JON ØLNES
NORWEGIAN COMPUTING CENTRE
NORWAY

**DEVELOPMENT OF SECURITY POLICIES** *F3*

# Development of security policies

Jon Ølnes

Norwegian Computing Centre (NR), P.O.Box 114 Blindern, N-0314 Oslo, Norway

E-mail: Jon.Olnes@nr.no

**Abstract**

A security policy is a total plan for the security of an enterprise. The policy must be well planned and duly balanced with respect to required and sufficient security. There is no pre-defined answer for *your* company. The policy must be founded on the (unique) organisation and culture of the enterprise in question. This paper discusses the various stages of a method for development, implementation and maintenance of security policies, with emphasis on the organisational and human aspects of security.

Keywords: Security policy, organisational aspects, human aspects, policy development method

## 1 Introduction[1]

Data security is a hot topic in public media, and to be honest, a lot of what is written is nonsense. (Of course, there is a lot of sensible stuff too, but to tell the difference one often needs a high level of competence.) A typical article focuses on *one* threat, rising a lot of fuss about possible dangers related to this threat and "absolutely necessary" countermeasures against it. At one instant, we are all being invaded by crackers, while the next moment we run the risk of virtually being killed by virii. Stories like these are probably good for the sales records of the more or less coloured (professional and other) press, but they are not good for anything else.

Do not get me wrong: data security *is* important, and I believe in statements that the subject is not taken seriously enough by a lot of enterprises. However, if one sets out to do something about security, a random approach - casual measures based on press stories or other sources - is not going to work well. There are very few absolute truths in data security. One of the few is that "a chain is not stronger than its weakest link". By using a random approach, one runs the risk of introducing countermeasures that can be likened to a fireproof door in a wooden wall - expensive, and with little or no effect. A well balanced security policy should encompass all parts of an enterprise. In this paper, I will mainly discuss data security.

Another statement, which is almost an absolute truth, is: "there is no pre-defined answer for *your* company's security policy". Almost, because some enterprises with high security requirements may be subject to detailed rule-sets governing their security. It goes without saying that enterprises of various sizes and purposes usually will have widely different security requirements. Even comparable enterprises may differ a lot in organisation, culture and generally in the way they do their work. It is possible to learn from others, but not by taking over their solutions without criticism.

There are two key-words concerning a correct level of security: "required" and "sufficient". We all know that if security is too lax, the result can be of severe consequence to the enterprise. However, most enterprises exists not only to be secure, but to perform useful work. By overemphasising security, one may seriously hamper productivity, through unnecessary overhead, or because people do not feel comfortable with the conditions they work under.

1. This paper is written in an unusual (for a scientific paper) personal style. This reflects a conclusion of the paper, that no single answer exists for development of security policies. The contents of the paper should be taken as my personal view, which can hopefully provide others with food for thought.

The single most important prerequisite for a well balanced and efficient security policy is common sense! This goes for all the numerous decisions that must be taken during the process. The next prerequisite is to have a good general view of the situation of the enterprise, as a basis for introduction of effective countermeasures based on a cost/benefit analysis. This work has to be carried out individually for each enterprise, but preferably using a well defined *method.*

# 2 Method for security policies

The figure on the next page gives a rather detailed view of one possible method. This is my version of a well-accepted procedure which, with some variations, can be found in a lot of books and papers.

Again, it is important to emphasise that this is not *the* answer, and I encourage the readers to remain critical to this as well as anything else presented in this paper. My intention is to pinpoint the importance of having a methodical approach to development, implementation and maintenance of a security policy. Which methodology one chooses, is probably of less importance, as long as the choice is well founded.

Referring to the figure, during the development phase for the security policy, one starts from the top, and proceeds until one is left with an acceptable risk. Next, the policy is implemented by placement of responsibilities, and implementation of the security measures selected. Documentation is especially important during this phase. The lower part of the figure represents the phase of normal operation and maintenance, where on special events, one has to return to stages of the development or implementation phases.

# 3 What is security?

A generally accepted definition of security cannot be found. Some position papers, like "Green Book on the Security of Information Systems" by the Commission of the European Communities, and "Guidelines for the Security of Information Systems" by OECD, characterise security by three parameters: availability, correctness / integrity, and confidentiality. This gives a very broad definition, encompassing topics some of us would prefer to categorise under "safety" or "reliability". Regardless of the definition selected, the points below can be useful as parts of a characterisation of the term security:

- Security is a part of the total quality of an enterprise.

