The four dimensions of security incident information management

The Learning Needs Assessment (LNA) identified four distinct phases in security incident information management:

Dimension 1: To inform immediate reaction and response to a security incident

Purpose: Information is sought and used by decision makers and the affected staff to inform the immediate response to the incident.

Coverage: The information has to help to identify what support is required for the affected staff and whether the organisation needs to implement any immediate changes in its operations such as restriction of movement or temporary suspension of operations. There is a direct link between the required information and the response options that can be considered.

Reporting: Organisations need an effective information flow that ensures that all relevant staff at HQ, regional and country officer are provided the necessary information and that the information triggers response mechanisms.

Sharing: Information about the incident may be shared with other organisations working within the same country to allow them to take the potential precautionary measures to prevent the incident from reoccurring.

Tools: a) matrix on connection between information and response. b) Guidance on emergency communication

Dimension 2: To implement lessons learned after a security incident for follow-up action

Purpose: The incident post mortem is carried out after the emergency is over. It is conducted among staff directly affected by or involved in the responses and the organizational decisions that may have contributed to influencing how the incident occurred. The main objective is to understand what happened with a view to planning and implement any necessary changes and procedures that will help to prevent, reduce the risk or lessen the impact of similar events.

Coverage: This phase requires qualitative information used for a frank assessment of contributing factors that increased vulnerability and influenced the specific reactions that occurred as the event unfolded. The information gathering process is conducted in the an atmosphere of confidentiality and trust in staff.

Reporting: Reporting focus on the key findings and lessons learned to ensure that others not closely involved, in particular at HQ and regional offices, understand the incidents and how processes could be improved. Reporting should be done in a way that it constructively informs security management frameworks and the programs, and the review of SOPs and strategies (see level 3).

Sharing: Organisations may choose to share the final analysis of conclusions of how to better manage particular situations with other agencies if they wish to do so.

Tools: a)Interview guidance that helps in the conduct of qualitative interviews to uncover the origin and contributing factors of the incident. b) Good reporting formats that assist strategic decision-making.

Funded by
European Union
Humanitarian Aid

Dimension 3: To inform strategic decision-making in the organization

Purpose: Regular analysis at HQ level is carried out to identify trends and patterns to inform strategic long-term decision-making for the entire organisation. The purpose is to take stock of the changing nature of incidents, to understand the most challenging working environments and the organisation’s overall exposure and to identify the best strategic responses. The information is used to consider implications for good management which can include, where to operate, how to communicate, what insurances to include, to what extent security management has to be budgeted within country operations among other things. Some organisations carry out such analysis on an annual basis, others more frequently. While others do not regularly discuss their security incident profile.

Reporting: This analysis is made possible based on effective information flow between field offices and headquarters. The available data is analyzed and the analytical conclusions are reported to senior management and possible programme managers. Reporting of incidents should not be limited to the dramatic incidents but the full range of incidents including the near misses. It is assisted by an effective incident information management system that classifies events and provides trend overviews based on quantitative information. Organistions have different mechanisms in place to report, collect and record country level incidents in a central place. Some use email correspondence, others used excel spreadsheets. Some have custom made online reporting systems others subscribe to the services of not for profit or commercial providers for such systems. The analytical conclusions derived from the global overview of all incidents combined with the qualitative insight gained under Level 2 of information management are reported in an accessible and actionable way to senior management and other relevant colleagues such as from the HR department, the legal department and programme managers.

Sharing: Agencies might find it useful to compare their incident trends against that of similar organisations (benchmarking). Such an approach requires sharing of key trend data between agencies in an anoymised format that no longer allows identification of a single agency through for example the Aid in Danger – Security in Numbers Database.

Tools: a) Guidance on understanding the available internal incident reporting systems, b)Guidance on standardization and categorization, c)guidance and on effective analysis, d)guidance on effective communication of trends

Dimension 4: To understand the NGO humanitarian security context

Purpose: The aim of this analysis to better understand the overall and unique NGO humanitarian security context to inform strategic decisions, global communication and self-reflection among agencies. INGOs and LNGOs may experience unique security challenges due to the environment they work in and the way they deliver their services. Analysis of the patterns of incidents reported by INGOs and LNGOs are the most effective source of information of the specific security context. The analytical conclusions derived from the global overview of humanitarian security incidents can be used by organisations to bench-mark their own trends (see level 3) and to inform strategies and communication within organistions and the humanitarian NGO sector as a whole. It can be a useful tool to inform the media and to influence public opinion and government donors.

Coverage: This analysis is based on the security incidents experienced by humanitarian agencies only (rather than the general security context) and includes the full range of incidents from as many organistions as possible. This analysis is made possible based on pooling of confidential agency data and the analytical conclusions that can be drawn from it. Reporting of incidents should not be limited to the dramatic incidents but the full range of incidents including the near misses. It is made possible by effective internal incident information management systems and the willingness of organistions to share this information. It requires standard classifications to be used to make the information comparable between organisations which can be provided by the Aid in Danger – Security in Numbers Base Project.

Reporting: Requires effective information flow from the contributing agencies to the data pooling facility and effective communication of trend analysis to key decision-makers and opinion-makers.

Sharing: Data pooling for insight into the unique humanitarian security incident patterns requires that agencies are willing to share their aggregate security incident data based on confidentiality aggreements.

Tools: a) Guidance on good formats in which to submit incident data into the pooling format. b) Guidance on communication of analytical results.

Funded by
European Union
Humanitarian Aid