Human Error

and

Information Security

Marcel E.M. Spruit

Department of Information Systems
Delft University of Technology

April 2000

TUDelft

Abstract

Traditional information security relies heavily on physical and logical security measures. When information security proves to be unsatisfactory and security incidents happen, the usual response of people and organizations is to strengthen the existing physical and logical security measures.

However, this underestimates the impact of human behavior on information security. Information security relies heavily on adequate functioning of people involved. Most security incidents are the result of human errors.

Improve people's knowledge about information security is not sufficient to prevent security incidents. Adequate protection against human error requires understanding of human behavior and the factors that cause errors, as well as knowledge on what security measures are possible and appropriate to prevent errors.

This paper presents a description of the human aspect in relation to information security and measures that prevent human error and thus improve information security.

Keywords

Information security
Risk management
Human behavior
Human error
Indirect error
Countermeasures

Introduction

Information systems and the information they contain are of vital importance for organizations. For that reason information security is highly important. Despite this, the information security requirements are violated again and again. Many users, system administrators and others do not act in accordance with agreements and procedures with respect to information security. And many managers do not take their responsibilities with respect to information security. This results in security breaches.

Traditional information security aims at solving such problems by improving the physical and logical security measures. Furthermore, the emphasis is on detection of violations and punishment of culprits. This approach is considerably less effective than one might expect. Actions to improve people's knowledge about information security have marginal effects. And despite strengthened security measures, the security discipline is still violated.

The question is whether it really is so difficult to make people act in accordance with information security needs. To answer this question, this paper first focuses on human behavior and the factors that influence behavior, and subsequently on human error and how to prevent this.

Human behavior

Behavior is everything a person does or says [Bernstein et al., 1994; Robbins, 1992; Spruit, 1999]. Behavior is determined on the one hand by the person's characteristics and on the other hand by the environment that enables, encourages, enforces, or blocks specific behavior (see Figure 1). The environment influences the person's characteristics, for example the person's knowledge and experience. This in turn influences the person's interpretation (perception) of the environment and therefore the person's behavior. The person's behavior can influence the environment, for example by modifying it, but the behavior can also influence the personal characteristics of the person, for example the person's experience.

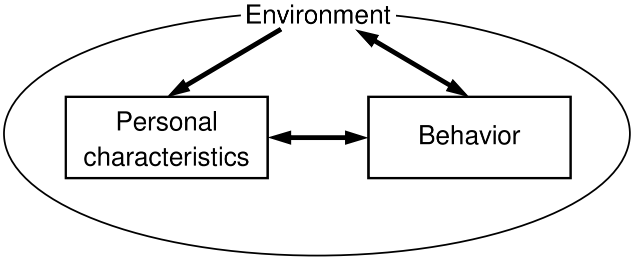

Figure 1: Model of behavior.

Behavior is made up of two components: *unconscious behavior* and *conscious behavior* (see Figure 2). Both can be influenced by the environment, for example because certain behavior is enforced or blocked. Therefore, one can influence unconscious and conscious behavior by *modification of the environment*. For example, one can enforce specific behavior by modifying the environment in such a way that the required behavior is the most logic or even the only possible behavior and that unwanted behavior is blocked. Modifying the environment includes modification of human-computer interfaces to increase the ease of use and to prevent errors.