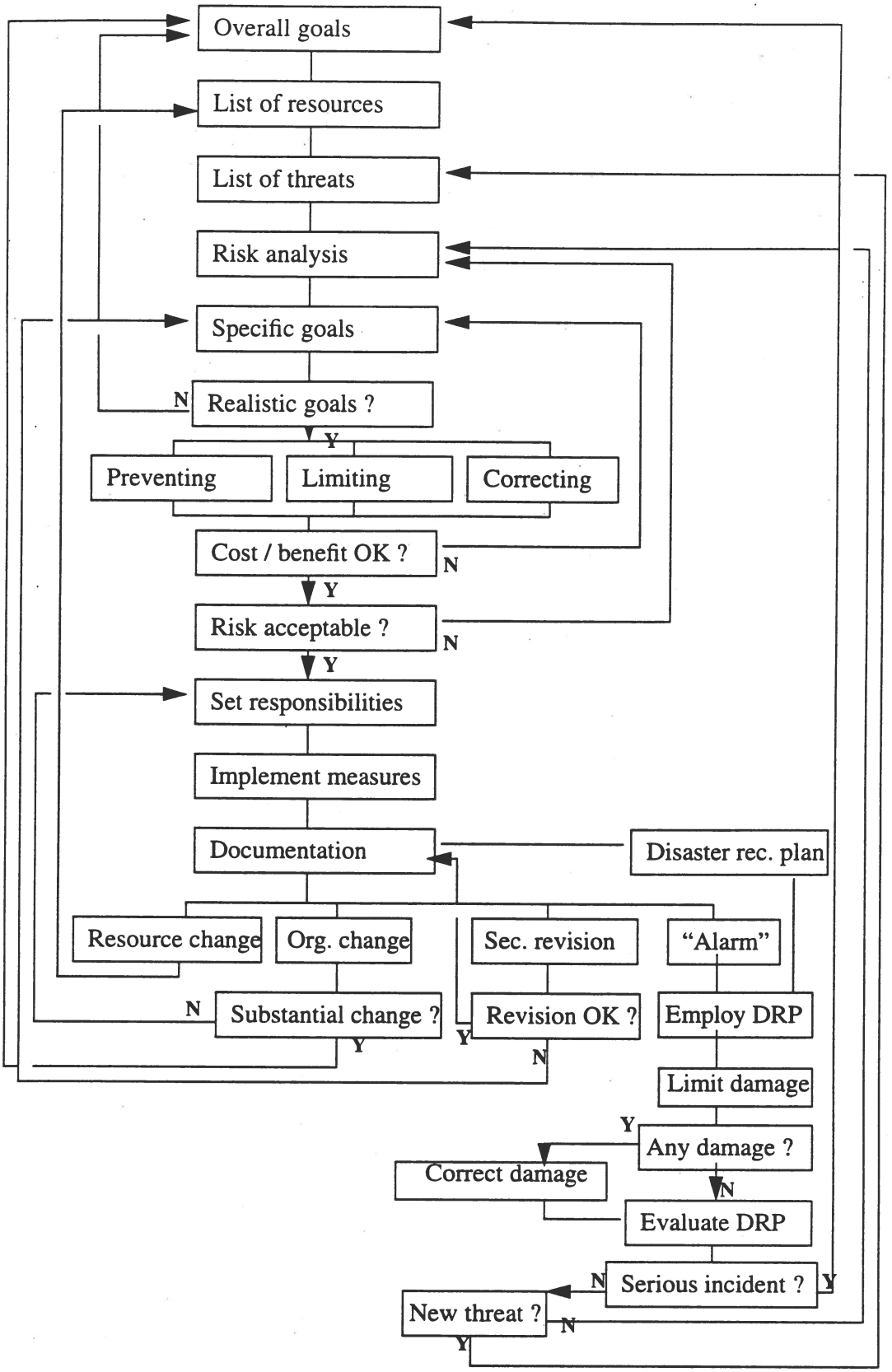
Very few aspects of security contribute directly to the quantitative results of an enterprise (although some may do, like stability of computer equipment). However, if one is concerned about quality assurance, security should be an aspect of this work.

- A lack of breaches to security is no evidence that security is sufficiently taken care of.

