

# M

## anaging organisational shift towards an improved security policy

### Purpose:

To learn how to manage organisational shift towards an improved security policy.

Steps and issues around which the process will be built:

- improving management of the security strategy
- improving the security management implementation process
- what is the entry point? What body is responsible for it? What is the starting point? How to proceed? What about the implementation? What are the pros and cons? What are the obstacles?

### Handling security challenges: step by step security management

Security management never ends and is always pragmatic, partial and selective. This is because:

- ♦ There are limits to the amount of information you can deal with - not all factors affecting security can be grouped and treated simultaneously;
- ♦ It is a complex process - time and effort are necessary to create awareness, develop consensus, train people, deal with staff turnover, implement activities, etc.

Security management can rarely attempt a comprehensive, long-term overview. Its contribution lies in the ability to prevent attacks and highlight the need for organisational strategies to cope with these. This may not seem very ambitious, but we must not forget that often too few resources are allocated for security!

When reviewing a defender's or an organisation's security practices, you may find that some sort of guidelines, plans, measures or patterns of behaviour are already in place. Conflicting forces will be involved, ranging from stereotypical ideas about security practices to a reluctance to increase existing workloads by incorporating new security activities.

Security practice is typically a fragmented and intuitive work in progress. Security management should aim to make step-by-step changes to improve performance. Security rules and procedures tend to emerge from the parts of an organisation covering specific areas of work, such as logistics, a field team especially concerned with its security, or a manager under pressure by donor concerns about security, etc.

Step-by-step security management opens the door to informal processes and allows space for new practices to take root. Sudden events, such as security incidents, will prompt urgent, short-term decisions that, if properly managed, will shape longer-term security practices for the whole organisation.

**Security strategy improvement: possible entry points.**

Once the need for improving security has been established, it needs to be promoted. There are several entry points for it (either in or outside the organisation):

**Inside the organisation:**

- management, board of directors or leaders
- intermediate/ executive level
- staff, rank and file
- a combination of all above possibilities.

**Outside the organisation:**

- donors
- partners, counterparts
- similar organisations working in the same network.

**Let’s compare their advantages and disadvantages.**

| POSSIBLE ENTRY POINTS TO PROMOTE THE NECESSITY OF CHANGES? | ADVANTAGES   | DISADVANTAGES   | POSSIBLE SOLUTIONS  |
|--|--|---|---|
| <b>ENTRY POINTS INSIDE THE ORGANISATION</b>                |  |   |   |
| MANAGEMENT, BOARD OF DIRECTORS OR LEADERS                  | <ul style="list-style-type: none"> <li>• Can call meetings or general assemblies</li> <li>• Have historical memory</li> <li>• Moral authority</li> <li>• Institutional support</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Perceived as ‘imposing security’ and generate disinterest- make it too formal, rigid, distant be patronising</li> <li>• See security as an issue affecting them only</li> <li>• Dismiss it as not a priority</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Meetings or general assemblies</li> <li>• ...</li> </ul> |

|   |  |   |   |
|---|--|---|---|
| INTERMEDIATE/ EXECUTIVE LEVEL   | <ul style="list-style-type: none"> <li>• A view on the upper and lower levels</li> <li>• Easy access to both other levels</li> <li>• Convivial communication channel between both levels.</li> <li>• Communication</li> <li>• Technical capacities to implement security changes</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Often this level does not exist</li> <li>• Partial focus: on one side or area only</li> <li>• Distracted by personal career interests</li> <li>• “Too” technical if not involved in political and field activities</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Involvement procedures (both towards directors and towards members in general)</li> <li>• ...</li> </ul>   |
| STAFF, RANK AND FILE <ul style="list-style-type: none"> <li>• ...</li> </ul>          | <ul style="list-style-type: none"> <li>• Can mobilise people</li> <li>• Aware of the mechanisms and details of everyday work</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Might have problems with managers or with hierarchy</li> <li>• ...</li> </ul>  | <ul style="list-style-type: none"> <li>• In general, with the group as a whole, acknowledge the problem, the need for everyone’s input and the need for solutions. Then, delegate solution-finding to a working group</li> <li>• ...</li> </ul>   |
| <b>ENTRY POINTS FROM OUTSIDE THE ORGANISATION</b>                                     |  |   |   |
| DONORS, PARENT ORGANISATIONS, <ul style="list-style-type: none"> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• More distance</li> <li>• No direct interests.</li> <li>• May have more comprehensive experience</li> <li>• Could call meetings with any and all the above levels without conflicts of interest.</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• May have credibility problems or little knowledge of the work that is being done.</li> <li>• Approach might be “too” technical and technical approach</li> <li>• ...</li> </ul>  | <ul style="list-style-type: none"> <li>• Point out common interest in security</li> <li>• Donor organisation prefers to invest in an organisation taking care of security rather than risking losing its investment in an organisation that disregards security</li> <li>• Inter-organisational security depends on common security attitudes and rules</li> <li>• ...</li> </ul> |

