Security Management in Humanitarian Organisations

Bob Ghosn

1 Introduction and Definitions

Humanitarian organisations tend to follow a rather ambiguous approach to security. On the surface, they usually recognise the value of professionally managing their security. However, security management is still too often seen as an alien concept grudgingly imported into the humanitarian world.

There is still a strong belief that good intentions, morals, international law and an often self-proclaimed humanitarian mandate are enough of a shield to ensure the security of humanitarian organisations. Facts in the field negate this belief daily, often in a sad and cruel way.[1] From Syria to Mali, it is clear today that for humanitarian organisations to remain relevant for the lives of people in need, they have to develop effective security management systems that allow them to meaningfully operate in dangerous environments. This chapter explores the main features of effective security management in humanitarian organisations, discussing concepts that are very common in the humanitarian literature. However, these concepts are often defined differently by different experts and organisations. For the purpose of this paper, we use the following definitions.

Security is achieved when the risks for an organisation, its staff and its beneficiaries in a specific geographical area of operation are identified, assessed and mitigated.

Special thanks to Sadia Bundgaard for her valuable editing of this text.

[1] According to Aid Worker Security Database, in 2014, 190 major attacks targeted humanitarian workers, http://www.aidworkersecurity.org.

B. Ghosn (✉)
Independent Humanitarian Worker, Brussels, Belgium
e-mail: solferino1859@gmail.com

H.-J. Heintze, P. Thielbörger (eds.), *International Humanitarian Action*,
DOI 10.1007/978-3-319-14454-2_23

Risk is the possibility of harm or injury occurring. Each risk is a factor of a threat and a certain level of vulnerability.

A *threat* is an event that might occur and could cause harm or injury to staff members or beneficiaries, loss or damage to property or equipment, programme disruption, damage to the organisation's reputation. Threats are analysed through two criteria: the likelihood of their occurrence and their impact if they occur.

Vulnerability denotes how exposed an organisation is to each threat. It can stem from factors either at the organisational level such as identity, perception or programmes or at the individual staff level such as nationality, gender, behaviour and perception. Two examples may help to illustrate this point: in an area that poses a security threat for European staff due to kidnappings, the vulnerability of an organisation to this specific threat depends on the number of European staff deployed. On the other hand, an organisation implementing vaccination campaigns in areas were vaccination is ill-viewed by certain armed groups is vulnerable to threats by these groups because of the very nature of its programmes.

Impact is the consequence of a threat that actually occurs and may affect staff, beneficiaries, the organisation and the programmes.

A security plan contains documents that include context and risk assessments, a security strategy, as well as the procedures that staff should follow to manage security risks. A model security plan has been designed by the European Interagency Security Forum (EISF).[2]

As explained, a threat is the result of the likelihood of an unwelcome event combined with its actual impact. Consider the following example: an organisation is working on monitoring human rights violations in a certain area and collects testimonies against perpetrators. The organisation might assess the likelihood of armed actors accessing these sensitive data as very low. However, should it happen, the impact on the population would be dire as armed groups would certainly want to retaliate and silence possible witnesses. The threat for data security is thus higher than the simple likelihood of data theft because its adverse impact would be very high. Threats should therefore be assessed based on the likelihood of their occurrence and their impact. A mathematical formula allows us to illustrate how the importance of a threat is the result of a combination of its likelihood to happen and impact:

$\text{threat} = \text{likelihood} \times \text{impact}$.

A risk is the result of a combination of threat with vulnerability. We can also illustrate it by a mathematical formula:

$\text{risk} = \text{threat} \times \text{vulnerability}$.

A combination of the two formulas leads to the following equation:

$\text{risks} = \text{likelihood} \times \text{impact} \times \text{vulnerability}$.

These formulas illustrate how security management aims to keep risk as low as possible by reducing or mitigating vulnerability, likelihood and impact.

[2] See European Interagency Security Forum: Security to go: a risk management toolkit for humanitarian aid agencies, http://mhpss.net/?get=263/Security-to-go_A-Risk-Management-toolkit-for-humanitarian-Aid-Agencies3.pdf.

Thus, security management as part of humanitarian operations requires humanitarian actors to constantly heed a number of fundamental pillars:

- Recognise the different security threats.
- Assess each threat's likelihood to actually occur and its impact in case it does.
- Determine the organisation's vulnerability to each threat.

Based on these assessments, one may determine security risks and design security plans. Security plans aim to reduce risk and mitigate impact, focusing on a combination of measures to reduce

- the likelihood of a threat;
- the vulnerability of the organisation to a threat; and
- the impact of a threat when it occurs.

Consider the following example: there is an increase in night-time robbery in an unspecified context in an unspecified area. Humanitarian organisations should identify this new trend through constant monitoring of the situation and review their security plans to find ways to reduce the newly augmented threat. They could, for example, decide to set up a curfew for the staff (ban night travels) and provide safe transportation for the staff after working hours. Both measures reduce the likelihood of night robbery in the streets. Organisations could also ensure that the staff does not carry valuable or sensitive equipment or data when outside the office, thus reducing the impact of a possible incident.

Risks should be constantly monitored as they continuously vary based on political, military or social developments. This is especially relevant in volatile environments where humanitarian actors operate on a regular basis. Security measures are only useful as long as they match the actual risks. In the example at hand, the measures implemented would lose their relevance in the wake of a new threat of house robberies. Thus security management should always remain contingent to changes in the security landscape and adapt according to these.

2 Context Assessment and Stakeholder Mapping

The first cornerstone of security management is to know and understand the context an organisation operates in. Different contexts will generate different risks, thus requiring different sets of security measures and mitigation strategies. Context analysis is an essential prerequisite for comprehending the environment that organisations operate within and in understanding the dynamics at stake. Such assessment usually includes acquiring knowledge about all or part of the following issues:

- history and politics of the context;
- main religious practices and beliefs;
- different ethnic/religious/cultural groups, geographic distribution and living habits;

- interaction between said groups;
- wealth distribution, main source(s) of revenue, poverty pockets;
- technology landscape, most used communication tools, Internet penetration, cell phones, mobile Internet, most followed and used sites;
- criminality levels, most common crimes, geographical distribution, prison system;
- legal framework (both official and customary), law and order;
- law enforcement: different agencies, capacity, integrity, allegiance, agenda and focus, training;
- corruption: petty and larger, prevalence, social acceptance;
- geography, transport and commerce routes;
- main political stakeholders, the structure of their constituency, their political aim;
- main armed groups, their funding and military capacity;
- other humanitarian/development actors, their current focus and future plans.