Most security countermeasures take effect only when special events happen. If the countermeasures are inadequate, such events may have disastrous effects. It is possible to be lucky for a very long period of time. Inadequate security can be likened to running a business without insurance.

- Every security measure introduces security risks.

This may sound controversial, but a few examples may explain the statement. Use of passwords for access control, introduces risks related to password administration. Countermeasures which constrain the activities allowed by employees, imply increased risk that some employees may circumvent the constraints. Increased availability of resources may cause threats to confidentiality. The effect of a security measure is the sum of a positive and a negative component.


Overall goals
List of resources
List of threats
Risk analysis
Specific goals
N
Realistic goals ?
Y
Preventing
Limiting
Correcting
Cost / benefit OK ?
N
Y
Risk acceptable ?
N
Y
Set responsibilities
Implement measures
Documentation
Disaster rec. plan
Resource change
Org. change
Sec. revision
"Alarm"
N
Substantial change ?
Y
Y
Revision OK ?
N
Employ DRP
Limit damage
Y
Any damage ?
Correct damage
N
Evaluate DRP
N
Serious incident ?
Y
New threat ?
N
Y

- Security has its prize.

Direct costs in terms of money spent, and side effects like reduced performance of equipment due to extra overhead, are some aspects of this. In many cases the main cost will be reduced efficiency due to more cumbersome work procedures and constraints placed on the employees. 100% security is impossible, and costs increase sharply as one approaches this limit. Cost/benefit evaluations are crucial to obtain a suitable level of security. Note that some measures for increased availability and correctness may in fact save more costs than the amount spent on them.

# 4 Overall goals

At the very beginning of the process of developing a security policy, it is necessary to determine approximately which level of security one should aim for. Usually one knows quite a lot about which resources must be considered as vital, and which threats one is exposed to, and whether this suggests that a high level of security is needed.

In most cases, the enterprise is responsible for its own security, and runs the risk alone. However, frequently there are customers involved, who may impose their security requirements on the supplier. In yet other cases, laws and regulations may dictate certain security measures, e.g. concerning treatment of personal data.

Thoughts must be given to possible consequences of a breach in security. Direct economic loss due to extra expenses, reduced efficiency, or maybe even cancelled contracts, is the first issue which comes to mind. Legal prosecution and claims for compensation are also possible. Long-term effects due to negative publicity and possibly a weakened position in the market should be taken into account. In some cases, the very existence of an enterprise may be threatened.

Following such initial thoughts, some overall goals for the security work may be defined. Some of these goals may be quite specific, while others will be in terms of points to be investigated in further work. A scenario approach, where consequences of a few typical security related events are studied, may be useful.

One quite specific goal is determination of allowable consequences of a breach in security, e.g. what is an acceptable interrupt from (nearly) normal operation following a fire, a serious theft or an equipment breakdown?

Another example of an overall goal concerns confidentiality of data:

- Everything is in principle available to everybody, and exceptions are made only where necessary. This may be suitable in an university environment, or in a small company where everybody works on approximately the same topics.
- Access to resources is granted only when explicitly needed ("need to know" principle). In larger enterprises, this will often be the only sensible approach.

Other important decisions to be made at this stage are: determination of the time frame for the security work, budget and assignment of resources for the work, and how to organise the work.

# 5 Survey of requirements

## 5.1 Resources

The resources of an enterprise may be grouped into four categories: human resources / competence, localities / infrastructure, equipment, data / information. For all categories, it is necessary to survey vital resources. Usually, a grouping or a further classification will be done to simplify the picture.

Data and information is the most complicated resource category to survey. Assignment of sensitivity levels, as done for defense or national security purposes, is one possibility but often this may not be suitable. Note that different representations of data must be considered: on-line accessible, disks and floppies, backup copies, printouts on paper.

One advantage of modern computer technology is that the equipment itself is rarely a critical resource. Provided that a proper insurance and adequate agreements with the supplier are in place, equipment may be replaced within a reasonably short time. However, loss or damage to equipment will often cause loss or damage to data.

## 5.2 Threats and risks

Frequently, in security literature, one runs into statements like: "then a risk analysis is done", concealing the fact that this may very well be the most complicated part of the security work.

The ideal situation is a complete list of all security relevant events that may happen, including their probabilities, and the damage they will cause. This is an impossible task. In most cases, it is very difficult to survey threats and risks, and chances are that some threats are overlooked or over-focused. Probabilities of security events, and estimates of the damage that may result, have a high uncertainty. Still, it is necessary to obtain a picture of the threats and risks one is exposed to.

