Competing against human failing

M.E.M. Spruit

Traditional information security is heavily relying on physical and logical security measures and motivated people. When the effectiveness of information security is unsatisfactory, the traditional approach is to focus on improving security means on one hand and motivation of people on the other hand. Nevertheless, such an approach does not work well in many situations. Usually, the influence of human aspects is underestimated considerably. In this paper we present a way to deal with the human aspects of information security, using ideas from organisational psychology and incident analysis.

1 INTRODUCTION

More and more people are involved in information security, directly or indirectly. Therefore, it is very important that everybody knows his or her responsibilities with respect to information security. This of course applies to people playing a key role such as managers and security officers, but it also applies to all people playing a less prominent role. They all have their own responsibilities and everybody should take that responsibility. Nevertheless, many users, system administrators, and others do not comply to agreements and procedures with respect to information security. And many managers do not take their responsibilities with respect to information security. This positively will result in security breaches.

Traditional information security aims for solving such problems by strengthening the security measures and improving the security awareness. Furthermore, the emphasis is on detection of offences and punishment of culprits. This approach is considerably less effective than we might expect beforehand. Marginal improvements are usually obtained by information campaigns, awareness campaigns, instruction flyers, and so on. And despite strengthened security measures, the security discipline is violated time after time.

The question is whether it really is so difficult to let people act consistent with information security needs. To answer this question we first focus on human behaviour and the factors that influence behaviour. Subsequently we focus on human failing and how to prevent this.

2 HUMAN BEHAVIOUR

Behaviour is everything a person is doing or saying. Behaviour is determined by the person's characteristics and by the environment that makes a given behaviour possible or even enforces a specific behaviour. We distinguish between two kinds of behaviour (Robbins, 1992; Bernstein et al., 1994):

- unconscious behaviour;
- conscious behaviour.

2.1 Unconscious behaviour

Unconscious behaviour is characterised by automatic actions. These actions usually are the result of a long learning period. Examples are walking, reading, etcetera. But daily actions in the job can also become more or less automatic.

Automatic actions usually are performed relatively reliable. However, in exceptional situations the environment requires different actions. In those situations automatic actions lead to failures easily.

There are two ways to change unconscious behaviour. The first way is to *make the unconscious behaviour conscious*, so that it is possible to change behaviour just like other conscious behaviour. The other way is to enforce specific behaviour by *modification of the environment* such that the required behaviour is the most logic or even the only possible behaviour.

The *alertness* influences the adequacy of unconscious behaviour. The alertness can be improved by the following aspects:

- The work needs to be a challenge.
- The work should provide enough variation.
- There should be sufficient possibilities to relax.

2.2 Conscious behaviour

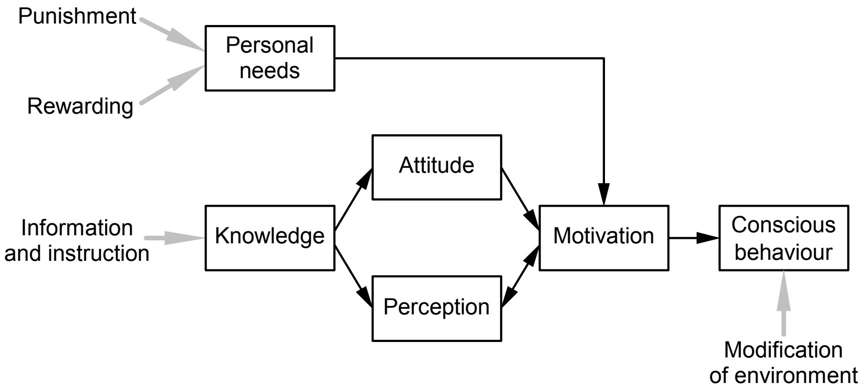

Figure 1 Factors that influence conscious behaviour.

Conscious behaviour (see Figure 1) is influenced by motivation, that is the will to do something. Motivation in its turn is influenced by perception of the environment (‘What can be done?’), attitude with respect to information security (‘What has to be done, in my opinion?’) and personal needs (‘What do I profit?’). Another way to influence behaviour (similar to unconscious behaviour) is to enforce specific behaviour by *modification of the environment* such that the required behaviour is the most logic or even the only possible behaviour.

Both perception and attitude are influenced by knowledge of the subject, information security. Furthermore, motivation can have a positive effect on the perception (increasing the alertness). One can increase knowledge of a specific subject by means of *information and instruction*. This is of course effective only when the present knowledge is insufficient. Note that increasing the knowledge can be contra-productive, because it learns people unwanted actions that are possible.
The personal needs have a direct relation with motivation. To comply to the needs (*rewarding*) the motivation can be influenced positively. To discourage unwanted behaviour by *punishment* is less effective.

