

# Integrating Security into the Corporate Culture

by: Steve Purser, 10/06/2004

<http://www.securitydocs.com/library/2631>

## Introduction

At a major security conference several years ago, I asked a group of security professionals to define risk in such a way that it could be understood by non-specialists and then to suggest different ways of reacting to risks once they had been identified. Interestingly enough, many of those present were able to come up with good examples of risks, but defining risk in practical terms as a concept turned out to be a difficult exercise, even for security professionals. Equally interesting was the fact that although everyone realized that risks could be managed by some kind of mitigation exercise, very few people identified the option of transferring the risk to a third party (e.g. by insurance or contractual means) and even fewer suggested that it might make sense to simply accept certain risks. The important point here is that thinking about risk is not necessarily simple and even the experts can have difficulties when they are put on the spot.

Nevertheless, the notion of risk is at the heart of information security. Implementing real security involves understanding security-related risk and reacting appropriately and, in general, the better employees are at doing this, the more secure the enterprise will be. Put another way, even well-designed technical controls and procedures will be of limited value if the staff involved do not understand why they have been implemented, what they are accomplishing and their limitations. As the previous paragraph illustrates however, achieving this level of understanding represents a major challenge and normally involves a great deal more than an annual awareness initiative. Indeed, for many organizations this will involve a cultural change requiring the integration of security concepts into the working culture.

Recent surveys in the area of information security confirm that there is still a lot of progress to be made in this area. Hence, one of the key findings of the 2004 CSI/FBI Computer Crime and Security Survey is that although organizations view security awareness training as important, they do not on average believe that their organization invests enough in this area [1]. This conclusion is supported by the Ernst & Young 2003 Global Information Survey, which reports that only 29% of organizations list employee awareness and training as a top area of information security spending [2]. Much along the same lines, the Australian Computer Crime and Security Survey 2004 notes that “the most common challenges and difficulties respondent organizations faced were changing user attitudes and behavior (reported by 65% of respondents) and keeping up to date with information about the latest computer threats and vulnerabilities (reported by 61% of respondents)” [3]. Finally, the DTI Information Security Breaches Survey 2004 points out that the relatively low priority businesses give to educating their own staff is surprising given that a significant proportion of businesses recognize a need for more information security advice from third parties [4]. These results are largely in line with previous surveys in this area [5].

This short paper analyzes why organizations should consider spending more time on developing a culture that is both aware and capable of responding to security-related risk and goes on to suggest ways in which this could be achieved.

## Why culture is important

Before examining techniques for introducing cultural change, it is useful to look at some of the ways in

which the level of staff awareness and training can have a drastic effect on the success or failure of the security process as a whole or on specific security mechanisms and procedures. In order to make the point, we will (rather arbitrarily) look at four separate areas within the information security process:

1. The decision making process.
2. Client-side security.
3. Server-side security.
4. Recognizing and handling incidents.

Of these examples, the first provides the best example of how a lack of education and awareness can fundamentally compromise the whole information security process. In order to understand this, it is important to realize that one of the biggest paradigm shifts that has taken place in the area of information security in the last decade is the realization that security is a business issue. In other words, although much of the analysis, design and implementation of security solutions will require highly-competent technical staff, the key decisions should be driven by business concerns and not technical ones.

When viewed from an opportunity and risk perspective, this makes a lot of sense – organizations take risks every day and the way in which they take risk can be considered to be a part of their business model. Indeed, there is nothing particular about security-related risk, except perhaps that it can be extremely difficult to understand when IT systems are involved. When viewed from an awareness perspective however, the survey data cited in the introduction suggests that this is a rather hopeful view of things and, in reality, many organizations might not have attained the level of user awareness and education necessary to make this model work in practice. Organizations that have adapted their core processes to align with this model without having achieved the necessary awareness may well find that the real decision making is taking place outside the agreed procedural framework. Under such circumstances, business managers will not have the knowledge or understanding necessary to make an informed decision and are more likely to blindly accept recommendations made by specialists, rather than to challenge them.