This is a non-exhaustive list and should be adapted to each context. Wherever possible, assessing trends should be preferred to static snapshots; for example, the trends of criminality in the last six months is more telling than detailed crime statistics for the last month.

Clearly, the context assessment's value is not restricted to security assessment. It is also of great value for programming. Good programming and effective security management operate hand in hand and rely on each other at every step. Organisations should approach security management as an integral part of programming, as we discuss below.

Context assessment is time and resource intensive. It is, however, the basis of effective security management and proper humanitarian programming. The context assessment should be constantly reviewed to reflect changes in the field reality. A good context assessment should be designed to allow for updates and offer the possibility of reading trends and changes.

3 Security Stakeholder Mapping

Security stakeholders are the main actors that are influenced in the security area. They include law enforcement agencies, armed groups, private actors with security clout, etc. A list of such stakeholders should include any group capable of jeopardising the security of organisations if it decides to do so. The purpose of this mapping is so that the concerned humanitarian organisation understands the security dynamic in its area of work. Security stakeholders are usually plotted on a matrix that reflects their interest in and support to the organisation, as well as their power and influence (see Fig. 1). Based on this mapping, the organisation will decide how to interact with security stakeholders.

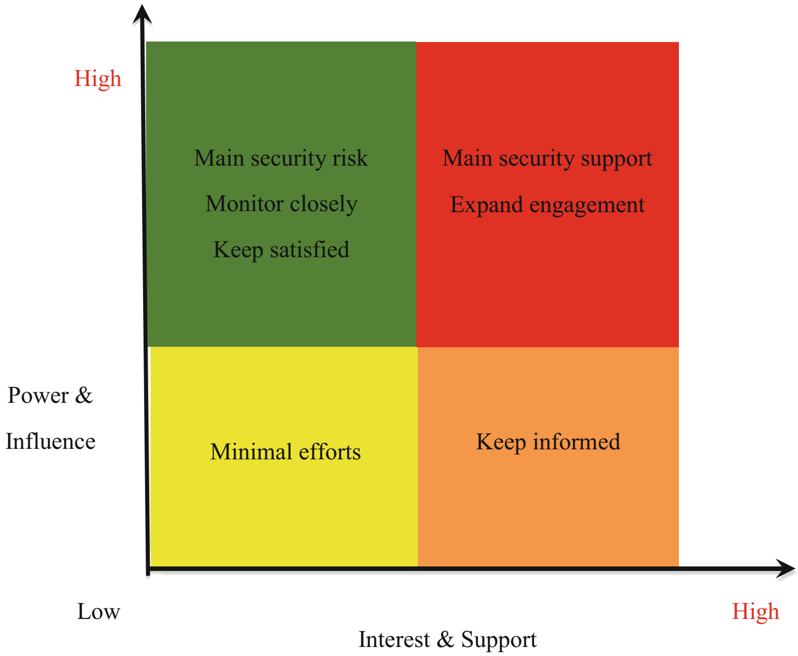

Fig. 1 Security stakeholders. Developed by the author, Bob Ghosn

4 From Context to Risk Assessment

Based on the context assessment, organisations should list all threats in the context given. For each threat, the organisation concerned should identify likelihood and impact, as well as its vulnerability to it.[3] Usually, humanitarian organisations assign figures to likelihood, impact and vulnerability in order to be able to compare risks (see Table 1).

- In this case, the likelihood of a car accident is considered high because the organisation has had several accidents over the last months. Their impact is also high because they generate high tension with the local population. Locals often block the organisations' vehicle from passing through their village, weeks after accidents. The vulnerability is also high because the organisation relies very heavily on car trips.
- Riots are very likely to happen. Tension has been simmering for weeks, and several leaders are calling for demonstrations. Last year, similar demonstrations turned into riots for days. Downtown shop owners were seen moving their valuables to other location and covering shop windows with steel curtains. If

[3] See definitions above for Impact, Threat and Vulnerability.

Table 1 Threats and risks for humanitarian organisations in dangerous areas

	Threat	Likelihood	Impact	Vulnerability	Risk level
1	Vehicle accident	3	3	3	27
2	Riots	4	3	2	24
3	Carjacking	4	4	4	64
4	Staff sexual violence/ rape	2	5	4	40
5	Kidnapping	2	5	5	50

Developed by the author, Bob Ghosn

the organisation's office is looted in a riot, the impact will be high because they store a lot of valuables, sensitive data and cash in the office. However, the office is not very vulnerable to riots since it is located in an area that is remote from downtown, where demonstrations and riots usually happen.

- There have been several carjackings in the last weeks, and the trend is increasing. Carjacking will have an important impact because it touches upon the staff's physical safety (in previous carjackings, violence was used against passengers). They are vulnerable to it because they rely very heavily on car trips on the very roads where carjacking has occurred in the past.
- Sexual violence/rape is not very likely to occur. The last case happened two years ago, and perpetrators were publicly brought to justice. Its impact would obviously be enormous as it touches upon the physical integrity of the staff. They are very vulnerable to attacks because they often have all-female teams working in the field on reproductive health with women's groups.
- Abductions are not very likely. There have not been any in the area. However, abducting humanitarian workers is now a global trend. Its impact would be obviously huge, as it threatens the life of the staff. They are very vulnerable to it because they never took any measures to mitigate this risk since no such incident ever occurred in the area.

5 From Risk Assessment to Security Planning

Based on the risk analysis, humanitarian organisations will devise or update their security plans to mitigate the risks or impact of threats. Priority should be given to the highest risks.

