crisis, and give you confidence in your understanding of the immediate steps to be taken afterwards.



### Learning Objectives

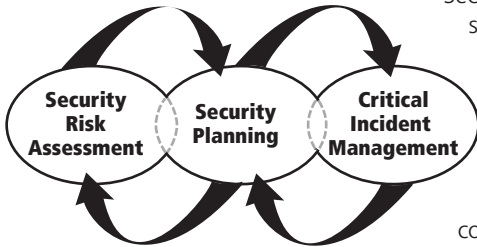
In this chapter you will learn about:

- The relationship of critical incident management to contingency planning, and other security planning measures of the overall SRM approach.
- The stages of a critical incident and the immediate response.
- Some tools and methods for improving your immediate and short-term response to such incidents.
- Reporting thresholds for different levels of security incident reporting.



## 10.1 Critical Incident Management and Security Planning

Critical incident management is a risk management process that is linked directly to security risk assessment and the security plans and planning discussed in the previous chapters. It is an integral component of the overall SRM approach.



Security plans are based on the threats identified in the security risk assessment process. We have seen that specific security contingency plans should be developed for particularly high-risk possibilities you have identified. If the SRA has been done well, you will likely have identified the types of critical incidents or scenarios that have a high possibility of affecting your office or staff in the field. If the contingency planning process has included key staff members who have talked through the actions to be taken

in such an event, then it is reasonable to expect that the staff will perform better should the actual event occur. The extent to which these plans are disseminated to all staff and rehearsed in realistic drills will also effect how fast and how well-organized the initial response will be.

Because the relationship between planning and response is so essential, it can be difficult to define the exact boundary between the contingency planning process and critical incident management. In general, we may say that critical incident management technically begins when the event itself occurs, but many of the steps required to manage the crisis effectively must be taken, or planned for, well before then.

## 10.2 Stages of a Critical Incident and Response

While every critical incident is different, many elements of a successful response are common to all. It can be helpful to consider the sequence of events in a crisis as successive stages, each with its own priority actions. The section below outlines six successive stages that apply to most critical incidents.

### 1) Anticipation and pre-emption

While technically completed before critical incident management begins, this first phase sets the context for you as an incident manager. It will give you ready-to-use tools for an immediate response should an emergency situation occur. Previous chapters have already detailed the value of completing the following measures before an incident occurs.

- Threat and risk assessment
- Implementation of mitigation measures
- Contingency planning
- Briefing and rehearsals



**Question**

*Once a critical security incident occurs, what must you, as a manager, do first?*

---



---



---



## 2) Initial reaction

Imagine that a bomb blast or a rocket attack has just occurred, or you have just received a panicked radio call from your field team's vehicle driver saying that they are coming under hostile fire. A critical incident has happened or is happening; what do you do now? The first few minutes are critical; what has to be done first? Before you do anything, pause and take a deep breath. Get control of yourself—a panicked manager will only contribute to the chaos of the situation. You will first want to determine:

- **What information you need to know right away?** What essential pieces from the story are missing? Remember the key words: *what, when, where* and *who* (which for you will include knowing which of your staff members, if any, are involved). Why and how may not be immediately answerable but will come later.
- **What decisions need to be made, and when?** Does the decision need to be taken immediately? If so, then don't delay. But if not, the quality of the decision may benefit from further time for reflection and gathering of facts. Studies of past responses to critical incidents show many cases where quick managerial decisiveness was exactly what was needed, but also show others where hastily made decisions only added to the confusion. First deciding what you need to decide can be a wise investment of time.
- **Who needs to be notified immediately?** You will be ahead of the situation if you have asked and answered this question already during your planning process.

## 3) First steps

If you are directly involved in a critical incident, the most immediate measure is always to save lives—your own and as many others as you can. You will also be working to limit the extent of the damage. This may mean putting out burning fires, keeping unaffected staff members and others from entering unsafe situations, using first aid to keep injured staff from dying, limiting movement of staff to reduce overall chaos, assigning (or re-assigning) needed tasks, and other measures to maintain an orderly and effective response.

After saving life, your next priority is usually accounting for all staff for whom you are responsible and confirming the identity of any casualties. Equally important at this stage are immediate actions to protect other uninvolved staff from being affected by the incident, e.g., by sending a warning or restricting movement as necessary. Your initial communications should be to those most able to help you (normally first-response authorities) and to those who need to be alerted to prevent them from becoming involved (e.g., your staff and partners).

If you are managing a critical incident from afar, or simply receiving the information from the field, it is important to remember that the priority to save lives takes precedence over your need for information; you may need to give colleagues time to handle the situation before they can report accurately. Nevertheless, an alerting report should be provided as soon as possible, and should include information on any staff members involved, measures taken to protect other staff and immediate support needed.

### First Steps Checklist

- Undertake immediate steps to save lives (your own and others)
- Confirm information/identity of casualties
- Account positively for all staff
- Limit movement of staff or relocate as necessary
- Alert first-response authorities
- Alert other agencies in the affected area



**Question**

*Once you have gained your composure and taken immediate life-saving measures, what steps can you now take in order to gain control of the situation rather than just responding to it?*

---

---

---

---

---

---

**4) Establish control**

Establishing control means gaining the initiative in the response so that you and others are not constantly responding to the next urgent request or need, but rather, taking proactive measures in order to reduce the overall chaos of the situation into a logical system of response. This lets you set priorities and assign responsibilities so that important activities are not overlooked while the crisis team responds to the urgent issues relating to the incident. During this phase, you should:

- Send an initial incident report. Do not delay because information is incomplete, this is normal in the initial stages of an incident. Rather, send what information you have in a brief alerting report now, qualifying clearly where facts are unknown or assumptions are based on as yet unsubstantiated data. Follow up with a more detailed report later when the situation permits. The golden rule is: when in doubt, send a report (a sample format for an alerting report appears later in this chapter).
- Establish your incident management team, and assign clear roles, per your security plan or scenario-specific contingency plan.
- Consider establishing an incident management operations center to centralize information and key staff assigned to the incident management team.
- Establish liaison channels with other concerned parties (family members, partner agencies, authorities, other responders, in some case media members). Identify appropriate focal persons who will deal with these specialized areas.
- Consult specialists for specific information or advice in relation to the incident that has occurred. For example, after a fire or bombing incident, you might require a structural engineer to determine whether or not it is safe to use part of the building. If MEDEVAC is required, both medical and logistic experts will need to be consulted.

**5) Establish an incident management routine**

For serious incidents resulting in multiple casualties, significant delay of operations, or an investigation, the overall crisis response will begin to take on a routine of its own. The response dedicated to the incident and its results may take weeks, months, or longer. Dealing with family members, media reporters, and local and international authorities can become a full-time job for some members of the office. It is best to recognize this possibility from the beginning and to assign adequate resources. The key to managing the overall operations in these situations is to keep other important and ongoing activities running as well as possible, and to divide the



responsibilities of the staff to keep all from being consumed by the critical incident response. To do this, you will need to:

- Appoint an incident manager.
- Establish meeting and reporting schedules and routines.
- Redistribute non-essential tasks.
- Begin planning for recovery and counseling of those involved.
- Start the “lessons learned” process.



### Question

*Once a critical incident is past and special response procedures begin winding down, where do you focus your attention before returning to “work as usual”?*

---



---



---



---

### 6) Post-incident stage

The critical incident management stage will eventually come to an end. Slowly but surely, life will return to its normal pre-incident pace and activities. It is important at this time to reflect on what has happened and to document procedures that worked well and those areas where further improvement is needed to be ready for future incidents. Remember that the incident will very likely change your threat and vulnerability analyses, and your day-to-day routines. You may never return to the same working norms that existed before the incident due to changes in your security procedures, and possibly your field program designs. Specifically you will want to:

- Analyze the incident and the response.
- Revise security procedures and plans accordingly.
- Facilitate recovery for those involved in the incident which may include counseling and other social or even psychological support.

## 10.3 Tools and Methods

There are many tools and measures that you can use to increase your speed and efficiency in critical incident response. Some of the most basic and most useful items to have in place before a critical incident occurs are shown below:

- Specific security scenario-based contingency plans
- Rehearsals and drills of emergency procedures
- Standard Operating Procedures (SOPs) for key incidents, and responses (e.g., building evacuation, fire response, taking shelter if under fire)
- Standby arrangements with other potential responder.
- Communications systems – with emergency back-up provided
- Staff tracking systems
- Information management systems and procedures
- For larger offices or operations, a room specially dedicated and equipped to serve as an Operations Center in time of emergency



**Specific security scenario-based contingency plans** have already been discussed as a vital tool of critical incident management. Remember that good plans should involve likely partners in the planning process, and should be reviewed and updated regularly.

**Rehearsals, drills and exercises of emergency procedures** “Practice makes perfect” is the common saying, and it is true for critical incident response as it is for any other activity. There are three levels of practice to consider using in your office or operation:

- 1) **Rehearsals** are designed to *familiarize staff with the planned responses*; they may involve full walk-through of the plan, or merely “talk-through” the sequence of events. These activities are explanatory in nature and are done to make the plans clear in physical terms, to the staff.
- 2) **Drills** are practices of specific activities that are done routinely, usually on a predetermined schedule. The most common of these is the *fire drill* or building *evacuation drill*. It is announced that a drill is planned at a set time so that people can schedule important meetings and other activities around it. The drills should be observed by managers and any errors or misunderstandings corrected.
- 3) **Exercises** are designed to *test staff*, as individuals or teams, on how they would react in an emergency situation. These activities are also planned to avoid disrupting other planned and important events, but should be announced to the staff with an element of surprise. The idea of these security exercises is to determine if staff can act quickly in a simulated emergency, know the correct protocols, and can solve unanticipated problems that may arise. In some cases elaborate informational inputs and simulated emergency effects can be simulated to add realism to the exercise.

**Standard Operating Procedures (SOPs)** – SOPs do not need to be as rigidly prescriptive as regulations, rather they can serve as default procedures to be implemented automatically unless circumstances dictate otherwise, thus reducing response time. These are generally concise in nature and describe step-by-step responses, with titles like: *Treatment for Snakebite, Taking Cover If Under Fire, Response to Fire in the Building or Guest House, Earthquake Safety Procedures*, and so on. The particular SOPs that are written for your office naturally depend on where you are and what threats you may expect to encounter. These are similar to contingency plans, but are simpler and more generic in nature.

**Stand-by arrangements** – In situations where there are other potential rescuers or responders nearby or with superior equipment or abilities, you should investigate the possibility of making stand-by arrangements for their services in the case of emergency. Exact services needed, whom to contact and how, and expected cost or reimbursement should all be clarified in advance.

**Communications systems** – If you cannot locate and communicate with your staff in an emergency, you will not be able to manage the incident. Considerations here include the electronic and technical specifications of the equipment and systems, e.g., do you have the equipment you need, is it in good working order, will it work in an emergency, and do staff know how to use it?

**Staff tracking systems** – Efficient ways to quickly find and communicate with staff require more than equipment. Procedures for using the equipment in an emergency and structures or systems for quickly contacting all staff are also essential. In high-risk areas you may need to control staff movements and ensure that contact can be made and maintained without delay. This includes organizational arrangements like a warden system or telephone information “tree” that organizes contact data and identifies responsibilities for contacting each staff member.

