CASE EXAMPLE:

The organization “Terra Forte” started a new campaign against the predatory actions of a foreign mining company within its territory. Campaign activities began to have repercussions and the institution realized that its team might be under surveillance. To protect the integrity of its information and the security of the organization’s members, it took the following measures:

**1) Classification:**

Initially, a small communications team came together to map the organization’s information, looking at all the files the organization produces and where they are.

Example:

|  |  |
| --- | --- |
| **List of documents and information**  | **Where they are** |
| Financial documents  | Administrative computer  |
| Publications | Website and communications files |
| Political strategy messages  | WhatsApp chat  |
| Personal data of the team | Google Drive and personal Facebook profiles |
| Plane tickets  | Employee e-mails |
| Photos of public activities  | Facebook page |

After locating this information, they begin to classify each document’s sensitivity according to the information within it, specifically separating those that included information that may be strategic for their adversaries and sensitive in terms of the team’s protection. To this end, they undertook an analysis of the activism context within which they operate, since data sensitivity may change, depending on political events.

|  |  |  |
| --- | --- | --- |
| **List of documents and information** | **Where they are** | **Sensitivity**  |
| Financial documents  | Administrative computer  | High |
| Publications | Website and communications files | Medium |
| Political strategy messages  | WhatsApp chat  | High |
| Personal data of the team | Google Drive and personal Facebook profiles | High |
| Plane tickets  | Worker e-mails | Low |
| Photos of public activities  | Facebook page | Low |

**2) Reduction:**

Following this stage, the organization began to mark information that may be deleted or hidden.

|  |  |  |  |
| --- | --- | --- | --- |
| **List of documents and information** | **Where they are** | **Sensitivity**  | **Reduction** |
| Financial documents  | Administrative computer  | High | Maintain the document  |
| Publications | Website and communications files | Medium | Maintain the document |
| Political strategy messages  | WhatsApp chat  | High | Record necessary information and delete conversation |
| Personal data of the team | Google Drive and personal Facebook profiles | High | Hide public information  |
| Plane tickets  | Worker e-mails | Low | Delete old e-mails  |
| Photos of public activities  | Facebook page | Low | Delete photos that expose people |

**3) Fortification**

Following initial recognition of the information, classification and reduction, the organization began to plan how to fortify the security of sensitive data and to improve protection of its information and team.

To this end, it undertook an analysis of security tools and strategy options through an implementation plan. This plan took account of such things as passwords, encryption, VPN, security plans for trips and events, and social network privacy settings.

Example:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **List of documents and information** | **Where they are** | **Sensitivity**  | **Reduction** | **Fortification** |
| Financial documents  | Administrative computer  | High | Maintain the document  | More secure administrative password and installing antivirus software on the computer |
| Publications | Website and communications files | Medium | Maintain the document | Website security configurations, back-up of digital files |
| Political strategy messages  | WhatsApp chat  | High | Record necessary information and delete conversation | Use encrypted chat for sensitive communications (Signal) |
| Personal data of the team | Google Drive and personal Facebook profiles | High | Hide public information  | Pass sensitive data to a secure cloud such as Netcloud. Configure social network privacy settings. |
| Plane tickets  | Worker e-mails | Low | Delete old e-mails  | Prepare a security plan for trips |
| Photos of public activities  | Facebook page | Low | Delete photos which expose people | Configure privacy settings for the Facebook profiles of page administrators |

**4) Create trusted networks:**

In preparing the plan, the organization realized that many things would require third-party help, either for technical implementation or to defend the current campaign. They also understood that they could collaborate with others, sharing the experience of the plan and their precautions.

To this end, they began to list allies in a number of areas:

* Information technology
* Advocacy
* Media
* Research institutes
* Social work
* Psychological support
* Etc.

With this information, they began to plan targeted communication about how different contacts could create networks to become stronger and to care for one and other, together.