For instance, analysing our case above, one finds that carjacking (3) poses the highest risk for humanitarians. The organisation concerned can, for example, explore the following security measures to mitigate this problem:

- Consider alternate routes that are safer (decreases likelihood).
- Explore how to reduce car travel by setting up bases near target areas where the staff can stay overnight and reduce car travel (decreases likelihood).
- Use air travel if possible (decreases likelihood).
- Approach other organisations to organise convoys when travelling (decreases vulnerability).
- Set up a two-vehicle travel rule (decreases impact).
- Approach authorities to request more security/patrolling on the travel routes (decreases likelihood).

The second-highest risk is abduction (5). This is a risk that the organisation has never considered before. Thanks to the security assessment, it is now on the table, and security planning regarding this risk should start. The organisation can, for example, explore the following first actions:

- Check with other organisations regarding their assessment of the abduction risk and how they deal with it.
- Who should do what? How to react? Review your entire security plan in view of an abduction.
- Review passive security in the office and living quarters in view of abduction risk.
- Have discussions with your staff about kidnapping risks and listen to their concerns and suggestions.
- Ensure that some measures are taken to mitigate the abduction risk.

The third-highest risk stems from sexual violence/rape (4). The organisation can, for example, explore the following security measures to mitigate this risk:

- Change the practice of all-female teams and always have a male accompanying female teams (decreases vulnerability).
- Engage in a discussion with female staff about how they feel about this threat and what measure they suggest to mitigate it. All of their recommendations should be received with a very welcoming ear.
- Ensure that post-rape kits are readily available and psychosocial support is readily available either in-house or outside the organisation (decreases impact).

Vehicle accidents (1) cause the second-lowest security risk. The organisation can, for example, explore the following security measures to mitigate this risk:

– Explore how to reduce car travel by setting up bases near target areas where the staff can stay overnight and reduce car travel (decreases likelihood).
– Use air travel if possible (decreases likelihood).
– Set up lower speed limits (decreases both likelihood and impact).

Although riots rank lowest on the risk level scale, they still constitute a significant risk. The organisation can explore security measures to mitigate this risk. They include reviewing the relevance of holding valuables and sensitive data in the office and considering to secure cloud storage of data and the storage of valuables in different locations (reduces impact). As mentioned above, the risk assessment and the matching security plan should be constantly reviewed and adapted to ensure they reflect the reality in the field.

6 Securing People Not Career Paths

It is important that all security measures adopted by humanitarian organisations actually aim at reducing vulnerability to an actual risk, its likelihood or its impact. Security measures that do not actually make people safer should be discarded.

Security plans and rules should not include steps that aim at shielding the organisation or higher management from administrative or even legal consequences. This is a dangerous drift that is, unfortunately, very common in the current humanitarian landscape.[4]

This is counterproductive, as it adds an undue burden on security management. More importantly, such behaviour nurtures what we refer to as 'open umbrella culture', that is to say, the managers' focus shifts from safeguarding the security of people to protecting their careers and, sometimes, the organisation's liability in the aftermath of a possible security incident.[5] The priority drifts from mitigating the risk of an incident to ensuring that if an incident occurs, managers' careers will not be impacted. This is not only morally dubious but also a proliferating problem.

Once managers start acting on the premise of protecting their careers, this unwelcome trend may spread across the entire organisation like a wildfire. The entire security management system becomes paralysed by bureaucracy, disconnected from reality and completely risk-averse, making actual humanitarian action nearly impossible.

7 Security Is Everybody's Business

It is important for humanitarian organisations to nurture a culture of security amongst its entire staff. Security management should be portrayed as part of the identity and the daily work of the humanitarian organisation and not a stand-alone feature separate from programming and managed by security officers or managers.

Security management should be intertwined with programming. Planning aid activities without taking into account security parameters will invariably lead to unrealistic implementation plans. In addition to being a waste of time and resources, planning with no security inputs generates a series of missteps when

[4] As an example, in Iraq, a humanitarian organisation forced its staff to file leave requests before some field trips. In case of a security incident, the organisation could deny responsibility.

[5] The signs of such prevailing culture are the number of disclaimers staff are required to sign.

the organisation moves towards implementation; tension will rise within the team as planning collides with security constraints. Staff and management will be under undue pressure to speed up implementation or design and utilise often unsafe implementation means. Beneficiaries will see their expectations disappointed and their needs uncovered as the organisation will not be able to deliver on its commitment due to faulty planning.

Programming should incorporate security management to ensure that planning remains in the realm of reality and safety. At every stage of programming, from the initial needs assessment to the design period, security management should be incorporated in the process. Security management in humanitarian organisation is not what keeps the staff safe. It is an enabler that allows the delivery of humanitarian aid to those in need. Rather it is through the involvement of security management in the planning at every stage that the organisation will find ways of continuing to operate. It is the constant interaction between programming and security management that grounds the implementation plans in reality and allows a realistic chance of timely and effective implementation.

In order to ensure this strong link between security management and programming, it is primordial for staff to be trained in security and to imbibe that security is everyones responsibility and that part of their job is to contribute meaningfully to security management. In the field of security, availability of information is key. A security plan based on incomplete information will be faulty, and people will get hurt as a result. It is impossible to identify trends and risks without comprehensive access to updated information.

Having constant access to security information is essential for effective security management in a humanitarian organisation. Efforts should be made at all levels to facilitate the flow of security-related information towards the security management process. The constant flow of security information is the lifeline of security management; without it, security management is akin to running downstairs in darkness. A security plan based on incomplete information is by design a faulty one, which will not provide the needed security and will have adverse, sometimes lethal, consequences.

Continuous efforts should be made to ensure that security information flows freely towards and within organisations and feeds into security planning.

Several types of information sources are usually of security value. We have discussed the importance for humanitarian organisations monitoring online discussions and tapping into available information offered by private intelligence agencies. The two other sources of information we address here are other humanitarian organisations and the organisations' own staff.[6]

[6] There are obviously other sources of information ranging from open source media to confidential discussions with stakeholders.

8 Sharing Keeps Everyone Safe

Humanitarian organisations often compete for resources, field presence and programming. This is an unfortunate fact of the humanitarian landscape, and as much as we can lament it, it is reasonable to expect this situation to prevail.