**Information management systems** – Reporting systems are needed to ensure managers at all levels receive information promptly. Do you know which kinds of reports are required, by whom, and under what circumstances? Information management systems can include consideration of what details can be publicized (possibly posted on a web page to facilitate rapid dissemination) and what facts will need to be controlled tightly (e.g., names of casualties). The information management



system can be very simple, from spoken instructions to staff on what information to release and what not to release, to sophisticated communications networks. Whatever system you have, the point is that in a critical incident, important situational information must reach decision-makers, and important decisions, requests, or orders must reach their intended destinations.

**Operations rooms or “Ops Centers”** An operations center is the hub of activity for the critical incident response. It may be very formal, with pre-assigned equipment, or may be ad-hoc, and rebuilt from remaining still-functioning equipment. In principle, the Ops Center activities should be dedicated to the strategic overview of the incident so that managers can respond appropriately rather than in a piecemeal manner. The staff of the Ops Center will collect and analyze information and make decisions that protect life and property. The goal is to allow continuity of the organization's program or activities to the extent possible, while those dedicated to the Ops Center focus on the urgent activities associated with the critical incident. Staff assigned to this duty must be properly trained, and be given the proper authority to carry out actions that are necessary to respond to the disaster, and which may not be their normal or day-to-day activities.

The tools and methods shown above illustrate an important point made at the beginning of this chapter: it is difficult to define the exact starting point of critical incident management because so many steps essential for good crisis management can only be taken well in advance of the incident. Simply put, good critical incident management depends on good security assessment and good plans and planning.

## 10.4 Information Management

Much of critical incident management is essentially information management. Deciding how much information to report can be difficult. In dangerous field situations where there are many security-related incidents, which incidents do you report? In some cases over-reporting can be problematic in that important incidents may get lost in the paperwork, or those receiving the reports may become so accustomed to receiving security reports on so many routine incidents that they fail to distinguish the difference between major and minor security incidents.



### Question

*How do you decide which security incidents to report and which ones not to report?*

---



---



---



---



---



---



## *Security incident reporting thresholds*

In high-risk environments, many small incidents occur, sometimes on a daily basis. It is not necessary to treat every security incident, or the news of every incident, as a **critical** incident. It is important to match your response to the need, and to modify the overall reporting level so that in the event of a significant security incident, important details do not become lost in the paperwork. In general, there are three levels of information to consider in your security reporting. There are some incidents that you should:

- 1) Report immediately
- 2) Include in your next routine or regular security report, even if it is not going out today
- 3) Note, but not report

The brief descriptions below explain each of these levels in more detail. Note that this is general guidance for security incident reporting; your own organization may have specific policies or rules which you should follow. Before going to the field you should know to whom or to which office in your organization you should report such incidents.

---

### *Report the incident immediately if:*

- The incident involves the arrest, detention, serious injury or death of a staff member.
- A staff member was injured or property was damaged in a malicious act.
- Staff had to take immediate actions to prevent possible serious injury/property damage.
- The incident could have a serious and immediate impact on the safety of staff.
- The incident involves a personal threat to a staff member.
- The incident is likely to receive substantial media coverage – your headquarters will not want to learn of this event on the evening news, send your report so that they can better respond to queries from the media that may follow the initial news coverage.

---

### *Include in your next regular periodic report if:*

- The incident indicates a general tendency or trends in the security situation.
- The incident could impact the agency in the medium/long term.
- The incident involves partner agencies not directly related to the organization's activities.
- The incident is minor (no injury/minimal damage) and does not have an impact on the organization's operations.

---

### *Don't report:*

- Random incidents not involving organization staff or partner agencies that do not indicate a significant tendency or trend.
- Information that will be seen by government interlocutors or other partners and may make your report seem to be a military or intelligence report.
- Generally, information concerning intimate matters such as sexual assault should not be reported through ordinary channels, especially when the victim specifically asks you not to do so. Your organization may have special procedures for handling such incidents with confidentiality.



Security reporting: some standard reports in UNHCR				
Type	Purpose of the Report	Frequency or Deadline	Addressees <i>Action/TO &amp; Info/CC</i>	Response or action expected
<b>Incident Report – Alerting</b>	<ul style="list-style-type: none"> <li>Inform management and others</li> <li>Initiate follow-up action</li> <li>Generate lessons learned</li> </ul>	<ul style="list-style-type: none"> <li><b>Alerting</b> – as soon as possible</li> </ul>	<i>As appropriate –</i> Head of office Country Representative	<ul style="list-style-type: none"> <li>Acknowledge and alert key actors.</li> <li>Mobilize support to assist office/staff as necessary.</li> <li>Allow affected office to manage its own situation by taking care of external involvement</li> </ul>
<b>Incident Report – Full Report</b>	<ul style="list-style-type: none"> <li>Record in incident database</li> </ul>	<ul style="list-style-type: none"> <li><b>Full report</b> – within 24 hours</li> <li>Report on follow-up investigation when complete</li> </ul>	Country security officer(s) or security focal points Headquarters-Bureau/Desk Officer	
<b>Routine Security Report</b>	<ul style="list-style-type: none"> <li>Provide update on current risk assessment in duty station</li> <li>Record and analyze incidents during the period</li> <li>Record safety management measures being taken/under consideration (including MOSS revisions)</li> </ul>	<p><b>No Phase:</b> Should be included in Monthly General SITREP.</p> <p><b>Medium threat (UN Phases I and II):</b> Report to HQ every two weeks (if possible to be timed to feed into overall situation report) by security officer or focal Point</p> <p><b>High Threat (UN Phases III to V):</b> Weekly report to HQ from security officer or focal point</p>	Headquarters-section responsible for security Other security management officials (e.g., in UN System, Designated Official, Chief Security Advisor, etc)	<ul style="list-style-type: none"> <li>Inclusion of key points in general reporting</li> <li>Influence on mainstream operational plans/ conduct</li> <li>Follow-up by section responsible for security at HQ non resource requests or liaison at with other HQ sections</li> <li>Oversight and evaluation from security section</li> </ul>

The following template can be used for a serious security incident report if you do not have an organizationally-required or specific format to follow. This one is slightly modified from a standard format used by UNHCR.

**Security Incident Report (Alerting Report)** — *Note: should be filed within 24 hours of the incident*

---

DATE \_\_\_\_\_ TIME \_\_\_\_\_

LOCATION \_\_\_\_\_

TYPE OF INCIDENT \_\_\_\_\_

**Organizational staff involved:**

NAME \_\_\_\_\_ NATIONALITY \_\_\_\_\_ ORGANIZATION \_\_\_\_\_

**Non-organizational staff involved:**

NAME \_\_\_\_\_ NATIONALITY \_\_\_\_\_ ORGANIZATION \_\_\_\_\_

**Short description of incident:**

**Details of loss, damage or destruction to:**

Organization property:

Personal property:

**Details of any injuries:**

**Immediate steps taken to ensure safety of other staff in area:**

**Other support needed/requested:**

**Additional information, comments assessment:**

## Summary



### Key Points

**Critical incident management** refers to actions that take place after a serious security incident has happened. However, many tools and preparedness measures needed to respond appropriately must be in place before the incident occurs.

---

The stages of critical incident and response that managers should understand are:

- Anticipation and pre-emption
- Initial reaction
- First steps
- Establishing control
- Establishing a routine
- Post-event activities

---

Several useful tools and measures should be in place to afford the manager full ability to respond effectively to a critical incident. These include:

- Contingency plans
- Rehearsals and drills
- Standard operating procedures
- Guidance notes
- Communications
- Staff tracking systems
- Information management systems
- Operations rooms

---

Not every security incident is a critical incident and not all security incidents should be reported. In general, there are three levels of security incident reporting that should be considered:

- 1) Report immediately
- 2) Include in periodic reporting
- 3) Note, but don't report

---

Standard formats and templates for security reporting can be helpful as information checklists to promote completeness of the report.



## Chapter 10 Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

- T**  **F** 1. Any reported security incident should be considered a critical incident.
- T**  **F** 2. Critical incident management is dependent entirely on the strength and character of the manager; preparedness measures may reassure staff, but will not be truly useful in the event of a serious security incident.
- T**  **F** 3. Critical incident management and Security Risk Management mean the same thing.
- T**  **F** 4. The first step to be taken after a critical incident is to get control of yourself and your own emotions.
- T**  **F** 5. Critical incident management is limited to those actions that occur within the first 24 hours after a serious security incident.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following would be useful to have in place before you are required to manage a critical incident?
  - A** Assessment of threat and risk.
  - B** Briefings and rehearsals.
  - C** Contingency planning.
  - D** Detailed reports of all security incidents that have previously occurred, regardless of their scale or impact.
- 7. Which of the following are examples of immediate steps to take in the event of a critical incident?
  - A** Undertake immediate life-saving activities.
  - B** Confirm information/identity of casualties.
  - C** Account positively for all staff.
  - D** Limit movement of staff or relocate as necessary.



**Chapter 10**  
**Self-Assessment Questions** *(continued)*

8. Which of the following should the critical incident manager do in the *post incident phase*?
- A** Analyze the incident and responses.
  - B** Return all security procedures and practices to pre-incident norms as soon as possible.
  - C** Update plans and revise procedures accordingly.
  - D** Assist recovery for those involved in the incident through counseling and other types of support.
9. Which of the following tasks should be performed in the Ops Center after a critical incident?
- A** Assemble information to understand the strategic overview of the incident.
  - B** Ensure that all program activities continue as they were before the incident.
  - C** Provide social and psychological support for incident victims and colleagues.
  - D** Focus on the urgent activities associated with the critical incident so that others can deal with other operational concerns.
10. Which of the following security incidents should be reported immediately?
- A** Staff of your organization, while undertaking a road mission to the border, narrowly avert being caught in the crossfire of a skirmish between armed combatants and are forced to return to the office.
  - B** Children are playing football in a field beside your organization’s building; one child accidentally kicks the ball through a window in your office, causing \$50 in damage.
  - C** An angry crowd of demonstrators gathers outside your office protesting your organization’s presence in the country; one person throws a rock through a window, causing \$50 in damage.
  - D** A staff member is arrested by the local police for drug possession charges.



**Chapter 10**  
**Answer**  
**Key**

- |     |            |    |   |
|-----|------------|----|---|
| 10. | A, C, D    | 5. | F |
| 9.  | A, D       | 4. | T |
| 8.  | A, C, D    | 3. | F |
| 7.  | A, B, C, D | 2. | F |
| 6.  | A, B, C    | 1. | F |

# Chapter 11

## Security Relationships in the Field

*United Nations staff of the World Food Programme (WFP) unload bottles of clean drinking water for hurricane victims in Gonaives, Haiti, as members of the Argentinean battalion of the United Nations Stabilization Mission in Haiti (MINUSTAH) provide security.*



UN Photo by Logan Abbasi

This chapter examines how relationships with other organizations and people can affect your security in the field. In the increasingly complex humanitarian working environment, the number of organizations responding to emergencies has grown significantly. While many actors may be involved in addressing the situation, complete harmony of goals and objectives cannot be assumed. Still, even when organizational mandates differ, there may be common ground to pursue mutually desired outcomes together. Safety and security is often one such common area, and recognition of the value of working together to keep staff safe is a salient trend in modern field operations.