A first step may be to imagine the consequences of a breach in security with respect to a resource for the enterprise. Then, a coarse list of events that may cause such a breach, and some statements about their probability may be compiled. A division into accidental breaches, like human errors, fire, power failure etc., and deliberate breaches, like theft, fraud, sabotage, cracking etc., may be helpful.

This task may be repeated several times in order to refine the list, following a gradual development of a better understanding of the problems by the persons performing the analysis.

Determination of risks and consequences related to deliberate threats will typically be more uncertain than analysis of accidental threats. An evaluation of possible sources of deliberate attacks (employees or outsiders, casual attackers or aggressive competitors), and what the attacker can gain from a successful attack, is useful.

Usually, one will start to plan for actual countermeasures already at this stage of the work.

## 5.3 Specific goals

The survey work ends with specification of more detailed goals concerning the security of the enterprise. Some goals are quantitative, as availability of computer equipment in percentage of total time, or: "in case of a severe fire, we shall be operating almost normally in new localities within x days". Other goals, especially for protection against deliberate attacks, can only be described in more general terms. It is important to document which threats one chooses not to consider, usually because their probability is low. E.g. nuclear war will not be considered by a majority of enterprises.

The goals must be realistic. If a preliminary conclusion is that the overall goals are too ambitious, or should be more ambitious, or the amount of resources dedicated to the security work is wrongly specified, one has to revise the overall goals.

# 6 Selection of countermeasures

## 6.1 Characterisation of countermeasures

Roughly speaking, three main categories of countermeasures exist:

- preventing, to prevent incidents from happening;
- limiting, to discover and possibly cut off incidents;
- correcting, to repair the damage done after an incident.

Within each category, there are again three types of countermeasures:

- physical, typically related to buildings and other environments of the enterprise;
- logical, like passwords or other means for access control to computers;
- administrative, which are work procedures and routines, and rules for behaviour.

The three types go together. As an example, if it is decided to lock the door to a room, rules will be defined for access to keys and to the room.

All categories must be planned. One important correcting measure is restoration of data from backup. This of course depends on the availability of the backup copies. Note that most countermeasures encounter more than one threat.

Almost all literature on security policies include a list of different physical and logical countermeasures which "have to" be implemented. In many cases, the whole publication consists of this list, without any further explanation. My view is that there are very few "have to" security measures, and the relative importance of different measures may vary a lot from one organisation to another. Thus, no list of technical countermeasures is given here, just a few points which are important in nearly all cases:

Even enterprises with very low security requirements will need proper routines for backup. At regular intervals, backups should be taken and stored at a location some distance away from the computers.

Keep your system free from errors and weaknesses! This sounds obvious, but it is not easy in practice. Many organisations lack the necessary competence, and this goes for a lot of providers as well. In addition, many providers will try short-cuts to save time and money. Many programs and systems have known security relevant bugs (which may have been corrected in later versions), and the art of system configuration is full of caveats. Thus, selection of competent providers becomes an important security measure, unless the organisation itself is highly competent.

The system configuration should be kept as simple as possible, and unnecessary functionality avoided. "Divide and conquer" if your system gets complicated, e.g. by placing critical functionality in separate network segments or separate computers.

Physical and logical countermeasures are not broken, they are circumvented. It is possible to ensure that users have to choose good passwords, and that they have to change their passwords frequently, but this is of little use if the passwords are written down and tacked to the screen.

## 6.2 The human factor

For most enterprises the employees are the most important resource, and the most important security threat. One severe problem is that security measures counteracting human actions, tend to be a lot more controversial than technical measures.

The importance of a security conscious and motivated staff cannot be overemphasised. People will simply not accept restrictions in their daily work unless they see that the restrictions are sensible and necessary. Strong restrictions that are not accepted by the employees, will simply not be followed. Even if they are strictly enforced, the dissatisfaction and opposition that may be raised, will in itself constitute a security threat.

Hence, it is absolutely necessary to engage the whole organisation in the security work, preferably during the development phase, and at least during the implementation phase. Feedback on what is regarded as acceptable or not, must be taken seriously. It is probably a prerequisite that the employees learn, and accept, to regard themselves as a security threat, but also that each employee sees his/her role in the efforts to avoid security incidents. Information and education are important preventive countermeasures. Try to establish work routines and a company culture on: "this is the way (or not the way) we do things here".