However, humanitarian organisations need to understand that notwithstanding jockeying for funding and programming, in the field of security, if information is not shared, people will be harmed as a direct consequence.

It is therefore vital that humanitarian organisations set up, in every location, effective systems to facilitate and encourage the sharing of security information, such as security forums or security coordination meetings. The working arrangements should provide for real-time information sharing[7] to allow swift reactions to unwelcome and unforeseen developments.

In addition, headquarters should issue clear instructions to encourage the immediate and transparent sharing of security information. This should not be left to the chemistry amongst local heads of office or security managers. It should be a clear policy of the humanitarian organisation.

Lastly, organisations should commit to maintaining the confidentiality of security information accessed through the security coordination mechanism. This is key as organisations will be understandably reluctant to share privileged security information, unless they trust that it will remain confidential. Security forums should have effective and strict protocols for managing confidential data that all participating organisations are comfortable with. Humanitarian organisations will only share privileged information if they trust the confidentiality of the forum.

9 Let It Flow, Keep It Simple

Within organisations, there are often unintended impediments to easy and quick information sharing. Reporting, action plans and other working documents tend to continuously grow longer and heavier. This is not the place to discuss how humanitarian organisations are unduly overburdened by donors' bureaucratic requirements, but it is certainly an important question to discuss in appropriate forums.[8]

Regarding security, it is important for humanitarian organisations to realise that long security documents are seldom read, and, when they are, they hardly make a lasting impression and are quickly forgotten. When drafting security rules, drafters should put themselves in the shoes of a new staff member and draft the document in a way most conducive to helping the staff understand and remember the content.

[7] Arrangements can range from a WhatsApp dedicated group to a specific radio channel, depending on the context.

[8] The Good Humanitarian Donorship has contributed to this discussion.

Images, interactive scenarios, videos and other audiovisual support are always more effective than long texts.

Similarly, security updates (for example, a new development, a security incident or a near miss) should be concise and accessible. Lengthy forms, cumbersome processes and tedious reporting are counterproductive as they disincentivise the staff from properly reporting events in a timely manner, thus depriving the security monitoring system from possibly important elements regarding changes in the security landscape.

Humanitarian organisation should set up clear and simple ways for staff to report on all matters of security, be it a security incident, a near miss or a new security development.

The reporting system in place should be designed in a way that guarantees that

- the staff is able and comfortable to use it;
- it is always immediately available[9]; and
- received information will be swiftly processed.

To illustrate this, the reporting system in place should ensure that security information is

- not buried in lengthy operational reports;
- reported too late because the staff did not have immediate email access;
- not reported because the staff feared it would adversely affect the career of a colleague who breached security rules; and
- not acted upon because it slept in a mailbox until it lost its relevance.

10 Keep It Focused and Separate

Security reporting by staff often involves issues going beyond security matters. It often touches upon human resource issues, usually regarding staff behaviour and respect of security rules.

On the one hand, it is understandable that reporting staff may feel conflicted between the desire to provide accurate reporting and the desire not to harm themselves or colleagues.

On the other hand, effective security management requires knowledge of all information as accurately as possible without sugar-coating or blind spots.

The best way to avoid this dilemma is to keep security reporting separate from any other process or reporting. The staff should be able to trust that security reporting will be processed and solely used to actually improve security and not for any other operational purpose such as staff management, reward or penalty. The staff should be able to trust that information they report on security is only used to

[9] If preferred communication means are not available 24/7 alternate communication system should be set up, including emergency telephone numbers etc.

improve security management and for nothing else. Processes for assessing staff performance should be clearly separated from security incident reporting. It is important to build an effective firewall between the two to ensure that the staff feels confident enough to accurately and freely report security incidents.

Assessing compliance of individual staff members with security rules is essential. Each humanitarian organisation should have an ongoing process that serves that purpose. The point here is ensuring and monitoring compliance as an important task that is not separate from analysing security incidents. To illustrate with an example, organisations should constantly check that the staff buckle their seat belts and respect speed limits on the road, irrespective of whether a road accident has already occurred or not. Checks should be conducted on a regular basis, and faulty behaviour should entail consequences.

The objective of security incident reporting and analysis is to deal with the immediate consequences of the incident and improve security plans in light of an accident or a near miss. It is crucial to ensure that the management of security incidents remain focused on these objectives and does not drift into finger pointing. Defining individual responsibilities is important but should not be done within the security management processes. Individual responsibility is assessed through human resource mechanisms or ad hoc fact-finding task forces, which should remain separate from security management processes.

The following scenario may serve as an example: a team of a humanitarian organisation operating in a conflict area travels at night in an area that is deemed safe for day travel because the organisation enjoys high levels of acceptance by local stakeholders. The team is stopped at a checkpoint for 1 h. Team members are threatened at gunpoint, robbed of all their valuables and finally asked to be on their way.

In such a situation, a three-tier process should be triggered with three distinct points of focus:

- providing all needed support to the affected staff.
- review of security plans based on the incident; and
- individual staff accountability.

Each one of these processes should be implemented independently of the others to ensure each one's integrity.

The first process is ideally driven by a health specialist. It involves providing psychosocial support to staff and their loved ones as needed. We will not delve into the details of staff support here.

The second process is a security review of the incident. It focuses on understanding its impact on the current assessment of the area as safe for day travel. The fact that the incident occurred at night does not mean that it is of no consequence for day travel in the area. Typical questions include: who was manning the checkpoint? Why did they stop and threaten the team? In light of the incident, the team will review all elements that led them to conclude that the area was safe for day travel. Contacts with local stakeholders will be strengthened to better understand their perception of the organisation and the mission. There is also another important security component to this incident. During a security review, it is important to understand why the team decided to breach the security rules in the first place and drive at night. If the team was not safe in the location they were supposed to stay overnight or if the team felt it needed to get out during the night to fulfil expected tasks, this information is of crucial importance for the security reviews. Decisions have to be made to avoid repetition of similar situations. However, it is not relevant for the security review to understand whether Robert, Beatrix or Khadija decided to breach the security rule and drive by night. It is not for the security review to assess who is actually responsible for the breach and how to hold him or her accountable.