The entrance process can be implemented by all organisations, regardless of their size, stability, location.

### **Which is the body responsible for the improvement process?**

Now that that entry has been gained (the need has been promoted and acknowledged), some part of the organisation has to lead the process. Which body will be made responsible for the security improvement process? There are several possibilities:

- ❑ Ad hoc members of the organisation (they are part of the organisation and are chosen by it (usually they also have other responsibilities). It can also be a working group (made of people from various areas of work)
- ❑ An outside-inside person: a person partially involved in the work and who interacts closely and continuously with the people from the organisation (for example, a person who used to work for the organisation).
- ❑ A consultant or adviser: interacts with the ad hoc security person or with the working group (a short-term interaction).

**Let us examine the advantages and disadvantages of these different approaches.**

| <b>BODY RESPONSIBLE FOR THE IMPROVEMENT PROCESS</b> | <b>ADVANTAGES</b>   | <b>DISADVANTAGES</b>   | <b>POSSIBLE SOLUTIONS</b>  |
|---|---|--|--|
| AD HOC PERSON FROM THE INSTITUTION                  | <ul style="list-style-type: none"> <li>• Centralised information</li> <li>• Easy access to information</li> <li>• Clarity in terms of responsibility</li> <li>• Easy decision-making - fewer people involved</li> <li>• Chosen for their skills</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Work overload - weakened collective commitment</li> <li>• Excessive dependence on one person</li> <li>• Possible lack of feedback on plans and ideas.</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Distinction between promotion/coordination and implementation</li> <li>• Temporary workload reduction to enable the focus on security.</li> <li>• Support personnel</li> <li>• Constant circulation of strategies so as to ensure progressive feedback</li> <li>• ...</li> </ul>  |
| WORKING GROUP                                       | <ul style="list-style-type: none"> <li>• Sharing and comprehensive approach of the work on security</li> <li>• Extensive and diverse experience-</li> <li>• More human resources</li> <li>• Distribution of responsibilities: more clarity for initiative and activity.</li> <li>• higher probability for protocols to be followed.</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Work overload</li> <li>• Slow consensus building when taking decisions</li> <li>• Circulation of information less fluid -higher number of persons to be trained for the task.</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Adequate distribution of skills and duties</li> <li>• Involvement of the management level</li> <li>• Rotation, training and commitment to proactive progressive circulation of output in construction in order to get feedback and share the process.</li> <li>• ...</li> </ul>   |
| AN OUTSIDE-INSIDE PERSON                            | <ul style="list-style-type: none"> <li>• Larger objectivity in risk analysis</li> <li>• Skilled person, trusted by the organisation</li> <li>• Full commitment</li> <li>• Proven receptivity -awareness of strengths and weaknesses</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Discontinuity</li> <li>• May weaken the group commitment</li> <li>• May undermine the due ownership of the whole process and topic.</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Train 1 or 2 team members</li> <li>• Continuous circulation of output in progress and feedback from the whole team</li> <li>• Consensus building and agreements</li> <li>• ...</li> </ul>   |
| CONSULTANT OR ADVISOR                               | <ul style="list-style-type: none"> <li>• Can train the team</li> <li>• Specialised consultancy</li> <li>• Clarity in monitoring the process</li> <li>• Recognised advice</li> <li>• Active follow-up process</li> <li>• Less affected by internal organisational issues</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Can generate dependency instead of skills</li> <li>• Can be seen as “someone there to do the work” instead of “someone there to ease the work”</li> <li>• May undermine the due trust within the organisation</li> <li>• Increased costs</li> <li>• Consultants in this field are rare</li> <li>• Difficulties in organising the work schedule</li> <li>• Might have insufficient knowledge of the context</li> <li>• Might produce a plan and rules inappropriate for the work context</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Clarify as much as possible with everybody: explain the consultant’s role, scope.</li> <li>• Raise the importance of security with other agencies in order to tackle and share the issue</li> <li>• Hold security training of trainers in organisations and institutions (facilitators)</li> <li>• Briefing on work context</li> <li>• ...</li> </ul> |

