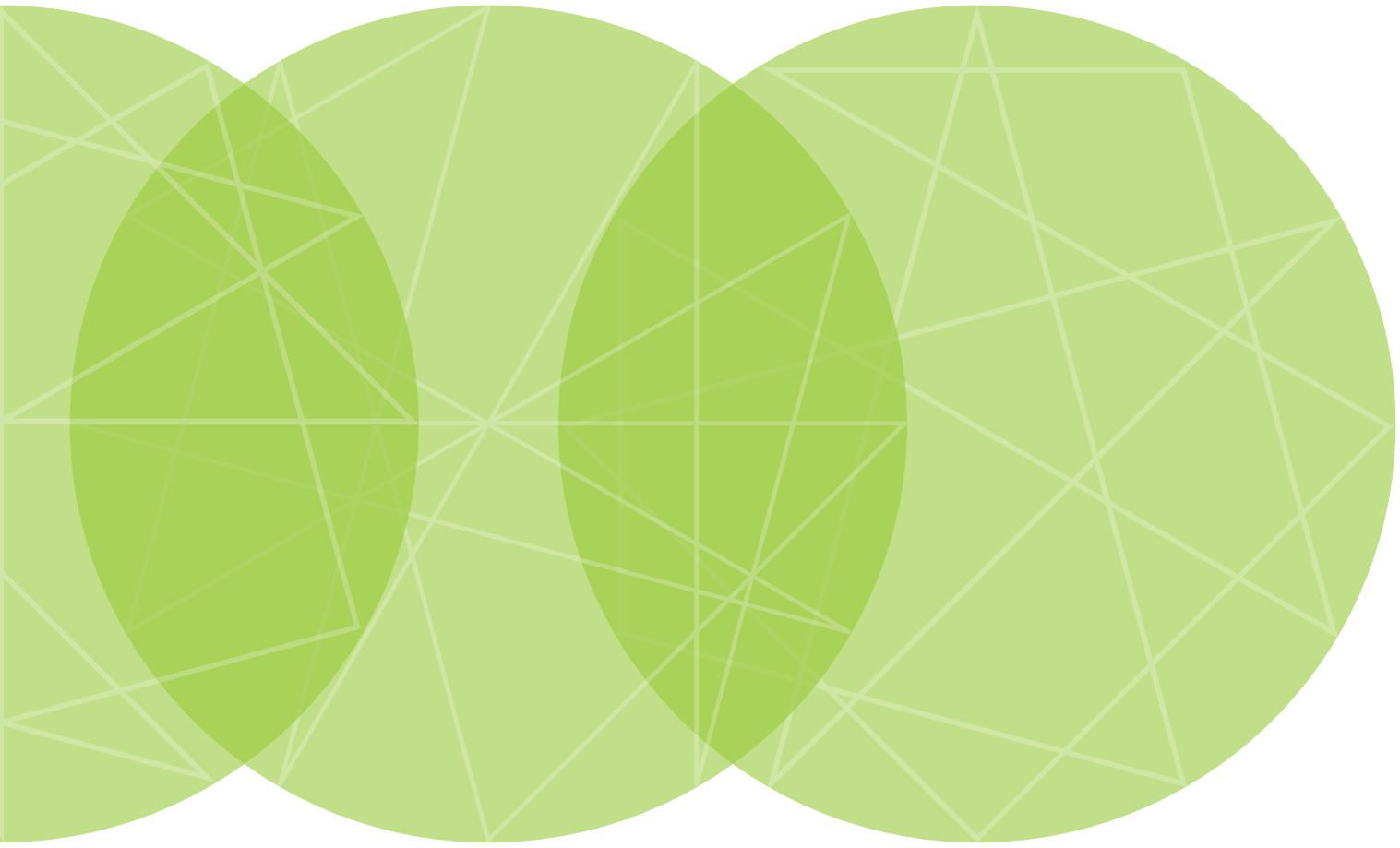
eisf

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them

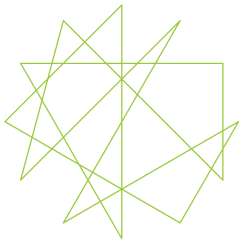
Koenraad Van Brabant

EISF Article Series



European Interagency Security Forum (EISF)

eisf



European Interagency Security Forum

The European Interagency Security Forum is an independent platform for Security Focal Points from European humanitarian agencies operating overseas. EISF members are committed to improving the safety and security of relief operations and staff in a way that allows greater access to and impact for crisis-affected populations.

The Forum was created to establish a more prominent role for security management in international humanitarian operations. It provides a space for NGOs to collectively improve security management practice, and facilitates exchange between members and other bodies such as the UN, institutional donors, research institutions, training providers and a broad range of international NGOs.

EISF fosters dialogue, coordination and documentation of current security management practice. EISF is an independent entity currently funded by the US Office for Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), and member contributions and is hosted by Save the Children UK.

Acknowledgements

This Briefing Paper was written by Koenraad Van Brabant and edited by the EISF Secretariat.

The basics of this article were developed in the context of the revised 2010 edition of the Humanitarian Practice Network (HPN) Good Practice Review on Operational Security Management in Violent Environments. It has significantly benefited from EISF discussions about organisational incident reporting systems in the spring of 2011, in Rome and Brussels. The encouragement of Oliver Behn and Madeleine Kingston, formerly at the EISF, is greatly acknowledged. The author is furthermore also very grateful to Shaun Bickley, who organised the peer review of an earlier draft while juggling many other tasks and responsibilities during a period of transition at the EISF and to the three perceptive and constructive reviewers Christina Wille, Sean Denson and Lauren D'Amore.

About the Author

Koenraad Van Brabant has over 20 years of experience of working in conflict environments and on conflict issues. Several years of humanitarian field work in different countries were followed by a great reflective learning opportunity as part of the Humanitarian Policy Group at the Overseas Development Institute in London. His own field experience has led him to challenge the generally absent or weak security management practices that were the prevailing situation fifteen years ago. Intensive collaborative work with a variety of practitioners then culminated in the Good Practice Review on Operational Security Management in Violent Environments (2000). Over the past 8 years he has immersed himself deeply in peacebuilding issues, largely as Head of Reflective Practice and Learning at Interpeace, a Swiss-registered international peacebuilding organisation. He is now an independent consultant and can be reached at navigation360@gmail.com

Contents

Summary

Over the past decade we have seen the increased circulation of safety and security incident-related numbers and statistics. The variety of numbers and statistics that come to us from different sources, and the different pictures they seem to paint, have become quite bewildering. The purpose of this article is to provide guidance on how to use and produce incident statistics and analysis, by considering three questions:

1. Why are incident statistics on safety and security important for aid organisations?
2. What should aid organisations keep in mind when considering and comparing different statistics?
3. Can aid agencies produce and contribute to relevant and good statistics and if so, how?

Section 2 starts off by considering the types of question we hope to see answered by safety and security statistics. These can be grouped around questions relating to: incident patterns, motives, incident impacts, and safety and security management performance. Statistics are important because they provide information on the changing nature of threats, how incidents impact on organisations and how well threats are managed. They can also be used as a tool for communication and advocacy purposes. Incident statistics, therefore, are part of the strategic management of individual aid agencies and of the relief sector as a whole. Section 2 highlights the fact that many organisations have difficulties with obtaining accurate and reliable incident information to enable statistics to be developed and that they often lack a robust incident reporting system that is consistent and efficient.

Section 3 considers some of the problems that should be kept in mind when comparing and analysing statistics. The problems relate to questions around:

- **definition:** this mostly relates to the concept of what constitutes an incident and who constitutes an aid worker.
- **reporting/recording:** in some contexts with many severe incidents, minor incidents are often less recorded. Under-reporting might also occur because of fears related to accountability or the loss of jobs.
- **comparison:** different statistical analyses analyse different things over different time periods. Also, not all analyses take into account the overal population size, which makes it more difficult to get a sense of proportion.
- **interpretation:** the overall picture can get distorted due to a limited number of high risk geographical areas or the relative exposure an organisation faces (e.g. organisations operating in conflict environments are likely to have more exposure to risks). It can also be difficult to determine the motive behind an attack.

Section 4 provides some guidance on how aid organisations should deal with these different kinds and types of statistics. It proposes a classification systems according to several parameters:

- Is the information global, area-specific or organisation-specific, and does it refer to an overall population or to the population of aid workers?
- Does the information refer to a single threat/type of incident or to multiple ones?
- Does the report try to estimate the denominator population that gives a more accurate picture of trends over time or does the report only provide changes in absolute numbers?

Several examples are provided to illustrate the different sort of statistics that are available. The section concludes by pointing to the relative scarcity of certain statistics or their limited use in aid agency security management, such as statistics on the impacts of programme suspensions and closures due to aid agency insecurity or on the cost-benefit of an organisation's investment in safety and security management.

The various annexes support and/or elaborate on different themes of the main text, but can also be used as stand-alone resources.

- **Annex 1** provides a more elaborate list of the bigger questions that we hope incident statistics and their subsequent analysis may shed light on.
- **Annex 2** gives an overview of the global trends regarding major security incidents affecting aid workers.
- **Annex 3** provides guidance on how to (re-) design an organisational incident reporting system, following the observation in section 2 that many organisations lack robust incident reporting systems and have difficulties obtaining accurate and reliable incident information.
- **Annex 4** summarises two examples of comprehensive organisational incident statistics.
- **Annex 5** provides a tentative framework for the assessment of the financial aspects of safety and security management.

Introduction

Incident recording and incident pattern and trend analysis are part of a general risk management framework (ISO 2009) and of safety and security risk management in particular (GPR8 2010).[1] Over the past decade we have seen the increased circulation of safety and security incident-related numbers and statistics. The variety of these numbers and statistics and the different pictures they at times seem to paint have become quite bewildering. Certain incident statistics on safety and security give insight into global trends of (violent) incidents that affect aid workers, but there remains a question about what aid organisations can actually get out these statistics.