Motivation tends to decrease with time, as well as the eagerness to follow established routines. Measures to keep the security consciousness high are needed.

Concerning deliberate attacks, like theft and sabotage, it can be stated that dissatisfied and disloyal employees are the most important threat, and the most important countermeasure is to run a proper policy for staff treatment. Attacks by intruders are for the time being a minor threat to most enterprises, but regarding data security, such threats are going to grow in importance, following increased use of public and private computer networks.

It is a paradox that even computer systems with high security requirements need maintenance staffs which are given full privileges to system and data, including data to which they should normally have no access whatsoever. Systems which restrict the privileges of the maintenance personnel, should be requested.

## 6.3 Cost/benefit and risk evaluation

As stated: security has its prize. Security countermeasures should be selected based on a cost/benefit evaluation. This is a difficult task. The costs implied by a given measure can be calculated in most cases, but potential costs which may result from omitting the measure (i.e. the benefits), are difficult to estimate. If the costs exceed the resource limits set aside for the security work, it is necessary to revise the specific, or maybe even the overall, goals.

As a rule of thumb, the cheapest solution is to go for preventive measures. However, in some cases it may be more beneficial not to protect against less likely threats, and run the risk of paying for correction of possible damage instead.

No countermeasure can provide 100% security, and, as stated earlier, the introduction of countermeasures introduces new threats. After selection of countermeasures, it is therefore necessary to perform an evaluation of the remaining risks. If some of these risks cannot be accepted, a new round through specific goals and selection of countermeasures is necessary. As mentioned: risk analysis is a difficult task.

# 7 Implementation of security measures

## 7.1 Determination of responsibilities

Ultimately, the person responsible for corporate security is the top manager. Even if others are responsible for the actual security work, the top manager must be prepared to face the consequences of a severe security incident. The manager must ensure that the secu-

rity work is properly taken care of, and he/she must regularly collect information to be sure that the security awareness is maintained.

Large organisations may establish a special security department, which often will report directly to the top manager. In smaller enterprises, a few persons may be selected to form the "security department", in addition to their other work. These will take the responsibility for the security policy itself, and for ensuring that the policy is followed.

Responsibilities for more detailed tasks must also be determined. Often, such tasks will form a natural part of the daily work for, e.g., the staff department, the caretaker, or the system administrator for the computer equipment.

One very important responsibility is detection of events that must cause changes or revisions to the security policy. One may find many seemingly excellent security policies, where by closer inspection, one will find that the person in charge of some task left the company several months ago.

The security awareness of each single employee is important, but delegation of responsibilities to the effect that: "everybody is responsible for this", will rarely work. For example, I will claim that in most companies it is indefensible to leave backup of the PCs to the individual members of the staff.

## 7.2 Documentation

As all other quality assurance work, the security policy and the process which led to its definition, must be documented - countermeasures, responsibilities and rationale. The importance of documenting even measures one chooses not to implement has already been mentioned. It is clear that a lot of this information may be very sensitive with respect to availability, correctness and confidentiality. Protection of the security policy itself must be a part of the policy.

The biggest problem concerning documentation is that it tends to be covered in dust. Requirements for keeping documentation up to date have been stressed several times already in this paper, but even updated information is useless if the intended users of the documentation (which will typically be other persons than the ones updating it) have forgotten that it exists.

There is no simple answer to this problem. In a security context, this can be regarded as a part of the process of motivating the staff. Regular reminders on the security policy may be effective both to keep up the consciousness, and to point at existing documentation.

The documentation must encompass preventive, limiting and correcting measures. Some measures in the last two categories take effect only in the case of extraordinary events. These are parts of a "disaster recovery plan" for the enterprise.

# 8 Maintenance and daily operation

Like other activities concerning quality assurance, the security work is a lasting process, where a continuous evaluation of the need for changes and improvements is necessary. Certain events will cause such updates:

## 8.1 Change in resources

Resource changes will normally cause changes in security measures. When old resources are removed, measures may become unnecessary, while new equipment and new data may require the security policy to be updated. Thus, one must return to the survey of resources, and repeat the steps from there onwards considering the new situation.

Concerning availability and correctness, a policy for replacing old equipment and programs with new versions is important. New versions should not be used in production until they are stable. At the same time, old versions should be removed quickly to avoid disorder.