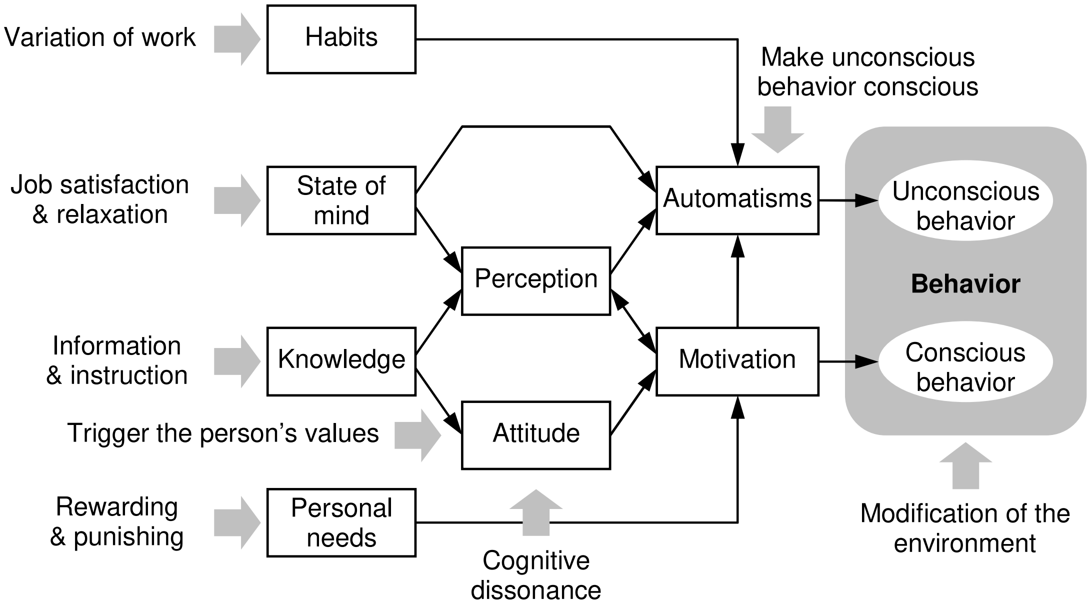

Figure 2: Factors that influence behavior.

Unconscious behavior is characterized by *automatisms* (automatic actions) which are based on habits. *Habits* are the result of a long period of learning and sinking in (e.g. walking, reading, speaking, etcetera), but may also result from daily activities on the job which are performed repeatedly. Activation of habits is influenced by the *state of mind* (emotion) of the person concerned and the person's *perception* (the observation and interpretation) of the environment.

Automatisms usually result in the expected outcome as long as the environment does not change and there are no exceptional situations which require different actions. However, if the environment changes or requires different actions, then automatisms easily lead to errors.

It is possible to influence unconscious behavior by *making unconscious behavior conscious*. Consequently the resulting behavior can be influenced, just like other conscious behavior. Another way to influence unconscious behavior is by *variation of work*, which obstructs the growing of habits. Habits that do not exist, cannot be activated.

Last but not least, the *state of mind* (emotion) is an important control of unconscious behavior. The state of mind is influenced by *job satisfaction and relaxation*.

Conscious behavior is influenced by *motivation*, that is, the will to do something. Motivation in its turn is influenced by the person's *perception* (the observation and interpretation) of the environment ('What can be done?'), by the person's *attitude* (opinion) with respect to information security ('What has to be done, in my opinion?') and by the person's *personal needs* ('How do I profit from it?'). We discriminate between *intrinsic motivation*, which is based on the person's perception and attitude that is already present within a person ('inside'), and *extrinsic motivation*, which requires an external incentive like a reward ('outside').

Perception, or the person's observation and interpretation of the environment, influences the person's motivation, but the person's motivation can in turn have a positive effect on the perception by increasing the person's alertness, which results in an improved interpretation of the environment.

Attitude, or the person's opinion about the environment, also influences the person's motivation. The attitude itself is strongly influenced by the person's values. These values have grown over a lifetime and cannot be changed by others easily. However, in an organization one can *trigger the person's values* and let the person take the necessary actions in accordance with these values. For example, explaining the reasonableness of certain measures may convince the person to comply with these measures.

Another way of influencing attitude is by making use of *cognitive dissonance*. This is based on the fact that an inconsistency between a person's behavior and attitude creates discomfort. If there is an inconsistency, known as cognitive dissonance, the actual behavior could hardly be denied afterwards, so the person will change the attitude to reduce the inconsistency [Bernstein et al., 1994; Festinger, 1957]. Cognitive dissonance can be used to change a person's behavior by applying delicate pressure to provoke behavior that is not in accordance with the person's attitude. As a result the person will adjust the attitude in such a way that it matches the behavior. Afterwards, the changed attitude will again result in the new behavior. However, only slight changes in attitude are possible. Furthermore, the pressure applied should be so delicate that it is not experienced as manipulation, because then the effect may be contrary.

Both perception and attitude are themselves influenced by the person's *knowledge* of the subject: information security. One can increase knowledge by means of *information and instruction*. This has to be tailored to the individual needs, as people generally let their own interests come first. Of course, information and instruction are only effective if the present knowledge is insufficient. Note that increasing the knowledge can also be contra-productive, because it may also teach people unwanted actions.

Personal needs influence the person's motivation as well. Complying with the person's inner needs (*rewarding*) can improve the (extrinsic) motivation. Discouragement of unwanted behavior by *punishing* is less effective. Generally the effectiveness of rewards and punishments is overestimated. One reason is that it affects only conscious behavior. Another reason is that the (intrinsic) motivation of employees is usually rather good. Unlike what many people think, average employees are intrinsically motivated to do their jobs well and they are aware of the requirements of information security. However, security rules are often unclear and inadequate.