To optimise motivation the following aspects are important:

- *Reasonableness* (Metaal, 1997). People want explanations for measures that are implemented and actions they have to perform. If explanations are unsatisfactory, or even absent, motivation decreases.
- *Expectancy* (Robbins, 1992; Luthans, 1984; Vroom, 1964). The motivation to perform depends on the strength of an expectation that the action will be followed by a given outcome, and on the attractiveness of that outcome. The outcome has to be related clearly to the action required, and alternative actions must not be rewarded.
- *Equity* (Robbins, 1992; Luthans, 1984). People perceive the outcomes of their actions in relation to what they put into it. They compare the input-outcome ratio with relevant others. The result of this comparison has impact on motivation.
- *Conformity* (Bernstein et al., 1994; Robbins, 1992; Asch, 1955). Group members like to be a full member of the group. Therefore, people conform their behaviour to that of other group members. People particularly conform to persons in which they recognise a certain authority (hierarchy or skills).

Generally the effectiveness of rewarding and punishments are overestimated. One reason is that it is effecting conscious behaviour only. Another reason is that the motivation of employees usually is rather good. Unlike what many people think, average employees are intrinsically motivated for their jobs and they are aware of the information security needs. However, security rules are often unclear and inadequate.

3 HUMAN FAILING

Actions can lead to security breaches. The majority of security breaches is caused by human failing (Spruit and Looijen, 1996). Some actions can lead to a security breach directly (direct failing), other actions seem to be correct but nevertheless they lead to a security breach (indirect failing). Most security breaches are not the result of malice intention (Spruit and Looijen, 1996).

3.1 Direct failing

Figure 2 shows the scheme of direct failing. A person with a given state of mind makes a failure (conscious or unconscious) which leads to a disturbance. Without adequate security measures the result is a security breach.

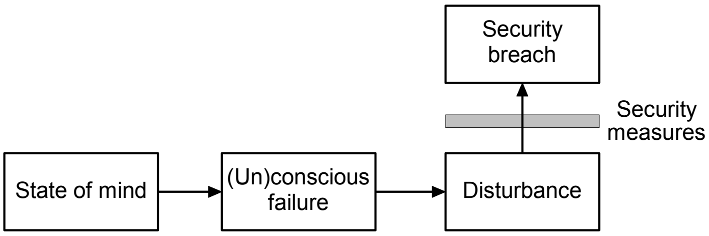

Figure 2 Direct failing.

We can recognise different kinds of failing. For example, deleting a data file by accident is quite different from stealing data deliberately. Therefore we distinguish, similar to the distinction between unconscious and conscious behaviour, between failing in unconscious behaviour and failing in conscious behaviour. Based on Reason (1990) we recognise the following kinds of human failing:

- Failing in unconscious behaviour:
  - *Slips*. Automatic actions that are wrong in the given situation.
  - *Wanderings*. Failures caused by flagging of concentration.
- Failing in conscious behaviour:
  - *Mistakes.* Actions that would be correct in another situation, but not in the actual. Mistakes are based on a wrong perception of the environment.
  - *Offences*. All actions where rules are violated deliberately.
    - Offences in good faith:
      - *Single offences* usually happen when the situation is exceptional and the rules are not applicable anymore.
      - *Frequent offences* are violations of rules that usually are unclear or inadequate. It is not exceptional that such violations are implicitly permitted as long as no problems arise.
    - Offences in bad faith:
      - *Criminal offences* are offences like theft, hacking, etcetera.

3.2 Indirect failing

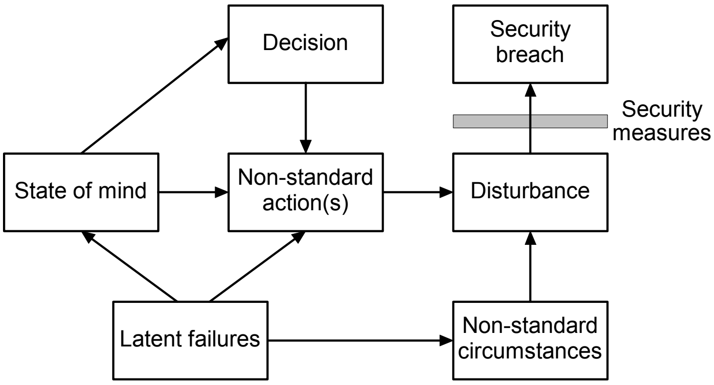

Figure 3 Indirect failing.