### Learning Objectives

This chapter presents an overview of some important field security relationships. It gives some guidance in developing and maintaining useful security relationships in situations that can be of benefit for all. In particular, you will learn about:

- Security relationships with the host government.
- Security relationships with and among NGOs and other partner agencies.
- Security relationships between humanitarian and military organizations.
- Staff security and the security of beneficiaries.



## 11.1 Security Relationships with the Host Government

According to generally recognized principles of international law, primary responsibility for the security and protection of humanitarian personnel resides with the host government. This obligation flows from the responsibility of states to maintain law and order within their borders. In general, humanitarian organizations expect that security and protection should be provided in this way by the national governments of the countries in which they work. While not always possible, this is the expected international norm.

*“IGOs (Inter Governmental Organizations) should extend security protection provided for UN organizations to NGHAs (Non Governmental Humanitarian Agencies). Where security services are provided for intergovernmental organisations, this service should be extended to their operational NGHAs partners where it is so requested.”*

– The Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief Annex III: Recommendations to Intergovernmental Organisations

*“Clarity of host nation responsibility acts as a vital reinforcement of operational effectiveness...the UN should concentrate on enhancing co-operation and collaboration with country law enforcement agencies in countries which have well developed security structures. ...In countries where a fully functioning national government may not yet exist, there is the further opportunity to engender host nation security capacity partnership with member states.”*

– Letter from Sir David Veness to Designated Officials and Heads of Agencies

However, humanitarian staff sometimes work in areas where the host government’s capacity to ensure law and order is minimal or doubtful. In these cases, additional precautions become necessary to reduce risk to acceptable levels. This learning module has focused on analyzing such situations and implementing appropriate measures. Nevertheless, the operating principle must remain to involve the host nation in staff security wherever possible and to actively encourage it to fulfill its obligations under international law. Rather than immediately seeking alternatives when government capacity appears inadequate, offices should consider whether targeted support could rectify the deficiencies and increase the capacity of host nation agencies to be reliable partners.



**Question**

*What steps should humanitarians take when building relationships with host government authorities to improve field security for staff?*

---

---

---

---

---

Some important security counterparts to consider are the local or national police, the fire department and paramedics, and sometimes the armed forces. In rural and border areas, humanitarian field staff may also interact with gendarmerie, immigration and border police forces, special guard forces assigned to camp security functions, and various military and paramilitary forces. Some general guidelines for approaching partnership with these elements are listed below; however, as always, practices must be adapted to the realities of the specific environment.



**Learn who the right contacts are and establish relationships.** You should know which agencies and organizations are involved in your security and have names and contact details readily available. Of course, the first step in any partnership is building confidence and trust, and this can only be achieved by devoting time and effort to the relationship

**Clarify needs and assess capabilities and limitations.** Don't assume that your government partners understand your expectations of them; discuss clearly your anticipated needs and desired reaction. Equally, you should strive to understand the abilities, limitations and likely responses of partners, and plan accordingly or where possible, seek ways to improve deficiencies.

**Consider sensitization or orientation.** It should not be taken for granted that host government security partners know and understand your mission, mandate, or basic operating principles. In some cases, sensitization concerning your organization's mandate, international humanitarian and human rights law, and the various Codes of Conduct that may apply to your organization, can be an effective tool in preventing problems.

**Consider targeted training and other capacity-building support.** Your organization or other partners may be able to provide further specialized assistance for host nation security partners. For example, personnel trained in community-based approaches (including community policing techniques) may be able to share expertise on methods of resolving conflict without resorting to deadly force.

Special difficulties can arise in situations where the host nation's human rights practices are doubtful. This is especially true when the situation involves your beneficiaries, as calling upon law enforcement may be perceived as placing people's basic rights in jeopardy. For example, in some countries calling the police to respond to an incident of refugee misbehavior may be perceived as UNHCR's "retracting its protection" of that refugee, in the worst case leading to the fear or possibility of *refoulement* (sending refugees back into danger by returning them to the countries they have fled).

Managing the dilemma of ensuring both adequate security and respect for human rights is not easy. Concerned staff (managers, security officers and others) must learn the capabilities and inclinations of their counterpart agencies and first-response law enforcement agencies and, if necessary, work to raise their awareness of international norms and basic human rights.

Should there be a need for police intervention for security purposes, humanitarians should advocate for the basic preconditions of humane treatment and due process. In the event that a person of concern is detained, staff should visit the person and ensure the provision of these basic rights. Where these principles are not respected or are in doubt, your office may need to refer the matter to your headquarters and other partners as appropriate for further attention. In all cases, the office should not fatalistically accept dangerous or otherwise inappropriate behavior; your response should be to encourage host nation partners to fulfill their functions in a manner that respects international standards.

## 11.2 Security Relationships with and among NGOs and Other Partner Agencies

Recent years have seen a sharp rise in the number of organizations responding to large-scale humanitarian emergencies. It is perhaps for this reason that there has also been increased recognition of the value of achieving more effective partnerships, both in confronting humanitarian challenges and in response to security threats.

UNHCR, in its organizational security policy first published in 2002, recognized an obligation to assist in the safety of collaborating NGOs. The policy states that "[UNHCR] Offices should seek to



help them achieve the same level of field safety for their personnel as UNHCR has put in place for its staff, to the extent allowable by mandate and capacity.” This formulation expresses the ideal to which offices should strive, while recognizing that in practice there will always be limiting factors.

UNDSS published a paper entitled “Saving Lives Together” in 2006 that echoed this spirit of security cooperation among humanitarian partners. Intended to serve “as a framework of best practices on security collaboration which may be implemented without imposing upon our respective mandates or compromising the neutrality of humanitarian efforts,” the document offered further practical suggestions on how agencies can cooperate in the field to keep their staff safe.

NGOs, of course, constitute a diverse group, and it is impossible to generalize for all the security relationships that exist among them and between them and the UN, national authorities, and others. Their many mandates and missions may preclude some actions and their differing organizational cultures can make some joint activities difficult. However, as field environments remain as insecure as ever, basic actions for the common safety of humanitarian staff are increasingly becoming the norm among even the most independent-minded NGOs.



**Question**

*What steps should humanitarians take when building relationships with host government authorities to improve field security for staff?*

---

---

---

---

---

---

---

---

---

---

Security-related cooperation with partners can take many forms and levels, from basic information-sharing to sharing equipment and even joint planning for security-related tasks such as staff evacuation. Listed below are some general practices that illustrate some of the possible levels of coordination.

**Share information on security incidents and threats** – This is the most rudimentary form of cooperation and should be considered standard procedure in nearly all cases. Even the most independent-minded organization should see the utility of sharing immediately security-related news that could affect all humanitarians working in the area. Ways of accomplishing this include:

- Creating an email “security group” composed of heads of all local agencies and security focal points, and establishing as standard procedure the inclusion of all on any incident reports.
- Organizing regular security meetings with agency heads or security focal points, or have a security officer or security focal point do so.
- Appointing, or encouraging local NGOs to appoint, a collective security focal point, who may interact with local law enforcement officials and security officers of the UN system. This can be an effective option when those other interlocutors would not otherwise have the time to meet with all agencies regularly.



- Where resources permit, recruiting an inter-agency security expert to provide support services for a network of humanitarian partners. By pooling resources, this approach can make accessing the needed expertise cost-efficient for all.
- Including security as a fixed agenda item in local operational planning meetings (and ensuring it is not neglected thereafter).

**Put information-sharing systems or measures in place** – Other humanitarian field offices, including UN offices should inform collaborating NGOs of the security guidelines in place for their own staff and encourage their adoption by the NGOs as a matter of prudence, while respecting their right of final decision.

**Conduct useful shared security briefings and trainings** – In offices where a professional security officer is assigned, the security officer should, in principle, be available to provide briefings and training for staff of partner agencies (subject to time constraints and the desire of the partner organizations). At a minimum, written security briefings could be shared with partners if appropriate, and it should be standard procedure to invite partners to attend security trainings unless there are specific factors prohibiting this.

**Make other technical expertise available to partners** – The security officer may also provide expertise in areas such as security risk assessment, instructions for guard forces, and assisting in recruiting security professionals, time permitting. In such cases it must be clear that such assistance does not imply liability resulting from any actions or advice taken.

**Conduct joint contingency planning** – Wherever practical, partners should be included in planning for security-related contingencies that might impact the partner's staff as well.

**Combine voices in advocacy** – Several partners together may have greater bargaining power in negotiating with the host government or other interlocutors. Advocacy applies as well to the UN-NGO relationship, where UN agencies may play a role in urging greater host nation support for NGO partners as well as UN staff, for example by allowing the use of telecommunications equipment and frequencies where these are restricted.

**Share administrative and logistic support** – This may include assistance in obtaining and transporting needed equipment (where permitted by local laws).

**Loan or give equipment** – In some instances, an organization may provide items such as radio handsets and other telecommunications equipment, or emergency equipment for vehicles, on a temporary or permanent basis—pending availability of resources. With UNHCR, for example, this measure is the exception rather than the rule, but is sometimes justified in remote and isolated areas where staff safety is vitally linked to partner safety, or where necessitated by unforeseen changes in the security situation. It goes without saying that in such cases, steps to ensure accountability of the equipment are a must; however, these administrative considerations should never, in themselves, supersede the imperative to avoid loss of life.

**Conduct joint emergency evacuation planning** – In Chapter 9 we saw that planning for evacuation is part of the due diligence of a manager working in an insecure area. Where like-minded humanitarian agencies are working together in a remote and dangerous environment, it only makes sense that planning should be conducted jointly to the extent possible.

A question of frequent concern is the responsibility of UN agencies to NGO partners in the event of an evacuation of international staff. When UN Security Phase 5 is declared, the responsibility of evacuating international UN staff from danger falls to the common UN system. Officially, the UN security system will only accept responsibility for evacuation of international UN staff, and international staff of organizations who have agreed to participate in the UN security system on a global cost-sharing basis. This means that UN agencies on the ground may not have the authority to guarantee evacuation of staff for partner staff.



Although the UN cannot legally assure the evacuation of agencies not participating in the UN common system, history shows that partner agencies have often been included in UN evacuations on a case by case basis (subject to subsequent reimbursement from the evacuated organization). This means that while managers in UN agencies should be cautious not to make formal guarantees, they can increase preparedness by accounting for NGO partners in evacuation planning as far as it is logistically and financially feasible, permitted by administrative and host-country rules, and desired by the individual NGO. For example, they may include the partners in contingency planning sessions, maintain lists of staff potentially requiring evacuation, anticipate the number of spaces needed (e.g., on a helicopter or airplane) and keep the partner agency informed of developments.