This article seeks to provide some guidance by looking at three questions:

1. Why are incident statistics on safety and security important for aid agencies?
2. What should aid agencies keep in mind when considering and comparing different statistics?
3. Can aid agencies produce and contribute to relevant and good statistics and if so, how?

Annex 1 provides an overview of questions that we hope incident statistics and their analysis may shed light on.

Annex 2 provides a trend analysis of major security incidents affecting aid workers, derived from data from the Aid Worker Security Database.

Annex 3 provides a detailed list of attention points when (re-) designing an organisational incident reporting system.

Annex 4 provides two additional examples of organisational security statistics.

Annex 5 discusses the relatively less developed attempts to generate and provide financial analysis related to safety and security management. These annexes can be used as stand-alone resources.

1 Within the ISO 2009 framework, incidents constitute one important indicator of the monitoring and review of the risk management framework (sections 4.5 and 5.6). They are also one factor of information for establishing the external context (section 5.3.2), for defining risk criteria (section 5.3.5), and for risk identification (section 5.4.2). Incident information, but also financial information, informs decisions about the allocation of appropriate resources (see section 4.3.5).

Why are incident statistics on safety and security important for aid organisations?

The development and gathering of safety and security related statistics and their analysis and interpretation is an essential part of wider safety and security management practices (GPR8 2010). Yet statistics are only relevant and interesting if they provide us with information about questions of interest. Broadly speaking, we hope that incident statistics and their analysis can provide us relevant information about questions in the following categories:

- **Incident patterns:** The types and nature of incidents, their geographical distribution (globally, within certain geographical areas, within the areas where your agency works) and trends over time: in the short term (say, 12 months), in the medium term (say, 2-4 years), and in the longer term (say, 10 years);[2]
- **Motive:** Particularly where violence is involved, who are the perpetrators, why did they do it, who was targeted and why? And if it turns out that an NGO was in fact a target, what were the reasons for it?
- **Incident impacts:** What has been the material, financial and especially human cost of safety and security-related incidents on the individuals directly affected (the agency and/or its operational partners) and the target populations for the programme?
- **Agency safety and security management performance:** What is the relative effectiveness of safety and security management, with regard to specific threats, and also benchmarking against comparable agencies with comparable exposure? (Are we doing well enough to reduce the number of incidents and their impacts? And what is the financial cost-benefit balance of our investments in safety and security management)?

Annex 1 of this article includes a more comprehensive list of the *big* questions of interest.

In short, it can be concluded that organisations analyse and interprete statistics to:

- try and anticipate the evolving and particularly the future reality and landscape of threats globally or in more circumscribed geographical areas;
- assess their own organisational performance regarding the management of safety and security, to evaluate operational effectiveness, the allocation of scarce resources and consider their duty of care and due diligence (see Kemp & Merkelbach 2011);
- gather evidence for various communication and advocacy purposes, potentially ranging from negotiations about insurance premiums to public advocacy for more financial resources for aid agency safety and security management or for stronger global promotion of international humanitarian law and the respect for aid workers it enshrines.

2 The Open Source Centre produced a highly visualized incident-analysis of terrorist incidents in Afghanistan for the period 2004-2008 with data derived from the Worldwide Incident Tracking System (WITS). To give a better sense of the cross-border nature of the violence, it added data about suicide attacks in Pakistan in 2008. The database allowed the Open Source Centre to analyse and visualize incidents along various dimensions (e.g. geographical, temporal, type of threat and perpetrator). In October 2008 the Open Source Centre also developed a predictive forecast of where future Afghan attacks were most likely to occur. It found that 92% of incidents reported in the WITS database occurred in locations predicted to have at least a medium probability for terrorist incidents, and about 69% of recorded incidents in locations deemed to have a high probability (Open Source Center 2009).

Incident statistics on safety and security are useful tools for organisations to provide them with information on the changing nature of threats, how incidents impact their organisation and how well they are managing the risks to which they are exposed. However, many organisations have difficulties with obtaining accurate and reliable incident information to enable statistics to be developed. Organisations often lack a robust incident reporting system that is consistent and efficient or struggle to put an incident reporting system in place. These difficulties arise because an incident reporting system may:

- be seen as unnecessary bureaucracy and paperwork;
- trigger unwanted interference from HQ;
- record many incidents which might make the programme, or those managing it, look bad.
- reveal that an incident was - intentionally or not - provoked by things the staff of an organisation did or failed to do;
- lead to a downsizing or temporary suspension of the programme, putting jobs at risk etc.

However, for the improvement of organisational safety and security management it is essential to have a robust reporting system in place. The relief sector as a whole has an interest in the global picture of patterns and trends, but this cannot be built up with a fair degree of reliability unless individual agencies have and are willing to share their own incident statistics. Statistics therefore are an integral part of the strategic management of individual aid agencies and of the relief sector as a whole.

Annex 3 provides guidance on how to (re-) design an organisational incident reporting system.

Two additional points are worth making here:

- Incident data (and data on near-misses) and statistics and their subsequent analysis provide necessary information, but are not sufficient to assess whether your safety and security management is *enabling* you to operate in dangerous environments. Such an assessment requires a broader range of information, in particular insight about the context and environment, as well as the agencies' own potential vulnerabilities.
- Second, the contribution of incident statistics towards indvidual and organisational learning is likely to be limited, compared to an in-depth incident analysis that includes an evaluation of the safety and security system in place, of the incident response and the management of its aftermath. The statistical analysis of incident data does not provide the same level of detail and depth that a comprehensive incident analysis can give. Hence the analysis of incident data may be an essential component in the development of safety and security management policies, but it is not, by itself, likely to trigger behavioural change.

The challenges of working with statistics

Security incident statistics are produced by a variety of sources. Yet, when we take several of these reports, we notice that they do not seem to paint the same pictures. Indeed, we find ourselves confronted with generic problems when comparing statistics on the same issue, but resulting from different exercises. The major problems relate to definitions, geographical variations, reporting, comparison and attribution of motives. To illustrate this see the following box, as well as annexes 2 and 4.

Box 1: Some examples of one off studies considering inter-agency incident data

1. An early study (Sheikh et al. 2000) examined 382 deaths among humanitarian workers (this definition includes peacekeeping personnel). It concluded that 67.4 per cent were the result of intentional violence, 17.1 per cent the result of car accidents (a higher rate within the sub-population of UN peacekeepers) and only 4.5 per cent of the total due to 'other causes' (though 33 per cent of NGO deaths (excluding peacekeepers) could be attributed to other causes). Other interesting conclusions from this study were:
   - Over 30 per cent of deaths in the sample occurred within the first three months of a field assignment. A major factor of vulnerability therefore seems to be lack of familiarity with the new environment. Length of previous field experience did not correlate with the time of death. In short, 'more experienced' staff are not necessarily less vulnerable in a new environment (from this observation, it can be argued that agencies which rotate international staff rapidly on short-term assignments indirectly put them at higher risk than those which encourage and support longer-term field assignments).
   - The average age of death for national and international staff was in their late 30s. This implies that 'younger' (less experienced) aid workers are not necessarily more at risk.
2. King (2002) subsequently examined a data set of 158 aid worker fatalities between 1997-2001. He found 47 per cent attributable to acts of violence.
3. Another study (Rowley et al, 2008) looked at data provided by 18 agencies, but instead of looking at fatalities it analysed (violent) incidents during the period September 2002 to December 2005. The study subsequently analysed the consequences of these incidents, namely death, medical evacuations and hospitalizations. The conclusion was that intentional violence accounted for 55 per cent of all deaths reported, and that 50 per cent of cases of intentional violence were lethal.

3.1 Problems of definition

The two most significant problems of definition relate to the concepts of 'incident' and 'aid workers'. Even if reporting discipline were similar throughout all agencies, differences in data and data patterns can occur because of different definitions of what constitutes an incident (or a reportable incident)[3] or of who counts as an aid worker or an aid worker involved in humanitarian relief? Do members of a church group who distribute relief supplies in the aftermath of a disaster to members of their religious community count as aid workers in humanitarian relief? Do UN peacekeepers or UN election observers qualify as aid workers?

Additional questions that come up are:

- Should the staff of an international humanitarian aid agency based in (relatively safe) international headquarters be counted as part of the 'aid population' even though they have no exposure to any field-related risks?
- Should staff members who travel to the field be included and those who stay in headquarters be excluded?
- Should we distinguish between different types of of aid agencies (UN, Red Cross, NGOs) and how does this influence how we interpret data?

3.2 Problems of reporting and/or recording

In countries with many severe incidents, minor incidents are often less recorded, because the threshold of what seems important is much higher. Also, when reporting incidents, aid agencies not only rely on internal records, but also on media and other open source reports. It is recognised that this may introduce a bias towards the more spectacular and/or more deadly incidents which might be reflected in the type of incidents that aid agencies record and the way that they do it.

Incidents might also be under-reported out of fear that the person in charge will be held accountable for the incident or because staff are afraid they will lose their jobs if the agency decides to withdraw from an area. Sensitive incidents such as sexual assault or gender-based violence are also often under-reported, sometimes because the person affected is reluctant to report out of shame or does not trust the agency/person in charge to resolve the incident in a meaningful way.

3.3 Problems of comparison

Different exercises analyse different things

Some reporting exercises look at all reported incidents, some look at all violent incidents, major security incidents or malicious acts and some look at the most extreme consequence of an incident i.e. fatalities, whether caused by violence or not.

Different exercises cover different time periods

Several of the exercises consider data over time periods apparently chosen on an *ad hoc* basis. Effective trend analysis would require regular rather than one-off analysis. It might also be interesting to chose time periods in relation to potentially game-changing events. Potentially game-changing events can be internal (i.e. related to your safety and security management practices such as the deployment of regional security advisors) or external (i.e. related to events in the world outside such as the apparent consolidation of international drug trafficking presence in West Africa, or Kenya's military entering Southern Somalia to fight al-Shabaab). Seasonal differences should also be taken into account. For example, in some areas there is often less conflict in rainy periods due to constraints on movement.