Human failing can be the result of a concurrence of circumstances. Decisions or actions that seem to be correct lead to a security breach nevertheless. The scheme in Figure 3, based on Groeneweg (1996), shows the arising of a security breach out of a concurrence of circumstances. A certain decision in a specific situation results in a security breach. Other decisions do not result in such a security breach. Neither does the given decision when the circumstances are different. We illustrate the scheme by using an example:

> An employee has to finish a proposal, to get an important order. However, at 5 p.m. he hasn't got as far as that. His boss pushes him to work overtime, and thus he works deep into the night. When he leaves the building he has forgotten to switch off his PC. Usually that wouldn't be a problem, as the security guard will do this on his round, but the guard already did his round. Early next morning a cleaning person finds the PC, and he copies the proposal. Later on it appeared that a competitor was able to get the order by being a little bit cheaper.

How is it possible that the decision to work overtime (*decision*) results in the loss of an order (*security breach*). The decision was quite normal, given the circumstances. However, we can point out a couple of unfavourable circumstances, like the pressure of time and the lack of adequate arrangements for working overtime (*latent failures*). When the employee left the building, he was very tired (*state of mind*), and so he forgot to switch of his PC (*non-standard action*). The security guard already did his round and therefore he could not switch off the PC (*non-standard circumstance*). Because of this concurrence of circumstances a cleaning person could easily copy valuable data (*disturbance*). Use of encryption (*security measure*) could reduce the damage. However, the data was not encrypted, so the security breach was a fact.

Usually a huge number of non-standard actions and circumstances are possible. Therefore it is hardly useful to identify and eliminate all potential non-standard actions and circumstances. Direct influence of the state of mind is even more difficult. However, the identification and elimination of latent failures, and the implementation of additional security measures are very well possible. So, to prevent security breaches to happen as a result of a concurrence of circumstances we have to focus on elimination of latent failures and implementation of additional security measures.

4 PREVENTION OF HUMAN FAILING

Most security breaches are the result of various kinds of human failing (Spruit and Looijen, 1996). Only a small number of those breaches are caused by people with malice intention. Most failures or offences occur in spite of good intentions. Many breaches are even the result of such a concurrence of circumstances that we cannot speak of failures or offences anymore (Groeneweg, 1996). Nevertheless many traditional security campaigns focus on the prevention of offences. A more effective approach against human failing consists of the following phases:

- Eliminate latent failures.
- Eliminate slips, wanderings and mistakes.
- Eliminate offences.

- Implement additional security measures.

4.1 Elimination of latent failures

In the example above we saw that a normal decision (to work overtime) could result in a serious incident (loss of an order). The key persons in that scenario could hardly be blamed for their behaviour, as they couldn't assess the potential consequences. So it makes no sense to improve their security awareness. In fact, the only effective way to prevent such a bad concurrence of circumstances to happen is to deal with the concurrence at source, that is to eliminate latent failures. In the example the latent failures can be eliminated straightforward:

- Pressure of time: A better planning and distribution of work decreases the need for working overtime.
- Lack of adequate arrangements for working overtime: Working overtime requires an adequate place of work, equipped with possibilities to relax and security services during night hours.

Of course, many more latent failures are possible. To look for latent failures in a structured way, Groeneweg distinguishes the following areas of attention (Groeneweg, 1996):

- The structure of the organisation and its management.
- The design of the whole plant and its equipment.
- The availability and applicability of equipment and tools.
- The availability and adequacy of operating procedures.
- The availability and adequacy of maintenance procedures.
- The communication lines between employees, departments and divisions.
- The management of conflicting objectives, like time pressure versus security.
- The quality of the working environment (temperature, noise, etcetera).
- The maintenance of the working environment.
- The skills of employees.

One has to examine each of these areas carefully to look for latent failures. Eliminating all latent failures that were found, reduces the probability that employees will initiate actions or circumstances that can lead to unwanted consequences.

4.2 Elimination of slips, wanderings and mistakes

In many circumstances, including their job, people perform automatic actions (unconscious behaviour). When circumstances allow automatic actions, or even ask for such actions, it usually is not effective to prevent this. If modification of automatic behaviour is necessary, it might be more effective to modify the environment such that the behaviour which is the most logic, or even the only possible, matches the behaviour which is required (*Modification of environment*).

An advantage of automatic actions is that they are performed relatively reliable. The disadvantage is that the adaptability to exceptional circumstances is rather low.

If exceptional circumstances are possible then it might be necessary to get rid of the automatic components of the behaviour (*Make the unconscious behaviour conscious*). This however is much more difficult than it sounds. Moreover, it is difficult to prevent the employees forming new automatisms in the new environment.

To prevent unconscious failing and mistakes as much as possible, employees need to be alert (*Alertness*). Therefore the job needs to be a challenge, it should provide enough variation, and there should be sufficient possibilities to relax.

4.3 Elimination of offences

Offences in good faith

Single offences usually happen if the situation is exceptional and the rules are not applicable anymore. In such situations one has to check whether violation of a rule is justifiable. If so, one can consider to modify the given rule. However, a specific rule usually cannot be adequate in any exceptional situation. Therefore it might be a good choice to leave a rule, which is clear and feasible, unchanged although it is not perfect. If violation is not justifiable, then one should look for the reason of violation. Probably the offender didn't know the specific rule. In that case the rule has to be made known (*Information and instruction*).

