## INNEHÅLLSFÖRTECKNING

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2.</td>
<td>Development Trends in Computers</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>A Description of the Survey</td>
<td>6</td>
</tr>
<tr>
<td>3.1</td>
<td>Cathegorization of EDP users and how to find suitable representatives</td>
<td>6</td>
</tr>
<tr>
<td>3.2</td>
<td>Given premises</td>
<td>8</td>
</tr>
<tr>
<td>3.3</td>
<td>Method used in assembling the results</td>
<td>11</td>
</tr>
<tr>
<td>4.</td>
<td>Results of the Interviews</td>
<td>13</td>
</tr>
<tr>
<td>4.1</td>
<td>Requirements for protection</td>
<td>13</td>
</tr>
<tr>
<td>4.2</td>
<td>Level of fulfillment of requirements, today and within five years</td>
<td>17</td>
</tr>
<tr>
<td>4.3</td>
<td>EDP and the society</td>
<td>23</td>
</tr>
<tr>
<td>5.</td>
<td>A Personal Point of View</td>
<td>26</td>
</tr>
<tr>
<td>5.1</td>
<td>Social integrity</td>
<td>26</td>
</tr>
<tr>
<td>5.2</td>
<td>Security of investments</td>
<td>27</td>
</tr>
<tr>
<td>5.3</td>
<td>Reliability</td>
<td>27</td>
</tr>
<tr>
<td>5.4</td>
<td>Information security</td>
<td>28</td>
</tr>
<tr>
<td>5.5</td>
<td>Data quality</td>
<td>29</td>
</tr>
<tr>
<td>5.6</td>
<td>The availability via EDP of public data</td>
<td>29</td>
</tr>
<tr>
<td>5.7</td>
<td>The cost of computer security</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>31</td>
</tr>
</tbody>
</table>
ABSTRACT

The goal of COMPUTER SECURITY 1981 is to predict the demand for protection of electronic data processing (EDP) and for the information processed. To predict the future demands on computer security we have discussed the issue with several people involved in one way or another with EDP. These discussions, our own knowledge other background material have been the material for discussions amongst the authors. The results are divided into two parts. In the first part (section 4) we have been as objective as possible. In the latter part (section 5) we have discussed the differences between the results in section 4 and our own opinion as professional researchers.

In addition the report covers a summary of how EDP is used 1981 and a section describing the structure of the security field (which we have used in the interviews) and an outline of the investigation.
1. INTRODUCTION

The goal of COMPUTER SECURITY 1981 is to predict the demand for protection of electronic data processing (EDP) and for the information processed. The year 1981 is not meant to be exact, but merely a notion of "near future". The inspiration to perform this investigation came from Björn Rotsman of SAAB-UNIVAC. As a representative of a computer manufacturer he was interested in what effect the current discussion about the dangers of EDP and the invasion of privacy will have on the future customer specification of EDP systems. Technological developments, both hardware and software, the increasing use of EDP and the common knowledge about EDP will also affect the security requirements.

Although the investigation is supported financially and was done in cooperation with SAAB-UNIVAC the research group (the authors of this report) at Linköping University is solely responsible for the results and conclusions described in the present paper.

The security issue cannot be separated from the over-all data processing problem. Hence it is necessary in an investigation of COMPUTER SECURITY 1981 to discuss the development of EDP as such. This has been done in previous investigations by Swedish authorities (reference (1) and (2)). A summary of those results and results obtained by us during the investigation can be found in chapter 2.

To predict the future demands on computer security we have discussed the issue with several people involved in one way or another with EDP. We have tried to cover a broad spectrum of EDP applications. We have talked both to ultimate users of the EDP system and to EDP professionals. Each person involved has been introduced in our terminology and our classification of security problems. This is described in more detail in chapter 3, which also describes the structure of the investigation.
We have used the results of the discussions mentioned above as material for discussions within the group. With this background we have to the best of our knowledge predicted the requirements on computer security 1981. Along with the requirements we have predicted the degree to which these are satisfied. These results are described in chapter 4.

As the discussions in the group went on we realized that our own opinion as professional researchers in the field differs in some cases from the average. We feel that it is important not only to predict the most probable future, as is done in chapter 4, but also to publish our own opinion about which security problems are most important and how they can be solved. These more subjective results are covered by chapter 5.

The scope of this report is limited to computer security problems in Sweden. Thus we have not discussed problems connected with international data communication and information processing in other countries.
2. DEVELOPMENT TRENDS IN COMPUTERS

An attempt to predict the future development of computer systems can never result in anything but a subjective opinion. Thus in this section we try to limit the number of possible misjudgements by discussing factors only of relevance to data security. But let us first summarize the general trends.

