Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping

Acción contra el Hambre (ACF-Spain) Case Study

Gonzalo de Palacios

Introduction

Acción contra el Hambre (Action Contre la Faim, ACF-Spain) is a Spanish humanitarian organisation and part of the ACF-International Network. Since its creation in 1995, ACF-Spain has been working in different countries and contexts, where security management is implemented and adapted through GPR8 'Operational Security Management in Violent Environments' (Van Brabant, 2010). For ACF-Spain, incident reporting serves two main purposes: supporting victims of incidents and being able to take the necessary steps in order to prevent the occurrence of new incidents.

In 2008 ACF-Spain started registering incidents from all its countries of operations (15 to 20 countries) in a systematised way using an Excel workbook. Incidents were reported from field sites to the Country Coordination Office and from there to Headquarters in Madrid. Although this was a positive initiative, as it began to provide evidence for identifying trends, victim profiles or most vulnerable locations, it had some limitations in relation to the access of information from countries of operation and the efficiency of the reporting process itself. In order to be able to analyse the information, the data contained in the incident report in Word format had to be transferred manually to the Excel workbook, taking a considerable amount of time. One of the gaps in the registering system ACF-Spain identified at that time was being able to pinpoint on a map where incidents were happening, something that Excel cannot offer. Despite this we managed to generate from our Excel database map layers in KML (Keyhole Markup Language), which allowed us the possibility of viewing through Google Earth where incidents were happening. The process was still very inefficient, with numerous mistakes, and the resulting KML was too heavy. After doing research, we identified various possibilities for incident reporting and mapping, such as open GIS software, Open Data Kit from Google, SharePoint from Microsoft, internal Project Management software and Ushahidi.

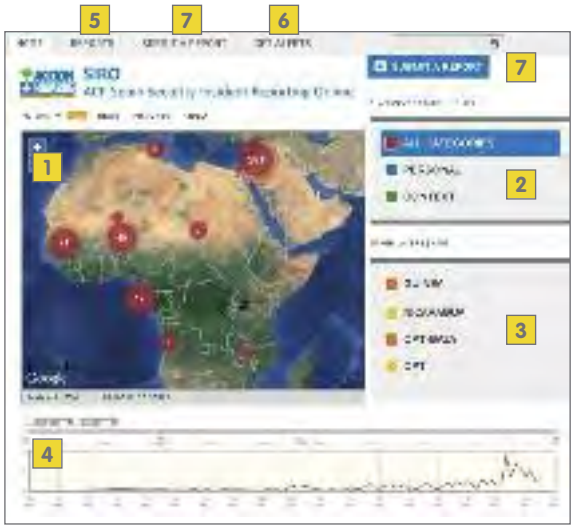
These systems were compared and evaluated. It was determined that an incident reporting system should improve reactivity to support incident victims (see Porcaro and Walker, pp. 33-36); be able to map not only where incidents occurred (see Sambuli and Awori, pp. 27-31); but also statistics from the database, security perimeters and levels, and evacuation routes and maintain a database of security-related information to help ACF-Spain improve its incident reporting system, refine the analysis of trends through the consolidation of information, and ease decision making for security management. In summary, an incident reporting and mapping system should allow registration, consolidation and graphical representation of security incident information. From a technical point of view, other factors were considered, such as cost, licence, bandwidth, access and permissions, authentication, mobile device support, compatibility with other systems, flexibility and adaptability of the tool, the possibility of mapping polygons, routes and areas, the possibility of getting reports and alerts, and the possibility of importing/exporting information from/to other software.

An illustration of the system would be:

The result of the analysis and comparison identified Ushahidi as the system that best suited our needs.

Applicability of Ushahidi in security risk management

Ushahidi,[115] 'testimony' in Swahili, is a web-based platform initially developed in collaboration with Kenyan citizen journalists to map violence in Kenya after the post-election fallout in 2008. We selected Ushahidi because it fulfilled the technical and functional criteria aforementioned. In particular, Ushahidi is an open source platform, so there is no cost related to the procurement of a licence; information is protected with authentication access; is easy to customise without a system administrator; documents, images, photographs and videos can be uploaded; locations where incidents have taken place are easy to identify and placemarks can be added; it can be used on mobile devices (both for sending reports and recording them in the database); it allows encrypted access to the incident register panel and the export/import of information to/from other software; and it offers the possibility to generate graphs from the information contained in the database (only by category in a certain period of time).