## What is the starting point of the process?

Now that entry has been gained and the responsible body has been appointed, where can the latter start from?

The starting point ought to be the evaluation of the whole-organisation security policy implementation process. Starting from the evaluation (or diagnostics) will determine the priorities and the possible solutions (best practices according to the stated needs, organisation profile and mandate). A plan will then be drawn up aiming to structure the improvement process. The plan will include intermediate goals in order to monitor whether and how progress is achieved. In addition, the plan will clarify the role and responsibilities both of the person/people in charge of the process and of the organisation members. The plan will also include a schedule. At the end of the planned process, an evaluation of achievements will take place.

Diagnostics ⇨ priorities ⇨ possible solutions  
⇨ improvement plan ⇨ evaluation

Once priorities are determined, the decision about their order of implementation might be easier if criteria are set: emergency, current available resources, etc

Flexibility is an essential factor throughout the process. However, what is the minimum needed in order for the improvement process to have a genuine opportunity to achieve positive results? Answering this question before the process starts is crucial.

## Diagnostics and improvement plan.

The diagnostics can be carried out using can use the “risk assessment” and the “security wheel” tools, described in previous chapters of this manual (any organisational review methodology can also be useful for this).

It is well known that this step should involve all concerned people and work teams within the organisation.

The improvement plan has to be **realistic** and **appropriate** to the profile and needs of the organisation. Here is a possible sequence of steps:

- 1 ♦ Identify the organisation’s expectations and expected outcomes of the security improvement plan.
- 2 ♦ Diagnose together, reach a consensus and share ideas about the current structure of security management (application of the “risk analysis” and “security wheel”): Indicate the progress, shortages and needs.
- 3 ♦ Indicate and discuss the best practices to be implemented in tackling the shortages and needs revealed.
- 4 ♦ Indicate the desirable and desired objectives of the improvement plan.

- 5 ♦ Outline the activities required to reach those objectives and what can reasonably be expected for each activity (this will enable progress towards the objectives)
- 6 ♦ Outline the necessary resources (financial, human, time, technical resources). Define the responsibilities and work schedule.
- 7 ♦ Define what risks arise from achieving these objectives and outcomes.
- 8 ♦ Define indicators for monitoring progress and final results.
- 9 ♦ Share the plan with all the involved parties in order to get feedback, to improve it and to generate the approval necessary for its implementation.
- 10 ♦ Implement the plan and decide on time frames for progress monitoring and for possible changes to the process.

### **The process: Implementing the improvement plan.**

The process includes a series of meetings and interviews with people or teams working within the organisation or in contact with it (in this case, there must be previous agreement from the organisation, indicating the specific people and/or organisations with whom security can be discussed). The exchange can start with a general introductory meeting, which may be followed by more meetings. These meetings provide the space in which to define diagnostics and discuss the implementation of the improvement plan. Moreover, the meetings can deal with specific items or they can accompany the specific work of the organisation from a security and protection standpoint.