With respect to motivation there are some preconditions to be considered:

- Related to *intrinsic motivation* (specifically attitude):
  - *Reasonableness* [Bernstein et al., 1994]. People want explanations for measures that are implemented and for actions they have to perform. If explanations are unsatisfactory, or even absent, motivation decreases. Motivation also decreases if measures are applied wrongly by others, or imposed actions repeatedly lead to undesired results.
  - *Conformity* [Bernstein et al., 1994; Robbins, 1992; Asch, 1955]. Group members like to be a full member of the group. People therefore conform their behavior to that of other group members. This decreases with anonymity within the group, and it increases in ambiguous situations and in relation to subjects about which the group is unanimous. People particularly conform their behavior to that of persons in whom they recognize a certain authority (based on hierarchy or skills).
- Related to *extrinsic motivation* (specifically rewards and punishment):
  - *Expectancy* [Robbins, 1992; Luthans, 1985; Vroom, 1964]. The motivation to perform well depends on the strength of the expectation that the action will be followed by a given outcome, and on the attractiveness of that outcome. The outcome has to be clearly related to the action required, and alternative actions must not be rewarded.
  - *Equity* [Robbins, 1992; Luthans, 1985]. People perceive the outcomes of their actions in relation to what they put into it. They compare the input-outcome ratio to the ratio achieved by other people whom they consider comparable. The result of this comparison has impact on motivation.
  - *Continuity* [Bernstein et al., 1994]. Discourage (punishment) of undesired behavior is only effective if there is adequate supervision. People return to their old (undesired) behavior as soon as the supervision stops.

People look for benefits (rewards) within a limited range. They are very susceptible to benefits on the short term, even if that is at the expense of much larger benefits on the long term. Furthermore people usually focus on their immediate surroundings, at the expense of affairs far away. In short, people’s behavior is ruled by short-term profits within their own neighborhood. However, security campaigns often focus on long-term targets. This is probably the reason why security campaigns are usually not effective: they require a sacrifice on the short term to yield profit on the long term. To improve people’s motivation with respect to information security, one has to explain the long-term targets, but additionally one has to examine whether the short-term pros and cons are well balanced. People will only exhibit the necessary behavior if the balance between short-term pros and cons is advantageous for them, while the preconditions mentioned above are also met.

Human error

People make errors and errors can lead to incidents. The majority of incidents with respect to information security are caused by human errors, although they usually are not the result of malicious intent [Spruit and Looijen, 1996].

Figure 3 shows the basic scheme of human error. In a certain environment a person makes an error (conscious or unconscious) which results in an incident. For example, an employee deletes the entire customer file instead of only one customer record by accident. In the absence of security measures, repairing the damage of such a mistake may require significant cost and effort.

There can be a delay between the actual error and the manifestation of the incident. For example, when a maintenance mechanic forgets to switch on the uninterruptable power-supply system after maintenance (human error), it takes until the next power failure before the connected equipment crashes (incident).

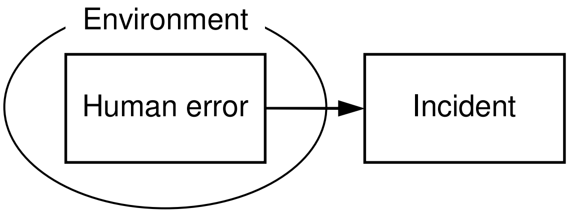

Figure 3: Direct error.

We can recognize different kinds of error. For example, deleting a data file by accident is something quite different than stealing data on purpose. Based on the work of Rasmussen [Rasmussen, 1986] and Reason [Reason, 1998] we distinguish the following kinds of human error:

- Error in unconscious behavior (referring to routine activities):
  - *Slips*. Automatisms that are wrong in a given situation. Slips can be caused by interruption of routine activities, or by the presence of a strong habit.
  - *Lapses*. Necessary actions which are not executed. Lapses can either occur when people miss a signal from the environment (inattention, indifference or external distraction), or when people forget something (out of sight, out of mind).
- Error in conscious behavior:
  - *Mistakes.* Actions that might be correct in another situation, but not in the actual situation. We discriminate between:
    - *Rule-based mistakes*, which are mistakes in familiar procedures applied to frequent decision-making situations. These mistakes relate to a wrong perception of the environment.
    - *Knowledge-based mistakes*, which are mistakes in unknown problem-solving situations. These mistakes relate to insufficient expertise.