Some exercises refer to a denominator population while others do not. Also, different exercises refer to different denominator populations

The term 'denominator population' is a construct from 'denominator', the bottom part of a fraction in mathematical terms, and 'population', which is the overall reference group of people within which you study the occurrence of a phenomenon. So we say for example that for a given disease we have a morbidity rate of 165 per 10,000 and a mortality rate of 17 per 10,000. The denominator population in this instance would be 10,000.

A reference to population size gives you a sense of proportion and allows for better interpretation of trends. To illustrate this very simply: Two organisations each experience 35 serious incidents in a given year. The total number of staff (including of partners) of one organisation is 395, while for the other it is 4,312. For the first organisation this amounts to one incident per 8.86 staff/year, while for the second it amounts to one incident per 0.81 staff/year.

3 The approach taken by the Security in Numbers Database (SiND) avoids (or postpones) the problem of definitions by focusing on the core narrative information, and looking at the 6Ws: Who who did What to Whom, Where, When and with what Weapons.

Now suppose that the following year both organisations each experience 45 serious incidents. Taking the absolute numbers, it seems that the situation has deteriorated for both. However, this interpretation changes if we take note of the fact that the first organisation has significantly expanded and now has a total staff population of 700, while the second organisation contracted and now has a total staff population of 3,300. In this second year, the first organisation experienced one incident per 6.42 staff, while the second organisation experienced one incident per 1.36 staff. Contrary to the impression given by the change in absolute numbers, the change in rates in fact show an improvement for the first organisation (from one incident per 8.86 staff to one incident per 6.42 staff) and a deterioration for the second organisation (from one incident per 0.81 staff to one incident per 1.36 staff).

Problems also occur when we try to compare between different populations. A major distinction that can be made is that between the overall population and the aid worker population. In addition, the aid worker population needs to be more precisely defined. Are we talking about aid workers in general (including humanitarian, development aid workers and peacebuilders) or aid workers in humanitarian relief? And who else is included? Are local, national and international staff included, as well as dependants and associated personnel (e.g. consultants, labour contracted for a humanitarian project, staff of partner agencies)?

Box 2 looks briefly at two of the most prominent cumulative databases about aid worker incidents, and highlights some of the important differences between them.

Box 2: Cumulative multi-aid agency databases

Useful global statistics about safety and security incidents affecting aid agencies can only come from comprehensive and cumulative aid worker incident databases. At the moment, there seem to be two such databases, each of which has already shown their usefulness (see Stoddard, Harmer & Haver, 2006 and 2011, and Stoddard, Harmer & DiDomenico, 2009, and Wille & Fast 2010a, 2010b and 2011).

The **Aid Worker Security Database** produces one of the most influential analyses of global trends regarding aid worker security. The primary sources for this database are public reports, and information provided by individual aid organisations and by inter-agency security platforms in operational areas. These incident data are complemented by the results of research to quantify the population of aid workers in the field over time. It is important to note that the data set concentrates on major security incidents affecting the staff of aid organisations working in humanitarian relief. Major security incidents are defined as 'killings, kidnaps and attacks resulting in serious injury' (2009 Policy Brief p.2). Since 2006, the database has also documented instances where insecurity has restricted access to populations in need (Stoddard, et al. 2006 and 2011 & Stoddard et al. 2009). Annex 2 provides an overview of the main conclusions of three consecutive analyses.

The **Security in Numbers Database** (SiND) takes incident data from collaborating agencies and from media sources, and organises the data structure around the questions: Who did what to whom, where, when, (why) and with what weapons? It does not contain information about the denominator population. SiND includes a much broader range of incidents than the Aid Worker Security Database. It covers incidents that vary in type and severity from threats to injury and violent death. It can track events against aid organisations, their programmes, their staff members, programmes and physical infrastructure. It also includes information on aid agency responses to such events. It therefore can produce customised data analysis for aid agencies or topical analysis (Wille & Fast 2010a, 2010b and 2011).[4]

4 The different reports,vary in their use of six or seven 'Ws', sometimes including the question 'why', making it seven 'Ws'

3.4 Problems of interpretation

The potential problems of reporting and recording also alert us to the fact that the data does not speak for itself. The following are some of the important attention points that encourage caution and care when interpreting our 'data'.

Geographical concentration

The overall picture can get distorted by a limited number of high risk geographical areas where most (or most dramatic) incidents occur.

For example, consider the Aid Worker Security Database analysis for the period 2006-2008 (Stoddard et al. 2009). This analysis concluded that no less than three quarters of all serious incidents had occurred in seven countries. In ranking order these were Sudan, Afghanistan, Somalia, Sri Lanka, Chad, Iraq and Pakistan. The big 'drivers' of the increase in the overall number of serious incidents were Sudan, Afghanistan and Somalia. Interestingly, if these three countries were taken out, then for the rest of the world the period 2006-8 actually showed a decline in overall attack rates on aid workers, from 2.7 to 2.4 per 10,000 aid workers.

Relative exposure

When making comparisons between organisations, we should be careful about how we interpret results. For example the analysis carried out by the International Federation of the Red Cross and Red Crescent Societies (IFRC) which is discussed in Annex 4, shows a very low number of incidents of violence. That may be due to the quality of the IFRC security management, but is probably also related to the division of labour within the Red Cross and Red Crescent Movement, with the International Committee of the Red Cross (ICRC) being the organisation operating in situations of conflict, while the IFRC is responsible for responding in the aftermath of disasters. The ICRC and the IFRC therefore have somewhat different levels of exposure.

Motives

Another problem when analysing security incidents relates to targeting. There are definitely instances where we are fairly certain that the organisation was targeted even if the exact motives are not clear. In other instances however we fall back on speculation. Our reporting and our analyses should signal the degree of confidence, so that we can produce two figures: one without any doubt and another figure with a remaining degree of doubt.

Motives are hard to determine. The ambush of an aid convoy by an armed group involved in an insurgency against the government can be a targeted attack, but is it for military purposes, for economic gain (war economy), for political reasons (e.g. to show that the government is not in control of its territory) or a mix of all of the above? Motives may also change. How do you classify a kidnapping in which the kidnappers initially made political and economic demands, but in the end settled for a ransom payment alone?

The notion of a 'malicious act' (see the UN example in paragraph 4.5) derives from insurance terms and does not equate with 'targeted'. It would include being the victim of a landmine explosion years after a war has ended, or getting seriously injured because you are in the 'wrong place at the wrong time'.

This discussion of some of the general problems with statistics is not meant to suggest that all exercises are methodologically flawed, but to explain why the multiplication of statistics does not mean that we automatically have a clearer picture to act upon strategically or managerially. Secondly, it also signals the importance, when producing such statistics, to provide transparent methodological information and caveats – something that not all the authors of such reports do.

4 Categories of incident statistics

It is clear that there is a huge variety of safety and security-related statistics available. This section proposes a basic classification system to make it easier to handle this variety. We can differentiate firstly between global, area-specific and organisational statistics, and secondly between statistics referring to the safety and security of the aid worker population and that of the population as a whole. Both types of populations can be numerically determined/estimated, or not. Within those parameters we can then differentiate between statistics referring to a single type of threat/incident or several types of threats/incidents.

Table 1: classification of safety and security statistics

	Global	Specific area	Organisational
Aid worker population (estimated or not)	Single/multiple threats or incidents	Single/multiple threats or incidents	Single/multiple threats or incidents
Overall population (estimated or not)	Single/multiple threats or incidents	Single/multiple threats or incidents	Single/multiple threats or incidents[5]

Several examples are provided for different categories in the remainder of this section.[6]

4.1 Single threat/incident statistics with global span for the global population

Global statistics may not be a priority for aid organisations, but they are not irrelevant. They can draw our attention to certain threats that get less publicity, such as a high prevalence of kidnapping in certain countries and they may orient aspects of humanitarian relief/preparedness as they apply to large operations and constitute threats to the aid worker population as well. However, global statistics often do not tell us that much – at least not for operational security management purposes. They may confirm, for example, that air travel is safer than road travel and that travel on motorbikes is more dangerous than travel in cars. But for practical purposes, a blacklist of airlines with problematic maintenance standards and safety records is more useful than overall air crash statistics. Those general statistics can indicate high 'danger zones', but we would have identified many of these in any case.

Airplane crashes

There is a fairly complete global record of aircraft crashes worldwide covering almost 100 years. The records show that between 1918 and early January 2011, 129,229 people are estimated to have died in a total of 19,980 airplane accidents, with another 107,170 injured. In 41.49 per cent of the plane crashes there were no survivors while in 42.84 per cent there were some survivors (for the other cases no information on casualties was available). In 67.67 per cent of the crashes, human error was the principal cause, technical failure in 20.72 per cent, bad weather conditions in 5.95 per cent and sabotage in 3.25 per cent. 50.39 per cent of the accidents occurred during landing, 20.96 per cent during takeoff and 27.73 per cent during flight (the small remaining percentage occurred during taxiing and parking). The records are cumulative, which means that the number of crashes and of dead and injured increases over the years.[7]

5 In this particular instance this category does not apply, since aid workers make up the overall population of an organisation. For this box the interpretation of 'aid worker' and 'total population' would of course have to be amended with for example 'aid worker' being all the personnel in field level positions and the total population being 'all personnel'.

6 The various examples in the text and the annexes are purely for illustrative purposes, to show the bewildering array of figures available and the challenge of drawing managerial conclusions from them. No guarantee is offered by the author of this article that the figures quoted are reliable. There are also many more relevant examples. The selection of those in this article does not imply a judgment about their quality or reliability relative to others. Sources are typically identified except for commercial providers, because the information may be open to paying clients only and/or to avoid an impression of promoting one commercial information and analysis provider over another.

7 Aircraft Crashes Record at: http://www.baaa-acro.com/Statistiques%20diverses.htm.

Road safety

In 2009 the WHO produced the first, and so far only, 'Global Status Report on Road Safety'. It estimates that over 1.2 million people worldwide die each year on the road. Between 20-50 million suffer non-fatal injuries. Over 90 per cent of the fatalities on the road occur in low- and middle-income countries, which have only 48 per cent of the world's vehicles. Almost half of the fatalities are 'vulnerable road users', such as pedestrians, cyclists and users of motorised two-wheelers. This proportion is higher in poorer economies (WHO 2009).