### 11.3 Security Relationships between Humanitarian and Military Organizations

Civilian interaction with military forces, or civil-military coordination (CMCoord) has become one of the most controversial topics within the humanitarian community. While many emphasize the mutual advantages, and sometimes necessity, of working together, others fear a blurring of roles and a loss of humanitarian identity that can jeopardize access to beneficiaries and put aid workers at increased risk.

Consider the following two quotations, suggesting widely different conclusions regarding the utility of civil-military cooperation:

*"For the last two years at least, NGOs have been voicing concerns about the threat 'hearts and minds' activities [the use of aid by military forces to gain the support of a population] pose to humanitarian agencies – in terms of perceptions of their independence and concomitant security. These concerns have gone largely unheeded. Only after the murder of five MSF workers in June 2004, and the subsequent withdrawal of that organization from Afghanistan, has the issue received the attention it requires... Surely this high price should never be levied again. It is imperative that militaries, and their political masters, either prove that the risks posed by 'hearts and minds' operations are outweighed by the security benefits, or else they should cease including them in their portfolio of military activities."*

– Provincial Reconstruction Teams and Humanitarian-Military Relations in Afghanistan  
Save the Children London, 2004

*"To enhance the protection of the Canal Hotel compound, United States military personnel established an observation outpost on the roof of the hotel and placed a five-ton truck to block access to a service road that runs parallel to the western perimeter wall... UN Senior management in Baghdad was uneasy with this highly visible military presence... (they) asked the Coalition Forces to withdraw their heavy equipment from the front of the compound, dismantle the observation post on the roof top of the building and remove the obstacle on the access road... Later, the U.S. military laid concertina wire across the access road, but again the United Nations requested that the obstructions be removed. The access road was open to traffic on 19 August and was used by the attackers to approach and target the UN building ..."*

– The Report of the Independent Panel on the Safety and Security of the UN Personnel in Iraq 20 October, 2003.

Is the increasing involvement of military actors in humanitarian activities, including for purposes of gaining popular goodwill (i.e., "winning hearts and minds"), a dangerous erosion of humanitarian space, as the author of the first quotation suggests? Or is the military potentially a beneficial presence, ensuring the safety humanitarian workers, as one might conclude from the second citation?

Complex humanitarian emergencies have increasingly seen humanitarian and military actors operating closely within the same space. In such cases, humanitarian agencies often benefit from, or even depend on, the military for support.


**Question**

*In what useful ways or areas has the military supported humanitarian programs and activities without being in direct conflict with humanitarian principles or concerns?*

---



---



---



---



---

Military organizations are generally organized and equipped for purposes that are very different from humanitarian organizations. Nevertheless, their many strengths do overlap, particularly in the areas of logistics, engineering, command, control and communications, and, of course, security. Military forces have usefully supported humanitarian missions in the following ways:

- Providing or contributing to security for beneficiaries and staff
- Ensuring safe, weapon-free areas to carry out humanitarian operations
- Escorts
- Mine action
- Logistic support: airlift and other forms of transport
- Logistic support: infrastructure and engineering
- Evacuation (including MEDEVAC)
- Information sharing (in support of needs of beneficiaries and security of staff)

However, there are potential dangers for humanitarians interacting with the military. Those undertaking working relationships with military forces should consider the possible results of cooperation, or even perceived cooperation with the military:

- It can compromise neutrality and impartiality of humanitarian staff.
- It can blur the role of the military and humanitarian actors.
- It can compromise humanitarian independence of action.
- Military forces may not share the same goals or priorities.
- Military methods and tactics may not be compatible.
- It can lead to local dependence on the military.

Balancing potential benefits and risks of interaction requires considering a number of independent factors. One is the particular armed force with which cooperation is envisioned. It is important to remember that the term “military” comprises a wide range of organizations with varying degrees of professionalism and international legitimacy. Simply put, all militaries are not alike, and the degree of interaction that is appropriate will depend in part on the particular armed force being considered. Some different categories of armed forces include the following:

- UN-controlled peacekeeping forces (e.g., “Blue Helmets”).
- UN-authorized military forces (i.e., not organized or led by the UN but implementing a mandate authorized by the Security Council; recent examples are the Economic Community of West African States Monitoring Group (ECOMOG) in Sierra Leone and African Union forces in Sudan).
- Armed forces of the host country.
- National guard of the host country, or other forms of “levees.”



- Other national armed forces.
- National paramilitary forces and militias.
- Non-state armed forces (e.g., rebel armies, irregular militias).

On the whole, space for cooperation between humanitarian organizations and the first two categories (UN-led or UN-authorized) is usually greatest, while interaction with the last (irregular forces) is generally undertaken in exceptional cases only. These considerations, however, must take into account further situational factors.

One such factor to be considered is the type of cooperation envisioned. The appropriateness of a mission will depend on many situational factors. One general principle, articulated in Inter-Agency Standing Committee (IASC) guidelines, is that, where possible, military forces should be discouraged from playing the role of the humanitarian aid providers; i.e., their role in relation to humanitarian actors should be limited to helping create a secure operating environment that enables humanitarian action. However, there are cases where a direct military role is necessary, as in the tsunami relief effort in early 2005. In all events, careful consideration should be given to whether other means are available (the military should be a provider of last resort) and humanitarian actors should retain the lead role in undertaking and directing humanitarian activities.

Finally, the nature of the general situation plays a large role in determining the appropriateness of civil-military cooperation. In cases such as a large-scale relief effort in the wake of a natural disaster, where there is no fighting and all parties are generally welcomed, opportunities for cooperation with military forces may be great. In situations where armed forces are engaged in active conflict, the same level of interaction may compromise an aid organization's neutrality and put its staff at risk. However, applying these guidelines requires caution, as situations are rarely entirely one extreme or the other. This lesson was evident in recent disasters in Indonesia and Sri Lanka (Tsunami of 2004-05) and the south Asia earthquake of 2005, where natural disasters were superimposed upon pre-existing enmities (separatist conflict in Aceh and Sri Lanka, and a tense border dispute between India and Pakistan). Because of ongoing conflicts or tensions in these areas, it would have been dangerously wrong to assume that military presence was unequivocally welcomed by all.

In analyzing situations such as these, it can be useful to consider the degree of **consent** for the military actors involved, and level of **force** being used. In a situation where the military is accepted by all parties and force is not being used (e.g., some disaster relief and post-conflict peace-building situations), the space for interaction with the military is increased. Where the military is not accepted by all sides, and force is being used (e.g., combat situations), the opportunity for civil-military coordination is limited.

At a minimum, humanitarian organizations should ask the following questions before working closely with any military force:

- What will be the impact of cooperation on your organization's perception of impartiality and neutrality?
  - Will it compromise your organization's access to beneficiary populations?
  - Will it potentially make your staff a target?
- Are the military's goals compatible with your organization's goals?
- Is there consent of all parties?
- Will it limit your independence of action?
- Will it lead to dependence on the military?
- Are there other means available?

Should you determine that interaction is in your organization's best interest, and in the best interest of the people you are trying to assist, you will need to communicate with military forces. Simply



talking to soldiers can be difficult for some humanitarian field workers. One factor that often complicates communication is the difference in organizational culture.

**Understand the differences between military and humanitarian work cultures** – The humanitarian community and professional armed forces both have strong organizational cultures which shape the actions, perceptions and beliefs of individuals. Differences in these cultures can be a significant cause of misunderstanding between groups and people. Some typical examples:

- **Hierarchy and structure** – Humanitarians tend to value flexibility greatly; hierarchy is a “necessary evil.” The military places great value on unity of effort and sees the chain of command as a source of order and stability. This means that in the military, issues must be directed to the appropriate level; addressing them to someone who does not have decision-making authority is fruitless.
- **Decision making** – In humanitarian organizations, a good leader is expected to be a consensus-builder; compliance with a decision stems from inclusion of the stakeholders. A military leader is expected to be decisive; compliance stems from the strong leadership or authority of the leader. Humanitarians are often more tolerant of a slow or messy process if it leads to a result that all can “buy into”. In the military it is understood that the leader decides and not all decisions can please everybody.
- **Communication style** – Humanitarians tend to value speech that conveys compassion and respect while avoiding insensitivity. Military culture often favors a more direct, blunt style.
- **Purpose of humanitarian assistance** – For aid workers, the basic aim of humanitarian assistance is to provide lifesaving emergency aid to those in need, without regard for race, religion, ethnicity, social/political group, or other affiliation. This is often true for militaries as well, but national objectives will be a factor. Do not take for granted that military forces share the same assumptions or goals; be sensitive to divergent interests.

This section is only a primer for a subject on which there is vast and growing literature. Those seeking further information and guidelines concerning the civil-military relationship can refer to a number of instructive documents produced by the United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA), including *Civil Military Guidelines and Reference for Complex Emergencies* (2008) and *Guidelines on Humanitarian Negotiations with Armed Groups* (2006); as well as UNHCR’s handbook, *UNHCR and the Military, a Field Guide* (2006).

## 11.4 Staff Security and the Security of Beneficiaries

This section concerns the security “relationship” between humanitarian organizations and the people they seek to help. By and large, efforts to ensure the security of beneficiaries complement and reinforce measures to improve staff safety. However, instances can occur when the two goals appear to be in opposition, and this can pose acute managerial dilemmas. Do extremely urgent needs on the ground justify accepting increased risks? When do the dangers to staff outweigh the imperative to assist others in need? And what can be done in cases where beneficiaries themselves can become a source of risk to humanitarian workers, even as they try to protect them?

### *Integrating staff and beneficiary security*

Most humanitarian workers would probably agree that efforts to ensure the security of beneficiaries generally go hand in hand with steps to improve staff safety. Examples of where these two objectives are compatible and mutually reinforcing include efforts to ensure safe, weapons-free areas for humanitarian operations, civil-military coordination to provide security, host nation coordination for police and other law enforcement presence, and establishing security protocols in camps and other refugee-populated areas.



**Question**

*What can you do at the field level to keep the overall operating environment safer for everyone in violent situations?*

---

---

---

---

---

In 1998, UNHCR’s Policy Research Unit (now Evaluation and Policy Analysis Unit) produced a conceptual framework proposing an incremental series of responses to problems of instability in conflict-affected areas. The “Ladder of Options” approach, while specifically intended for camps and other refugee-populated areas, generally applies to most insecure areas. Its basic principle is that in nearly all cases, the solution involving the minimum necessary force is preferable. The “steps” on the Ladder of Options are:



Many local security situations fall within the range of Options 1 and 2, where a number of good practices have been developed:

- Establish or call for mechanisms for the enforcement of law and order, including sufficient police/guard presence.
- Train, sensitize and build the capacity of local police.
- Consider specially vulnerable groups (unaccompanied women and minors, the elderly, minority groups) in action planning and take appropriate measures to ensure their safety. This may include special considerations for camp layout and design, distribution of goods and coverage by law enforcement.
- Where possible, establish support agreements in writing, such as MOUs (Memoranda of Understanding) or MOAs (Memoranda of Agreement).
- Advocate for and facilitate adequate camp governance, management and maintenance.
- Provide an efficient and transparent means of addressing complaints or problems identified by disaster-affected people.
- Establish effective and proactive information programs to keep the community informed and avoid the spread of rumors.
- Where possible and appropriate, involve the beneficiaries in their own security, and strengthen working, self-policing mechanisms.