- *Violations*. All actions where rules are violated deliberately. We discriminate between:
    - Violations in good faith:
        - *Single violations* usually happen when the situation is exceptional and the rules no longer apply.
        - *Routine violations* are violations of rules that are usually unclear or inadequate. It is not unusual that such violations are implicitly permitted as long as no problems arise.
    - Violations in bad faith:
        - *Criminal violations* are acts like theft, hacking, sabotage, etcetera.

In Figure 2 we have seen that there are several types of measures which can be used to influence behavior, and thus human error. Table 1 shows the potential impact of different types of measures on each type of human error. It is clear that *modification of the environment* is very effective, as any type of error responds to this type of measure.

Error type Type of measure	Slips	Lapses	Mistakes	Violations
Modification of the environment	●	●	●	●
Make unconscious behavior conscious	●	–	–	–
Variation of work	●	O	–	–
Job satisfaction & relaxation	–	●	O	–
Information & instruction	–	–	●	O
Trigger the person's values	–	–	O	●
Cognitive dissonance	–	–	–	O
Rewarding & punishing	–	–	–	●

●	Significant impact
O	Some impact
–	Negligible impact

Table 1: Effectiveness of types of measures per error type.

Prevention against human error

Most incidents are the result of several kinds of human error [Spruit and Looijen, 1996]. Only a small number of those incidents are caused by people having evil intentions. Most errors occur in spite of good intentions. Nevertheless many traditional security campaigns focus on the protection against violations, and especially on those carried out with malicious intent.

A more effective approach focuses on the whole spectrum of human error and consists of the following:

- Elimination of slips and lapses.
- Elimination of mistakes
- Elimination of violations.

Elimination of slips and lapses

In many circumstances, including those of the workplace, people perform automatisms (unconscious behavior). The advantage of automatisms is reliable performance. The disadvantage is low adaptability to exceptional circumstances and changes of the environment. When circumstances allow automatisms, or even ask for them, it is usually not effective to prevent that they are used. If modification of unconscious behavior is necessary, it might be more effective to modify the environment such that the behavior which is the most logical, or the only behavior possible, matches the behavior which is required (*Modification of the environment*).

If changes in the environment or exceptional circumstances might arise, it can be necessary to get rid of automatisms (*Make unconscious behavior conscious*). However, this is much more difficult than it sounds. Moreover, employees may well form new automatisms in this new environment (*Variation of work*).

To prevent lapses caused by inattention one must assure the work provides enough job satisfaction and sufficient possibilities to relax (*Job satisfaction & relaxation*). The prevention of lapses that occur when things have been forgotten can only be combated by making use of measures which offer signaling functions, like the (automatic) diary, tool-supported procedures, checklists, (automatic) supervision, team work, etcetera (*Modification of the environment*).

Elimination of mistakes

Mistakes can occur either in familiar situations (rule-based mistakes) or in situations which are unknown (knowledge-based mistakes). Both types of mistakes can be prevented by modifying the environment in such a way that procedures are convenient and the required behavior is the most logical, or even the only possible kind of behavior (*Modification of the environment*). Furthermore, employees can be supported by decision-support tools or other knowledge tools.

The cause of rule-based mistakes can be a wrong perception of the environment or a misjudgment of the situation. Both perception and judgment can be improved by effective alertness, which requires work that provides enough job satisfaction and sufficient opportunities to relax (*Job satisfaction & relaxation*). A misjudgment of the situation can also be based on insufficient expertise. In that case the knowledge on the subject has to be improved (*Information and instruction*).

Knowledge-based mistakes are generally based on lack of expertise in a given situation. The probability of making this kind of mistakes can be decreased by enhancing the expertise (*Information and instruction*).

Elimination of violations

Violations in good faith

Single violations usually happen if the situation is exceptional and the rules are no longer applicable. If violation of a rule has occurred, one has to check whether the violation was justifiable. If so, one can consider modifying the rule. However, a specific rule cannot be adequate for any exceptional situation. Therefore it might be a good choice to leave unchanged a rule that is clear and feasible even if it is not perfect. If the violation is not justifiable, then one should look for the reason of the violation. Probably the offender did not know that specific rule. In that case the rule has to be made known (*Information and instruction*).