4.2 Single threat/incident statistics globally but also in relation to specific areas/countries

Kidnapping

Some suppliers of global security information produce periodic reports of kidnapping around the world. One estimate of the total number of kidnappings worldwide in 2008 put the figure at 8,000, with 90 per cent of those kidnapped being locals rather than foreigners. A report also stated that globally there has been an increase of approximately 100 per cent in kidnapping between 2002 and 2008. Given that many kidnappings remain unreported, the actual total figure may be significantly higher. One estimate is that only 1 in 10 kidnapping incidents are reported to the authorities.

Various statistics show the outcomes of kidnappings. One author states that research suggests that about 66 per cent of kidnap victims are released safely after payment of a ransom, about 15 per cent are released without ransom payment and without rescue and around 10 per cent are released through a rescue operation (Nicholson 2008).

The top continent for kidnapping remains Latin America, although the phenomenon is increasing in other parts of the world. In 2008 the top ranking countries were Mexico, Pakistan and Venezuela. Iraq, previously the scene of many kidnappings (general, not specific to aid workers) no longer figured in the top ten list by 2008. Significant increases in kidnapping were observed in 2008 in Somalia and Afghanistan, while the rates in Colombia and Brasil decreased. When absolute numbers of kidnappings in a country are related to the population size of that country, then Honduras and Guatemala remain among the countries with the highest risk of kidnapping in the world.

4.3 Single threat/incident statistics affecting the personnel of one organisation

Medical evacuations and health-related deaths in UNHCR

One example of an organisational analysis is that of UNHCR looking at the causes of medical evacuations and deaths among its field employees for the years 1994 and 1995 (Peytremann et al. 2001). A total of 162 medical evacuations and 37 deaths were reported over these two years, for a monthly average of 4,151 field employees.

Of the 162 medical evacuations, 94 involved men and 68 women. The major causes for evacuation were infectious diseases, including HIV/AIDS (17%), obstetric-gynaecological conditions (15%), accidents (15%), eyes-nose-ears or throat/dentistry (11%), astro-intestinal diseases (10%).

The major causes of fatalities were infectious diseases (41%), cancer (24%), accidents (16%), and cardiovascular diseases (11%). Expatriate employees represented two-thirds of the cases and 59 per cent of the cases occurred in Africa (there are indications that a significant proportion of the infectious diseases concerned AIDS-related diseases among local African employees).

4.4 Multiple threats/incidents affecting multiple organisations in a given area

NGO Safety in Afghanistan

The Afghanistan NGO Safety Office (ANSO) produces regular reports, with mapping, trends and other analysis. For example, its report for the first quarter of 2011 (ANSO 2011) looks at attacks on NGOs by armed opposition groups, confidently distinguishing such attacks from criminally motivated incidents. For both types there is a larger trend picture, as well as a map visualising the more serious NGO incidents for the first three months of 2011. It does not seek to estimate the NGO population. Its overall assessment is that NGOs are not routinely targeted by the Taliban as a matter of policy but are being impacted by an increase in overall violence in the context. It therefore ranks collateral damage and accidental strike with an IED as the highest risk factors at that moment (ANSO 2011: 1). The report also contains a second section that looks at the overall trends of armed opposition attacks since 2006, and compares the attack rates per province for the first quarters of 2010 and of 2011.

Security incidents in North Kivu

In August 2009, the Office for the Coordination of Humanitarian Affairs (OCHA) produced a report analysing security incidents in North Kivu province of the

Democratic Republic of the Congo (DRC) from January 2008 to June 2009 (OCHA 2009). The report comes with tables and graphs but – somewhat surprisingly - without maps. Some of the key observations are:

- Incidents against humanitarian workers (not defined in the report) have increased by 26 per cent in the first six months of 2009, compared to the same period in 2008. Incidents in Goma City have increased by 44 per cent for the two semesters compared;
- About 81 per cent of criminal activity in urban areas of Goma took place during the evening or at night, while 91 per cent of security incidents in rural areas took place during the day;[8]
- Armed groups were responsible for the majority of criminal acts in 2008, while bandits accounted for most security incidents in 2009 (the report does not explain how we confidently assess the difference between armed groups and bandits);
- NGOs are a primary target of criminal activities in rural areas (86%), with UN agencies less likely to be targeted (14%) - a difference attributed to the UN's use of MONUC military escorts. In urban areas however UN staff appear as vulnerable as NGO staff.

4.5 Multiple threats/incidents for an organisation globally

The following discussion of fatalities among UN employees for the period 1992-2008 differentiates between civilian staff and uniformed personnel and between national and international staff. Since it refers to the proportion of national to international staff, there must be a reasonable estimate of the personnel population of the UN, even if that is not included in the report or its analysis.

Fatalities in the UN

The 2008 report of the Independent Panel on the Safety and Security of UN Personnel and Premises Worldwide took a look at the UN statistics since 1992. It found that:

- Since 1992 a total of 270 UN civilian staff members and 2,468 uniformed personnel have been killed as a result of malicious acts, including murder, bombings, landmines and hijacking.
- Of the 270 civilians killed, the majority are locally recruited staff – 215, or 80 per cent. This is largely consistent with the overall proportion of national to international UN staff.
- In the past, this violence represented isolated incidents or was the result of being in the wrong place at the wrong time. The new analysis found that violent incidents were more often the result of deliberate, political targeting (UN 2008, para 14). Yet, the report cautions against becoming overly preoccupied by targeted attacks. The UN statistics for the period indicate that the number of UN personnel killed by groups hostile to the UN is relatively small compared to those killed by armed robbery, banditry, carjacking and other malicious acts (ibid para 20).

In Annex 4, two additional examples are provided for multiple types of incidents affecting the staff population of two aid organisations (the Peace Corps and the IFRC), of which the latter provides greater area-specific analysis. Many more examples can be found and can generally be classified according to the parameters given above.

4.6 Rare statistics

It is worth noting that despite the large supply of security-related statistics on offer, certain types of statistics and analysis seem rare:

- Financial figures and evaluation of the cost-benefit of aid agency investments in safety and security management (see Annex 5 for a tentative framework).
- Detailed information about costs and benefits (to different stakeholders) of programmatic operations suspended or prematurely closed/abandoned because of security conditions or security incidents. The different stakeholders include the field-based population of aid workers, the agency as a whole and the beneficiaries.
- Statistics referring to the safety and security of the intended beneficiaries of aid operations. Where they exist (notably for fairly stable camp populations with a significant presence of aid agencies, or where it is collected by human rights and protection agencies), they may be used for programming or general advocacy, but do not typically seem to be included within aid agency safety and security management. Yet if we argue that we are prepared to raise our threshold of acceptable risk if there is a larger number of people in greater need of assistance or under greater threat, then such information does play a role in operational security decisions and the subsequent evaluation thereof (risk/benefit analysis).

8 This may be a more common pattern, see e.g. Insecurity Insight 2010: Security Facts for Humanitarian Agencies. How do security events affecting humanitarian aid agencies differ between urban and rural environments? http://www.insecurityinsight.org/files/Security%20Facts%201%20Urban%20Rural.pdf

Concluding remarks

Safety and security incident statistics and their interpretation are an important component of a comprehensive risk management system for the aid sector as a whole and for individual organisations specifically. They can provide information on the changing nature of threats, how incidents impact on organisations and how well threats are managed. Moreover, they can be used as a tool for communication and advocacy purposes.

Nevertheless many organisations still lack a robust organisational incident reporting system through which they can obtain accurate and reliable incident information from which statistics can be developed. This is central to organisational safety and security management and the continuous improvement and strengthening of such a system should be an organisational priority. Although problems of compatability may remain an obstacle, an increase in the number of aid agencies with robust incident reporting systems and practices could provide a stronger basis for more comprehensive statistics at field and global level (see Annex 3 for guidelines on designing or re-designing an organisational incident reporting system).

The increased numbers of security personnel, and their improved networking, means that we now have access to an increasing number of reports that provide incident statistics and analysis. These reports are often useful, but can also become confusing. The question that arises is to what extent these different reports and databases can be used to compare and draw conclusions on the wider picture of incidents affecting aid worker safety and security.[9] While it is possible to assess global trends on the number of violent incidents affecting aid workers, uncertainties remain due to problems of definition, reporting/recording, consistency and interpretation. Moreover, when it comes to assessing other types of broad trends, such as statistics on lasting injury or death among aid workers that are the result of health and accident-related causes, the relevant data sets seem largely missing.

What can be concluded is that we need to resist the temptation to take one set of statistics as providing a robust picture of the actual risks that aid workers face. However this does not mean that we should give up on incident statistics. They can contribute to a better understanding of the risks aid workers face, especially when combined with a comprehensive incident analysis and a good understanding of the operating context and the organisation's specific strengths and vulnerabilities.

9 The difficulty of producing, comparing and interpreting statistics should caution us against dramatic statements such as the headline: 'international aid work (is) a deadly profession' (Deen 2006). Although this is the title of a short press article, it reports on the 2006 UN report on 'Safety and Security of Humanitarian Personnel and Protection of UN Personnel'. The press report states that (based on on-the-job death rates compared with total population at risk) aid work is one of the most hazardous civilian occupations. It would rank fifth after loggers, pilots, fishermen and structural iron and steel workers – based on US Department of Labour figures. This of course is a conclusion derived from dubious statistics: It is unlikely that the US Department of Labour has reliable figures on all loggers or fishermen worldwide, or even in 'developed' countries. Nor is it likely to have reliable figures on 'aid workers' of all nationalities and even for all international aid agencies, including non-US ones.

ANNEX 1

What do we hope to get from incident statistics and their analysis?

This annex provides an overview of some of the big questions that we hope incident statistics and their subsequent analysis may shed light on. As this article indicates, the available statistics only provide us with partial information on global patterns and trends. But a robust organisational incident reporting system can provide us with fuller information on our own organisational situation and can contribute to richer and better global statistics.