A quick look at Ushahidi for NGOs

The main page offers a quick view on a map [1] of the reported incidents. The map represents the total number of incidents or the incidents in a given period (the timeline can be adjusted). These incidents are represented on the map according to categories [2] defined by the system administrator and displayed in different colours or icons. Layers representing areas, locations, meeting points, routes, etc. can appear on the map if uploaded [3]. The layers have to be created first in KML format and can be easily uploaded to the platform. Each layer can be given a colour to represent levels of risk or other categorisation used by the organisation.

There is also a graph [4] that shows the evolution in the reporting of incidents over time. All the reports that have been introduced into the system can be seen [5], and there is also the possibility of viewing reports in a given time range, according to category, country or any other customisable field. It is possible to activate alerts [6] and be informed via e-mail of incidents reported in a particular location. This can also be customised by incident-type.

115 The original Ushahidi website was used to map incidents of violence and peace efforts throughout Kenya based on reports submitted via the web and mobile phones. Ushahidi has grown into a global non-profit technology company that aims to change the way information flows in the world and empower people to make an impact with open source technologies, cross-sector partnerships, and ground-breaking ventures. For further information see http://www.ushahidi.com/ [Accessed 1 September 2014].

The online template for reporting incidents [7] is also displayed on the main page. It has some compulsory fields and the exact location of each incident can be pinpointed on a map. The categories for the template are the same ones that are shown on the map [2]. The rest of the template can be customised according to the information that an organisation wants to collect.

The system can be public or password protected. It also has the possibility of administration settings for customising fields and options. The level of access for different users can be set up depending on the criteria determined by the platform administrator.

Reporting a security incident

The ACF-Spain incident report template in Word format was replicated in the Ushahidi incident report web site. This allowed for reports to be made in a more efficient way, as well as offering a single data entry that is transferred directly into a database for extraction and analysis. Who reports an incident is something that can be decided by the organisation, and can depend on internet access, the need for review before information is made public, etc. Once an incident is reported, it will automatically appear in the restricted area (depending on the user privileges and profile) which allows an authorised user or administrator to review the information reported before it is made public – a function available within the organisation and for registered users with a password. The information can be modified by an authorised user in order to ensure the report meets the standards set by the organisation. The incident reporting template has the capacity for private fields, for certain user profiles, as well as public fields. In this way, additional information can be added to the reports by the person reviewing and validating them. An example could be incident severity, which it may be important to harmonise across an organisation and not leave up to the criteria of the person reporting: the theft of a car can be rated as having a high impact in a country with low criminality rates and as low impact in a country with high criminality rates, depending on who reports the incident, but from an organisational security management point of view the impact may need to be rated equally.

The system can be set up so that once an incident is reported, an email is sent to the person in charge of reviewing the incidents, or the report can be automatically validated. Triggers for these different actions can be customised in terms of who submits the report, the location, keywords used, category of incident or when the incident was reported. As mentioned before, each report has to be verified and approved by an authorised user or administrator before the report appears in the public part of the platform. For ACF-Spain it is important to have this option in order to comply with the EU Data Protection Directive (95/46/CE), and to prevent misuse of the platform or the possibility that it might become a way of denigrating staff. If an incident report includes information considered as confidential or affecting the private sphere and image of a person, it can be corrected and the name replaced by a generic denomination.

Because of the sensitivity of the information contained in the Ushahidi platform database installed on the ACF-Spain servers, we decided to password-protect it and maintain it under an https protocol. The platform allows anyone with access to the site to report incidents. However, we decided, from the point of view of internal process, that only Country Directors, Logistics Coordinators or Security Managers could upload/report incidents through the system. The basis for this decision was that the organisation considered it important that security managers at country level were aware of incidents happening in the countries where they were working, and that they should not find out about incidents after Headquarters in Madrid did. Subsequent access to information once the report has been validated is open to the entire organisation.

ACF-Spain has internally classified security incidents into three categories: incidents resulting in direct harm to ACF-Spain (to be reported in all circumstances); incidents with no harm to ACF-Spain but with consequences for its security or operational management (near misses, recommended to report them); and incidents with no harm nor other consequences (interesting to report them). All these types of incidents can be reported through the platform. This is helping us identify trends, training needs, new risks, etc., but can also be used to evaluate the level of risk of new intervention areas or likelihood of incidents through the evidence collected. Real-time information extraction can establish how many incidents have been reported, their type, severity, the number of staff affected and their gender and profiles. This information allows security managers and country directors to compare security incidents between countries of operations.