The fact that user awareness and education has a big impact on client-side security is easy to understand. Even when client software and operating systems are locked down (and in principle inaccessible to the end user) it is clear that poor decisions made by the latter can easily compromise security. Hence, user communities that do not appreciate the techniques that are used to spread viruses and other malicious code via E-mail and web channels will be more open to infection by malicious code in the window of risk before the corresponding pattern files are available. Similarly, inappropriate responses to pop-up boxes during a web session can have wide reaching consequences. More fundamentally, where users do not enforce a minimum of physical security over their personal computers or laptops, not only are they open to theft, but it may be possible to modify the configuration using attacks that exploit the boot sequence (similar to NTFS-DOS or linux boot disk attacks). Widening the discussion to other types of client device, staff that upload business data to PDA devices may not take the time to consider what the impact will be should the device be lost or stolen, whereas those that limit the use of PDAs to receiving and sending E-mail have little control over the information that is sent to them (and so may unwittingly store confidential information on the device).

Taking the example of malicious code one stage further, it is obvious that once a client has been infected, it is usually only a matter of time before servers are infected too. For example, where infection spreads by infecting files, the file server will be infected as soon as the client saves an infected file. A more interesting example of where poorly adapted cultural values can have a big impact on server-side security is in the area of system administration. Where administrators consider repetitive tasks as dull and uninteresting, these tasks may not get done or, at best, they may be carried out reluctantly. For instance, due to the complicated syntax of entries in the log files, performing a correct log analysis for

some platforms requires highly-skilled staff. Where such staff are in short supply and there are more interesting tasks to be done, there may be a tendency to avoid the more routine work. More generally, it is often easier to motivate engineers to implement new technology than to administer it once it is in place.

The last example in this section is concerned with recognizing and handling incidents. Whereas recognizing some incidents (such as a virus infection) is relatively straightforward, others can be very difficult to recognize. Personnel that are sufficiently aware of security issues and correctly trained in their day-to-day activities should be capable of developing a 'feeling' for what constitutes normal behavior of the system or process they are dealing with. This is extremely important as the control system (i.e. the procedures and mechanisms deployed to reduce IT security related risk) is designed to cope with known risk scenarios. Where unusual risk scenarios crop up, the capability of recognizing unusual behavior is at the root of incident recognition. Furthermore, the extent to which the organization is really secured will also depend on the ability of staff to handle incidents appropriately, which usually means understanding and correctly using existing incident handling procedures.

These short examples illustrate that real security is not just a question of well-designed technical infrastructure and tight procedures. In order to ensure the right result, staff must understand the framework they are working in and be capable of adapting their behavior to respond to new and unforeseen events.

### **Introducing change**

Introducing cultural change is an immense task and often involves challenging established ideas and working methods that have (to some extent) survived the test of time. Achieving something so fundamental requires a consistent and coherent approach using all the communications channels offered by the organization. In this context, it is important to note that informal communication is as important, if not more important, than more formal channels. In other words, if the wrong person says the wrong thing in the coffee bar, this can destroy months of hard work. It is therefore useful to look at methods for changing cultural values by classifying them into methods that use informal channels and methods that are more structured.

There is a lot of established documentation on formal methods for ensuring that security awareness is integrated into the culture of the enterprise [6]. Much of this documentation concentrates on the security awareness program and security skills-training. Informal methods for introducing cultural change include most initiatives outside the scope of structured initiatives such as these. Informal communication is so important because it occurs so often – under such circumstances, small negative messages can quickly become major issues. Hence, the first step in changing company values is to ensure that the information security department is passing a consistent message across all communications channels.