## 8.2 Organisational changes

Too often, when an incident occurs, one discovers that the person in charge of some task left several months ago. Changes in the organisation or the staff of an enterprise will almost always necessitate changes in the security policy.

Regarding simple changes in personnel (someone leaves, is employed, or is moved), the only necessary action is usually a reassignment of responsibilities. The new person in charge will of course need education and information. Substantial changes in the organisation may however imply a total revision of the security policy, perhaps even a revision of the overall goals for security.

## 8.3 Security revision

In quality assurance, periodic tests of the efficiency of the implemented measures are regarded as important. Likewise, the security policy and its effectiveness should be tested at regular (or irregular - one may for example simulate a "disaster situation") intervals. The most important effect of such revisions is to maintain and increase the motivation of the staff. The effectiveness of measures will increase when people are steadily reminded of their existence, provided this is not taken as unnecessary fuss.

Errors and defects which are discovered by a security revision, must of course be corrected. The evaluation of those parts of the security policy which are covered by the revision, should in all cases be documented.

# 9 Extraordinary events, disaster recovery plan

100% security cannot be obtained. There will always be a remaining risk of "alarms". Most such events are far from what one would normally call a "disaster", and should be treated through carefully planned limiting and correcting measures. Typical examples are mistakes by users of computer equipment, equipment failure, minor power breaks etc.

However, more serious incidents may also occur, like fire, theft, sabotage, intruders trying to gain access to computers etc. If the defense against such events is based on improvisation when the event occurs, one runs the risk of a real disaster. It is important to realise that it is impossible to plan in full details what is going to happen in extraordinary situations. However, when guidelines and principles are reflected in the disaster recovery plan, the chances of taking correct decisions on the fly will increase a lot. Exercises, either in the form of simulated events, or as paper exercises, may help to ensure that the awareness is kept high.

Important decisions to be documented in a disaster recovery plan, are who must be notified in the case of certain alarms, and who should take command. An almost military command system, where the "superior" makes the decisions, and takes responsibility for them, will frequently be an advantage in such situations. One should document guidelines for what actions a "subordinate" can take on his/her own initiative, until the person in charge can take over (for example: "all possible actions to stop an intruder in the system, including a power down of the equipment, but no corrective or other actions after the attack is fought back"). If the person in charge cannot be found, it should be made clear who can substitute him/her.

In almost all cases, the most important task is to limit damage, even if this may hamper an investigation of the sources of the incident. The next step will be to determine to what extent damage is done, followed by the necessary corrective actions.

Related to extraordinary events are guidelines for relations with public media - who is allowed to make statements, and what can be said? If one suspects that something criminal has happened, a decision must be taken on whether to investigate the matter or not, and in case, how much resources to spend on an investigation.

An "alarm" is a particularly realistic test of the disaster recovery plan. The experience gained from this test must of course be evaluated, and the plan must be updated wherever necessary. It may also be necessary to have a look at other parts of the security policy, e.g. to determine whether this was a threat that was forgotten when the policy was formed, or if the risk was underestimated.

# 10 Conclusion

Security is a part of the total quality of an enterprise. The purpose of this paper has been to present a method for development, implementation and maintenance of security policies. A methodical approach is a prerequisite for a well balanced policy. Security policies must live with the organisation - they need administration and maintenance.

Enterprises differ, and there is no single answer to the organisation of their security. Technical security measures are one side of the coin, but in most cases the human factor is more important - the engagement of the individuals working in the enterprise in the implementation of the security measures, as well as protection against threats from the same employees.

However, to reach an effective security policy, providing *required* and *sufficient* security, the most important prerequisite, for which there is no substitute, is *common sense*!

# 11 Acknowledgements

Throughout this paper, no references or citations are given. Of course this does not mean that this is all original work, only that no explicit base material was used during the preparation of the paper. I find it impossible, in retrospect, to trace all ideas back to their sources, and to determine when I know that the ideas are my own, if anyone else has thought of this ahead of me. However, two documents must be mentioned:

- Holbrook and Reynolds, "Site Security Handbook", Internet RFC 1244 (available from numerous sites for anonymous ftp)
- Fites, Kratz and Brebner, "Control and Security of Computer Information Systems", Computer Science Press, ISBN 0-7167-8191-3

Also, I owe a lot to numerous discussions with professor Sverre Spurkland at NR.