10 Communications Tips For Security Managers

Steve Purser

Steve Purser is the director ICSD Cross-Border Security Design and Administration at Clearstream Services, Luxembourg and is also a founder member of the Club de Sécurité des Systèmes Informatiques au Luxembourg (CLUSSIL). He is also the author of “A Practical Guide to Managing Information Security” (Artech House (2004)).

Of all the skills that the modern security manager must possess, good communications is arguably the most basic. Most of us have seen innovative ideas fail at some time or other because they weren’t communicated in the right way and many of us have watched our own projects flounder for similar reasons. Speaking as part of a generation that was taught to fight for what it believes in, it is easy to appreciate how enthusiasm and the will to succeed can quickly become a handicap if not managed correctly. As a practicing security manager I continually meet people who are good at arguing their case, but it is far more difficult to find people who have the patience to listen to other points of view and to adapt their game plan accordingly.

The fact is that good communication is extremely difficult. Where information security is concerned, discussions can easily become clouded by specialized terminology and the complex nature of the tools used to solve particular problems (cryptographic techniques provide an ideal example). As security managers we therefore need to continually challenge the way we communicate, not only to ensure that we understand the problems and react appropriately but also to create a long-term atmosphere of confidence and mutual trust.

I propose the following tips for improving communications based on my own experience. Whilst many of these statements might appear to be trivial or self-evident, I challenge the more sceptical reader to take a moment to think about how successfully they put these rules into practice.

1. Prepare beforehand

Not many of us would think of taking an exam without preparing correctly – the outcome is often too important to justify taking such a needless risk. Interestingly, my experience is that many people are prepared to enter into important discussions without adequate preparation; meetings are an excellent example.

Most meetings are not set up to simply exchange points of view on a particular subject. More often than not the purpose of the meeting is to achieve an objective. In addition, those attending the meeting will quite often have their own (unpublished) objectives. If we are to achieve our objectives, it will help enormously if we have a clear understanding of what these objectives are and what other attendees of the meeting are trying to achieve. This will allow us to identify any common ground and to be aware of potential obstacles, which in turn will enable us to develop a strategy for the meeting. In many cases, a proactive approach will make it possible to agree the outcome of the meeting before it actually takes place! Obviously, preparation for meetings includes ensuring that important decisions get recorded in the minutes, even if everyone agrees with them – this can save a lot of trouble later on.

The essential part of preparing for any dialogue is predicting and understanding the position of the other party with respect to what will be discussed. The more accurately we can determine this beforehand, the better our strategy for dealing with any differences of opinion will be.

2. Use face-to-face communication

It is not difficult to understand this guideline, but it can be difficult to apply it effectively, especially where there is an element of confrontation involved. I have personally witnessed countless numbers of hostile mail exchanges, which have been quickly resolved once the concerned parties agreed to meet face-to-face. Face-to-face communication has many advantages over other forms of communication:

- We can see and react to the non-verbal signals.
- It is psychologically more difficult to use extreme language and gestures, which tends to result in a more reasonable dialogue.
- Communication is synchronous, which allows discussions to proceed in a more natural manner.
- It demonstrates a certain commitment to resolving the issue.

Where face-to-face communication is not possible (due to geographical constraints for example), teleconferencing and/or telephone conversations are preferable to written communication. Electronic mail is a poor communications medium for contentious subjects.

Effective face-to-face communication is also an excellent way to prepare acceptance of important documentation and in many cases it is an essential step in the process. No matter how well they are written, analytical documents are not very effective instruments for changing established habits or for dealing with fear. In fact, for emotive issues, simply distributing an analytical document without having prepared the audience beforehand is almost certain to result in failure.

3. Listen first then speak.

At a security event some years ago, a delegate asked me if he should be considering deploying intrusion detection technology. The question itself was not unreasonable, but it was interesting to note that it was the availability of the technology that had caused this person to start thinking about the whole area of intrusion and not the underlying problem. I find this phenomenon of *technology push* disturbing because it implies that we are listening more to vendors than to our own people – there is nothing new about many of the problems that the latest technology is helping to solve and in many cases they can be effectively controlled by a combination of existing technology and non-technical solutions.