One example of where this might not necessarily be the case is the user support process. Supporting users who are experiencing problems with security mechanisms is a 'front-line' activity and requires the ability to make suitable compromises in order to unblock users who cannot work. Because this activity is driven by business units experiencing problems it is a good opportunity to demonstrate commitment to solving problems. In fact, approached in the right way, this activity can be used to encourage a collaborative approach and to foster active participation of end users in the information security process. Unfortunately, it is very easy for administrators to inadvertently give end users the wrong impression when performing this kind of work – particularly when controls are temporarily deactivated. The solution is to ensure that security administrators are fully aware of the key messages passed in more formal training and to encourage them to reinforce these messages when commenting on problems and

potential solutions - users greatly appreciate it when administrators take the time to explain what is going on and why the standard security controls are not working correctly.

Perhaps the most important informal method of introducing a security minded culture is to ensure that there is a continual drive within the enterprise to publish the objectives of the information security group and to make staff aware of progress and how they can contribute to the success of the initiative. This can be considered as an internal marketing and sales activity, aimed at raising the profile of information security as a whole and encouraging staff to get involved. Although we will consider this to be an informal method of introducing cultural change, it is clear that such an initiative will require careful planning if it is to succeed. In particular, it is worth identifying key decision makers and different groups of staff within the enterprise and tailoring the information that is sent to them to their requirements. Hence, business managers are likely to be interested by a new approach to analyzing risks that provides them with more control over systems in their area, but are much less likely to be interested in an initiative to integrate security into the development lifecycle. Similarly, technical staff might appreciate the opportunity to learn about implementing cryptographic solutions but not to understand the finer points of the latest regulations on data privacy.

The classical approach to improving security awareness is to design and deliver a security awareness program, tailored to the needs of the enterprise. Whilst such an initiative cannot replace the need to correctly control informal communications channels, it remains true that the awareness program is an important tool in changing attitudes to security within the enterprise. To get maximum benefit from such a campaign, it is worthwhile defining measurable objectives and identifying metrics to measure to what extent these objectives have been met. Typically, it will be necessary to create a proposal with an accompanying business case for an initiative of this size and concrete, measurable objectives will strengthen this case.

Just as tailoring information to the needs of the recipient is important for promoting the information security group, it is also important to take account of different target groups within the organization when designing the awareness campaign. The core of the campaign will then contain a common set of messages, applicable to all staff, and a series of more targeted messages and examples, destined for particular groups. Wherever possible, it is recommended that security officers try to obtain active participation of senior staff in presentations – this is easier to organize when target groups have been defined in advance. Having a member of the executive management team open awareness sessions with a prepared statement adds credibility to the initiative and demonstrates the support of top management. Finally, for those departments that have the manpower, it is useful to have a member of the information security group present at each presentation to keep record of discussions and questions – this can then be fed back into future sessions.

Awareness campaigns should be planned and executed as periodic events and not as a one-time exercise. For most staff, once a year will probably be sufficient to meet their needs, particularly if specific skills training is also planned. It often helps to run a pilot project before launching a full blown campaign, but care needs to be taken with planning. It is clear that an awareness campaign that runs over the summer months will have to struggle with multiple absences due to holidays (and the need to use remaining staff for business critical activities).

Finally, it is important to realize that awareness is only the first step towards obtaining active participation of staff and many staff will require more focused training in order to understand how security concerns affect their day-to-day activities. Since such training necessarily involves a mixture of business skills and security-related skills, it is a good idea to work with business managers to organize and follow-up on such training. Ideally, the relevant business manager will identify the needs, working alongside the security officer and will arrange for training and follow-up of his or her staff.

Staff that are both aware of general security issues and correctly trained in their respective areas should be well positioned to participate actively in the security process. In particular, referring back to section 2 of this article, such staff should be capable of recognizing unusual behavior and reacting appropriately. An organization that has achieved this will have established a security minded culture.

### **Aligning the security approach with the company culture**

Unfortunately, having a set of methods for introducing change does not in itself guarantee success and achieving the desired result will require applying these methods with a lot of preparation and forethought. In this context, it is extremely important to ensure that the security process responds to the needs of other business processes and not the other way round - approaches that are too ambitious and involve significant changes to existing culture are likely to be a lot less successful than those which aim to integrate security practices into the existing culture gradually.