- Establish mechanisms for regular, systematic monitoring including regular international presence.
- Provide for community activities, particularly for unemployed youth.
- Establish staff safety protocols within camps (setting “minimum standards”) and adhere to them.

### ***Balancing staff safety and beneficiary safety***

There are also times, however, when the safety of staff and that of the people you are seeking to help appear to be in opposition. This is the case when people needing assistance are located in insecure and conflict-ridden areas, and providing the protection and assistance that they need may put staff at risk. This can pose acute managerial dilemmas. When is the risk to staff tolerable and does this point change when needs on the ground are extremely urgent? Is there a balance point where dangers to staff outweigh the urgency of the needs?

There are few absolutes in such cases beyond the managerial responsibility never to expose staff to undue risk. However, in these cases, criticality assessment can be an important managerial tool. In Chapter 8 you saw that criticality assessment encourages managers to weigh risks to staff (as expressed in your risk analysis) against the importance of the programs being undertaken. While it cannot produce absolute answers, and should never be used to justify taking unacceptable risk, criticality assessment can help clarify thinking and lend support to a decision based on reasonable risk once it is taken.

Finally, in certain cases, the beneficiaries themselves may become a source of risk to staff.



#### **Question**

*What reasons can you list why victims of natural or man-made disaster might constitute a threat to humanitarian field staff?*

---



---



---



---



---



---

Humanitarian workers sometimes experience threats, intimidation and even violence from the people they are trying to protect. Here many factors are beyond our control: desperation and distress caused by traumatic experiences, policies or actions taken by governments or other parties, insufficient assistance, and frustration at the difficulty of finding a solution to their plight, to name a few. Other factors, however, are within our ability to influence. Below are several common elements that can contribute to tension within the beneficiary group that humanitarian workers can usually influence to some degree.



Many people, including disaster victims, refugees and other displaced persons, may resort to threats, intimidation or violence when:

- **They are not treated with uniformity, respect and sensitivity** – Unclear or irregular distribution of aid, application of procedures, long periods of unavailability, tardiness for scheduled interviews or reacting with insensitivity to the concerns of those needing assistance can aggravate an already delicate situation.
- **There are perceptions of improper or unethical behavior** – This can include fraud, favoritism, abuse of power and other irregularities. Ensuring a transparent and uniformly applied process and establishing dispute resolution mechanisms that are perceived to be fair and neutral can be part of the solution. Above all, regular managerial oversight and timely intervention are essential in identifying problems and dealing with them before they become dangerous.
- **There is insufficient information, inaccurate information or rumors** – Information management emerges as one of the common factors of many incidents of violence among beneficiary populations.
- **Policies are not clear or fully understood or there are perceptions of uneven or unfair applications of the policy** – Similarly, tension can arise when policies change abruptly, or faster than the community can understand or absorb them. Humanitarian agencies may find themselves vulnerable because of sudden policy changes coming from the host government, donor countries or other parties over which they have little control.
- **Events are poorly planned or culturally insensitive.**
- **People are tired of waiting** – This may be the case when there are delays in providing needed assistance.
- **People have reason to believe that violence and intimidation will be effective** – When people see that the tactics of intimidation work, they are encouraged to use them again. This underscores the critical importance of setting and holding a policy of zero tolerance of inappropriate conduct among program beneficiaries; there can be no flexible or wavering line in cases of unacceptable and unlawful behavior, even if this means having recourse to law enforcement authorities.

Those interested in reading more on the relationship between beneficiary and staff safety can refer to the *Handbook for the Protection of Internally Displaced Persons* (IASC, 2007); *Operational Guidelines on Maintaining the Civilian and Humanitarian Nature of Asylum* (UNHCR 2006); and *Operational Protection in Camps and Settlements* (UNHCR, 2005).

## Summary



### Key Points

**Security relationships** with the host government are critical in all countries where governments are in control. According to generally recognized principles of international law, primary responsibility for the security and protection of humanitarian personnel resides with the host government.

---

Some basic steps to make the most of government relationships for improved security include:

- Learning who the right contacts are and establishing relationships
- Clarifying needs and assessing capabilities and limitations
- Providing sensitization or orientation activities where needed
- Providing targeted training and other capacity-building support

---

Security relationships with and among NGOs are complex and not easily categorized. One area, however, that is generally accepted as being useful for improving security for NGOs, is improved cooperation in various security-related field activities. Some examples of the range of coordination activities that can improve NGO security include:

- Sharing information on security incidents and threats
- Conducting useful shared security briefings and trainings
- Making technical security expertise available to partners
- Conducting joint contingency planning
- Combining voices in advocacy

---

Security relationships with military organizations have both potential benefits and risks for humanitarian agencies. Areas of useful cooperation in the field in which the military can improve staff security include:

- Providing or contributing to security for beneficiaries and staff
- Ensuring safe, weapons-free areas to carry out humanitarian operations
- Escorts
- Logistic support
- Evacuation (including MEDEVAC)
- Information sharing (in support of needs of beneficiaries and security of staff)



Potential risks of interaction with the military include the following:

- It can compromise neutrality and impartiality of humanitarian staff.
- It can blur the role of the military and humanitarian actors.
- It can compromise humanitarian independence of action.
- Military forces may not share the same goals or priorities.
- Military methods and tactics may not be compatible.
- It can lead to local dependence on the military.

---

In general, consideration of the appropriateness of any interaction should take into account the military organization involved, the type of cooperation proposed, and the overall situation. Humanitarian organizations should always consider the following questions before working closely with any military force:

- What will be the impact of cooperation on the organization's perception of impartiality and neutrality?
- Are the military's goals compatible with your organization's goals?
- Is there consent of all parties?
- Will it limit your independence of action?
- Will it lead to dependence on the military?
- Are there other means available?

---

Security relationships between humanitarian workers and their beneficiaries are generally mutually reinforcing; however, there are instances where they may appear to be in opposition, and situations may occur where beneficiaries themselves pose a threat to humanitarians.

---

In complex field situations where safety and security for humanitarian workers and beneficiaries are lacking, one approach to considering response measures is the "Ladder of Options":

- Option 1: Preventive and corrective measures
- Option 2: Reinforcing existing national law enforcement
- Option 3: Deployment of international observers
- Option 4: International support to national security forces
- Option 5: Deployment of international police forces
- Option 6: Deployment of regional military forces
- Option 7: Deployment of international military forces  
(under Ch. VI of the UN Charter)
- Option 8: Deployment of international military forces  
(under Ch VII of the UN Charter)



## Chapter 11

### Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is True or False

- T**  **F** 1. Many people, including disaster victims, refugees and other displaced persons, may resort to threats and intimidation when they are not treated with uniformity, respect and sensitivity.
- T**  **F** 2. Sharing information on security incidents and threats should be avoided since most organizations' mandates do not allow for such exchanges.
- T**  **F** 3. According to generally recognized principles of international law, primary responsibility for the security and protection of humanitarian personnel resides with the host governments of the countries in which they work.
- T**  **F** 4. Despite some differences in organization and operating norms, military forces and humanitarian organizations can be safely assumed to share the same overall objectives in responding to a humanitarian emergency.
- T**  **F** 5. When there is a need for police intervention with the local community or program beneficiaries for security purposes, humanitarians should advocate for the basic preconditions of humane treatment and due process and recognition of applicable human rights laws.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

6. Which of these measures would be considered the last step to be taken on the "Ladder of Options" conceptual framework of incremental responses to problems of insecurity in camps and other refugee-populated areas?
- A** Deployment of international military forces (under Ch VII of the UN Charter).
- B** Reinforcing existing national law enforcement.
- C** Deployment of regional military forces.
- D** Deployment of international observers.
7. Which of the following are true regarding cooperation between humanitarian organizations and the military?
- A** Such relationships usually improve the perceived neutrality and impartiality of humanitarian staff.
- B** Such relationships help to clarify the roles of the military and humanitarian actors.
- C** Such relationships can compromise humanitarian independence of action.
- D** Such relationships are always beneficial in conflict situations where the military will be needed to provide security.



**Self-Assessment Questions** *(continued)*

8. Which of these activities might help humanitarian organizations increase the capacity of host nation agencies so that more reliable security partnerships could be pursued?
- A** Learning who the right contacts are and establishing working relationships.
  - B** Clarifying your own security needs and realistically assessing government capabilities and limitations.
  - C** Providing sensitization or orientation activities for government counterparts.
  - D** Providing targeted training and other capacity-building support.
9. Which of the following conditions apply to the UN's role in evacuation of humanitarian staff in case of a serious security incident or situation?
- A** When Security Phase 5 is declared, the responsibility of evacuating international UN staff from danger falls to the common UN system.
  - B** Officially, the UN security system can only accept responsibility for evacuation of international UN staff and international staff of organizations who have agreed to participate in the UN security system on a global cost-sharing basis.
  - C** UNHCR guarantees the evacuation of staff for any partner organization, should the security situation warrant evacuation of UNHCR staff.
  - D** UN evacuations of international staff automatically include international staff of all humanitarian organizations affected by the same threat.
10. Imagine that humanitarian organizations are responding to a large-scale natural disaster in an otherwise peaceful country. Which of the following might humanitarians consider useful and legitimate support from units of a foreign armed force that is contributing to the response?
- A** Identification of most vulnerable people or groups in a community to receive relief assistance.
  - B** Ensuring safe, weapons-free areas to carry out humanitarian operations.
  - C** De-mining activities.
  - D** Logistic support in major disasters such as airlift and other forms of transport.



**Chapter 11  
Answer  
Key**

- |    |   |     |            |
|----|---|-----|------------|
| 1. | T | 6.  | A          |
| 2. | F | 7.  | C          |
| 3. | T | 8.  | A, B, C, D |
| 4. | F | 9.  | A, B       |
| 5. | T | 10. | B, C, D    |

# Chapter 12

## Security and Stress

A UN Assessment Team, including representatives of the World Health Organization, UN Security and World Food Program, discuss plans before landing in Shardi, Pakistan for assessment of the earthquake response area in October 2005. Difficult and hastily arranged assignments undertaken with new teammates, long hours, uncertain expectations, and under dangerous field environments can lead to significant stress.



UN photo by Evan Schneider

*"I needed to mourn the people I lost and all the suffering children. It is incredible, the way it suddenly hits you after the real threat is over."*

– A former UNICEF Programme Coordinator in Burundi

*"We need to create support systems that will be in place before, during and after deployment of staff; and that will be fully sensitive not only to the physical security of those at risk, but also their mental and emotional health. Exhausted, stressed and inadequately supported staff cannot do their jobs effectively. They may want, and try, to tough it out, but in the final analysis, everybody is damaged."*

– United Nations Secretary-General Kofi Annan

Stress and security are closely interrelated. A tense security situation will raise the general level of stress, and serious security incidents can cause serious traumatic stress disorders. Stressed-out people in insecure situations will raise the level of risk to themselves and others. High levels of stress impact on the quality and accuracy of judgment, causing staff members (and managers) to miscalculate the risks involved in dangerous situations.