In the first place a continuing increase in use of computers can be anticipated, both in regard to the number of computers and to the way they are used. Secondly data communication will increase and be made easier due to the introduction of data transmission networks. Thirdly batch processing is decreasing and is only used when it has advantages over real-time processing. Finally the tendency to distribute computer utilities and databanks will be increased. Altogether this will lead to a large increase of the number of terminals.

Factors governing development are technical achievements and economical considerations. In the technical field the years to 1981 are not expected to bring about any new revolutionary techniques. Hardware will be based on the techniques used today. It is inexpensive and will become even more so. However development of software is an expensive venture especially for complex systems as Data Base Managers and Operating Systems. Hence it is generally agreed that software will be the constraining factor in the development of new computer systems.

To enhance performance computers will be microprogrammable. One of the reasons being the possibility of providing structure sets adapted to different programming languages. Also new system architectures with distributed computational facilities will appear. Virtual memory techniques will become standard and back-end computers that manage communication with secondary storage will come as did front-end computers to handle data communication.
The most common processor architecture will continue to be of the uniprocessor type. But multiprocessor architectures will also be used mainly for real-time applications. To increase system reliability multiprocessors will be equipped with fail-safe facilities. Other architectures such as matrix processors and pipeline processors will be used but they will not become very common.

Processor architecture has influences on the possibility of implementing secure Operating Systems. Research in this area has showed the need to integrate design of processors and Operating Systems. Computers have been built along these lines of thought. However the great amount of money invested in existing software by the large computer manufacturers makes it improbable that they will produce such computer systems. Possibly small manufacturers will do so before 1981.

In software, database management will continue to be a field of development. Probably the main progress will be made in more effective storage principles but security related problems will also be considered. This leads us to expect that most administrative information systems will use database techniques in the early eighties. Another field in software is programming languages. The problem oriented languages of today will still be used in 1981. Yet an increase in the use of interactive languages will be evident. For system programming new high level languages will be developed partly because new programming techniques such as structured programming should be applicable.

At last we note the fact that micro-computers will make it possible to distribute intelligence in a way that has not been possible before. Micro-computers will be and are used to create a large variety of special purpose computers as well as small general computers and intelligent terminals. Such equipment can easily be connected to a central computer.
to make data exchange possible. Such a communication network will be star configured which in general will be the dominating type of computer network. The data transmission networks will not change this. The possibility of connecting computers with each other will not lead to multi-computer systems because of the lack of software. But a change in the use of data communication can be foreseen. Problem solving via connection to time-sharing systems will decrease because transmission cost will become high relative to the decreasing cost of computers. Data communication will mainly be used when large program systems or databases have several scattered users.
3. A DESCRIPTION OF THE SURVEY

3.1 Cathegorization of EDP users and how to find suitable representatives

From section 2 it is clear that the EDP field is very wide and should be expected to have grown considerably in five years. In order to get a sufficiently good overview of this field we have found it necessary to divide it into a number of significant classes each one representing a unique but typical system configuration. Our classes are:

I Direct response systems
II Batch oriented systems
III Systems for control and supervision
IV Hybrid systems

Our goal has then been to get a good picture of computer usage by finding one large- and one small-scale EDP-user within each class.

This technique means a sparse sampling over the broad EDP field but we believe that the cases which we have chosen strongly reflect our society and will do so even more five years from now.

3.1.1 Direct response systems

The first class of EDP systems consists of the so called direct response systems (sometimes "on-line" or "real-time"). These are characterized by interactive communication with the computer, meaning that the terminal which is used by the human being is in direct contact with the stored program in the machine. This leads to small turnaround times (orders of seconds). Still more characteristic is the fact that questions posed to such systems may only be taken from a very limited and well defined set. Some systems even have
specially made keyboards where a question is given only by pressing a button. In other cases it may happen that the allowed question structure is so complex that we prefer to regard it as a programming language (some time-sharing BASIC systems are examples of this).

As interesting representatives of the class of direct response systems we have chosen to concentrate on Police and Bank systems. In both these cases there exists rapid development toward real-time information processing.

An accountant at a small bank office and a police official represent the small-scale users. These are complemented by their respective main computer centers.

3.1.2. Batch oriented systems

A lot of EDP routines are not efficiently helped by direct interactive communication. Examples are monthly salary payments, statistical analysis or complex calculations. These routines are characterized by the fact that they are time consuming and/or involve lots of data. The results are often extensive and may mean a large printout from a lineprinter or microfiche equipment.