Although this might seem like an obvious statement, in reality it is likely to involve a lot of management. Consider for example a security group planning to implement a formal security framework, such as ISO 17799. There are a host of good reasons for choosing such an approach, but it is important to realize that staff who have nothing to do with information security are likely to see this as a new set of constraints, about which they initially know very little. In addition, the framework chosen might not integrate well with existing methodologies and practices, such as development methodologies for instance. Similarly, as we noted in the introduction to this article, approaches that aim to shift the ownership for making decisions to business managers, must allow for an extensive period of training and coaching as well as providing for the necessary support from IT teams when required.

More fundamentally, changing cultural attitudes is likely to meet with a certain amount of resistance to change [7] and successful approaches will seek to harness this reaction rather than trying to suppress it [8, 9]. One particularly useful way of coping with this problem is to let those involved drive the change process. Admittedly, this is not an easy thing to do where information security is concerned, as many of the techniques used to mitigate risk in this area require quite a lot of specialized knowledge. However, this complexity tends to be a consequence of the infrastructure that is being secured, and the basic concepts upon which a successful approach to information security are built are remarkably simple. As long as the information security group provides a sufficient level of guidance, giving business areas control over their own security issues is a very effective way of achieving change.

Finally, it is worth taking a moment to consider the importance of language in this change process. Discussions about IT security 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 a result, many within the enterprise are likely to view the whole of information security as a difficult and highly-specialized discipline. Such a viewpoint is unlikely to encourage participation and an important step in involving users in the process is getting over the language barrier. Security personnel can avoid this by orienting the discussion around the risks and core concepts, which in themselves are not too difficult to understand. Hence, whilst a non-specialist might find it difficult to understand the concept of a Message Authentication Code (MAC) or Digital Signature he/she will probably appreciate the need for preserving the integrity of their data.

### **Getting feedback.....and reacting to it**

Feedback from staff is likely to arrive in a variety of different forms. There will be informal feedback

and formal feedback. Once again, the informal feedback is likely to be more reliable than any feedback received through more structured channels as many people are reluctant to express themselves fully through a channel where their views will be recorded for all to see. The most important thing about feedback is to provide evidence to those providing it that it has been taken into consideration (even if the idea has been rejected) – there is little worse than being ignored after having taken the time to provide a point of view.

For more structured initiatives, such as the awareness program, feedback should be planned into the project. In the last section, it was mentioned that it is worth putting a member of the information security group in each presentation so as to record ideas, suggestions and other interesting feedback. In this particular case, it is also a good idea to ask attendees to fill in evaluation forms (preferably on an anonymous basis). Further feedback can be obtained by interviewing the respective line managers to see whether or not they have noticed positive change as a result of the exercise – this would be done after a period of several weeks. Initiatives such as these also lend themselves well to an approach based on metrics and these metrics would typically be designed to illustrate how the objectives are being realized.

Just as it is worth considering making users responsible for specific security issues in their area, so it is worth encouraging staff to take responsibility for implementing their own suggestions for improvement. This involves staff in the process (which is the overall goal), empowers them to deal with their own issues and ensures that they pick up experience on the way. This might not always be possible, particularly where the level of risk is high and deadlines are tight, but such an approach can certainly be used to deal with less pressing problems.

## Conclusions

Experience shows that understanding and dealing with risk is not a trivial task and even experts can experience difficulties when put on the spot. Nevertheless, information security is all about reducing certain types of risk to an acceptable level. Although what constitutes acceptable risk will vary from organization to organization, it is clear that the better employees are at understanding and dealing with security related risk in general, the more secure the enterprise will be. It is therefore somewhat surprising that surveys continue to indicate slow progress in the area of security awareness training and education.