The nature of incidents:

- What are the main direct causes of injury and death of aid workers globally?
- How many incidents resulting in injury or death are caused by violence?
- How many incidents are caused by political violence targeted at aid workers? Is this situation improving or getting worse?
- How do incidents affecting aid workers compare to comparable categories of people such as journalists or human right workers operating in violent environments?

The locality and distribution of incidents:

- Where in the world do most incidents occur?
- How are different types of incidents distributed around the world?
- How many incidents affecting the population at large have taken place in an area within a given time period?
- How many incidents have affected aid agencies in this area and time period?
- What is the geographical distribution of incidents for our agency?
- Are there medium-term changes in these geographical patterns?

Incidents and those affected:

- How are incidents affecting aid agencies distributed among major categories of agency: the UN, Red Cross movement, international NGOs, national/local NGOs and community-based organisations? How are you doing compared to other agencies?
- How do incidents affecting aid workers as a whole distribute among international and national/local staff, and men and women? How do they distribute among functional roles (e.g. guards, drivers, warehouse personnel, health workers etc.)? What is the distribution within your agency? What have been the outcomes of these incidents for those directly affected?

The costs of incidents:

Direct:

- How much did we spend in direct costs on safety and security management this year?
- What proportion is that of our total annual turnover?
- How much are the direct financial losses this year due to security incidents?
- How are these financial losses geographically distributed?
- What is their proportion to our total annual turnover; to our total investment in security management over a given time period?

Indirect:

- Globally how many humanitarian programmes have had to be suspended or prematurely closed/abandoned for security reasons within a given time period?
- What is the geographical distribution of these suspensions/closures? What is the story for my agency? What has been the cost (or saving) to our programme budget? What can we say about the 'human cost' of aid-not-delivered?

Security management performance:

- Are we allocating our limited security management resources correctly?
- What do 'incidents' tell us about the effectiveness of our safety and security management efforts?

ANNEX 2

Trend analysis of major security incidents affecting aid workers

Some of the most influential statistics are those derived from the Aid Worker Security Database.[10] It is important to bear in mind that these concentrate on 'major security incidents' affecting aid workers.

1997-2005

- Since 1997 and particularly since 2005 there has been a marked increase in the absolute number of reported *major security incidents* affecting aid workers. Yet, if we look at the total aid worker population, estimated at 136,000 in 1997 and at roughly 242,000 in 2005, the increase in relative terms is less serious.
- Between 1997 and 2005 the number of major violent incidents affecting UN and ICRC staff has decreased while the number affecting NGOs and national Red Cross/Crescent Societies increased.
- While the trend was already somewhat visible prior to 1997, the majority of aid worker victims since that year are nationals of the country in question (78%). Globally, the incidence rate for internationals is stable or declining while it is growing for national staff. One possible important contributing factor to this may be the tendency to operate by remote management, essentially keeping international staff at a (safer) distance and working through national staff or national/local partners.
- In about 59 per cent of the incidents, it could be determined with reasonable confidence who was behind the attack and that it was intentional. The analysis showed a clear predominance of aggression for political motives rather than economic ones.

2006-2008

- The absolute number of attacks against aid workers has risen steeply, with 2008 the deadliest for the whole period since 1997.
- There is a particular upswing in kidnapping.
- The overall increase in major violent incidents compared to the earlier reporting period outweighs the increase in the estimated aid worker population (estimated at 290,000 in 2008). In other words, there is a relative increase and not just an increase in absolute numbers.
- There is also a notable increase in the rate of attacks against international staff, particularly for NGOs.
- Only the ICRC has seen a decline in attack rates over these 3 years.
- The rate of politically motivated attacks rose from 29 per cent of the known total in 2003 to 49 per cent in 2008 (the other violent incidents are seen as economically motivated or the aid worker as such not being targeted).

10 See: Stoddard, et al. 2006, 2011 & Stoddard et al. 2009

2009-2010

- Although there has been a surge in attacks in Afghanistan, there is a modest decline in the global number of violent incidents compared to the peak in 2008, albeit still a very high number of aid worker victims.
- The decline in attacks is more related to the shrinking presence of international aid agencies in the most violent settings, especially Somalia and to a significant degree also Darfur (Sudan), rather than to improved security conditions.
- Possibly as a result of aid agency adaptations to high insecurity environments, there is a significant rise in aid worker kidnappings and in the use of major explosives such as roadside, vehicle and body-borne improvised explosive devices.
- National aid workers suffer fewer attacks per capita than their international colleagues, but given their larger numbers they form the majority of victims.
- The security needs of national aid workers require dedicated and specific attention, and the perceived inequity in the security support they receive compared with their international colleagues needs to be addressed.

The most recent report drawing on the Aid Worker Security Database has a short methodological section that clarifies the understanding of 'major incidents' and of 'aid workers'. The Aid Worker Security Database does not count peacekeeping or human rights personnel or UN personnel outside of the UN aid agencies. But it does include contracted personnel such as guards or drivers (Stoddard, Harmer & DiDomenico 2009: 2). However, the unspecified 'formula' to estimate the number of humanitarian workers in the field globally on the basis of staffing figures from the major humanitarian organisations remains relatively rough, particularly given that most victims are 'nationals' and because of the plethora of 'national/local' agencies that increasingly occupy the frontline roles in the most dangerous environments.

ANNEX 3

An organisational incident reporting system

Contents

Introduction

Organisational incident reporting can serve three purposes:

1. Managing the incident response and incident aftermath;
2. Providing the basis and trigger for in-depth incident and incident response analysis and review of the broader context analysis;
3. Generating organisational statistics for broader analysis and management response.

In addition, robust organisational incident reporting systems provide reliable information that can contribute to inter-agency databases from which a more global picture can be built up.

The analysis and subsequent management of individual incidents is a critical learning (and accountability) aspect of incident reporting. An analysis may indicate that an incident was preventable or that impact was effectively mitigated thanks to a robust security system or good practices.

Smaller agencies may find little value in investing in a robust incident-reporting system if they have few incidents. Even if they were to gather incident data, the data record is unlikely to be large enough to allow for meaningful analysis and most learning will come from a robust analysis of each individual incident. This, however, does not mean that they should not keep any records as disciplined incident reporting remains equally important for smaller agencies. It enables the timely management of the incident response and aftermath of the incident, as well as contributing to area-specific incident statistics.

This annex, however, focuses on the production and analysis of data for broader organisational management purposes and to contribute to wider inter-agency trend analysis. So what are some of the major attention points when (re-)designing an organisational incident-reporting system?

1. Be realistic about what statistics can tell you – and what not

A good incident reporting system is a better basis for management reflection than an impressionistic picture, possibly distorted by a single dramatic incident that may be the exception rather than the rule. The assumption here is of course that your database contains most of the incidents that did take place. It provides one factual basis for reflection about the risks you have faced (in the past) but is only one, limited component of a broader organisational practice of risk management.[11]

This type of factual basis can help you assess whether change is taking place over time (for the better or for the worse) and what those changes might be (indicators); whether the current level of organisational investment in safety and security is adequate; whether limited resources may have to be concentrated differently from their current allocations (e.g. to certain geographical areas, certain types of incidents, certain types of personnel, specific issues that may have gone unnoticed etc.) and what to focus your training and management on. The results of the analysis and interpretation of your organisational incident record can be used in additional ways:

- To raise awareness about safety and security, among personnel in the first place but also among members of the Board, and therefore strengthen the organisational culture in this regard;
- To provide potential new personnel – or personnel to be re-deployed to new environments with factual information that can contribute to their 'informed consent';
- To negotiate with insurance providers. While insurers may rely on 'global statistics' (which are not as robust as they may appear), you can highlight the specifics of your particular situation. This might persuade them to lower premiums, or at least not to increase them.

11 See Merkelback and Daudin 2011, for an insightful discussion about the implications of the ISO Risk Management Guidelines for aid agency security management.

Even a very good organisational incident record is not enough, *by itself*, to assess how effective your security management is, to anticipate future threats or to compare the effectiveness of your security management with other organisations:

- **Assessing the effectiveness of your security management.** Seeing a decline in the number and gravity of incidents may indeed be an indicator of the growing effectiveness of your security management. But apparent improvements might also be the result of under-reporting, an agency becoming more risk averse, or simply a period of 'luck'. The analysis and interpretation of statistics may warrant such conclusion, but the numbers by themselves are not enough. An assessment of the effectiveness of security management requires an analytical narrative about the quality of prevention, survival tactics of those caught in incidents, and the quality of the incident response and overall incident management, as mentioned above.
- **Anticipating future threats.** The current situation and recent trends cannot be automatically extrapolated towards the future, certainly not for specific operating environments. A deeper and ongoing anticipatory understanding of the contextual and situational dynamics will be required. It is possible to speculate about the evolution of threats in one region if it begins to develop the conditions and characteristics that already prevail in another region (e.g. if global takfiri or radical jihadist networks and ideologies were to insert themselves into the rebellion in southern Thailand, new threats would be likely to appear here). It should be kept in mind that no past record can totally reduce the fundamental uncertainty about the future.
- **Comparing the effectiveness of your security management with other organisations.** The type and gravity of incidents that two different organisations experience cannot be compared without considering the exposure of these organisations. For example, they can both be of the same size, but with one mostly operating in natural disaster environments and the other mostly in conflict situations with significant levels of violence (e.g. recall the contrasting roles of the IFRC and the ICRC). The potential for comparison increases when we look at the security performance of different organisations within the same operating environment. Even then, there are factors other than the incidents that should be considered such as the possible perceptions of the profile of staff or of core activities. For example moving food and medical supplies can actually constitute a greater risk than moving vaccines in the same operating environment. Food and medical supplies are likely to be more attractive to fighters than vaccines and therefore constitute a more dangerous commodity.