The third process aims at assessing the responsibilities behind the violation of the security rules. Travelling at night in an area that is deemed safe only for day travel is a clear breach of security rules. Why and how did the team decide to disregard the rule? Was this part of their prerogative, and if not, who overstepped his/her prerogative, and what measures, if any, should be taken against staff members?

It should be very clear to all staff members that the three processes are run independently. Each one should be led by a separate person, typically from the fields of health (first process), security (second process) and management (third process): the staff should be allowed to report and contribute freely to each process. If the firewall between the three processes is not trusted by the staff, it may alter their reporting, providing a partial, if not biased, picture of the situation, negatively impacting the quality of the three processes. The main objective of establishing separate processes is to create an environment conducive to accurate staff reporting.

Consider this second example on the importance of staff being able to report freely on security-related issues: a staff member knows that a driver's brother has joined an armed group. The driver feels he should just ignore the problem by not talking about it. He does not talk about it to his supervisor, fearing he might lose his job. If unreported, such a situation might expose the organisation to a new risk that is not part of its risk assessment. The fellow colleague and even the driver himself is more likely to report such a security development through a *security-only* channel, if he trusts that the information will only be used to assess and mitigate the risk. Based on this assessment, mitigation measures such as restricting field trips of this driver to certain areas can be put in place, and the situation may be monitored. The staff, including the driver himself, will only report the problem if they trust that this will make the entire organisation (including the driver) safer and not result in disciplinary proceedings questioning the driver's capacity to act impartially. Although the latter point might be an issue for discussion, the point here is that the staff feels that such information can be quickly and freely shared through *security-only* channels in order to improve the security of everyone. A human resource/management discussion of the issue will only come if the security risk is deemed too high after monitoring. In the meantime, the organisation security avoided a blind spot because the information was shared.

Within this approach of parallel processes, there is a need to set up a system that allows for key information to be shared across processes, to ensure a comprehensive view. This merging of information should take place at the senior management level, with the staff being informed about the proceedings from the beginning. This consolidation should focus on the important takeaways and not get bogged down in details. Before sharing the results of each process externally, some personal data can be anonymised,[10] and the organisation should ensure that information provided by the staff for specific purposes (for example, security) is not used in other ways (for example, disciplinary action) without his/her informed consent.

11 Security Management Strategies

Humanitarian organisations use a mix of three strategies to manage security risks: acceptance, deterrence and protection.

11.1 Acceptance: The Holy Grail?

Acceptance is a security management strategy that reduces threats by building relationships and trust. Acceptance is the favourite security strategy of humanitarian organisations. It is based on the reasonable assumption that a humanitarian organisation that is known and accepted within the local community will operate in a safer environment. If the local community understands and values the organisation's work, the former is more likely to act in ways that increase the latter's security, from warning it about threats to actually taking action to protect it. Acceptance is not a natural feature of humanitarian work. It cannot be assumed and must be nurtured.

Humanitarian organisations should not assume that local acceptance is a natural consequence of the good they are doing. This would be a false and dangerous assumption. Acceptance is highly dependent on a range of issues, including perception, transparency, daily behaviour and attitudes. Acceptance is achieved through daily engagement with communities and constant efforts. Even where local communities, overall, benefit from the humanitarian programme, acceptance should not be assumed.

Consider the following example: if an organisation is supporting a health care centre, this organisation should not assume that it is locally accepted by virtue of its support to this health care centre. Engagement with the community is very likely to show that issues such as access to services and possible unintended discrimination, payroll and recruitment matters, individual behaviour by staff, unrealistic expectations, as well as culturally sensitive topics such as reproductive health weigh heavily on the organisation's acceptance.

[10] Medical data from the support process should be managed in accordance with medical ethics.

Acceptance is an indispensable factor for any successful humanitarian operation, and it requires sustained engagement with all parties. However, humanitarian organisations tend to be overconfident about their local acceptance, assuming it on the basis of anecdotal elements such as welcoming behaviour of locals in a marketplace or friendly local staff. Therefore, organisations are often reluctant to recognise that they are not necessarily accepted in a community they are serving with dedication and commitment. This is very understandable from a human point of view. However, if, as it should be, acceptance is a key feature of security management, it must be approached in a dispassionate and professional manner. Acceptance is a security strategy that aims to specifically reduce identified threats. Thus, acceptance should be constantly monitored, and based on facts and trends the organisation should adapt both its security plans and daily practices in order to, respectively, take into account and bridge any observed acceptance gap.

Finally, humanitarian organisations should keep in mind that acceptance is not a magical wand that guarantees security. Sadly, there is no such thing. The highest level of acceptance is of no help to mitigate security risks such as being caught in a crossfire or faced with high levels of criminality following a breakdown in law and order. Such risks require different mitigation strategies that go beyond acceptance. In addition, in conflict settings, a good acceptance level by one party to the conflict often impacts negatively on acceptance by the opposing party. In addition, even where a humanitarian organisation is very well accepted by the local community, it remains exposed to the risk posed by actors from outside this community. For a mitigation strategy to be an effective risk, it must lead to acceptance by those who make up the source of the threat.[11]

11.2 Protection: Be a Harder Target

Protection is the second security management strategy. Protection reduces the vulnerability of organisations to a threat through a combination of passive measures and procedures. The objective of the security protection strategy is for any humanitarian organisation to become a hardened target, a target more difficult to attack.

Passive measures are physical features such as hardened walls, higher fences, stronger gates, safe room, bunkers, armoured vehicles, etc. A common example of a protection procedure is the decision by an organisation to always use two-vehicle convoys or to only allow daytime travel to prevent carjacking.

A protection security strategy does not reduce an identified threat. It reduces the vulnerability of the organisation and its impact when the threat materialises. The protection security strategy should be devised by taking into account two factors, in

[11] For details on acceptance, please refer to the Acceptance Toolkit: http://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf.

addition to the risk assessment: the profile of the organisation's presence and the level of protection used by other actors in the area.

Visible protection features such as high walls, fences or 24-h external lighting in electricity-scarce areas are likely to raise organisations' profiles and might increase the security risk.