### **Resistance to the improvement plan.**

Now that entry has been gained, a responsible body been appointed and the starting point and process plans been decided on, what resistance might there be from individuals?

As all the processes leading to changes in an organisation, the improvement plan may meet with resistance. However, it will also find approval and support. The point is therefore to see how to harness that support and argue the case against possible resistance.

The most appropriate way to undermine resistance is to genuinely listen to it and try to understand its underlying reasoning. Here again participation, active listening of all view points and expectations are fundamental to a good process.

It is essential that the improvement plan provides for ways to tackle possible resistance so as to avoid later improvisation and run the risk of the plan failing simply because of the earlier denial of possible resistance.

In this chart are some common resistance stereotypes, the reasoning behind those stereotypes and possible responses to overcome those resistance forces.

| COMMON RESISTANCE STEREOTYPES   | REASONING BEHIND THE STEREOTYPES  | RESPONSES TO OVERCOME RESISTANCE   |
|---|---|--|
| “We’re not being threatened” or “our work is not as ex-posed or contentious as other organisations’ work”.                                    | <ul style="list-style-type: none"> <li>The risk stays the same, it doesn’t change or depend on the fact that the work context might deteriorate or that the scenario might change.</li> </ul>   | <ul style="list-style-type: none"> <li>Risk depends on the political context, and the political context is dynamic: so is the risk.</li> </ul>   |
| “The risk is inherent in our work as defenders” and “we are already aware of what we are exposed to”.   | <ul style="list-style-type: none"> <li>The defenders accept the risk and it does not affect them in their work. Or, the risk cannot be reduced, the risk is there and that’s all there is to it.</li> </ul>                                       | <ul style="list-style-type: none"> <li>Meeting with inherent risk does not mean accepting the risk.</li> <li>The risk has at least a psychological impact on our work: it induces at the very least stress which affects the work.</li> <li>Risk is made of objective elements: threats, vulnerabilities and capacities: vulnerabilities and capacities belong to the defenders and are the variables on which defenders can work. By reducing vulnerabilities and increasing capacities, the risk can be reduced. It might not be eliminated altogether which does not mean that it cannot be reduced as much as possible.</li> </ul> |
| “We already know how to handle the risk”, or “we know how to look after ourselves” and “we have a lot of experience”                          | <ul style="list-style-type: none"> <li>The current security management cannot be improved and it is therefore not worth doing it.</li> <li>The fact that we have not suffered harm in the past guarantees that we won’t in the future.</li> </ul> | <ul style="list-style-type: none"> <li>Security management is based on objective elements that can be worked on.</li> <li>Look around and see how many defenders have suffered harm although they were highly experienced.</li> </ul>  |
| “Yes, the issue is interesting, but there are also other priorities.”   | <ul style="list-style-type: none"> <li>There are more important issues than security of defenders.</li> </ul>   | <ul style="list-style-type: none"> <li>Life is the priority. If we lose it, we will not be able to deal with all the other priorities.</li> </ul>  |
| “And how are we going to pay for it?”   | <ul style="list-style-type: none"> <li>Security is expensive and they cannot be included in fundraising proposals.</li> </ul>   | <ul style="list-style-type: none"> <li>How much do you think security costs? Quite a few security factors are behavioural and do not cost a penny.</li> <li>Investors will prefer to invest in an organisation covering security issues instead of running the risk of losing their investment.</li> </ul>   |
| “If we pay so much attention to security we won’t be able to do what is really important which is working with people and we owe it to them.” | <ul style="list-style-type: none"> <li>The fact that we are affected by security problems does not affect the people we work with. The quality of our work for people does not depend on whether we feel more secure.</li> </ul>                  | <ul style="list-style-type: none"> <li>Security is a matter of life or death.</li> <li>Because we owe it to people, we cannot run the risk of losing our lives.</li> <li>People run risks by entrusting us with their cases and if we do not work on our security it will affect them too; they might choose to use another organisation that has adequately planned its security and is thus also giving more security to other people.</li> </ul>  |
| “We don’t have time as we are already overloaded.”  | <ul style="list-style-type: none"> <li>It is impossible to find time in the work schedule.</li> </ul>   | <ul style="list-style-type: none"> <li>How much time do you think security takes?</li> <li>How much time do we spend reacting to emergencies instead of prevention? (most probably far more than the time required to plan security into our work)</li> </ul>  |