2. Be clear about what you want to record

What kind of data can you get out of your reporting system? Depending on the format and the system in place, it is possible to get some interesting breakdowns of the overall data according to different parameters such as:

- Types of incidents.
- Frequency of various types of incident – rather than focusing on the more dramatic ones.
- Area/location (differentiated for example into office, residence, rural, urban etc.).
- Time of the incident (date, period of year, day of week, time of day).
- Male/female.[12]
- Age of those affected/perpetrators.
- Race/ethnicity of those affected/perpetrators.
- Personnel status (international, national, local, volunteer, consultant, dependant etc.).
- Possibly: length of professional experience of person(s) affected.
- Possibly: duration of presence in location of person(s) affected.
- Whether victims/perpetrators had consumed alcohol or drugs prior to incident.
- Correlations between two or more of these parameters.
- Trends in all of this over time.

There are some further quantifiable measures you may be able to produce, such as:

- Ratio of incidents per denominator population (total head count or total exposure time).
- Average time of incidents per year e.g. globally one incident every 5 days.
- Vehicle accidents per number of vehicles on the road (denominator population).
- Vehicle accidents per X kms driven (requires you to keep exact vehicle logs and record this centrally).
- Trends in any of these over time.

12 Surprisingly gender information is missing in a significant percentage of incident reports (Wille and Fast 2011).

2.1 Scope – types of incidents

You definitely want to record security-related incidents, typically involving man-made violence or threats of violence. However, should you also include safety incidents, particularly those relating to accidents and health, extending to natural disasters or incidents such as fraud and corruption? (These are often considered under finance or HR policies. See also para 2.4.1). Moreover, it is important to consider how to record data on incidents such as sexual harassment or sexual abuse by personnel, or verbal threats by (former) personnel or other breaches of the organisational code of conduct.

2.2 Scope – what is the population covered by the database?

2.2.1 Internal

Interpreting statistics and trends becomes problematic unless you have a clear idea about the denominator population. You need to clarify who is included and who not: all field based employees of the organisation, all employees of the organisation, their dependants, contracted consultants, volunteers? What about casual labour, goods and service providers that are hired? There might be a tendency to exclude the latter group but what if they become hurt while on the job, or what if they are targeted exactly because of the work they do for an organisation?

The same consideration also applies to the question of whether you should only record incidents that happen when people are on duty and whether this applies differently to international and local staff. Moreover, what about a situation where a member of staff gets hurt when off duty, but the motivation behind the attack seems to be related to the association of this individual with your organisation?

Finally, when considering who to include, you should also ask what time intervals to use for the 'head count' to keep track of the changing size of your denominator population.

2.2.2 Partners

What about incidents affecting operational partners? Questions of legal liability are difficult to answer and are depending on the context and relationship (e.g. do you have a formal agreement to provide a partner with capacity support or (safety and) security management)? Additionally, there is the question of how to keep track of the denominator population of the partner.

2.2.3 Other aid agencies

What about including incidents affecting other aid agencies operating in the same environment? This may not be a realistic proposition since it is likely that you will only hear about some incidents and not others. Also, it is not really appropriate: your central organisational incident database is not a primary tool for real-time operational security management in a given operating environment.

2.3 Clarity of definitions

You need to be very clear about the definition of a reportable incident. For example, does this include breaches of security regulations? While a breach does not necessarily result in an incident, it can increase the exposure to risk and might therefore be relevant information for the consideration of the effectiveness of your security management. Also, if you want to include information on 'near misses' or 'close calls' you need to clarify what counts as a reportable near miss, as this is open to subjective interpretation.

When it comes to defining categories of incidents, there tends to be a fair amount of confusion within agency reporting systems that subsequently affects inter-agency databases. How, for example, to differentiate between theft, robbery and burglary or between fraud and embezzlement? What counts as sexual harassment or verbal threat? If you use a category called programme-related incidents (e.g. people in an IDP camp throwing stones at your vehicles), then such a term should also be clearly defined.

There will be further difficulty in classifying complex incidents with multiple, simultaneous consequences. How, for example, would you classify a night-time robbery in a residence in the course of which your female employee is sexually assaulted and her husband badly beaten up? Or what about the case of a car hijacked on the road, with the hijackers also abducting the driver? In this case you have both a vehicle theft and abduction. The incidents can be classified under more than one category, but should not be double counted subsequently.[13]

There are essentially three moments when incidents can be classified:

1. Immediately by the reporter of the incident,
2. By the person(s) entering the incident data into a database, or
3. By the person(s) subsequently analysing the data in the database.

13 For a representation that can depict multiple causes and multiple consequences, see Merkelbach and Daudin 2011: 43.

Consistency in classification of the data entered is critical. If for example, you want to classify incidents as minor, moderate or severe, you need to realise that these are subjective assessments. What is considered severe by one person may be classified as moderate by another; what is severe for the organisation might not be looked upon in the same way by the individual. Additionally, what is considered severe in one environment (where such type of incident is highly unusual) may be considered moderate in another (where it happens regularly).

Keeping the above in mind you may want to consider having a dedicated staff member or selected group responsible for data entry. Also note that if you work in different linguistic environments, you will need to develop clear definitions in the different languages.

2.4 Reporting systems

2.4.1 Multiple systems or one integrated reporting system?

In larger organisations, a number of different types of incidents will probably be routinely reported to units or departments other than the one dealing with security: for example, cases of fraud to Finance, incidents of sexual harassment to Human Resources and major vehicle accidents to Logistics. It is easy to see how the development of an incident reporting system under the umbrella of security could become an additional system, creating some confusion and the feeling of an additional burden.

One integrated system of reporting to one central location has significant benefits for those asked to report. It turns a security incident database into a more generic incident database. This may dilute the security aspect, but gives the organisation a clearer sense of the spectrum of risks it faces. In the latter case it may be sensible to operate the database under an 'organisational risk management group' rather than under the security unit and thus bring together different departments.

2.4.2 What type of recording system?

Several organisations currently record incidents on Excel spreadsheets, while others have a fully developed database. A database may be somewhat more complex to set up and maintain, and therefore will be more costly, but might allow you to explore the data in richer ways than a spreadsheet. Some databases allow you to export your data into spreadsheets. Small organisations (with a smaller number of incidents) are more likely to stay with simpler options. Organisations with a significant number of vehicles around the world may benefit from vehicle management software such as FleetWave.

2.4.3 How is an incident reported?

There are different organisational practices, none of which are exclusive:

- An on-line reporting system, which is fine as long as everyone has decent Internet access around the globe.
- Phone-in reporting, where someone in HQ will need to write down the information.
- E-mail reports with a regular text-format.

The question of how to report is of most importance for those who report: it needs to be practical. On the receiving end, it is content (for the database) and timeliness (from an incident-management perspective) that are most important.

2.4.4 Who can report an incident?

There are different options with relative advantages and disadvantages:

- One reporter: someone such as the head of delegation/field coordinator, or the security focal point in the field location;
- A few authorised reporters: holders of both the above roles and perhaps a few others in senior management positions in the field (e.g. head of admin and finance);
- All personnel: any staff member can report directly to HQ.

The arguments for or against the different options relate to internal controls. If everyone can report directly, the likelihood that certain incident reporting will be suppressed is lower. On the other hand, it can lead to a proliferation of reports in different forms (and languages), which may not be consistent with your definition of what is a reportable incident.

There is also a risk that records will not contain the minimum information required and may not have been subjected to checks and balances to ensure the accuracy of the report. If only one person is authorised to report there is a risk of subjective bias and potentially more leeway for the suppression of incident reports. A few authorised persons therefore may be the most effective middle ground.

2.4.5 What is reported?

The organisational incident report form can bring more clarity and consistency to the reporting process. The minimum content should be the event description for which you can use the method of the six 'Ws': Who did What to Whom, Where, When (and with what Weapon – if applicable)? The minimum content is descriptive or narrative and does not contain categories, which are left for the wider data analysis. An organisational incident report form can also have a menu of different categories, which the reporter can tick (perhaps with the option of ticking two categories simultaneously, to signal an incident with at least two major dimensions) or you can have an incident report form that both contains a narrative part and different categories.

It is important to be cautious about the use of qualifiers of incidents such as minor, moderate and severe. These qualifications may be fairly subjective, depending on the location (and what the people there are used to) and the individual (what s/he has experienced).

Incident reporting, however, is not carried out for the sake of producing statistics, but primarily for informing organisational incident management. Therefore statistics should ideally be complemented with additional information on areas such as:

- the conquences and the measures taken,
- whether assistance or decisions are required from HQ,
- why the incident was not avoided or prevented,
- how effective the organisational response was, etc.

This sort of evaluative exercise is critical to assess the effectiveness of your security management system, but it is not a must for your basic incident database. It will not be easy to group data or make correlations of the more qualitative information using a database unless this data is entered in fairly standardised format with key words and codings.

It is worth noting that not all information is necessarily reported at the same time. The descriptive information needs to come quickly and as a set. Additional relevant information may be reported in one or more subsequent communications (e.g. on the consequences and effectiveness of organisational response).

2.4.6 Who enters the information in the database?

Automated systems where an on-line incident report is automatically entered into a database seem the most efficient, but such systems can turn out to be less efficient later on, when it is time for analysis.

When you classify incidents (e.g. as minor, moderate or severe) you need to realise that these are subjective assessments. Also, if you want to classify incidents – at the point of entry into the database - with more nuance (e.g. differentiating between burglary, theft, robbery and embezzlement), you need to be sure that the information entered into the database conforms to the definitions you have for these. That too would require a check before it is entered.

This strongly suggests that it is best to have one or a few dedicated persons entering the data, so as to ensure internal consistency in the records.

There may be information that must be considered confidential such as certain health conditions, alleged sexual abuse by a staff member that is still under investigation, names of victims, those who report and alleged perpetrators etc. This also raises questions about who can enter such information into the database and who can access the information in the database in order to preserve necessary confidentiality.

2.4.7 Data interpretation

Mention has already been made of some of the straightforward attention points in interpreting the figures:

- Figures relative to a varying denominator population are more telling than absolute figures.
- One or more particular situations with a major impact can give a distorting picture of the overall figures and global trends.
- Consider reporting bias: an increase in the number of reported incidents may simply be due to an increase in reporting discipline.