Security management should constantly seek to strike the right balance between reducing vulnerability without increasing risk. Security decisions regarding protection should also take into account the level of protection used by other actors in the area. The protection measures taken by the humanitarian organisation in question should be in line with those implemented by other actors. If a humanitarian organisation deploys lower security protection measures than other actors in the area, it will become, de facto, a soft target and is very likely to be attacked, for opportunistic reasons.

One key component of the security protection strategy is to implement measures that would lower the impact of a security incident when it happens. Measures such as back-door emergency exit, available evacuation vehicles, attack-resistant safe rooms, encryption and cloud storage of data are the type of measures that can be taken to lower the impact of security incidents.

11.3 Deterrence: The Credibility Choice

Deterrence is the third security management strategy. It reduces the likelihood of a threat through counter-threats or undesirable consequences. The rationale is to deter actors from harming organisations by showing that such act would have adverse consequences. A deterrence strategy does not have to carry a threat of violence. For example, in order to deter a risk, a humanitarian organisation can highlight that it will

- pursue legal action against any unlawful behaviour;
- suspend its programmes if the security of the organisation is threatened; and
- pull out of the area if the organisation is targeted.

Traditionally, humanitarian organisations are uncomfortable with the deterrence strategy. They incorrectly perceive it to be at odds with their humanitarian values. While it is obvious that humanitarian organisations are unable to continue operating if the security situation does not allow for it, they tend to bury this scenario under a blanket of denial.

If humanitarian organisations choose to allow local actors to think that, whatever happens, they will continue their humanitarian work at any cost, then other actors can be forgiven for thinking, for instance, that it is acceptable and of no consequences to unduly turn back the organisation's vehicles at checkpoints or even to rob the organisation's office when they are short on cash.

For a deterrence strategy to be effective, it needs to be credible. And credibility is a choice that every organisation has to make. It is an all-important choice and not an easy one. It will have consequences, also on security. One possible and highly debated deterrence strategy is the use of armed guards and/or armed escorts. Traditionally, humanitarian organisations are quite rightly reluctant to use such methods.

Humanitarian organisations have to apply the right mix of these three strategies. It is a subtle balance to strike as there always tends to be tension between the different strategies. This balancing act should be constantly reassessed based on updated security information.

11.4 The Elephant in the Room: Risk Transfer

The term risk transfer refers to cases in which a humanitarian organisation shifts the risk exposure to another organisation, usually a smaller implementing partner. The latter then bears the burden of facing what is usually a high-risk security situation.

When a humanitarian organisation, or a donor for that matter, enters into an agreement with a smaller implementing partner to operate in a dangerous setting, the bigger organisation, or the donor, is under an imperative moral and arguably legal requirement to ensure that the underlining rationale for the agreement is not to, even unwillingly, transfer the risk to an organisation that lacks either the capacity or foresight to properly assess it or the means to refuse the contract, due to precarious funding.

Hence, humanitarian organisations that delegate implementation to other organisations in high-risk areas should always assess implementation agreements from a risk standpoint. It is not enough for the contracting agency[12] to find that the implementing partner brings an added value from a risk management point of view such as higher acceptance that will lower the risk or the ability to keep a lower profile that will decrease the vulnerability to threat.

It is not about comparing access capacity between contracting agency and implementing partner. The latter usually fare better in this comparison, but this is beside the point. The issue here is to ensure that the implementing partner is effectively identifying and managing the risk in a manner that is consistent with humanitarian agencies' standard practices. Shifting risks to a smaller humanitarian organisation, or a contractor, without looking into their ability to safely operate by identifying and managing those risks is irresponsible, if not reckless.

[12] Here the contracting agency is the organisation that subcontracts the implementation to an implementation partner.

12 First, Know Thyself

An important element of the context analysis is for the humanitarian organisation to define its desired identity, in a specific setting. This identity is usually built around a mix between the organisation's mandate and mission, its principles and its programmes in the area. It should be concise and expressed in easily understandable language. The organisation should ensure that all staff know and understand this information and are able to communicate it clearly and consistently externally.

In the humanitarian field, as in other areas of life, deeds speak louder than words. It is therefore essential to enforce strict rules to ensure that staff behaviour is entirely consistent with the organisation's desired identity.

Humanitarian organisations should keep in mind that outside perception of the organisation very often differs from their own. The perception of a situation is very different from the points of view of a local standing in the dust when a humanitarian convoy passes through the village every day and of a person sitting in the said vehicle listening to music. This is a fact, and organisations should accept it as such and act accordingly. There is nothing wrong with listening to music and villages have to be crossed on the way to implementing humanitarian action to be implemented and help people. The point is to understand how people perceive the organisation, which helps anticipate how people will behave towards it.

Hence, it is vital to constantly monitor the organisation's perception amongst the population and continuously devise and implement outreach efforts to align outside perception as closely as possible with the organisation's desired identity. A damaging perception of the organisation should not be allowed to build up, as it could potentially increase security risks.

In addition to the perception of the organisation, the perception of every individual staff member is also an issue that organisations should monitor. Staff members are not only perceived as such; they are also seen through the prism of their nationality, ethnicity, gender, attitude, etc.

13 Effective Security Management: A Legal Requirement

On 25 November 2015, an Oslo District Court sentenced the Norwegian Refugee Council (NRC) to pay Steven Patrick Dennis, a former NRC staff, 5.5 million Norwegian krone (approximately 650,000 USD) for compensation and gross negligence. The case was widely covered both in mainstream media and humanitarian spheres. Steven Dennis and three other NRC staff were kidnapped in June 2012 in Dadaab refugee camp, Kenya. Dennis was wounded during the incident, and an additional NRC staff member was killed. The four kidnapped members of staff were released four days later, following a security operation. Dennis sued NRC, and the Oslo Court found NRC to be liable for compensation and gross negligence.