|   |   |   |
|---|---|---|
| <p>“The community is behind us: who would ever dare hurt us?”</p>                 | <ul style="list-style-type: none"> <li>• We are part of the community. The community is not fragmented, does not change both in members and opinions.</li> <li>• The community cannot be influenced.</li> </ul> | <ul style="list-style-type: none"> <li>• The community is not homogenous and is also made up of those who might be affected by our work.</li> </ul>   |
| <p>“In our village, authorities have shown understanding and collaboration. “</p> | <ul style="list-style-type: none"> <li>• Local authorities are not affected by our HR work and will not change their minds.</li> <li>• There is no hierarchy between national and local authorities.</li> </ul> | <ul style="list-style-type: none"> <li>• Organisational historical memory will have examples of local authorities opposing HR work when their tolerance limits have been exceeded.</li> <li>• Local authorities have to implement orders from above. Authorities are made of people who might have an interest in protecting aggressors.</li> <li>• Political contexts change.</li> </ul> |

Now that entry has been gained, the responsible body has been appointed and has defined both the starting point and the process plans, and that individual resistance has been dismantled, what organisational factors might hinder or facilitate the change?

**Organisational factors that can either hinder or facilitate the organisational changes towards a better security policy.**

| WITHIN THE ORGANISATION          | FACTORS HINDERING CHANGE   | FACTORS FACILITATING CHANGE  |
|----------------------------------|--|--|
| Organisational culture           | <ul style="list-style-type: none"> <li>• Superficiality. Improvisation. Individual oriented.</li> <li>• Security not mainstreamed.</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Team work, awareness of work impact, active listening, consultation, consensual decision making procedures.</li> <li>• Security mainstreamed.</li> <li>• ...</li> </ul>   |
| Management attitude              | <ul style="list-style-type: none"> <li>• Authoritarian and dictatorial. Results driven. Distant. Importance given only to leaders and therefore, inclined to designing and respecting rules fitting their needs only.</li> <li>• Non reciprocal expectation that other members are there to serve the management.</li> <li>• Granting themselves privileges.</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• In touch with all members.</li> <li>• Recognition of the importance of the contribution of all to the achievement of the organisation's mandate.</li> <li>• Attention given to concerns of all staff and rank and file.</li> <li>• Openness.</li> <li>• Respect of rules.</li> <li>• ...</li> </ul> |
| Organisational structure         | <ul style="list-style-type: none"> <li>• Rigid.</li> <li>• Compartmentalised.</li> <li>• Inappropriate to the work.</li> <li>• ...</li> </ul>  | <ul style="list-style-type: none"> <li>• Suitable flexibility.</li> <li>• Coordination and communication fluidity between levels.</li> <li>• Reflecting the needs both of the people and the work.</li> <li>• ...</li> </ul>   |
| Knowledge of the security issues | <ul style="list-style-type: none"> <li>• Centralisation. Partiality. Low awareness of security issues in the field. Lack of objectivity little factual or substantiated knowledge of issues.</li> <li>• ...</li> </ul>   | <ul style="list-style-type: none"> <li>• Sharing experience and knowledge. Inclusive. Factual.</li> <li>• Systematic compilation of information and regular updates.</li> <li>• ...</li> </ul>   |

