

INFORMATION SECURITY - WHAT USERS CAN DO AND WHAT CAN BE DONE FOR USERS

Jozef Vyskoc jozef@vaf.sk
*Dept. Informatics, Faculty of Nat. Sci., Univ. of SS. Cyril & Methodius, Trnava,
Slovak Republic.*

Abstract: This paper offers a short trip into yet to be thoroughly explored area of users' involvement in practical IS security. It is based on author's experiences from various security projects and IS audits. As it talks about human beings, statements here should not be mechanically applied due to possible cultural, regional, etc. differences ... but perhaps it brings some inspiration to those struggling for difficult task to ensure secure operation of an IS.

1. INTRODUCTION

There are no doubts that the key roles in securing information systems (IS) are usually played by specialists like security managers, system administrators or ARE auditors. However, they are able just to provide basic conditions for secure and reliable operations, as there are ordinary users who make use of IS services using a number of workstations scattered through a building or even connecting from remote locations. In spite of that IS users and their behavior often are not satisfactorily addressed by security projects. Too often security specialists treat the issue in a greatly simplified manner assuming that people (IS users, managers, others) in a sense are mature enough to deal with IS so that issuing some commands suffices to direct them to a desired behavior. It appears, however, that efficiency of such approach is questionable ... let us cite one of the main findings from the Czech Information Security Survey 2003 [1]:

Generally low security awareness is still the biggest obstacle to a faster enforcement of information security in the Czech Republic...

“Command-based” thinking, while quite frequent among security specialists, does not respect the fact that when talking about real security of an IS one has to take into account that most IS users are usually persons whose qualifications quite rarely include deeper insight into the processes by which IS provides its services; the situation is even worse when considering ordinary users’ level of awareness on information security matters. That means ordinary users generally have better chance to act without thinking about security implications of their actions.

Experiences show that those responsible for, or at least interested in, security of IS operation usually meet with what seem to be an insurmountable task. Particularly, some users in real life often behave in ways that quite rightfully qualify them as being dangerous for IS security ... and despite that they have to have access to the system allowed. Quite naturally this results in somewhat mixed feeling of IT/information security specialists towards ordinary users. Dealing with users is really one of the most difficult task facing security professionals.

Perhaps every information security enthusiast at some point discovers that the problem of securing information system is not solvable by purely technological means. That means even with a collection of technical security measures implemented, real security can be achieved only when employees of the organization collaborate and behave in a way that does not block existing security measures, makes them inefficient or open some security hole. One who does not ignore differences between theoretical models and the real world situations simply cannot avoid taking into account so called human factor - i.e. people and their imperfection when comes to security, security awareness or security conscious behavior. The task is here and cannot be ignored – to reduce risk by ensuring a proper, security conscious conduct of users at least when their activities are related to the IS under consideration.

2. STANDARD PRACTICE

Let us take a look again at [1] to see how the organizations approach the task of increasing security awareness of their staff. As the report states, the approach seem to be independent of the size of the company. According to the [1], forms of improvement of the security awareness of staff are as follows

Staff Manual	9%
Addendum to Employment Contract	17%

Regular Training	21%
Control	37%
Internal Guidelines	72%

Here results of the Czech survey nicely correspond with my experiences in Slovakia. Shortly stated, standard approach to solve the problem of a proper users' behavior within the IS framework focuses on formulating a set of rules and regulations that users must follow, as well as penalties that apply if they don't. Alternatively just users' responsibility for relatively broadly defined proper conduct is stated there. These rules are then communicated to users. Moreover, to ensure that none can later claim ignorance, users are also often asked to sign a statement that they indeed were familiarized with such rules.