I strongly believe that a successful approach to securing information must reflect the culture and risk profile of the organisation. I also believe that in many organisations, developing a deep understanding of these two factors is likely to take a lot of time and to require a lot of listening. This is particularly so where organisations do not adopt a coherent attitude to risk. Consider for example the organisation that sets a highly risk-averse security policy and continually fails to meet it – this is an organisation that wants to be seen as risk-averse, but is actually happy to accept more risk in practice. Whilst some may argue that setting the bar artificially high is a good thing, this can easily lead to a lot of wasted effort and render the whole approach less effective than it could be.

Where information security is concerned, being a good listener therefore involves many things. In particular, it involves listening to the right people and having the patience and analytical skills to separate out the real requirements from the rest. Finally, it involves a certain amount of discipline, to make sure that the approach is driven by genuine requirements and not by nebulous concepts, such as best practice. Best practice can be a useful check to verify a solution that has been designed to meet requirements, but should not be used to drive those requirements.

In a nutshell, listening before speaking ensures that we do not propose the solution before we have truly understood the problem.

4. Use the right language.

One of the most powerful techniques for communicating well with others is to tailor the language to the profile of the person you are speaking to. This involves not only the choice of words, but also the whole way in which the argument is structured. In this respect, it is easy to understand why a business manager might not understand a technician describing a problem in terms of technical details, but it is less easy to see why similar problems occur when the explanation is given by someone who is able to simplify and to present the problem at the appropriate level of abstraction.

As an example of this, consider the notion of Return On Investment (ROI). Whereas the head of finance is likely to judge initiatives on hard numbers and to be less influenced by qualitative arguments, this is probably not the case for individual business lines or more customer-facing profiles. Therefore, in order to get approval for projects that are necessary but do not show a positive ROI in the classical sense, it makes sense to persuade the business first and then to enlist the help of business managers to get the approval of finance. Business managers that deal with customers regularly are more likely to be open to qualitative assessments of risk than the financial department. Few business managers would be comfortable with a significant risk that the company web page could be defaced, irrespective of whether or not the argument can be supported by a positive ROI.

Just as tailoring information to the needs of the recipient is important for obtaining approvals, it is also important to take account of different target groups within the organization when disseminating information. In particular, when designing an awareness campaign, it is a good idea to distinguish between the core messages, applicable to all staff, and more targeted messages and examples, destined for particular groups.

5. Be prepared to compromise.

Information security is about risk management and as we usually cannot reduce risks in this area to zero it could be said that we compromise all the time. In fact, as security professionals, we may err on the side of caution too often and miss useful opportunities. Given the role of the security manager, this is a natural reaction and I certainly wouldn’t advocate taking risks for no valid reason, but it is always worth examining possible compromises when they are suggested and understanding the impact. After all, if someone suggests a compromise, they usually have a good reason for doing so and if the compromise is an acceptable one, this can strengthen co-operation and help in building a long-term relationship.

Compromise is much easier to achieve when the approach to securing information is based on the analysis and mitigation of risk – it is more difficult to achieve in axiomatic approaches that rely too heavily on policy. Organisations that blindly follow policy in all circumstances are unlikely to achieve an optimal response to the risks they are facing because a policy statement cannot possibly take account of the contextual information characterising a particular situation. Policy statements are a useful device for dealing with known risk, but it should always be possible to challenge them using risk analysis techniques.

Just as the proverbial bough that doesn’t bend with the wind breaks, security approaches that do not allow for a healthy dose of compromise are likely to meet with resistance and, depending on the company culture, perhaps failure. The key is to achieve the compromise in a controlled manner, by making the deciding parties aware of the risks and other obligations (such as legal and regulatory restrictions) and the alternatives for dealing with these risks. The choice of which alternative to take then becomes a business decision.

6. Encourage others to participate in defining solutions.

Experience shows that projects and initiatives that require significant cultural change in order to succeed are likely to meet with a certain amount of resistance. Much of this resistance probably stems from the doubts or fears that many people experience when they are asked to make major changes to their usual working methods. It is easy to understand that an approach which imposes a solution without sufficient preparation and consultation is less likely to be successful than an approach in which affected parties are consulted and correctly informed from the start. Taking this argument one step further, people are more likely to buy in to an initiative if they can influence the outcome.

Where resistance to change is particularly strong, it can be useful to completely invert the normal process and to encourage staff members to take the lead in driving the required change. Such an approach is likely to be initially slower than the traditional approach, but the chances of achieving a durable solution are also much better if this process is correctly managed. Taking this process to the extreme, the target group is simply given the problem and asked to come up with the solution itself. The security team supports this process by ensuring that the problem has been understood and by making suggestions as possible solutions develop. Typically, this support work will involve de-mystifying concepts (such as the difference between authentication and authorization) and explaining where tools can be of use.