### Learning Objectives

This chapter outlines practical steps that humanitarian field staff and managers can take to reduce stress-related security risks. You will learn:

- The relationship between security and stress.
- The basic "need to know" information about stress.
- Some individual adapting and coping techniques.
- Advice for managing staff stress in insecure field offices.
- Advice for responding to critical stress incidents.



## 12.1 The Relationship between Stress and Security

Stress is a normal part of field life for humanitarian workers. A little stress helps us function at a higher level. Fear, for example, quickens our responses and makes us alert and hyper-aware, which can be very useful when under the threat of attack. We cannot stay in this heightened state too long, however, before ill effects are felt. As soon as the challenge (or threat) is overcome, the body recuperates and readjusts to a normal level. Stress becomes harmful when the challenges in the environment exceed our capacity to adapt to the challenge or when our adaptation lasts too long.

In dangerous field situations the usual stressors of humanitarian field work are amplified. Activities take on a sense of urgency and staff members tend to push themselves far beyond their normal limits. The length of time that staff members remain stressed increases and the opportunities for recuperation and repair become fewer. In many cases, even taking the time to recuperate from stress can bring on additional stressors related to feelings of guilt for abandoning colleagues or those in need of humanitarian services. These situations lead ultimately to poorer performance and bad decision-making. It is easy to see how insecure field situations contribute to stress, but how does stress contribute to higher security risk for the team in the field?



**Question**

*Stress is a normal response, but harmful stress can impact your security in the field. How? List as many ways as you can.*

---

---

---

---

---

Stress contributes to security risk in many ways. When the team members are over-stressed, free and easy communication among the members is often one of the first casualties. Without friendly support and information sharing among the team, a core part of the team's security awareness begins to fade. As stressed-out team leaders begin making mistakes, missions are sent to the field without proper preparation or planning. Small signs in the overall situational awareness will be missed. Previously cautious and careful team members may put themselves at greater risks. To further complicate this deteriorating security situation, team members' diplomatic and negotiation skills that might help diffuse a tense moment with a checkpoint soldier or angry disaster victim are also reduced by the effects of stress. Fieldworkers that are more temperamental and easily irritated increase security risks to themselves and the whole team.

## 12.2 Some Basic Information about Stress

Stress is an interesting topic in security risk management as it can be thought of as a kind of threat as well as a vulnerability. Many field staff in developing their office risk matrices include stress as a threat, to be either prevented or mitigated in their overall SRM approach. Most security officers prefer to categorize stress as a vulnerability—it is part of your individual security profile—but the important thing is that it is being considered and treated).



There are two types of stress to be concerned about in relation to staff welfare and security risk management—chronic stress and critical incident stress, both of these are common in insecure field situations, and both are represented by a wide range of effects from minor to severe.

**Chronic stress** (or cumulative stress) is defined as a state of prolonged tension from internal or external stressors, which may cause various physical manifestations, e.g., asthma, back pain, arrhythmias, fatigue, headaches, HTN (hypertension and high blood pressure), irritable bowel syndrome, ulcers, and immune system suppression. (*McGraw-Hill Concise Dictionary of Modern Medicine, 2002*). In its minor forms, this stress is commonly seen everywhere, wherever people “just need a break.” In its most severe form it can be debilitating and even result in “burnout” and other serious conditions.

**Critical Incident stress**, traumatic stress, and post traumatic stress disorder represent the increasingly severe ranges of stress reactions resulting from involvement or witnessing of extreme situations of shock, horror, or grief. This type of stress is also common in insecure areas where field staff may witness chaos, conflict, death, and destruction, or even be the victims of attacks. Post Traumatic Stress Disorder (PTSD) is the extreme form of this condition and can be characterized by intense fear, feelings of helplessness, or horror. Typical symptoms include “flashbacks” or persistent images or memories of the traumatic event, avoidance of images or situations associated with traumatic incident, and lowered responsiveness to other stimuli. Such symptoms lasting more than one month, resulting in significant personal distress or impairment in social or work functioning.

### *What you need to know about chronic stress*

There are a few points that everyone operating in insecure field environments needs to know about chronic stress. This list is not exhaustive, but it is important basic information for anyone involved in humanitarian field work.

- Stress is a normal part of life and it has an adaptive function. It generally helps us mobilize the energy needed to act upon new challenges from the environment. Stress loses its benefits for survival, and takes on a negative effect when:
  - The challenges exceed our capacity to adapt in a given period of time.
  - The challenges last for too long without a chance to recover.
- Stress can be caused internally (by our own expectations, internal conflicts, guilt, feelings of failure, etc.) and externally (by outside pressures, poor living conditions, real-life conflict and chaos in the working environment).
- Stress reactions occur in several different areas of our human makeup; emotional, physical, cognitive, behavioral and spiritual areas can all be affected.
- Stress reactions vary widely in individuals—there is not one absolute common norm.
- Stress management is not a one-time action; it is most efficient when practiced regularly.

Stress is experienced in a wide variety of ways by different people, with differing results. It is generally known that individuals will react differently to stressors depending on various factors in their lives. Some important factors that will tend to help people adapt and cope with stress better than others include:

- Positive previous experiences with stress, i.e. they have successfully managed stressful situations in the past.
- Wider repertoire of coping skills—they have different interests or avenues for dealing with stress such as interest in reading, music, exercise, or other activities.
- Personality profile that accepts stress rather than either denying or surrendering to stress.
- General level of well-being (physical fitness, emotional maturity).
- Support from the environment and social support.



These supportive factors suggest many options for managing our own stress, as well as helping colleagues and staff members with their stress.



### Evaluate Your Level of Stress

This simplified stress indicator test gives an indication of levels of stress you may be facing in a difficult field assignment. It incorporates elements of both chronic and critical incident stress, and may serve as a warning that you should seek some assistance. It also prompts those in stressful situations to design a simple personal stress plan. It is reproduced here from the brochure *Coping with Stress* by the American Red Cross.

To evaluate your personal stress level, answer these 10 questions using the following scale: 1 = Never, 2 = Sometimes, 3 = Often

SCORE

- 1. I have difficulty sleeping. \_\_\_\_\_
  - 2. I feel tense, irritable, and nervous. \_\_\_\_\_
  - 3. The smallest noise makes me jump. \_\_\_\_\_
  - 4. I am on the alert for dangers that threaten me. \_\_\_\_\_
  - 5. I feel distant from my colleagues and avoid them. \_\_\_\_\_
  - 6. My work no longer interests me and I feel that I have no future. \_\_\_\_\_
  - 7. I am very tired, physically and intellectually. \_\_\_\_\_
  - 8. I have attacks of giddiness, tight throat, sweating and palpitations, particularly when something reminds me of a traumatic event. \_\_\_\_\_
  - 9. I feel over-excited. I act impulsively and take uncalculated risks. \_\_\_\_\_
  - 10. I re-live a traumatic event in my thoughts, in my dreams, or in nightmares. \_\_\_\_\_
- Total Score** \_\_\_\_\_

*15 & under* Your state of stress is normal if one takes your working conditions into consideration.  
*From 16-25* You are suffering from stress and should take care of yourself.  
*From 25-30* You are under severe stress and should seek help from someone close to you.

### A Personal Plan

My identified stressors are: \_\_\_\_\_

My present stress relief practices include: \_\_\_\_\_

New stress relief practices I commit to: \_\_\_\_\_

## 12.3 Individual Adapting and Coping Strategies

When starting a challenging work assignment such as a refugee emergency, earthquake or flood response, it is important to be aware that stress will be present at all stages of the work. Disasters expose everyone involved to traumatic, distressing sights, sounds and situations, as well as all of the chronic work stressors described above. Scenes of massive death and destruction, the suffering of survivors, and the intense pressure surrounding the rescue effort takes its toll.

Experienced humanitarian workers offered the following suggestions to ease stress in the field in a study prepared by Community and Family Services International (CFSI), Manila, Philippines in 1999.



## Tools

# Personal Stress Readiness Checklist for Humanitarian Field Assignments

### Brief yourself

- Ask for information on the situation and what is most difficult, dangerous and disturbing about the work and living conditions.
- Determine the amount of self sufficiency necessary to obtain equipment and supplies to maintain yourself.
- Find an experienced mentor for the settling in period.
- Obtain a country and location-specific-security briefing.

### Use reliable strategies to cope in difficult circumstances

- Compartmentalize; focus on the task at hand.
- Adopt a small tasks, small goals "one day (or hour) at a time" approach.
- Monitor inner "self talk", avoid negative comments to yourself, use self encouragement.
- Work in pairs with a "buddy agreement" to keep an eye on each other.
- Adhere to regular shifts; break for water, food and rest.
- Know your personal signs of stress and exhaustion.
- Agree to periodic leave away from work site.

### Remember stress survival skills

- Use portable forms of exercise: e.g., calisthenics, jump rope.
- Practice simple relaxation techniques: deep breathing, stretching.
- Pay attention to nutrition; take care with alcohol, caffeine, sugar.
- Get sufficient sleep to avoid overdraft in your "sleep bank account".
- Develop and use a repertoire of comforting time-out activities that change your focus (books, music, games).

### Recognize critical events

Sudden, violent occurrences that present a threat to personal safety and assault one's sense of security and predictability in life are sometimes called Critical Events. Examples include:

- Witnessing the death or serious injury of another human being.
- Involvement in actual or potentially life threatening situation.
- Injury or death of a co-worker in the line of duty.
- Dealing with serious injuries and/or deaths of children.
- Exposure to mass casualties.
- Involvement with any event described as an atrocity.

Such events cause stress reactions that are less disturbing if you know they are normal responses to an abnormal event. If your work involves possible exposure to critical events,

you may find it helpful to be aware of what you or others might experience in the period following the event.

### What you may experience

- Periodic feeling of unreality, events seeming dream-like.
- Heightened response to loud noises, reminders of the event scene, or any other surprise.
- Discomfort at being alone.
- Discomfort being in a group.
- Difficulty concentrating on what to do next.
- Difficulty making decisions and thinking creatively.
- Difficulty relating to those who were not in the event.
- Difficulty resting and sleeping, fear of nightmares.
- Increase or decrease in appetite.
- Discomfort being in places that seem unsafe.
- Feeling vulnerable, afraid of losing control.
- Feeling frightened, sad, angry, irritable, confused.
- Feeling and being exhausted.

### Manage critical event stress

If you have been busy performing necessary tasks after the event, you may not react until you have less to do. A delayed reaction is common, but puts you on a different timetable from others. The suggestions below may be of help.

### Care for yourself

- Take care of yourself. Try to eat regular, easy to digest meals. Avoid sugar and caffeine when mood swings are a problem. Monitor alcohol use.
- Re-establish exercise routine. Even a twenty minute walk will burn off some of the chemical byproducts of intense stress, which remain in your body and contribute to fatigue and tension.
- Rest by choosing from your repertoire of soothing, distracting activities.
- Communicate about your experience in ways that feel comfortable. Writing an account of what happened and your reactions to it can be helpful.
- Do what you need to do to feel safe. Review security with a qualified colleague.
- Respect your feelings and ways of handling things and those of others. People cope differently.
- Check out how you are doing with a trusted person. Feedback as you begin to feel more like yourself can be helpful.
- Take part in available counseling and other recovery activities.
- Reconnect with sources of social and spiritual support.