Frequent offences are violations of rules that usually are unclear or inadequate. Usually it is widely known that such rules are not (anymore) adequate, and violations are generally accepted. In such situations other rules that are still adequate might be ignored as well. This of course doesn't improve the credibility of the management with respect to information security.

Integration of information security with other processes in the organisation, will improve employee's compliance to rules with respect to information security. It is important that security measures and procedures are implemented such that they don't require people to behave very different than they are used to (*Modification of environment*). One can even consider to modify procedures such that violation is not possible anymore. Anyhow, it should not be possible to do a job better or faster by working around specific security measures or procedures (*Expectancy*). In the first place this requires that the contents of each measure that will be implemented, and the consequent behaviour that is required from the employees, must be made very clear to the employees (*Information and instruction*). It is moreover very important that employees are convinced of the usefulness (*Reasonableness*). Since employees conform their behaviour to that of others, one has to take care that all measures taken and the corresponding behaviour are broadly supported, and that the management has to set a good example to others (*Conformity*).

Offences in bad faith

In case of minor offences ('Everybody does it!') the sense of values with respect to information security has to be improved. Employees must learn the right values (*Information and instruction*). Since employees conform their behaviour to that of others, one has to take care that the values are broadly supported, and that the management has to set a good example to others (*Conformity*).

In case of serious offences the major objective usually is to become much richer, or to cause considerable damage to the organisation. In such cases the motivation is already completely wrong, so it is not useful to influence the motivation in a subtle way. This kind of offences should be made impossible by taking measures (e.g. separation of jobs) which can prevent that one person gains considerable (financial) profit, or cause considerable damage (*Modification of environment*). If one cannot rely completely on such measures one has to add monitoring and prosecution measures (*Punishment*).

4.4 Implementation of additional security measures

In the example mentioned earlier an operational disturbance (the copying of valuable data) resulted in a security breach (the loss of an order). The resulting damage could be reduced considerably by using a simple security measure, namely automatic encryption of data files. Note that this should be done in such a way that employees do not get more passwords to remember.

In general, additional security measures prevent disturbances to escalate and become security breaches. Examples are: encryption, backup, logging, etcetera.

5 CONCLUSION

To get adequate information security, people has to act consistent with information security needs. However, you cannot make an omelette without breaking eggs, so failures will be made. Furthermore, external people might make failures, deliberately or not. Protecting against any human failure is very complex. A major reason is that a human failure is not just a human failure. There are several kinds of failures possible. Each of them has specific characteristics and therefore requires a specific approach, as described in this paper. Although most human failures are not the result of malice intention, many traditional information security programs focus on this kind of failures. Moreover, one often tries to trace back a security breach to somebody who made a failure, so he or she can get all the blame. In first instance it seems strange that such an approach, including punishment of the culprit, appears to be successful many times. However, in most situations this is more a matter of statistics: the probability that two similar security breaches will occur in a short period of time is very low. So, whatever measures are taken after a security breach, they always seem to be successful to prevent a similar security breach to happen again. This does not mean that the organisation is protected against slightly different failures and subsequent security breaches.

The information security approach described in this paper differs from the more traditional approach in the fact that it takes into account the complexity of human behaviour and the corresponding kinds of failing. Although this approach does not come up with completely new measures, it leads to a more consistent set of security measures which aim to protect against the broad spectrum of human failing. Furthermore, this approach provides a sound basis which can be used to evaluate the adequateness of measures implemented.

In general we can say that many information security programs do not spend enough effort on sifting the complexity of human behaviour and the consequences for human failing and the protection against it. Paying more attention to the human aspects can considerably improve the effectiveness of information security.

6 REFERENCES

Asch, S.E. (1955) Opinions and social pressure. *Scientific American*, 193, 31.

Bernstein, D.A., Clarke-Stewart, A., Roy, E.J., Srull, T.K. and Wickens, C.D. (1994) Psychology. Houghton Mifflin Company, Boston.

Groeneweg, J. (1996) Controlling the controllable. DSWO Press, Leiden.

Luthans, F. (1985) Organizational behavior. McGraw-Hill, New York.

Metaal, N. (1997) Motivatie wordt weer met een hoofdletter geschreven (In Dutch). *De Psycholoog*, 32, 17.

Reason, J.T. (1990) Human error. Cambridge University Press, Cambridge.

Robbins, S.P. (1992) Essentials of organizational behavior. Prentice Hall, Englewood Cliffs.

Spruit, M.E.M. and Looijen, M. (1996) IT security in Dutch practice. *Computers & Security*, 15-2, 157.

Vroom, V.H. (1964) Work and motivation. John Wiley and Sons, New York.