Letting end users drive the final solution has other advantages besides commitment. The average end user is likely to view a security problem from a different perspective than a security professional. Whilst a certain amount of confusion and false starts is inevitable in many cases, this perspective can lead to innovative solutions and can help counter the tendency of trained staff to fall back on the standard solutions.

7. Provide regular feedback to keep the dialogue alive.

Even the most interesting long-term initiatives can easily lose momentum if there is no strategy for keeping them alive. Keeping the dialogue active and maintaining enthusiasm can be a major challenge for this kind of project, so it is just as well to have an approach for dealing with this in advance.

The best time to start this preparation is during the planning phase. As most project plans are not strictly linear and allow for a certain amount of parallelism, it is worth thinking about how the plan can be used to motivate the team when scheduling tasks. Consider developing a plan with regular *milestones* and short task durations, because both serve as checkpoints for discussion. Achieving milestones provides positive feedback to all concerned and increases motivation. Using short task durations avoids the ‘80% complete but never finished’ syndrome – at the finish date the task is either complete or not – the situation is black or white.

For initiatives that are not project oriented, periodic status meetings can be used to achieve the same thing as long as there is a useful mechanism to drive the meetings with. Actions lists and issues lists are two useful devices for driving periodic meetings. Actions lists are simply a form of short-term planning and document the actions agreed for the next period. Issues lists, as the name implies, document known issues together with the person responsible for resolution, the deadline and the current status.

At the end of the day, it doesn’t matter how the dialogue is kept alive. As long as there are regular discussions with all concerned it will be easier to pick up on any problems and issues that are developing. This in turn brings an increased level of control.

8. Use the power of the group.

It sometimes happens that reasonable projects or initiatives are blocked by individuals for irrational reasons. This is an example of where a well-designed approval process can work against itself, allowing a single decision-maker to effectively block a potentially valuable initiative.

One technique that can be used to deal with this situation is to isolate the blocking party within a group. The idea is to arrange a meeting to discuss the way forward, where we can confront the person blocking the initiative with those decision makers that are favourable. This technique tends to be very successful when the reasons for blocking the initiative are not well founded, as most people are reluctant to expose personal or irrational motives in front of a group of peers.

The group approach is also useful when the reasons for blocking the initiative are valid ones, but here the objective is to look for creative ways to resolve the difficulties, rather than to persuade a reluctant stakeholder to follow a course of action that has already been decided.

9. Back up verbal agreements with written confirmation.

Getting a verbal agreement is usually the first step in launching initiatives involving other people. Whilst this is a major step, a verbal agreement suffers from several disadvantages:

- The details of the agreement may be interpreted differently by the agreeing parties.

- The details may be forgotten or modified over time.
- There is no point of reference to go back to in case of disagreement.

For these reasons, it is usually necessary to back up any important verbal agreement with a written confirmation.

There are many ways of viewing such a written confirmation. At one extreme, such a confirmation could be viewed as a sort of ‘contract’ binding both parties and for which any deviation must be justified. At the other extreme, it could be viewed as a simple recording device to ensure that the details are not forgotten or misinterpreted.

The way in which written agreements are handled will depend largely upon the relationship between the two parties, but as a generalisation, the more we err towards the ‘contract’ approach, the more cautious both parties are likely to be in carrying out the initiative. In some cases, this is exactly what we want to happen, but in many others this is too extreme and may stifle progress. It is therefore a good idea to make it clear from the start how we intend to handle a written agreement, so that we do not unnecessarily restrict an open dialogue.

10. Don’t take things personally!

This is perhaps the hardest guideline of all to follow. As dedicated professionals we all take pride in our work and invest a lot of time and effort into our projects – it is therefore extremely difficult to view our own initiatives with detachment. Getting too involved personally can be problematic however and can prevent us from making a good idea even better. This state of mind is typified by the person who defends his/her project to the better end – even when faced with better alternatives or useful variations on the original idea.

The trick here is to adopt a completely different way of thinking; if we are responsible for producing a given result it doesn’t matter who actually defines the solution as long as this solution is the right one. Even if the final solution is not the one we put forward, this initial idea acted as a catalyst in obtaining the final result and by getting to the best final solution we have achieved what we set out to achieve.