Other attention points that should be considered when interpreting, and that are based on more comprehensive incident reports than a basic 6W approach, are:

- **Change in practices**. For example, an increase in vehicle accidents might be the result of a shift in practice towards the use of more hired vehicles with a driver, over whom you have less control.
- **Responsibility**. It would be highly relevant to identify in how many of the vehicle accidents the driver was actually at fault. That requires additional inquiry and assessment beyond the basic incident information.

- **Was this a case of deliberate targeting or not?** As mentioned, the answer is not always certain, so differentiate between the instances where there is a high degree of confidence and those where there remains doubt.
- **Was this incident preventable?** Sometimes this may be straightforward, in other instances it will be a matter of judgment. A way to deal with this question is to assess the incident with both a stricter and a looser interpretation of preventable, and report both conclusions.
- **What do the trends (up and/or down) tell us about the effectiveness of our security management?** Again, a question requiring more incident analysis, ideally combined with security audits to determine the actual practices on the ground (compared to the desired practices).

3. How can you get your system to function?

It is not easy to introduce an incident reporting system in an organisation. Its purpose, rationale and expected benefits will need to be clearly communicated. It will take some time, perseverance and ongoing management support for the collective responsibility and discipline to take hold so that most incidents get reported.

There may be an assumption that it is easier to introduce an incident-reporting system in more centralised and formalised organisations than in more decentralised ones, since it is a fairly top-down exercise. This assumption is not necessarily correct, however, because these more centralised organisations might have more rigid structures that lead to greater resistance towards the implementation of new structures, in particular among people that are more 'distant' from HQ. In organisations that are smaller or that have a 'flatter' management structure and culture, there might be a somewhat higher level of trust between colleagues, and more focus on the common objectives rather than the institutional politics.

3.1 Possible resistance to incident reporting

Frequently mentioned possible reasons or concerns why incidents would not be reported are:

- It is seen as unnecessary bureaucracy and paperwork.
- It may trigger unwanted interference from HQ.
- Experiencing many incidents may make the programme or those managing it, look bad.
- It may reveal that the incident was - intentionally or not – provoked by things the staff of an organisation did or failed to do.
- It may lead to a downsizing or temporary suspension of the programme, putting jobs at risk etc.

3.2 Creating incentives to report incidents

The desired situation, however, is not one of resistance and monitoring to detect instances of omission and commission, but one where there is a broad understanding of the value of pooling certain information organisation-wide, leading to the self-discipline to report and to share. Identifying the importance of incident reporting in an organisational safety and security policy is a start, but the real challenge is turning policy into practice. What can be done in this regard is:

- Start awareness raising and understanding on the importance of incident reporting at the time of recruitment and induction and provide periodic reminders. Thereafter, there should be exchange and interaction between field level personnel and headquarters on the value of reporting systems, good practices etc.
- Show appreciation for the reporting of incidents (rather than only complaining about non-reporting), both immediately (informally), and also in more formal performance appraisals. This will encourage staff to continue the good practice.
- Give constructive responses from HQ to the reporting of an incident. This signals that the message has been heard and that the organisation as a whole feels responsible for the best possible handling of the situation – but also trusts field-based colleagues to do this well – unless or until there are indications to the contrary.
- Finally, show periodically what the database can produce, and how this is relevant for different people (and other stakeholders) in the organisation. This will encourage willingness to contribute.

3.3 Monitoring for problems with incident reporting

- Unreported incidents may come up during any type of country visit.
- Security or broader management audits may reveal unreported incidents.
- Establishing the date when an incident was reported, and crosschecking it against the date when the incident occurred, may reveal unacceptable delays in reporting.
- An effective whistle-blowing policy within an organisation can lead people to signal – safely and confidentially - that an important incident appears not to have been reported.
- Systematically debriefing outgoing staff may reveal unreported incidents.

3.4 Disseminating and sharing incident data reports

Finally, it is important to consider the internal dissemination of information resulting from an incident-reporting system, and whether the analysis should be made available beyond the organisation, for example by sharing with other aid agencies or by posting it on the organisation's website.

Consider also how often to provide internal updates and analysis, to those in the field, to management, to the Board (e.g. monthly, quarterly and/or annually). There should be an appropriate balance between overloading colleagues with reports and letting them wait so long for interpretive and analytical feedback that they lose interest in continuing to report. Above all, the reports should be interesting, relevant and visually attractive, with graphs, charts, maps and photos.

ANNEX 4

Examples of organisational safety and security statistics

Example 1: Overall statistics of the IFRC security unit

The Security Unit of the International Federation of the Red Cross and Red Crescent Societies (IFRC) has been producing annual analyses of all its reported incidents for several years. These reports have also circulated beyond the IFRC network. They are an excellent example of the value of developing a strong organisational incident-reporting system and analysing the data thus gathered on a longitudinal basis.

Some of the obvious strengths of this reporting system and the resulting analysis are:

- it has a reasonable estimate of the (varying) population that comes under its security umbrella;
- it classifies major categories of incident, namely as 'common crime' (broken down into 'theft, burglary, robbery' each with a specific definition); 'vehicles' (differentiating between vehicle accidents and vehicle incidents with injury): 'programme related incidents' and 'other' (incidents too rare to merit category of their own, but which can include for example detention by national authorities or abduction);
- it can correlate types of incident with geographical zones (region), and also see the evolution over time;
- it can differentiate by international and national staff, or by gender, and identify families/dependants and location (geographical zone).

The 2009 report provided analysis for incidents in 2008, and compared it with analysis for 2006 and 2007. Within the realm that comes under its responsibility, the total number of reported incidents in 2008 was 215, compared to 165 in 2006 and 135 in 2007. The increase is seen largely as the result of two factors: more member organisations coming under its security umbrella, hence a larger 'population' of personnel at risk (the denominator) and better reporting. Other highlights of the analysis are:

- While there is an increase in overall number of reported incidents, there were no significant changes between individual incident categories worldwide or per geographical zone;
- The largest category of incidents worldwide remain vehicle accidents, although its percentage of the total has decreased from 50 per cent to 30 per cent between 2006-2008. Over half of all vehicle accidents occurred in Indonesia.
- 63 per cent of all reported incidents occurred in the Asia/Pacific zone, which corresponds to the fact that the highest number of personnel are employed there (it also has a concentration of field-based security coordinators which is considered as another factor affecting the reporting discipline). The Asia/Pacific combined with the East Africa zone together account for over 90 per cent of all reported incidents in 2008, although the number of staff deployed in those two zones combined is only 70 per cent of the total;
- Where for all other types of incidents the Asia/Pacific zone dominated, this was not the case for robberies of which most occurred in Africa. The most violent crimes also occurred in Africa.
- When comparing reported security incidents to number of personnel not per zone but per country, then the two top countries in 2008 turned out to be Pakistan and the Maldives.

The analysis goes into greater detail, and is able to identify for example:

- The main items that were stolen (portable electronics such as mobile phones and laptops)
- Where and at what time of the day vehicle accidents tended to occur
- Where most robberies had taken place and at what times of the day
- Where and at what time of the day most burglaries had taken place

The analysis does consider the question of 'targeting' (distinguishes between programme-related targeting e.g. intended beneficiaries that angrily throw stones at the agency vehicle, and other types of targeting) and – interestingly- what percentage of incidents appear to have been preventable. It is justifiably cautious in coming to conclusions here. But, depending on how strictly you define certain parameters, it does suggest that around 30-35 per cent of all security incidents could have been prevented by applying common-sense measures or adhering to those in place.

Its 2010 report produced an analytical overview report for all reported incidents in 2009 but separated out incidents from Haiti because of its major impact on the overall figures. Indeed, half of all reported incidents came from Haiti, but also about half of all people under the security umbrella of the IFRC unit were deployed here. When Haiti was included, the global analysis showed an overall increase in the absolute number of incidents; when Haiti was excluded there was a global decline.

Example 2: Annual safety of the volunteer Peace Corps reports

Annual statistics and analysis reports for the Peace Corps since 2004 are available on its website.

The 2009 report looks at the overall picture of incidents in the previous year, but also at the period 2006-2009 and (where data are available) at the period 2000-2009. It uses an overall classification into threats, property crimes, physical assaults and sexual assaults, and provides further defined sub-categories under each of these (e.g. robbery, burglary, theft and vandalism; rape, major sexual assault and other sexual assault). The report does not just take the number of volunteers but calculates the actual volunteer years in the field, i.e. when they are considered to be really exposed to risk. This allows the comparison between regions and years not just of absolute number of incidents but of the more accurate incident rates.

The Peace Corps incident report mentions the gender and race/ethnicity of the victim, where and when the incident happened, what type of weapon was used and whether alcohol had been consumed prior to the incident (by the victim and by the perpetrator although this typically relies on the victim's testimony) and whether the (alleged) perpetrator was known to the victim or not. It also looks at when the incident happened during the (typically two-year) service of the volunteer. There is a question about whether the (alleged) perpetrator was apprehended, although in many cases this would require longer tracking of the incident than actually takes place.

On the basis of the above-mentioned information, the Peace Corps develops a 'profile' of the average type of incident and the average victim and perpetrator. Its annual report seeks to compare its own statistics with those of the overall US population, noting the differences in the incident reporting systems.

Finally, its annual anonymous survey of all serving volunteers inquires into safety and security incidents and reporting practices, signaling that there remains under-reporting (some of the underlying reasons for under-reporting are mentioned).

The Peace Corps incident reporting system and the analysis produced from it are handled by its Crime Statistics and Analysis Unit, which reviews incident reports and clarifies or corrects them if needed. The Unit's work is quality-controlled by the Office of Strategic Information, Research and Planning, which will verify a random sample of incidents to further ensure the accuracy of the annual reports.