Routine violations are violations of rules that are unclear or inadequate. Usually it is widely known that such rules are not (no longer) adequate, and violations are generally accepted. In such situations other rules that are still adequate might be ignored as well. Of course this does not improve the credibility of the management with respect to information security.

Integration of information security with other processes in the organization will improve the employee's compliance with rules on information security. It is important that security measures and procedures are implemented such that they do not require people to behave very different than what they are used to (*Modification of the environment*). One can even consider modifying procedures such that violation is no longer possible. Anyhow, it should be impossible to do a job better or faster by working around specific security measures or procedures (*Expectancy*) and management should never apply double standards (*Equity*).

The contents of each measure to be implemented and the behavior that is required from employees as a consequence, must be made very clear to the employees (*Information and instruction*). Moreover, it is very important that employees are convinced that the measures are useful (*Trigger the person's values: Reasonableness*). Since employees conform their behavior to that of others, one has to take care that all measures taken and the corresponding behavior are broadly supported, and that the management sets an example (*Trigger the person's values: Conformity*). If one or more key figures in the organization are not convinced of the necessity of information security, it is worthwhile to try to have them explain the necessity of the measures to others (*Cognitive dissonance*).

Violations in bad faith

In case of minor violations ('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*) and management should not apply double standards (*Equity*). The values need to be broadly supported and the management needs to set an example (*Trigger the person's values: Conformity*). Key figures who are not convinced of the necessity of information security might be mobilized to explain the necessity to others (*Cognitive dissonance*).

The major objective for committing serious violations is usually material gain or the desire to cause considerable damage to an organization. In such cases the motivation differs widely from the normal situations, so influencing the motivation in a subtle way is not possible. This kind of violation should be made impracticable by taking specific measures (e.g. separation of jobs) that prevent that one person can gain considerable (financial) profit or cause considerable damage (*Modification of the environment*). If one cannot rely completely on such measures one has to add monitoring and prosecution measures (*Punishment*). Monitoring measures should never be idle in a discernible way (*Continuity*).

Indirect error

The most obvious relation between human errors and incidents is that an error directly results in an incident. However, it is also possible that a specific human action only results in an incident by a concurrence of circumstances. It even is possible that the action is usually correct, but that only in an exceptional situation it results in an incident. This is referred to as indirect error.

Figure 4 shows the basic scheme of indirect error. In a certain environment that has been influenced unfavorably by a latent error, a person makes a (direct) error, which results in an incident. The latent error can be a (latent) human error, a non-standard circumstance, or a combination of these two.

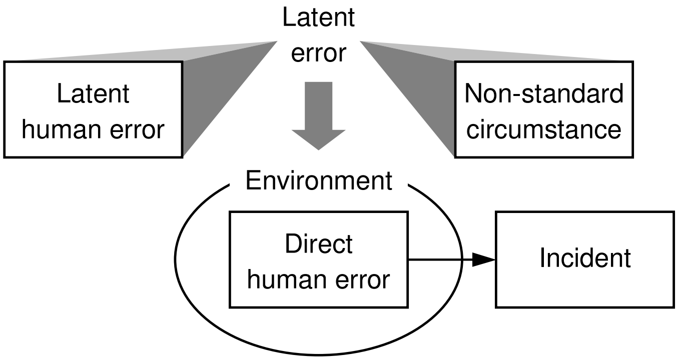

Figure 4: Indirect error.

Examples of latent errors are:

- A manager assigns an employee to a task that is too difficult (latent human error: a mistake), so the employee executes the task wrongly (direct error: a mistake).
- An employee detects a virus in an important file (non-standard circumstance); he panics and deletes the complete file in order to get rid of the virus (direct error: a mistake).
- The start of a blaze (non-standard circumstance) frightens the employee responsible for the backup procedure such that he forgets to take along the backup tape (direct error: a lapse).

Many severe accidents were caused by circumstances in which several latent errors in succession created a situation in which one (direct) error or action resulted in the final accident. For example, the error that caused the crash of a Piper private plane into an Aeromexico plane in 1986 was only fatal because it was built on the errors of three other people; by then the situation had grown so unsafe that only one more error (of the Piper pilot) resulted in a disaster, which killed 82 people [Neumann, 1995].