This landmark case established that a humanitarian organisation is legally bound by a duty of care towards its staff, even in very volatile environments. The Norwegian Court based its decision on a review of NRC security management, which it found below standards. It is remarkable to note that the Court probed the details of NRC security management and pointed out the following deficiencies:

- NRC decided not to use armed escorts against the recommendation of its own security team.
- Location and timing of the visit were maintained despite security concerns.
- The visit was a high-profile one with media coverage.
- NRC staff was not timely briefed about the security situation and so could not make informed decisions about participating in the visit, in full knowledge of the risks involved.

Impact and meaning of this landmark court decision has been widely discussed amongst aid workers and organisations.[13] In the wake of the decision, humanitarian organisations should prepare for a possible judicial review of their security management *modus operandi*. Appropriate and efficient security management of humanitarian operations has always been a moral and operational requirement. It is now, arguably, also a legal one. Although it is too early to foresee all legal ramifications and possible ripple effects of the Dennis decision, humanitarian organisations have to prepare for possible legal challenges to their security management and should ensure that they uphold their duty of care towards their staff.

14 The Cost Factor

Another challenge faced by humanitarian organisations is that proper security management is often expensive, while humanitarian budgets are restricted regarding security costs.

This, firstly, often forces humanitarian organisations to rely on ineffective half-cooked security management plans. However, the issue of available budgets is not the only challenge to effective security management by humanitarian actors.

Secondly, when budgets are available, humanitarian organisations should overcome a cultural resistance to invest sufficiently in security. There is a prevailing perception that humanitarian organisations are immune to risks as a consequence of the good they do and the purity of their commitment. This is factually incorrect, as shown by the high number of humanitarian workers targeted and sadly killed or harmed.[14]

[13] For a thorough analysis of the consequences of this case, see Hoppe and Williamson, ODI HPN, April 2016.

[14] According to Aid Worker Security Database, in 2014, 329 humanitarian workers were hurt in a security incident, 121 were killed, 88 injured and 120 kidnapped.

The third challenge regarding the security cost factor concerns security investments by humanitarian actors. Such investments should not be restricted to hardware, ranging from communication equipment to armoured vehicles, but also include technical means, training, staff and information access. All of these are crucial to monitoring security and effectively managing security risks. Humanitarian organisations should ensure that the technical means they use to monitor the security situation, such as software to aggregate trends, are up to current industry standards. Similarly, humanitarian organisations should have access to privileged information about specific contexts and situations, often provided by private intelligence agencies.[15]

Last but not least, security training by humanitarian actors should tap into state-of-the-art available training resources as the issue can literally become a question of life or death.

15 Security and Technology

Technology is increasingly intertwined with security. Still a relatively new but very promising field of action for humanitarian organisations, they should tap into the huge potential of digital technology to strengthen security management. Overall, there are five main areas to explore.

First, in many volatile contexts, where humanitarian needs are high, armed actors may have a strong social media presence on Twitter, Facebook, Telegram, etc. Monitoring and even reaching out to these groups online requires more than a Twitter or a Telegram account. Humanitarian organisations should be tech-savvy and acquire appropriate software and cutting-edge skilled staff to explore ways to effectively use the Internet and social media to identify trends that will meaningfully feed into their security analysis and improve their engagement with security stakeholders online.

Second, humanitarian organisations should dispose of an effective online presence to monitor the situation in their area of operation online, as well as their online reputation amongst security stakeholders. As we will see below, acceptance and perception are key to properly identifying and managing security risks. For example, if an armed group is frustrated by actions of a specific humanitarian organisation or falls victim to a rumour about this organisation, it is very likely that the group members will first vent their anger online. Provided with the proper equipment and staff, the organisation in question should be able to spot the social media chatter and the anger building up. It can then engage online, and in real life, to correct the misconception and, simultaneously, review its security plans, in view of

[15] The most renowned is the Economist Intelligence Unit that focuses on the economy. Some private intelligence agencies, such as Stratfor or Control risk, focus more on security while others such as Site Intel Group focus specifically on violent and jihadi groups.

this new development. This is not about spying or eavesdropping. Monitoring what is happening online is not any different from humanitarian staff traditionally engaging in mundane conversations in markets or around a teakettle to get a *feel* of the situation.

Third, humanitarian organisations should have the means to make their voice and their message heard online. A strong, professional online presence is essential in influencing perceptions, countering false assumptions, thus reducing the organisation's vulnerability to risks. In addition, in our digital age, security threats have become global. The days where security was a local matter are over. It is not enough for a humanitarian organisation to be accepted by local stakeholders in its area of operation or even in the entire country. News or rumours from a far-flung country travel thousands of kilometres at the speed of light and erupt on the screens of otherwise well-meaning security stakeholders. It can change their mood towards the organisation in a split second. In a real-life example, a humanitarian organisation that enjoyed broad acceptance in Southern Iraq had to scramble overnight and review its entire security management plan because certain Facebook postings in Somalia falsely claimed that the same organisation was poisoning Muslims. It is only thanks to effective online monitoring that the posts were spotted on time, thus allowing security arrangements to be immediately reviewed and an outreach effort to be launched to counter the false claims.

Fourth, there is an increasingly large digital dimension to analysing contexts and identifying risks. Humanitarian organisations should invest in areas such as big data analysis to explore ways of improving their security management. Google is exploring ways of anticipating flu epidemics in specific areas by analysing search queries. So far, this attempt has been labelled an 'epic failure'.[16] However, the potential of mining data for useful information is undeniable. Similarly, humanitarian organisations should explore ways of better understanding their working environment by analysing digital data. Fear of failure should not preclude innovative approaches. The connection between the digital and real world is a reality that creates both great opportunities and serious threats to humanitarian organisations. It is only by engaging in the field of digital data and pioneering new approaches that humanitarian organisations will learn how to harness opportunities and mitigate risks.

Fifth, the security management of humanitarian organisations can greatly benefit from an expert use of mapping and satellite imagery, as it strengthens the capacity of humanitarian organisation to identify and monitor humanitarian needs, as well as risks.

[16] What we can learn from the epic failure of Google flu trends, http://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends.

16 The Dangerous Double Fallacy of Zero Risk

Security management is about managing and mitigating risks. Properly identified and mitigated, risks do not disappear but can be lowered. However, it is important for humanitarian organisations to be transparent with their staff about security risks. Here again, denial is not a good strategy.