Whereas well-defined procedures and supporting technical infrastructure are important in reducing risk, real security involves active and informed participation of staff. Achieving the level of understanding and education required to be effective will prove to be a challenge for many organizations and will often involve a fundamental cultural change. There are many examples that illustrate why such a change is desirable. In this paper, we have briefly examined problems that can affect the decision making process, the impact of a poorly adapted company culture on client security and server security and we have seen that the incident handling process requires staff to recognize and respond to unusual events.

There are many ways in which we can act to integrate security within the company culture. Whilst there is a great deal of literature on formal methods, such as security awareness campaigns and security skills training, less emphasis is placed on the more informal aspects of communication. Ironically, the latter arguably have the greatest impact in influencing opinion. Examples of informal communications channels include casual conversations in the coffee bar and incidental comments made during routine support processes. In both cases, an inadvertent comment can destroy months of preparation. Informal communications channels are particularly well suited to an 'internal sales' initiative, aiming to raise the profile of the information security group. This is not to say that formal methods do not have their place and the traditional awareness program plays a critical role in improving staff knowledge. Awareness

campaigns require careful planning and should be designed with specific objectives in mind – this not only helps justify the business case, but is also useful for monitoring the impact of the initiative after the event. Skills training builds on top of awareness training and aims to impart specific security skills needed to perform particular tasks. Such training typically involves a complex blend of business knowledge and security knowledge and is therefore best managed in conjunction with the responsible business line.

When using these methods, it is important to consider how staff will react to proposals for change. A key step in gaining acceptance is to ensure that the information security process is designed to satisfy the requirements of core business processes and not the other way round. This can sometimes be difficult when using more formal methodologies or techniques. Although resistance to change is inevitable, this is not necessarily a bad thing and a healthy level of resistance can help improve the quality of the final deliverable. A powerful way of implementing change is to let those concerned drive the process – this tends to allay peoples fears and often produces creative solutions.

Once the process of change is underway, it is important to remain in control of the feedback process. Feedback too will arrive by both informal and formal channels, of which the former are likely to paint a more complete picture than the latter. Irrespective of the way in which it is delivered, staff both expect and have a right to know what is happening to their suggestions – in other words, the security group should take care to provide feedback to the feedback! This of course generates a true dialogue and the hope is that this will progress into more active participation. More structured initiatives require additional structured feedback and it is worth considering defining and tracking metrics in this area.

The ultimate goal is participation of staff and when staff can be persuaded to participate actively in both the initial implementation of an idea and in its refinement, this goal will have been largely met.

## References

- [1] The 2004 CSI/FBI Computer Crime and Security Survey, <http://www.gocsi.com/fo rms/fbi/pdf.jhtml>
- [2] Ernst & Young, Global Information Security Survey 2003, [http://www.ey.com/global/download.nsf/Russia\\_E/Globla\\_Info\\_Sec\\_03/\\$file/Global\\_Report.pdf](http://www.ey.com/global/download.nsf/Russia_E/Globla_Info_Sec_03/$file/Global_Report.pdf)
- [3] The Australian Computer Crime and Security Survey 2004,
- [4] The DTI Information Security Breaches Survey 2004, <http://www.security-survey.gov.uk/>
- [5] Steve Purser, “A Practical Guide to Managing Information Security”, Artech House, 2004, pp. 215-217.
- [6] Steve Purser, “A Practical Guide to Managing Information Security”, Artech House, 2004, chapter 9.
- [7] John Sifonis and Delfina Bisha, “Change, Culture and Social Networks”, [http://business.cisco.com/prod/tree.taf%3Fasset\\_id=103198&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3Fasset_id=103198&public_view=true&kbns=1.html)
- [8] Lukman Susanto, “Resistance is rewarding with change – Literatures Review” <http://www.susanto.id.au /papers/OCM.asp>
- [9] Peter de Jager, “Resistance to Change: A New View of an Old Problem”, <http://www.wfs.org/futcontmj01.htm>

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