InterAction (An American NGO consortium) members working in the Sudan and Gaza asked for guidance on how to cope with chronic and critical incident stress. InterAction's Staff Care Working Group responded to those requests by posting a simplified "pocket card" for dealing with stress on their Staff Care webpage at <http://www.interaction.org/staffcare>.



**Aid Worker  
Pocket Card**

**Tools**

Additional information on caring for yourself in difficult work areas, can be found at the card designers' (Idaho State University) website at <http://www.telida.isu.edu>

**CARING FOR YOURSELF IN THE FACE OF DIFFICULT WORK**

Our work can be overwhelming. Our challenge is to maintain our resilience so that we can keep doing the work with care, energy, and compassion.

**10 things to do each day**

1. Get enough sleep
2. Get enough to eat
3. Vary the work that you do
4. Do some light exercise
5. Do something pleasurable
6. Focus on what you did well
7. Learn from your mistakes
8. Share a private joke
9. Pray, meditate or relax
10. Support a colleague

**For More Information**

See your supervisor or visit [www.psychosocial.org](http://www.psychosocial.org) or [telida.isu.edu](http://telida.isu.edu)

This card is a service of the Idaho State University Institute of Rural Health, funded in part by Telehealth Idaho grant #5-D1BTM00042 US DHHS, HRSA Office for the Advancement of Telehealth. The contents herein do not necessarily represent the policy of the U.S. DHHS, and you should not infer endorsement by the Federal government.

**SWITCHING  
ON AND OFF**

*Your empathy for others helps you do your job. It is important to take good care of your feelings by monitoring how you use them.*

The most resilient workers are those that know how to turn their feelings off when they go on duty, but on again when they go off duty. This is not denial, it is coping strategy. It is a way they get maximum protection while working (feelings switched off) and maximum support while resting (feelings switched on).

**How to become better at switching on and off**

1. Make this a conscious process. Talk to yourself as you switch.
2. Use images that make you feel safe and protected (switch off) or connected and cared for (switch on) to help you switch.
3. Develop rituals that help you switch as you start and stop work.
4. Breathe slowly and deeply to calm yourself when starting a tough job.

**Finally, reflect on your experience and move on**

Intense field assignments are rarely "over" upon departure from the site. After stressful deployments some people experience an elevated mood that lasts for days or weeks. Others find the let-down sudden and may go through a grieving process and feel depressed. For some, flashbacks and intrusive images of disturbing events bring anxiety and continued stress, making it hard to let go and move on to new activities. People may dwell on their performance, wishing they had been



more effective. They may want to share what happened with those close to them or may find this painful. If after a few weeks discomfort persists, and you are still not able to return to your normal routine, you may need to seek professional help. Some organizations have staff welfare counselors who can offer specialized assistance; otherwise you should obtain a referral for assistance from a qualified professional.

Many people find that once the assignment is over, life slowly returns to normal and with normality comes a sense of new beginning born of having survived a challenging and dangerous experience. These people may be aware of new skills and competence acquired in coping with the disaster situation and feel satisfaction about this. Most people eventually accept the notion that such powerful experiences have positive as well as negative aspects and that memories of these become part of one's life. They become accustomed to reactions surfacing from time to time in response to subsequent disturbing occurrences or on the anniversary of the disaster event. They accept what happened and their role in it, but focus on the future. They move on.

## 12.4 Managing Staff Stress in Insecure Field Environments

As a manager there is much that can be done both to reduce stress in the office environment (chronic stress), and in responding to stress (both chronic and critical incident stress) once it occurs. Managers have the responsibility to manage their own stress as well as to monitor and deal with the stress of the field team. To do this better, managers need to understand some of the signs and precursors to serious stress situations. The following elements are likely to indicate particular vulnerability to stress on the part of the staff member:

- Health problems or personal injury.
- Lack of professional/social support.
- Lack of self-confidence.
- Poor atmosphere in the office.
- Family problems such as concurrent life crisis; divorce, illness, or death of family member.
- Extreme youth and inexperience.
- Relationship to or close identification with those being assisted.
- Distressing work episode involving traumatic exposure.
- Long task isolated from other workers.
- Previous life or work-related trauma surfacing with recurrent symptoms.

As a manager, you can do much to improve the situation. Some things that can help are to:

- Create a supportive climate.
- Establish healthy routines in the office.
- Promote the atmosphere of reasonable transparency.
- Provide the outlets for the staff in terms of exercise and relaxation.
- Facilitate staff familiarization with the organizational mechanisms for addressing grievances.
- Monitor the consumption of alcohol and nicotine.
- Monitor stress.

Checklists can be extremely useful tools for monitoring staff needs as well as performance during the course of a difficult emergency assignment. The following checklist is not an exhaustive listing, and can be modified to better meet the needs of your particular field situation.



**Tools**

**Everyday Care of Staff Checklist**

**Create a Supportive Climate**

- Social support is a key barrier against the harmful effects of stress. Supervisors can assist their team by creating and maintaining a supportive climate in which to carry out the work of the emergency.
- Supervisors and team leaders have a major responsibility to clearly give permission, both to themselves and to their team members, for self-care adequate to sustain energy. It is their responsibility to check that this approach is followed throughout the rescue and relief effort.
- This responsibility begins with assembling needed supplies, equipment and space allocation in readiness for 24-hour coverage of the emergency situation.

**Establish Routines**

- Institute shifts with breaks and rotation of workers from higher to lower stress tasks. Have this in place to greet arriving workers.
- Provide an example by rotating tasks, eating and resting. Check that members of the team do likewise.
- Plan the work, giving clear assignments and instructions. Make out a list that includes “hard” tasks requiring efficiency and skill, (example: logging information) and a separate list of “soft” tasks which can be performed by people whose ability has been temporarily impaired by shock, fear and stress, (examples: food preparation, cleaning).
- Establish a “buddy system” of pairs of workers who agree to exchange information about each other’s stress signals and then keep an eye on each other to mutually remind about self-care. Select a personal buddy yourself.

**Manage Information**

- Provide briefing to arriving workers that orients them to the current situation, and prepares them for the most difficult and traumatic aspects of the emergency scenario. Include cultural information for workers arriving from out of area.
- Arrange for workers to receive regular information about the well-being of their families and vice-versa.
- Organize rumor control and periodic situation reports.
- Connect worker’s individual tasks to the whole rescue effort, to give meaning to the work and lessen frustration. Avoid criticism when possible. Don’t assume that people know they are doing a good job.
- Establish end of shift sessions to exchange information, anticipate next steps and support workers leaving and arriving at the scene.

**Monitor Health and Well-being**

- Assign the task of health monitor to a team member, giving that person authority to oversee food provision, and to enforce rest and refreshment breaks.
- Instruct team members to eat, drink fluids and take the periodic breaks recommended. Set an example yourself by agreeing to be reminded about breaks for food, rest and sleep.
- Ensure work area has toilet facilities, first aid kit with analgesics, drinking water, appropriate snacks and drinks.
- Provide a rest area apart from the work with blankets, pillows, and reading material.
- Encourage no smoking in the work area, but do allow smoking in some designated place.

**Attend to Nutrition**

- Emergency work places great demands on the body. Certain levels of food and fluid intake are needed when the body is under stress. Overload of caffeine should be avoided. Caffeine raises anxiety and interferes with needed sleep in susceptible people. If team members cannot leave the work area for meals, every effort should be made to have hot food brought in to supplement snacks.
- Provide frequent small meals if possible. Snacks containing the kind of non-perishable items on the list below should be prepared in advance and kept on hand:
  - fruit (fresh and/or dried)
  - high protein snacks: cereal bars, nuts etc.
  - decaffeinated tea, coffee, soft drinks
  - fruit juices
  - milk
  - mineral water

**Monitor Alcohol Consumption**

- Provide education on the tendency in emergency operations to drink beyond the initial relaxing effect of a glass of wine and to numb crisis impact with evenings of drinking.
- Staff need to know how immoderate alcohol consumption places additional stress on both body and psyche. It affects metabolism, sleeping habits, is in itself a depressant, and causes hangovers—all detrimental to the health and efficiency of the crisis team.

**Provide Exercise Opportunities**

- Workers who are fit and exercise regularly may need exercise sessions during the acute period if their task assignment involves inactivity. Any sort of stretching, movement or exercise, during a break or after a shift,



releases tension and helps to maintain stamina and general good health. Stairs, if available, a jump rope, and weights or any other practical, safe aids to exercise may be used if the team is in confined circumstances.

### Monitor Stress Levels

- Support the health monitor, and observe worker's appearance as well as performance and adherence to on-off routines.
- Identify and support vulnerable team members who may suddenly show multiple signs of stress. Be

prepared to provide prompt assistance in the form of a break with immediate support, brief rest and refreshment, a chance to talk about what is bothering the person, and support for coping. Identify staff appropriate to supportive roles including both male and female team members within specific language and culture groups. Consider temporary reassignment to "soft" tasks with companionship for the affected person. National staff, who are often less experienced and closer to a traumatic situation involving citizens of their own culture and country may fall into this vulnerable category, but no staff member is immune.

## 12.5 Provide Support to Staff after Critical Events

Even with proper security protocols and mitigation measures, serious security incidents may occur. Staff may witness or be directly involved in serious crimes, accidents, or direct physical assault. What are the expectations of management and other colleagues in response to such incidents?



### Question

*What steps can be taken to lessen the impact of critical incident stress for those who have been involved in serious traumatic experiences or critical incidents?*

---



---



---



---



---

There are many possible actions that may have specific uses for responding to the effects of critical incident stress, depending on the incident, the location, the cultures involved, and other factors. Even so, there are some general guidelines that are likely to be applicable in most serious situations. In preparing to support staff and colleagues following critical events, it is important to pay attention to the following aspects:

### *Accommodate basic human needs*

In order to create an environment in which people may express themselves freely, the following steps are recommended for staff in the immediate aftermath of a critical event:

- Allow time for bathing, change of clothes and a meal in privacy and comfort. Staff should not feel they have to face anybody, including supervisors or colleagues, before they are ready.
- As team leader, welcome the group in person if possible, or designate your personal representative to do so. One or two staff from the office should be freed up to take care of needs and provide the link between the group and the office, as meeting a large group of colleagues can be overwhelming.



### Arrange for defusing

Defusing or “informal debriefing” often happens naturally as people come together at the end of the day and spontaneously discuss events. In the wake of a critical event involving staff, however, defusing should be organized to provide a more structured and protected environment in which those involved can express and share their experience. In facilitating such sessions think through the need for each of the following:

**Session leader** – If possible, the defusing session should be guided by a trained person. In the absence of specialized health or mental health staff, managers can initiate conversation about the event with the group. The session leader should be familiar with typical stress reactions and consult one or more of the many excellent resources in this area. (UNHCR staff should see *Traumatic Stress Reactions, UNHCR, 2001, Basic Stress Management for Difficult Assignments.*)

**Support and privacy** – Every effort should be made to keep the discussion supportive as well as protective of the privacy of those present. Expression of strong emotions makes people feel vulnerable. Angry feelings should be recognized as a normal response to a violent, upsetting event, and staff should be able to “let off steam” about these. Criticism of professional performance is not appropriate, and should be held for a later “Lessons Learned” meeting in which the event is reviewed from a different perspective.

