

# **Privacy and Secure Communication to Human Rights NGOs and Journalists in Peru:**

## *Project Overview*

### Goals

As information and communications technologies (ICTs) proliferate, communications and information are increasingly vulnerable to privacy and security threats. Non-governmental organizations in environments at risk, such as those engaging in human rights work (“HRNGOs”) are particularly at risk for various reasons:

- \* They collect and use often highly-sensitive information
- \* They are often positioned against governments and other powerful interests, many of whom have no qualms against employing invasive, destructive and even deadly force on those that oppose them
- \* They are heavy users of Internet communications
- \* They often are unaware of the potential dangers and insecurities
- \* They rarely have the finances and resources at their disposal to develop and deploy information security procedures.

With this in mind, Privaterra intended to research a methodology to bring privacy and security measures to HR NGOs. While we have conducted training workshops in the past, we wished to use this project to study the training methodology and see how it could become more effective.

Frequently, organizations would attend the training workshops but discontinue using the tools and habits after a brief while. We wanted to better understand why this happened and consider how to improve the methodology or reconsider the use of training workshops altogether.

The ultimate goal of Privaterra is to help secure HR NGOs in their usage of information and information technology.

### Stages

The research and training project relating to this report had three distinctive stages.

First, Privaterra developed a series of materials to use in training HR NGOs about privacy and security, focusing on digital communications and information collection and usage. These materials were revised after the second stage of the project, based on input from HR NGO personnel and our own observations.

Second, Privaterra ran a series of workshops and follow-ups training sessions related to data privacy and information security with HR NGOs located in Lima, Peru.

Third, Privaterra developed and launched a Web site designed to:

- \* Help HR NGOs and other interested parties understand the importance of privacy and security,
- \* Allow them to access Privaterra materials in a collaborative fashion, and
- \* Provide a venue for HR NGOs to communicate with Privaterra and with each other about issues relating to privacy and security

The Web site can be reached at <http://www.privaterra.org>

#### Workshop Overview

After introducing ourselves and our work, we explain basic data handling practices, the risks associated with using numerous different types of Information and Communications technologies and the tools and procedures which can be put in place. Calling on real-life occurrences, we demonstrate how common breaches of privacy and security can lead to serious problems if these are not addressed.

We explain the four major types of insecurities:

1. Environmental dangers, such as papers being destroyed through fire or rot.
2. Attacks that are unrelated to the work of the HR NGO, such as theft of computers by common thieves or viruses that go around the Internet.
3. Attacks that are directed at the work of the HR NGO, such as theft or destruction of computers by government operatives, or surveillance through bugging devices or hacking.
4. User error, such as forgetting to backup data, using a passphrase that is easy to guess, or encrypting only an attachment while leaving sensitive information in an unencrypted email message.

Then we introduce policy procedures and tools that can be used to minimize exposure to these insecurities. We help the organizations to install, configure and use these tools, ensuring that, whenever possible, the individual members of the HR NGO is actively using the tools instead of simply watching us do so. The members are encouraged to experiment with the tools.

Throughout the training procedure, emphasis is placed on the importance of developing a privacy consciousness. Using tools is much more effective when the user understands why the tool should be used, and what it can and cannot do.

After the workshop, we send follow-up emails to test the trainees. A few days later we return for a follow-up visit to further ensure the training was successful.

As well, we introduced designated local trainers who were charged with continuing follow-up activities. The HR NGOs were encouraged to develop on-going relationships with these local trainers to ensure their systems and offices remained relatively secure.