For instance, traditionally in ACF-Spain most reported incidents have been traffic and criminality related. For the first time in 2014 this pattern has changed due to the work done in different emergencies (Philippines, Middle East) and we have witnessed an increase in threats and harassment towards ACF-Spain staff. The identification of this new trend has allowed us to raise awareness of this fact and to prepare the necessary training and briefing for our staff. Similarly, we noticed an increasing number of traffic related incidents with motorbikes in the Sahel. The identification of this trend allowed us to take different decisions (training of users, hiring of drivers, reinforcing staff awareness) in order to minimise vulnerability to this risk.

Since the introduction of the incident reporting system through the Ushahidi platform, we witnessed a steep increase of incidents being reported (from an average of around 34 incidents per year to around 80). Our initial analysis was that not so many more incidents were happening, but that facilitating the reporting meant more incidents are being reported as consequence. Part of the information provided through Ushahidi is done through drop down menus, check boxes or option buttons, making the reporting simpler and faster. In other words, the complexity of the process can no longer be used as an excuse for not reporting incidents.

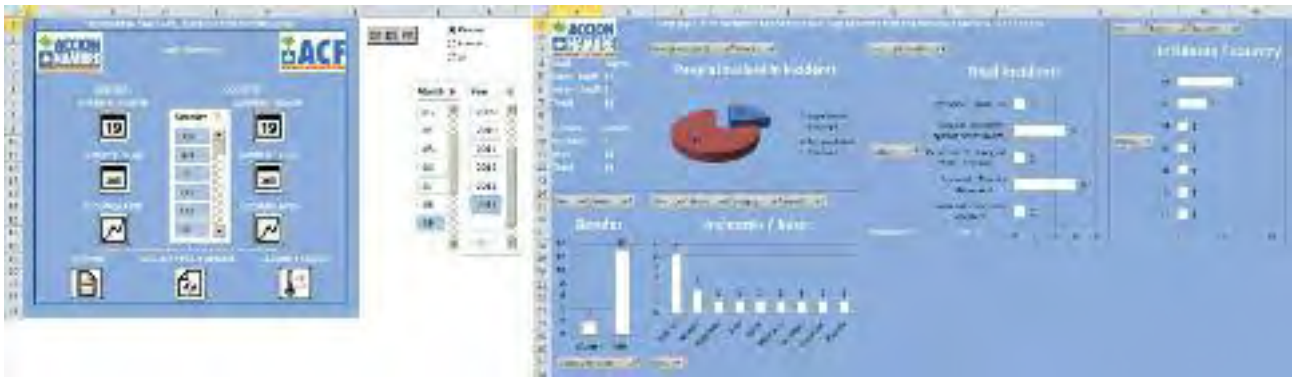
This analysis is being confirmed in 2014, where the number of incidents being reported at the time of writing (August 2014) is matching the figures for 2013, the year when the system started being used. However, facilitating reporting through the Ushahidi system was not the only stimulus for more incident reporting, since its use coincided with the creation of a full-time dedicated security manager at ACF-Spain. These figures will have to be confirmed in the coming years through more statistical evidence.

Nevertheless, we are still encountering delays in the reporting of incidents or resistance to the use of the reporting system. The delays in the reporting process are the same ones that were faced prior to installation of the Ushahidi system, most of them not related to the tool itself but to the internal understanding of what ACF-Spain considers incidents, what should be reported, etc. Access to the internet is becoming less of a problem, particularly in country capitals where the reporting is done according to the internal process explained above. Some of the delays in the reporting process may also come from lack of knowledge about the existence of the tool and insufficient appropriation of the tool by persons in charge of reporting (see Porcaro and Walker, pp. 33-34). Access to the platform has been facilitated by providing the URL in different locations of the organisation's intranet. Resistance to its use is not due to the tool itself, but to other factors (change management).

Ushahidi's interaction with other software: representing information

In ACF-Spain the previous reporting system of transferring information from a Word template to an offline Excel database, had been internally questioned because of the inefficiency of the process and the need to be more transparent and be able to share internally what was happening to our teams. Equally, an organisation needs to know how incidents are being managed in order to share lessons learned and practices.