In a situation of indirect error the direct error can be considered as the drop that makes the cup run over. The direct error can even be a decision or action which is normally correct, except in the situation created by latent errors. Nevertheless it is common practice to put all the blame on the person responsible for the action that led to the incident directly, deservedly or not. For example, the Piper pilot responsible for the final (direct) error in the situation of the Aeromexico crash was blamed for the accident.

Two mechanisms of indirect error can be distinguished:

- A latent error initiates a direct human error, which results in an incident.
- A latent error creates a situation in which a certain action (the direct human error) will result in an incident.

Both mechanisms can be illustrated in one example, which shows how the quite common decision to work overtime at home can result in the loss of an order:

Situation: An employee has to finish a proposal for an important order. However, at 5 p.m. he has not got as far as that. He is not in the position to work overtime at the office, as his wife is not at home and the baby-sitter is ill; he has to take care of the children. Considering the situation, he decides to finish the proposal at home, so he takes along all relevant data on a floppy disk. Unfortunately, on his way home a pickpocket steals his wallet containing the floppy disk. Later on it turns out that a competitor was able to get the order by bidding a little bit cheaper.

Interpretation: Taking a floppy disk with confidential data is a (direct) error (single violation), resulting in the disclosure of confidential data by the pickpocket. But at least two latent errors can be pointed out: the pressure of time, and the lack of adequate arrangements for working at home. The first one illustrates the first indirect error mechanism, because the pressure of time caused a shortage of time, which was the motive for taking along data for working at home. The second latent error illustrates the second mechanism, as this error did not lead to the incident directly; it only created an unsafe situation in which an error could have severe consequences.

Elimination of latent errors

The example with the pickpocket showed that a normal decision (to work overtime at home) could result in a serious incident (disclosure of confidential data). The key person in the scenario could hardly be blamed for his behavior, as he could not have foreseen the potential consequences. So it makes no sense to improve his security awareness. In fact, the only effective way to prevent such a bad concurrence of circumstances from happening is to deal with the source of the concurrence, that is, to eliminate latent errors. In the example the elimination of the latent errors is straightforward:

- Pressure of time: better planning and distribution of work decreases the need for working overtime.
- Lack of adequate arrangements for working at home: if an adequate place to work with a secure connection to the office has been installed, it is not necessary to take along confidential data.

Of course, many more latent errors exist. Figure 4 shows that security measures against latent errors generally have to deal with both latent human errors and non-standard circumstances. A range of security measures against direct human errors is available. As latent human errors are also human errors, the same kind of measures is effective to prevent latent human errors. In fact latent human errors only differ from direct human errors in the sense that for latent human errors at least one more error is required before they result in an incident. Prevention against non-standard circumstances is usually not feasible. Therefore, when dealing with latent errors, one should focus on security measures against (latent) human errors. Since a considerable number of latent human errors is based on mistakes and routine violations, measures against those kinds of errors are especially relevant for combating indirect error.

The manager who neglects security issues because he is not convinced information security is necessary is a special example of a latent human error (a knowledge-based mistake). As a result of this error employees can cause incidents, for example by violations. However, it is not clear beforehand whether the manager can be blamed for his attitude because he faces a dilemma [Reason, 1998]: to emphasize production, or security (see Figure 5). In the long term these are clearly compatible, but on the short term they may give rise to conflicts because the required resources (personnel, finance, time, etcetera) are limited. Allocation of resources to production will increase the production at the expense of reliability (security), and the other way round. Managers generally tend to attach more importance to production than to security. Two factors aggravate this tendency:

– Resources allocated to the pursuit of production have relatively certain outcomes; those allocated to enhancing security do not, at least not in the short term.

– The feedback generated by the pursuit of production is generally positive, unambiguous, direct and highly reinforcing; that associated with the pursuit of security is largely negative, intermittent and often ambiguous and deceptive.