|  |   |  |
|--|---|--|
| Lack of stability in the organisation; change fatigue. | <ul style="list-style-type: none"> <li>• Staff turnover.</li> <li>• Absence of historical memory.</li> <li>• Strain due to continuous changes. Absence of work continuity.</li> <li>• ...</li> </ul>  | <ul style="list-style-type: none"> <li>• Clear job description and contract with organisation stating commitment to give adequate notice of departure and to hand over knowledge and skills before leaving.</li> <li>• Regular evaluations.</li> <li>• Distribution of tasks that fit the time the staff have committed themselves to stay for. Induction and training</li> <li>• ...</li> </ul> |
| Work overload  | <ul style="list-style-type: none"> <li>• Insufficient and/or inadequate human resources. Stress. Loss of focus</li> <li>• ...</li> </ul>  | <ul style="list-style-type: none"> <li>• Prioritisation and (re)distribution of work.</li> <li>• Space to unwind</li> <li>• ...</li> </ul>   |
| Work planning  | <ul style="list-style-type: none"> <li>• Security is not clearly prioritised.</li> <li>• Security is not considered in the work plan.</li> <li>• Work plan is spontaneous and does not fit the aim and objectives</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Adequate security planning in work. Security is mainstreamed in the work plan. Adequate consideration is given to activities for which security is seen as insufficient and subsequent decisions are taken as to whether to carry them out if security conditions are not met,</li> <li>• ...</li> </ul>  |

Factors that do not specifically influence the organisational change towards improving the security policy:

- ♦ Size of the organisation
- ♦ The fact that the people responsible for security do or do not have higher education
- ♦ Religion
- ♦ Gender
- ♦ ...

### **Standards or good practices in managing protection and security.**

Now that entry has been gained, the responsible body has been appointed and has both found the starting point and planned the process, and that individual resistance has been dismantled, that the organisational factors hindering and facilitating the changes have been considered, what are the security and protection best management practices knowing that they depend on organisational structural models?

There are several options for managing security within an organisation, and it may be difficult to make a decision about which is the best choice. In the next chart we discuss three models and their pros and cons, along with some solutions.

| Structural models        | Where are security decisions made   | Advantages   | Disadvantages   | Possible solutions   |
|--------------------------|---|--|---|--|
| <b>Centralised model</b> | <ul style="list-style-type: none"> <li>• At management level, within a dedicated body.</li> </ul> | <ul style="list-style-type: none"> <li>• Easier to check that adequate experience and knowledge exist within the organisation.</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Work overload may inhibit the ability to take proper decisions</li> <li>• May be disconnected from the work in some areas.</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• One person at management level with executive ability acts on behalf of the management.</li> <li>• A security is appointed at management level but without executive ability.</li> <li>• ...</li> </ul> |

| Structural models          | Where are security decisions made   | Advantages   | Disadvantages   | Possible solutions   |
|----------------------------|---|--|---|--|
| <b>Intermediate model</b>  | <ul style="list-style-type: none"> <li>• Important and global decisions: at management level. Specific decisions: made by the people responsible for them in each area involved.</li> </ul> | <ul style="list-style-type: none"> <li>• Management is not overloaded.</li> <li>• Combination of skills and appropriate level. Closer to the actual work of each area.</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Conflicts about security might arise between the management level and the different areas.</li> <li>• ...</li> </ul> | <ul style="list-style-type: none"> <li>• Each person responsible for a specific area takes responsibility for security in that area. A security consultant may be appointed for the whole organisation: a person linked to a given area, for example administration or logistics, takes the responsibility for security and interacts with the person responsible for each different area but his/her own.</li> <li>• ...</li> </ul> |
| <b>Decentralised model</b> | <ul style="list-style-type: none"> <li>• Security decisions are made at all level because each person has an explicit responsibility for it.</li> </ul>                                     | <ul style="list-style-type: none"> <li>• Better fulfilment, contribution to the organisation's culture concerned with security.</li> <li>• ...</li> </ul>  | <ul style="list-style-type: none"> <li>• Discussions might take longer. Might apply mainly to small organisations.</li> <li>• ...</li> </ul>                  | <ul style="list-style-type: none"> <li>• There might or might not be people dedicated solely to security.</li> <li>• Each person might have that very responsibility in his/her job description or in their previous work.</li> <li>• ...</li> </ul>   |

### **Organisation staff/members' training.**

Now that entry has been gained, the responsible body has been appointed and has both found the starting point and planned the process, and that individual resistance has been dismantled, that organisational factors hindering and facilitating the change have been considered, that security and protection standards or best practices have been determined, what about training the staff?