Although as stated above it is possible to access reports according to type of report or location, the graphic and/or statistical representation of incidents has to be complemented with other software. At ACF-Spain we have used Excel 2010 to process the information from an XML file downloaded from



116

116 Information shown here does not necessarily reflect real information about incidents occurring to ACF-Spain.

Ushahidi (although CSV format downloading is also possible). Downloaded information can be drawn from approved reports, verified reports or reports awaiting verification or approval. A time range can also be set up. The information can be represented and managed in many different ways, and we are using it through a 'dashboard' file.

This dashboard is uploaded onto ACF-Spain's intranet so it can be used and consulted by organisation members when preparing briefings, risk analysis, reports, etc. The dashboard can show contextual incidents, direct incidents or both, but could be modified to show other information collected through Ushahidi's online template. At ACF-Spain it shows incidents per month, per year, accumulated at a global organisational level or per country. The file also shows the regularity of security protocol or the security level updates in all the locations where ACF-Spain works (although this information is not collected through Ushahidi).

Conclusions

Since ACF-Spain adopted Ushahidi as platform for incident reporting, we have seen an increase in the number of incidents reported as well as a decrease in the time between the occurrence of an incident and the moment it is reported. This has allowed us to support the victims of incidents better and to react in a timely manner to challenges encountered. There have been cases of incidents being reported through Ushahidi within hours of their occurrence. However, ACF-Spain recommends field teams to use the quickest way possible (telephone in most cases) if a severe incident occurs, in order to be able to provide support to the victims as fast as possible, and later on to provide more detailed information through the online reporting template. In a number of cases, having incidents being reported within hours of their occurrence has allowed us to provide prompt psychological assistance to staff members affected by incidents, as well as the activation of other contingency protocols.

The alert system that the administrator can activate to get a notification when a report has been submitted for validation (which can also be set up so all users receive an alert when a report has been validated) has improved the speed with which information is shared among all staff, from senior management to field teams through HQ support personnel. As a platform it has shown great stability and reliability, and we are currently using only a limited part of its functions and potential, bearing in mind that the platform is being constantly developed through the open source model. The Ushahidi platform can be downloaded directly from its web page. While the creation of templates and statistics does not require advanced computer skills, it does needs the engagement of IT staff for its installation on a server so that it can be used online.

There has been a great improvement in having real time information and in the efficiency of the reporting process. Ushahidi has enough flexibility to accommodate the incident reporting criteria of different organisations as well as the potential to be used for other purposes.[117] Through the use of the system it has been possible to identify potentially dangerous locations, conduct more accurate risk analysis and introduce more appropriate risk mitigation measures, all in a timely manner. However, Ushahidi is only a tool, and should be accompanied by training, awareness, promotion and communication of its added value. As such, ACF-Spain has been conducting briefings, trainings, field visits, communications and reports at internal level to promote the use of Ushahidi for reporting incidents and sharing information.

117 See, for example, http://harassmap.org/en/what-we-do/the-map. [Accessed 1 September 2014].

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 66 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Editors

Raquel Vazquez Llorente and Imogen Wall.

The editors welcome comments and further submissions for future publications or the web-based project. If you are interested in contributing, please email eisf-research@eisf.eu. Imogen Wall can be contacted at imogenwall@hotmail.com.

Acknowledgments

The editors would like to thank Lisa Reilly, EISF Coordinator, for her input and advice, and especially for her comments on the initial drafts. We would also like to extend our gratitude to Tess Dury, for her research support at the initial stages of the project, Brian Shorten for sharing his expertise with us, and Crofton Black for his early guidance and, as always, his continuous support.

Suggested citation

Vazquez Llorente R. and Wall, I. (eds.) (2014) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management*. European Interagency Security Forum (EISF).

Cover photo: Mary Kiperus, community health worker, uses a mobile phone for reporting to the local nurse. Leparua village, Isiolo County, Kenya. February, 2014. © Christian Aid/Elizabeth Dalziel.

Disclaimer

Other EISF Publications

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

Briefing Papers

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Reports

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez, R. (Sp. and Fr.) – EISF Secretariat

Managing The Message: Communication and Media Management in a Crisis
September 2013
Davidson, S., and French, E., EISF Secretariat (eds.)

Family First: Liaison and Support During a Crisis
February 2013 *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L. – EISF Secretariat

Forthcoming publications

Office Opening Guide