ANNEX 5

Financial security information

There is a remarkable shortage of attempts to assess the financial aspects of safety and security management, or at least to make this a significant topic of inter-agency discussion and dedicated research. Because of this, we cannot do much more here than encourage more attention to it and provide a tentative framework. This would look as follows:

Safety and security related investments – safety and security related costs and losses

Safety and security related savings

For each of the three categories it is possible, and necessary, to distinguish between a 'direct' and 'indirect' component. The table below provides examples.

Table 1: classification of safety and security statistics

INVESTMENTS	**DIRECT** • Preventative health: e.g. periodical medical checkups; vaccinations; malaria prophylaxis and treated mosquito nets; water filters and purification tablets. • Security assets: e.g. radios (a percentage of the cost as they also serve for regular operational communications), compound protection equipment such as burglar alarms and lighting. • Insurance premiums. • Dedicated personnel: in-house health officer, psychologist, security personnel etc. Depending on how you classify fraud and embezzlement you may want to take a percentage of the cost of financial personnel that engages in internal audits. • Hire of specialist services and personnel for prevention: e.g. a consultant to carry out a field-level security audit. • Competency development: costs of safety and security specific training or a proportion of the cost of broader training in which safety and security is also covered. • Safety and security related travel: field visit costs or a percentage thereof, attending inter-agency security related seminars etc. **INDIRECT** • Time of other staff also dedicated to safety and security matters (e.g. a percentage of the cost of field-level or HQ general managers)
COSTS AND LOSSES	**DIRECT** • Value of assets to be written off and their replacement. • Repair of assets damaged in an accident or incident. • Working time lost by staff affected by an accident or incident. • Cost of unplanned travel triggered by an incident. • Cost of unplanned hire of expertise to handle an incident (e.g. kidnap management). **INDIRECT** • Additional working time lost by other staff engaged in responding to the incident (this can include time of staff at HQ engaged in internal and external communications in response to a major incident). • Cash flow delay costs or loss of income because of suspension or premature termination of programme in the wake of an incident.
SAVINGS	**DIRECT** • Insurance payouts. • Expenditure savings due to temporary suspension of programme. **INDIRECT** • Savings from incidents avoided and ongoing business continuity in a risky environment.

A number of observations are required here:

- The table only considers the organisational investments, costs, losses and savings. It does not consider the possible costs of an incident (or savings from an incident avoided) to individual members of staff (and their dependants etc.) or beneficiaries. These two considerations, however, cannot be ignored: the employer has a 'duty of care' and the primary rationale for aid work is to provide support to people in need.
- It may be argued that there is a false distinction between investment (which is an expenditure) and the costs of responding to an incident (which is also an expenditure). Yet there is a significant difference between prevention and response, which is why we need to differentiate between these respective expenditures.
- Most financial systems of organisations should, quite easily, be able to yield those costs that are entirely allocated to safety and security-related matters. Most will not be geared towards producing proportionate costs (of multiple-use assets and people or multi-purpose training and travel), which will require a measure of estimation. Accurate identification of time investment of people not fully dedicated to safety and security would require that everybody keeps fairly accurate time sheets – an unlikely proposition. But reasonable estimates could at least be produced for demonstration purposes, e.g. in the context of a more serious incident that engages quite a few of the organisational human resources.
- One of the most challenging estimates would be that of savings from ongoing business continuity and incidents avoided or mitigated in a fairly risky environment. There are no simple methods for doing this. If most agencies operating in the same environment were to carry out a financial analysis of the incidents they suffer, this would provide some relevant reference, but that is very unlikely to happen. A rougher and more approximate measure would be for an organisation to do a financial analysis of a range of incidents around the world, which may produce some average costs per type of incident (this of course is a very rough measure as it ignores price differentials in different parts of the world, or for example the different costs of a kidnapping that lasts four days compared to one that lasts four months).

Where there are fairly good area-specific incident statistics, one could then calculate the probability of a certain type of incident (or accident) affecting the operation in that area – and produce a rough estimate of savings if you suffer fewer incidents than initially anticipated. A cost-benefit analysis like this is common in other sectors. For example, public health economists and professionals routinely work on the cost-benefit calculation of prevention of disease; while insurance companies calculate the risk and determine a monetary value for their insurance premiums that they believe will be higher than the cost of pay outs made.

Another possible approach would be to focus on cases where there is a reasonable amount of certainty that your safety and security management has played a significant role in avoiding or mitigating an accident or incident. Again this can be done relatively easily with regard to investment e.g. in driver training. If such an investment is followed by a significant decrease in the number of vehicle accidents, then you have a basis to make a reasonable estimate of your savings resulting from the training investment. This does become more difficult when potential injuries and deaths are brought into the cost-equation.

It is obvious that many of these calculations and cost-benefit analysis will be based on estimates at best, but this does not mean that they cannot serve a purpose.

Resource list

GPR8 (2010). *Operational security management in violent environments.* Good Practice Review 8 (new edition). Humanitarian Practice Network. London: ODI.

ANSO (2011). *ANSO Quarterly Data Report.* Quarter 1, Kabul.

Deen, T. (2006). *International Aid Work a Deadly Profession.* Inter Press Service.

International Organization for Standardization (ISO) (2009). *Risk Management – Principles and guidelines.* Geneva: International Standards Organisation.

Kemp, E. & Merkelbach, M. (2011). *Can You Get Sued? Legal liability of international humanitarian organisations towards their staff.* Geneva: Security Management Initiative.

King, D. (2002). *'Paying the Ultimate Price: An analysis of aid-worker fatalities'.* In: Humanitarian Exchange Magazine, Issue 21. London: ODI.

Merkelbach, M. & Daudin, P. (2011). *rom Security Management to Risk Management: Critical reflections on aid agency security management and the ISO Risk Management Guidelines.* Geneva, Security Management Initiative.

Nicholson D. (2008). *'Kidnap for Ransom'.* In: Australian Security Magazine. Available at: **http://www.eisf.eu/resources/item.asp?d=2071**

OCHA (2009). *Security Incidents against Humanitarian Workers.* DRC, North Kivu.

Office of Safety and Security (2010). *Safety of the Volunteer 2009: Annual report of volunteer safety.* Washington D.C.: Peace Corps.

Open Source Center (2009). *Afghanistan – Geospatial Analysis Reveals Patterns in Terrorist Incidents 2004-2008.* Available at: **http://www.humansecuritygateway.com/documents/OSC_AfghanistanGeospatialAnalysisRevealsPatterns_TerroristIncidents_20042008.pdf**

Peytremann, I., Baduraux, M., O'Donovan, S. and Loutan, L. (2001). *'Medical Evacuations and Fatalities of UN High Commissioner for Refugees Field Employees'.* In: Journal of Travel Medicine 8(3), pp. 117-121.

Rowley, E., Crape, B., Burnham, G. (2008). *'Violence-Related Mortality and Morbidity of Humanitarian Workers'.* In: American Journal of Disaster Medicine, 3(1), pp. 39-45.

Sheikh, M., Guttierez, M., Bolton, P., Spiegel P., Thieren, M. and Burham G. (2000). *'Deaths among Humanitarian Workers'.* In: British Medical Journal, 321, pp. 166-8.

Stoddard, A., Harmer A., & Haver K. (2006). *Providing Aid in Insecure Environments: Trends in policy and operations.* HPG Report 23, London: ODI.

Stoddard, A., Harmer A., DiDomenico V. (2009). *Providing Aid in Insecure Environments. 2009 Update. Trends in violence against aid workers and the operational response.* HPG Policy Brief 34, London: ODI.

Stoddard, A., Harmer, A., & Haver, K. (2011). *Aid Worker Security Report 2011. Spotlight on security for national aid workers. Issues and perspectives.* Dublin: Humanitarian Outcomes.

UN (2008). *Towards a Culture of Security and Accountability. The report of the Independent Panel on Safety and Security of UN Personnel and Premises Worldwide.* New York: UN.

Van Brabant, K. (2000). *Operational Security Management in Violent Environments.* Humanitarian Practice Network. London: ODI.

WHO (2009). *Global Status Report on Road Safety: Time for Action.* Geneva: WHO.

Wille, C. & Fast, L. (2010a). *Security Facts for Humanitarian Aid Agencies. How do security events affecting humanitarian agencies differ between rural and urban environments?* Insecurity Insight, Bellevue.

Wille, C. & Fast, L. (2010b). *Is Terrorism an Issue for Humanitarian Agencies?* Perspectives 3. Geneva: Security Management Initiative.

Wille, C. & Fast, L. (2011). *Aid, Gender & Security: The gendered nature of security events affecting aid workers and aid delivery.* Insecurity Insight, Bellevue.

Notes

Notes

Other EISF Publications

Briefing Papers

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011
Max Glaser (author), supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Pete Buth (author), supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Pete Buth (author), supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Robert Ayre (author), supported by the EISF Secretariat (eds.)

Reports

Risk Thresholds in Humanitarian Assistance
October 2010
Madeleine Kingston and Oliver Behn (EISF)

Joint NGO Safety and Security Training
January 2010
Madeleine Kingston (author), supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Christopher Finucane (author), Madeleine Kingston (editor)

Articles

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Koenraad Van Brabant (author)

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
(in Humanitarian Exchange 47)
June 2010
Oliver Behn and Madeleine Kingston (authors)

Risk Transfer through Hardening Mentalities?
November 2009
Oliver Behn and Madeleine Kingston (authors)
Also available as a blog at
www.odihpn.org/report.asp?id=3067

Forthcoming publications

Capacity Development and Security Management: Working with Local Partners

Gender & Security: Guidelines for Mainstreaming Gender in Security-Risk Management

Anticipated research projects/topics of research 2012

The cost of risk management

Guidelines for performing a security audit

How to develop a crisis management plan

How to set up an organisational incident reporting system

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

eisf

European Interagency Security Forum
c/o Save the Children
1 St John's Lane
London EC1M 4AR

EISF Coordinator
+44 (0) 207 012 6602
eisf-coordinator@eisf.eu

EISF Researcher
+44 (0)207 012 6726
eisf-research@eisf.eu

www.eisf.eu

design and artwork: www.wave.coop

First published March 2012