How effective is such an approach? Stating from my experiences not very much, and probably this is not just my feeling. Again, let us take a look at [1], particularly at what respondents considered to be major obstacles in the faster enforcement of information security in the Czech Republic. Here generally low security awareness scores the best, even with increasing emphasis – 31% in year 1999, 33% in 2001 and 35% in 2003 (just for comparisons, runner up is financial intensity with 20% in 1999, 14% in 2001 and 17% in 2003, followed by inadequate management support with 13% in 1999, 21% in 2001 and 14% in 2003). Hence it seems that “standard” approaches to ensure desired i.e. security conscious conduct of users fail.

The problem with such simple solution is that in fact it does not provide security to IS, it just provide a sort of alibi in case something bad happen. This does not mean that such rules are not necessary – but if no one cares whether users really understand rules, or even know how to fulfil the requirements, then such security measures provide no real security, just ease finding a scapegoat if something went wrong because of a user's misconduct.

This is just one manifestation of quite widespread “**passive“ approach to security, i.e. an approach where great effort is directed towards users' responsibility matters but very little, if any, attention is given to measures that can actually prevent undesirable events to happen.** In our opinion, however, the main goal in security should be to prevent (or minimize) losses, not just be able to determine who is responsible for the disaster. In the case of users this means that **one should also care whether users even know how to fulfil given requirements.** This is, however, harder task than just to assign responsibilities. It is much easier to simply state that “a user should not activate virus she received by e-mail and will be held responsible for any damages resulting from such activation“ than to ensure

that all users actually know how to prevent virus activation ... yet it is quite clear that the later yields more secure IS operation.

Educating users is a must, but it is efficiency that matters the most.

To make sure that users know what is accepted as proper conduct and how to prevent some undesirable events to happen, one has to educate them. Here again quite simple solution exist – give them text of all necessary rules and/or force them to attend a lecture given by some member of IT department (to save money as external specialist costs much more). However, as shown before, simple solutions often have questionable efficiency, and this one is no exception. Such approach, while in theory OK, fails in practice. The main reason seems to be users' lack of interest in such activities, thus their participation is usually only formal one. Why is it so?

In looking for answer to the question another survey [2] may be of some help. Particularly, when asked about responsibility for security, 57% of respondents admitted partial responsibility, while 31% of respondents think that ordinary user is not responsible for security at all. This is quite a high percentage, especially when compared with security specialists' expectation (100% for user's partial responsibility, see [2]). Naturally, one cannot expect much enthusiasm for security education when number of people believes that security "is not their business".

Computers security at its beginning was usually presented as restricted area where only a few technically competent computer specialists were allowed in. Seems that years of focusing on technical aspects of security backfire now as ordinary users feel no need to be involved in IS security matters. 'But I am no computer guy so I cannot be held responsible for security of IS' is quite a standard excuse when one try to appeal to users for a bit more security-conscious behavior.

On the other hand real life readily offers numerous examples of frequent ordinary users' inability to grasp even the basic security best practices or to exhibit some 'logic' when it comes to use of computers – at least when seen from computer professional's point of view. Numerous real-life stories told by experienced IT professionals about behavior of a certain fraction¹ of users

¹ It seems that there is no authoritative research done to estimate how big portion of users exhibit such properties, but numerous system administrators and members of IT departments I asked for their assessment independently of each other estimated that about 10-15% of their users are „hopelessly incapable“ to effectively work with computers... while another 15-20% of users overestimate their computer skills and act accordingly - without feeling a need to consult IT department. Both groups represent clear security risk.

further strengthen the feeling that users are generally dumb and unable to comprehend even their role in IS security. As a result many IT professionals resign to further involvement of users in security measures and turn themselves to technological means as these seem to be more comprehensible than users and their behavior. Others continue in their fight but usually without visible success – and not just because of poorly covered contempt for users' ability to deal with IT.

It appears that the central, more general, problem here is a communication gap between IT/information security professionals on one side and ordinary users (and managers as well) on the other. An independent observer even after a short time should be able to point out to quite important weakness in IT professionals' stance – while they are right in that IS security cannot be achieved by pure technological means and that management and users must be involved as well, they usually fail when they have to communicate that to the other side. It appears that in the IT professionals' arsenal of tools some very important items are missing, e.g. empathy towards ordinary users and their needs, knowledge of management jargon, patience, knowledge of modern management methods, communication skills, etc. Consequently they cannot win if what they try to communicate the other party perceives as naive, passing too much responsibility to the party, expensive or just unintelligible.