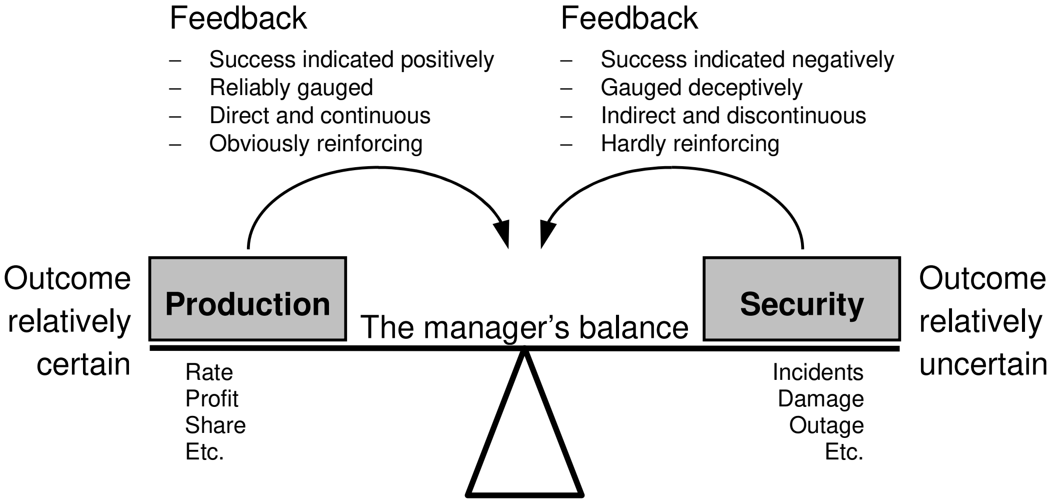

Figure 5: The manager's dilemma.

To prevent that managers disturb the balance with respect to information security, one has to provide adequate information concerning security. It is likely that managers whose strategies show an imbalance do not get the right information on security incidents or other relevant information on security. Most managers will be interested in information security if adequate information on security issues is offered.

Discussion

Information security aims at protecting information systems and the information they contain against a variety of threats. Although this paper focuses on the danger of human error, information security has to cope with other threats too, like natural disasters (lightning, floods, earthquakes, etcetera) and technical failures in hardware, software, or the infrastructure. Such threats can directly cause a security incident, but they can also act as non-standard circumstances inducing (indirect) human errors. Adequate information security takes into account all possible threats. Some threats can be averted by relatively simple and straightforward measures. For example, a malfunction in the power supply can be settled simply by using an uninterruptable power-supply system. Protection against human errors, however, is a complex task on all counts. Unfortunately, the majority of threats concern human errors.

Adequate information security makes use of preventive measures as a first line of defense, as well as additional measures as a second line of defense. Additional measures can prevent that minor incidents escalate into major incidents. Examples are: encryption, backup, disaster recovery, etcetera. To illustrate a second line of defense we refer to the example with the pickpocket mentioned earlier. In the example a certain error (taking along confidential data on floppy) resulted in an incident (disclosure of confidential data). The damage could have been reduced considerably if a simple additional security measure had been taken, like automatic encryption of data files. Of course this should be done in such a way that employees do not have to memorize a lot of passwords.

Conclusion

People contribute to each business process, including information security. Unfortunately, people make errors. Protecting information systems and the information they contain against human errors is very complex. A major reason is that there is not simply one kind of human error; several kinds of errors are possible. Each of these has specific characteristics and therefore requires a specific approach, as described in this paper. Although the majority of human errors is not the result of malicious intent, many traditional information security programs focus on this kind of errors. Moreover, often attempts are made to trace back an incident to somebody who made an error to assign blame. At first it seems strange that such an approach, including punishment of the culprit, appears to be successful. However, in most situations this is more a matter of statistics: the probability that two similar incidents will occur in a short period of time is very low. So whatever measures are taken after an incident, they always seem to be successful to prevent that a similar incident happens again. This does not mean that the organization is protected against slightly different errors and subsequent incidents.

The information security approach described in this paper differs from the more traditional approach in that it takes into account the relevance and complexity of human behavior and the corresponding kinds of errors. Although this approach does not come up with completely new measures, it leads to a more consistent set of security measures geared at protection against the whole spectrum of human error. Furthermore, this approach provides a sound basis which can be used to evaluate the adequateness of measures implemented.

Generally information security programs are not built to deal with the complexity of human behavior, the consequences of human error and the protection against it. Using knowledge on the human factor can considerably improve the effectiveness of information security.

References

Asch, S.E. (1955). Opinions and social pressure. *Scientific American*, 193 (5), 31-35.

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

Festinger, L. (1957). *A theory of cognitive disonance*. Row Petersen, Evanston.

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

Neumann, P.G. (1995). *Computer related risks*. Addison-Wesley, New York.

Rasmussen, J. (1986). *Information processing and human-machine interaction*. Elsevier Science, Amsterdam.

Reason, J.T. (1998). *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), 157-170.

Spruit, M.E.M. (1999). Competing against human failing. *Proceedings of the IFIP TC11 14th international conference on Information Security (SEC '98)*, 392-401.

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