Plan Benin

This case study examines how Plan Benin used FrontlineSMS for violence reporting, the associated data protection and security vulnerabilities, threats, risks and actions taken to reduce risks.

Project Description	Plan Benin used FrontlineSMS to track violence against children in Benin, West Africa.
Vulnerabilities	• Confidential information accessible by several third parties and internal staff • Data collection structure
Threats	• Internal staff who are not trained properly • Caseworkers and government staff • False information provided
Risks	• Unauthorized access to sensitive information • Additional violence and harm to the reporter and/or victim • Confidential information is posted publicly on the internet
Risk Reduction	• Security built into the design of the program

FrontlineSMS and Plan Benin

Plan Benin aims to strengthen the local and national reporting of trafficking and violence against children in Benin, West Africa and to lower the barriers to reporting these incidents for children and community workers. This project allowed children and the general public to send reports of violence against children via SMS. The information gathered was used to further understanding of the frequency, types and reasons for the violence that occurred.

Plan Benin used FrontlineSMS to facilitate and manage the reports received via SMS. FrontlineSMS was used to create a report when a child or community worker reported an act of violence. The SMS received by the program typically included the location and the name of the victim. The report was provided to the state child care staff or partnering government agency in order for them to respond to the incident in compliance with national protocol. The government child protection services investigated the incident and Plan Benin staff followed up to confirm that the casework was been established. Plan Benin also used Ushahidi to map the locations where violence has occurred.

Data Integrity Concerns

Confidentiality of the victim's information, including their location, was a priority for Plan Benin because privacy breaches at the community level could have had serious implications. Sensitive information had to be shared with a number of parties, meaning that the information was at risk of being leaked while in the possession of the state child care staff or the government agency dealing with the case. Those involved could have also been the perpetrators of the acts of violence, or could have played an active role in the violence. If an attacker discovered that a report was created on their behalf, the reporter and / or the victim could be at risk.

Additionally, the vulnerability of reporters was a concern for Plan because identification information must be provided to the mobile network operator in some of the countries in which the program operated, meaning that reporters were vulnerable to their personal information and SMS messages being discovered by perpetrators and others. Third parties who did not support the program could have bribed an employee of the network operator to obtain this information.

Leakage of Information by internal Plan Benin staff, even those who posted information on the Internet, was also a concern. Confidential information may have been posted intentionally or unintentionally due to the high turnover of staff and the challenges of providing consistent training. Plan Benin recognized that the probability of someone who lived locally finding and acting on this information was very low, but noted that it remained a concern.

The security of physical documents which contain sensitive information was a concern for Plan Benin, because they could be lost or stolen if left unattended by members of staff.

Plan Benin were also concerned about the accuracy and validity of the reports received. The project allowed the general public to provide reports. A lengthy follow-up process was carried out for each verified case; therefore, false information would result in a loss of time and resources.

Actions to Protect Data

Plan Benin's understanding of the sensitivity of violence helped them to reduce the risk of sensitive information being viewed or accessed by an unauthorized user or a third party. Plan worked to ensure that the reporting program did not expose reporters or victims of violence to additional risk, by having many discussions with local stakeholders to discuss how information flows. For example, the project considered providing phones to one person per village, but realized that this approach would give one person too much access to the cumulative reports. Therefore, the program requires reporters to use their own phones.

Plan Benin worked with local youth to understand and be able to address the potential risks of reporting. Groups of youth were also trained and provided with mobile phones and credit to collect media for the project.

To reduce the risk of false information being received or used by the program, Plan Benin has a defined process to scrub, categorize and authorize reports.

Conclusion

Plan Benin received and shared highly sensitive information. Due to the nature of the project, security was built into its design. This approach was effective in reducing the risks of additional violence to the reporters and the victims of violence.