The staff should be made aware of the risks and the security measures in place to manage these. On this base, they should be encouraged to decide whether a security situation is above or below their personal security threshold. Being transparent about security risks is part of the relationship of trust that humanitarian organisations should build with their staff. It is also important for security management. Staff unaware of security risks will lower their guard, sloppily apply security rules and not look out for possible changes in the security landscape. Risk-aware staff is a key component of any effective security management.

In contexts where security risks are low, organisation should not fall for the fallacy of zero risk, thus ignoring security management altogether. Certain security risks always exist. Lower risk still require identification, management and, maybe more importantly, monitoring. It is only constant monitoring that will allow organisations to spot and identify a change in the security landscape or a new worrying trend to which they have to adapt.

17 Good Staff Management for Good Security

Staff is the most important asset of any humanitarian organisations. Their behaviour determines the success or failure of any programme, and the same applies to security risk management. We do not delve into good staff management here but highlight the strong link between staff and security management. The better the former, the more effective the latter will be.

A positive culture, good team spirit amongst staff, proper dispute management mechanisms in place and people who are willing to help each other enhance an organisation’s security. This kind of environment leads to unobstructed information flows and the capacity to rapidly implement adjustments, when needed. A relationship of mutual trust between the staff and leadership nurtures a culture of security across the board where everyone feels part of the collective effort, including security management.

On the other hand, teams where staff members are unhappy and frustrated are prone to turf fights and silo thinking. This directly impacts security management as the staff members do not feel that they are part of the collective effort. Information is lost, and changes are cumbersome and slow to implement. The organisation loses its agility and timely adaptation to security changes. In addition, an unhappy staff is more likely to ignore security procedures, increasing security risks. Finally, a disgruntled staff often becomes a security threat.

Stress has a direct impact on security.[17] Under stress, people make poor decisions and often increase security risks. From a security management standpoint, it is essential for humanitarian organisations to manage the stress levels of its staff and to provide them with peer and professional support.

18 Conclusion

Security management is a key component of humanitarian action. Effective security management requires humanitarian organisations to grow and nurtures a culture of security within organisations. Contexts where humanitarian needs are the highest are increasingly violent, and this trend is likely to continue. In order to be able to operate in such violent contexts, humanitarian organisations have to improve and professionalise security management.

Security should not be an add-on to humanitarian programming. Effective security management is an enabler of humanitarian action and needs to be intertwined with programming. Planning humanitarian action without considering security management is a recipe for failure. Moreover, security management for humanitarian organisations cannot continue to rely on using non-humanitarian experts to transplant programming concepts developed by and for non-humanitarian actors into humanitarian settings.

If humanitarian organisations want to make a meaningful impact in dangerous settings, they must endeavour to improve both the theory and practice of security management, specifically for humanitarian contexts. They owe it to their staff and to the people in need.

References

European Interagency Security Forum: Security to go: a risk management toolkit for humanitarian aid agencies, http://mhpss.net/?get=263/Security-to-go_A-Risk-Management-toolkit-for-humanitarian-Aid-Agencies3.pdf

Hoppe K, Williamson C (2016) Dennis vs Norwegian Refugee Council: implications for duty of care. Online. ODI, http://odihpn.org/blog/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/ consulted on 24 June 2015

[17] For more on stress management in humanitarian organisations, please refer to the Antares Foundation (www.antaresfoundation.org) and the Headington Institute (www.headington-institute.org).

Further Reading

Allié M (2011) Acting at any price? Humanitarian negotiations revealed: the MSF experience. Hurst & Company, London

Behn O, Kingston M (2010) Whose risk is it anyway? Linking operational risk thresholds and organisational risk management. Humanitarian Exchange Magazine (47), June 2010

Collinson S, Duffield M (2013) Paradoxes of presence: risk management and aid culture in challenging environments. Humanitarian Policy Group, Overseas Development Institute

Egeland J, Harmer A, Stoddard A (2011) To stay and deliver: good practice for humanitarians in complex security environments. United Nations Office for the Coordination of Humanitarian Affairs (OCHA)

Fast L, O'Neill M (2010) A closer look at acceptance. Humanitarian Exchange Magazine, Issue 47, Humanitarian Practice Network

HAP International (2013) Guide to the 2010 HAP standard in accountability and quality management. HAP International, Geneva

Harmer A, Stoddard A, Toth K (2013) Aid Worker Security Report 2013: the new normal: coping with the kidnapping threat. Humanitarian Outcomes

Humanitarian Outcomes. Aid Worker Security Database. http://www.aidworkersecurity.org

Humanitarian Practice Network (2010) Operational security management in violent environments: Good Practice Review 8, revised edition. Overseas Development Institute

Kemp E, Merkelbach M (2011) Can you get sued? Legal liability of international humanitarian aid organisations towards their staff. Policy Paper, Security Management Initiative

Kingston M, Behn O (2010) Risk thresholds in humanitarian assistance. European Interagency Security Forum

Kingston M, Behn O Risk transfer through hardening mentalities? Humanitarian Practice Network. Online. http://www.odihpn.org/the-humanitarian-space/blog/risk-transfer-through-hardening-mentalities

Mission Ready. Online. Missionready.org.uk

Roberts DL (2006) Staying alive: safety and security guidelines for humanitarian volunteers in conflict areas. International Committee of the Red Cross

Stoddard A, Harmer A, Hughes M (2012) Aid Worker Security Report 2012: host states and their impact on security for humanitarian operation. Humanitarian Outcomes

Van Brabant K (2010) Managing aid agency security in an evolving world: the larger challenge. European Interagency Security Forum

Van Brabant K (2012) Incident statistics in aid worker safety and security management: using and producing them. European Interagency Security Forum

Wille C, Fast L (2013) Shifting patterns in security incidents affecting humanitarian aid workers and agencies: an analysis of fifteen years of data (1996–2010). Insecurity Insight

Bob Ghosn is an Aid and Human Rights worker. He has worked for several humanitarian agencies, including the International Committee of the Red Cross and the Belgium Red Cross. Views expressed here are personal.