**Educational focus** – Discussion of different physical, emotional, cognitive and other reactions that may be experienced in the circumstances should emphasize how normal these are. Team leaders, backed by a health-trained staff member if one is available, can offer suggestions on what to anticipate and how to cope.

**Critical event aftermath** – Because some staff members may experience delayed reactions, managers should monitor stress levels in the weeks following a critical event. If these are causing concern, the Staff Welfare Officer should be consulted about further levels of post-event support needed, either for individuals or team.

### Specific psychological interventions with critical events

In cases when critical events are severe, it is imperative that support is provided by a mental health professional. If the organization has trained professionals (such as UNHCR’s Staff Welfare Section), they should be notified of the event so that they can contact the staff and teams involved in order to assess their needs. Such interventions are delivered on the basis of guidelines developed by the World Health Organization (WHO) for dealing with post-traumatic stress reactions and are provided in a confidential manner.



#### Tools

#### Care Checklist for Others Exposed to a Critical Event

Use a common-sense approach sometimes known as “Psychological First Aid” to support the person’s coping and return of control in the immediate aftermath of a traumatic experience.

- Explain your position and role to the person you are supporting.
- Listen empathetically to what the person wants to tell you about the event.
- Arrange for medical support if needed
- Ascertain the person’s needs for:
  - Company/companionship
  - Privacy
- Provide a sheltered opportunity for:
  - Food
  - Bathing
  - Resting
  - Communication with family/friends
- Validate feelings and reactions (refer to *What You May Experience* above)
- Provide protection from additional trauma of:
  - Intrusive questioning
  - Unwanted exposure to the public
- Encourage re-establishment of personal routines.
- Answer questions honestly.
- Validate use of person’s stress management repertoire.
- Encourage one day at a time, small tasks,



### *Some useful resources regarding stress for humanitarian field workers*

The UN General Assembly has tasked the UN Department of Safety and Security (UNDSS) with developing a strategy to manage stress. UNDSS has a Critical Incident Stress Management Unit (CISMU) based in New York and in a number of field locations. UNDSS colleagues are available to respond to the psychological needs following security incidents. They coordinate their support to UNHCR staff with the Staff Welfare Section. The contacts of the CISMU are available through the local Field Security Coordination Officer (FSCO).

In UNHCR, the Staff Welfare Section (SWS) of the Division of Human Resource Management (DHRM) is mandated with taking care of the psychosocial well-being of UNHCR personnel members, regardless of contract. The services can be extended to the family members of the staff. Most of the work of the Staff Welfare Section is done through individual or group counseling; workshops and training; and policy development. Many larger NGOs and international humanitarian aid organizations have their own in-house resources for dealing with stress. Whatever your organizational affiliation, learn what resources are available to you in the field and use them when necessary. Some references are listed below that have proven useful for UNHCR staff members and others involved in humanitarian field work.

**Managing Stress in Humanitarian Emergencies**, UNHCR Staff Welfare Section, Geneva 2005. Much of this chapter is based on this document which can be found at [http://www.the-ecentre.net/resources/e\\_library/doc/managingStress.pdf](http://www.the-ecentre.net/resources/e_library/doc/managingStress.pdf).

**Traumatic Stress Reactions: an Informative and Educational Guide for Survivors of Traumatic Events**, UNHCR Staff Welfare Section, Geneva, 2001.

**Insights into the Concept of Stress**, Pan American Health Organization. This is a stress self-study workbook course designed to help aid workers identify and understand stress in disasters and traumatic situations. The workbook can be downloaded, by chapter at: <http://www.paho.org/english/ped/stressin.htm>

**Managing Stress in Humanitarian Aid Workers: The Role of the Organization** by John Ehrenreich, State University of New York. This online PowerPoint presentation is about leadership styles, teambuilding, policies, and practices that can help reduce and manage stress of humanitarian field teams. It can be downloaded or viewed at [http://www.idealists.org/media/pdf/psychosocial/managingStress.ppt#256,1,Managing Stress in Humanitarian Aid Workers: The Role of the Organization](http://www.idealists.org/media/pdf/psychosocial/managingStress.ppt#256,1,Managing%20Stress%20in%20Humanitarian%20Aid%20Workers:%20The%20Role%20of%20the%20Organization).

**Center for Humanitarian Psychology Information Sheets**. This online resource has several concise and practical information sheets on stress-related topics including *Resilience, Traumatic and Cumulative Stress, Tools to Cope with Stress, Depression, Compassion Fatigue, and Coping Mechanisms*. It can be found at [http://www.humanitarian-psy.org/pages/fiches\\_details.asp?id=26](http://www.humanitarian-psy.org/pages/fiches_details.asp?id=26).

**Humanitarian Involvement in Armed Conflict: The Stress Factor**, ICRC. This online resource is available at the ICRC website. It offers audio clips by Dr. Bierens de Haan, an ICRC psychiatrist. The program aims to provide psychological support for humanitarian staff working in conflict zones. The site is found at <http://www.icrc.org/Web/Eng/siteeng0.nsf/iwplList74/>.

## Summary



### Key Points

The relationship between security and stress is reciprocal; high levels of insecurity in the field will increase stress levels among humanitarian staff, and high levels of stress will lead to a riskier security environment. Something must be done to stop, or at least manage, this self-reinforcing and harmful cycle.

---

The basic “need to know” information about stress can be readily found from many excellent print and on-line resources. The primary points that all field personnel should know include:

- Stress is a normal part of life but can become destructive when:
  - The stressors exceed our capacity to adapt
  - The stressors last for too long without a chance to recover
- Stress can be caused internally by personal reactions and emotions, as well as externally, by events happening around us.
- Stress reactions affect our emotional, physical, cognitive, behavioral and spiritual selves.
- Stress reactions vary widely in individuals—there is not one absolute common norm.
- Stress management is not a one-time action; it is most efficient when practiced regularly.

---

Knowing about stress before undertaking humanitarian work in difficult environments is essential. Developing a personal plan, adapting, and using coping techniques will help you deal with stress in a more effective and positive way.

---

Those who are responsible for managing staff in the field should recognize their responsibility in the area of stress management as well as in other areas of responsibility such as program, administration and security responsibilities. Some basic measures managers can take to reduce stress on field staff include:

- Creating a supportive climate for staff
- Establishing routines
- Managing information
- Monitoring health and well-being
- Attending to nutrition
- Monitoring alcohol (and other drug) consumption
- Providing exercise opportunities
- Monitoring stress levels

---

Advice for responding to critical or traumatic stress incidents includes, among other things, providing for basic human needs, and being available to listen. For severe cases professional help may be required.

**Self Test**

## Chapter 12

### Self-Assessment Questions

Check *T* or *F* to indicate whether a statement is *True* or *False*

- T**  **F** 1. Stress has positive uses.
- T**  **F** 2. Critical incident stress—and not chronic stress—should always be of predominant concern to managers.
- T**  **F** 3. Critical incident or traumatic stress can result in “flashbacks”—intrusive mental images or memories of the traumatic experience.
- T**  **F** 4. Nothing can be done to mitigate critical incident stress. Only time will eventually soften the results.
- T**  **F** 5. Arranging for field staff to receive regular information about the well-being of their families and vice-versa can help to manage chronic stress in the office.

*Multiple choice. Mark ALL correct statements—more than one may apply.*

- 6. Which of the following are important points that all field staff should understand about stress?
  - A** Stress can be caused internally (by our own expectations, internal conflicts, guilt, feelings of failure, etc.) and externally (by outside pressures, poor living conditions, real-life conflict and chaos in the working environment).
  - B** Stress reactions occur in several different areas of our human makeup; emotional, physical, cognitive, behavioral and spiritual areas can all be affected.
  - C** Stress reactions vary widely in individuals—there is not one absolute common norm.
  - D** Stress is more common among women than men.
- 7. Which of the following factors might indicate that a staff member could be relatively more vulnerable to the negative effects of stress than other team members?
  - A** Lack of self-confidence
  - B** Family problems such as concurrent life crisis; divorce, illness, or death of family member.
  - C** Extreme youth and inexperience.
  - D** Distressing work episode involving traumatic exposure.



**Chapter 12**  
**Self-Assessment Questions** *(continued)*

8. Which of the following would be helpful in dealing with your own critical incident stress?
  - A** Taking care of yourself, for example by eating regular, easy-to-digest meals.
  - B** Re-establishing an exercise routine.
  - C** Comfort yourself by using your repertoire of soothing, distracting activities.
  - D** Increase exercise times and nutritional intake significantly to overcome serious deficiencies in body chemistry due to stress-induced toxins.
  
9. As a manager, which of the following steps could you take to reduce overall stress in the office?
  - A** Establish healthy routines in the office.
  - B** Require all staff to exercise more frequently in insecure areas than in low-stress situations.
  - C** Promote the atmosphere of reasonable transparency.
  - D** Provide the outlets for the staff in terms of exercise and relaxation.
  
10. Which of the following would qualify as critical incidents that might affect stress levels in staff members?
  - A** Involvement in an actual or potentially life-threatening situation.
  - B** Injury or death of a co-worker in the line of duty.
  - C** Dealing with serious injuries and/or deaths of children.
  - D** Exposure to mass casualties.



**Chapter 12**  
**Answer**  
**Key**

- |     |            |    |   |
|-----|------------|----|---|
| 10. | A, B, C, D | 5. | T |
| 9.  | A, C, D    | 4. | F |
| 8.  | A, B, C    | 3. | T |
| 7.  | A, B, C, D | 2. | F |
| 6.  | A, B, C    | 1. | T |



## UNHCR eCentre Learning Module Evaluation Form

### *Security Risk Management*

Date you finished this module \_\_\_\_\_

How much time do you estimate that you spent in completing the module (whether or not you did the exercises and answered the included questions)?

\_\_\_\_\_

Describe your previous experience with workshop design or facilitation.

\_\_\_\_\_

\_\_\_\_\_

How did you find the content level of this module?

Too simple    Easy    About right    Complicated    Too difficult

How did you find the language and structure of the module?

Too simple    Easy    About right    Complicated    Too difficult

How useful were the exercises and self assessment tests in the module?

\_\_\_\_\_

\_\_\_\_\_

How valuable do feel this module will be for your own personal or professional development?

\_\_\_\_\_

\_\_\_\_\_

Do you believe that you will use any aspects of this module in your work in the next year?

\_\_\_\_\_

\_\_\_\_\_

Any additional comments:

\_\_\_\_\_

\_\_\_\_\_

Please feel free to copy this form and mail or fax it to: UNHCR Representation in Japan  
UN House 6 F, 5-53-70 Jingumae, Shibuya-ku, Tokyo, Japan  
Fax: : +81 3 3499 2272

Or, if you prefer, email your answers to these questions to: [jpntocen@unhcr.org](mailto:jpntocen@unhcr.org)