The training may be held with the internal organisational resources (there may be people trained to give security training). The training may also be held jointly with other organisations (sending people to joint training sessions together with people from other organisations). If so, building one's capacities with other organisations might facilitate the subsequent exchange of security information and even the setting up of networks aimed at improving protection. Trust between organisations attending the security training is a must. Moreover, it is useful that organisations share interests and have similar areas of work and environments: rural and urban organisations for example have very different security needs.

Training can be implemented in many different ways. Arguably the most common are:

- ❑ Workshops (preferably in small groups of 10-15 people)
- ❑ Individual training (useful for complex tasks or for specific responsibilities, with on-the-job training)
- ❑ Conversational mode or semi-formal meetings (couching, active advice).

Carrying out at least some of the training outside the work environment is recommended in order to facilitate concentration and avoid the daily work tension. However it is often counterproductive to hold these activities after working hours ( i.e. at weekends) as it might send the wrong message: that security means more work -especially overtime, and that security is not important enough to be included in the normal work schedule.

## **How to improve the respect of the security rules**

Now that entry has been gained, the responsible body has been appointed and has both found the starting point and planned the process, and that individual resistance has been dismantled, that organisational factors hindering and facilitating the change have been considered, that security and protection standards or best practices have been determined, and the staff is trained, how can respect for security rules be improved?

The necessary conditions for the respect of security and rules plans are achieved through the following steps:

- ♦ Existence and development of an organisational security culture .
- ♦ Ownership of rules and of security plans.  
Participation in their design and improvement process.  
Training to clarify and understand them.  
Persuasion of both their adequacy and effectiveness.
- ♦ Drawing up an agreement between the individual and the organisation regarding compliance of security rules and plans.
- ♦ Regular intervention by the people responsible for security or information and training purposes, reminding the people of their reciprocal agreements and collecting the opinions of people about the adequacy and effectiveness of the rules.

What can be done in cases of non-compliance by security rules and plans?

- I** ● Find and solve the causes of the non-compliance (see chapter 2.2).
- II** ● If the cause of non-compliance is intentional and depends merely on the will of one individual, the following steps may be taken:
  - a ● Talk to the person (as the culmination of a previous process aimed at solving the causes of the non-compliance) in order to generate motivation and commitment.
  - b ● Take the issue up with the relevant work team, in the presence of the individual concerned (this step may sometimes not be adequate, depending on the situation)
  - c ● Apply a warning system (between 2 and 3 warnings)
  - d ● Apply a system of gradual sanctions which can culminate in firing the individual.

It is important to include in the agreement a clause referring to the compliance by the security rules and plans, so that all defenders are fully aware of the importance assigned to security by the organisation.

## Summary

Having a security plan does not mean it is implemented and respected. An appropriate process must be devised to manage security implementation, compliance and improvement. The more inclusive the process is, the more information about security needs can be gathered and the more ownership can be achieved.

There is no right or wrong organisational structure: each has advantages and disadvantages. It is therefore useful to analyse them in order to draw up a suitable process and give it as many opportunities as possible to succeed.

The improvement plan has to be **realistic** and **appropriate** to the profile and needs of the organisation.

Here are the successive steps of the process towards a better security policy:

- ♦ entry must be gained for security
- ♦ a responsible body must be appointed.
- ♦ the responsible body needs to find the starting point and plan the process
- ♦ individual resistance needs to be dismantled by active listening to determine the reasoning on which the individual bases their resistance, in order to phrase a suitable counter-argument (it is not enough to just give an opposite view to the resistance stereotype as the determining factor is the reasoning behind the stereotype: if the resistant individual's reasoning is right, so is their resistance)
- ♦ organisational factors hindering and facilitating the change need to be considered
- ♦ security and protection standards or best practices need to be determined
- ♦ staff / members need to be trained
- ♦ security compliance rules need to be improved.