3. DO USERS EVEN KNOW WHAT THEY CAN DO FOR SECURITY?

When talking about users' involvement in the secure operation of an IS one's chance to be convincing enough are better if he is able to provide some more details in a way understandable even by ordinary users. One has to keep in mind that ordinary users still perceive security as something technical, and that deep specialized knowledge on IT is necessary to be involved there. Thus the first step should be to explain that **they can contribute to the practical IS security even by making less errors and mistakes and by better understanding what they are doing when they work with IS.**

However, not every IT professional has the communication skills that attract attention of the listening party and it is a sad fact that this is often neglected when the instructor is to be chosen. Empathy helps here, informal talks in light, humorous tone to small groups of users seem to appeal to users better than dry scholarly lectures. Various interesting and humorous real-life stories seem to score the best – even ordinary user is more likely to remember dangers of information leak through careless use of standard office tools

when this threat is illustrated on real (or real-life looking) story, e.g. how someone through analysis of a document made available on a web discovered hidden comments, deleted parts, etc.

Internet is a rich source of various stories, proverbs, funny wisdoms, etc. that may be used to explain users their role in IS security, essence and reasons behind various security practices and procedures, even security principles. One just need to have in mind that exactness is not priority here and rather than strict scientific approach the goal is to communicate the message in easily understandable way. That is, a story told for educational purposes need not be strictly true, it just need to sound plausible enough ... and if possible also kindly humorous.

Example: *instead of dry instructions on how to manage passwords in a secure way one can explain basic principles e.g. by the following paragraph found on the Internet – "Passwords are like underwear: don't share them, hide them under your keyboard, or hang them from your monitor. Above all, change them frequently"*

Of course one has to have in mind that ordinary users are not IT specialists, thus it is not enough just to point out to some threat, but they must also be instructed how to avoid or minimize impact of such threat. For example in addition to explaining of what kind of passwords are "bad" one has to offer also a couple of easily manageable procedures that help to pick and remember "good" passwords.

4. WHAT ELSE CAN BE DONE?

What we have described above is just the basics, but important one. Nor all users are necessarily bad, lazy or dumb ... often they just need to comprehend how they may contribute to the overall IS security. Of course there always be users that resists even such approach.. But the fundamental goal here is not to achieve absolute, 100% security as this is in fact impossible in our imperfect world – what we want in practice is to reduce risks to some acceptable level, and reducing the probability of users misconduct contributes to that goal. The key lies in IT professionals' understanding and accepting users' limits and willingness to help them. But one need not to restrict such effort to education only, as one can help users also by devising ways and interfaces that guide them to the more secure use of IT tools. This promising area of research in security is still developing, but already provided interesting results – for a list of relevant works see e.g. [3].

5. CONCLUSION

There are no doubts that security cannot be achieved purely by technological means and that users have to be taken into account as well. Command-like style of managing users fails in practice. Change of a way how IT/information security professionals view users seems to be the key to more successful involvement of users in security matters – accept that users are not, and apparently never become, specialists in IT or security matters, and adapt your requirements to that fact. Be diplomatic, be creative, and above all be patient as here one deals with humans, not machines.

6. REFERENCES

- [1] Ernst & Young (2003), "Czech Information Security Survey". PSIB'03, DSM – data security management, NBU.
- [2] J. Vyskoc, L. Fibikova (June 15-16, 2001): "IT Users' Perception of Information Security". Proceedings, IFIP WG9.6/11.7 conference "Security and Control of IT in Society" - SCITS-II, Bratislava. available also on <http://www.vaf.sk>.
- [3] A. Whitten's bibliography of HCI Sec.
- [4] <http://www.gaudior.net/alma/biblio.html>