Such routines are best run in a batch environment which means that the program is given to the computer together with the data as an entity. Early computer systems were all of this kind. The input mostly consisted of a number of punched cards.

Batch systems of today get their programs from magnetic tape or discs while data still often comes from cards.

As representatives of this kind of computer usage we have chosen two service bureaus with considerable difference in size. The larger one serves large companies and governmental institutions while the smaller one serves small companies and firms.
3.1.3 Systems for control and supervision

A computer usage which is normally not considered an EDP application but should be involved in a discussion of data security is found in the control engineering field. These systems are used in industry for controlling industrial processes. Most of the required security is concentrated on reliability but some systems are so large and so important for society that security in a wider sense is of vital importance.

One example is the newly installed system at the Swedish Hydro-Electric power commission. The system (TIDAS) which has connections all over the country supervises the production and distribution of electrical energy. A lot of interesting properties are involved. One is that the system forms a large data net and as such is representative of a whole new class of future set-ups.

It may be expected that governments will use similar systems for duties like pollution- and traffic-control.

3.1.4 Hybrids

Computer applications that employ several of the abovementioned properties are grouped into the class of hybrids.

One example is the main computer centre used by the bank offices. Besides being used as an interactive direct response system at day time it is also used for batch processing at night. Still more contributions to this group are given by a hospital computer system and by some private companies.

Two of these are large, having their own computer centers. Also a small firm, typical of its group was chosen.

3.2 Given premises

A common starting point for this survey has been the actual reason for using EDP 1981. If EDP is to be used for a certain
purpose we expect the users (in a wide sense) to put demands on security. We will not take into account in this investigation whether a certain sophistication on the component level will be reached or not in 1981. Naturally we are not interested in solutions which are clearly unfeasable but we feel that it would stimulate system and component development if users stress security issues.

3.2.1 Structuring the concept of data security

This structure is based on [1]. We have made some modifications and additions to the model described in the reference. When discussing data security it seems natural to start with the actual information processing problem that is to be solved. Parts of this problem might be solved manually while other parts might need automatic processing.

A practical borderline between these methods is among other thing dependent on the demands that users will put on security. With users in this case we mean all those who are affected by the processing discussed. User demands may be divided into the following classes:

- social integrity
- security of investments
- reliability
- information security
- data quality

Social integrity means the user's safety that his social situation will not be changed in an unpredictable way.

Security of investment means the security of the actual investments being made to solve the information processing problem. Requirements will result in demands like fire and theft protection. In this survey we will only consider requirements regarding software investments.

Reliability regards the fact that demands will be put on the actual function to be performed. It must be correct and be
performed within a given time.

Information security means the security that the processed and stored information will not be changed, destroyed or lost in an unpredictable way.

Data quality needs a more thorough explanation. The input to the information process is characterized by the fact that an object is described by certain data. This data contains information which be used when drawing conclusions. Let us regard two different situations according to the following flow chart:

If the two conclusions drawn are equally good or bad then we say that the quality of DATA1 and DATA2 are equal. From this it is clear that data quality depends on how well the object is described in relation to the conclusion that is drawn. The quality related to some data is higher when that data describes a given situation better.

The way of judging data quality is thus to draw conclusions from various data sets followed by a comparison of the results.

In order to be able to fulfil the abovementioned security requirements these have to be traced down to demands regarding hardware, software, organisational methods and general protection.
3.2.2 Three scenarios

In addition to the previously given premises we consider three different possibilities regarding the public's opinion on a future computer based society.

The first case is one where the public is very critical of the use of EDP, only allowing use of computers in such cases where they are absolutely needed. Security aspects will play a dominant role in such an environment.

In contrast to this we also look upon a society where the public is unconcerned regarding the use of EDP. In such a case one would expect security aspects to be of minor interest.

Finally the third scenario considered is distinguished by a mainly positive view on EDP coupled to a concerned comprehension of how to use it. This is the situation that we consider to be the most likely.

3.2.3 Shaping the interviews

In order to get relevant information regarding use of EDP within the classes mentioned above, a number of interviews have been undertaken. Common to all these were that our general structure was presented beforehand. A number of basic questions concerning security and protection mechanisms were then posed. Most of the interview time was devoted to "free" discussions concerning aspects on future computer usage in relation to various scenarios.

Besides interviewing representatives of the various classes described we have also talked to politicians and other people working in governmental departments who are creative of public opinion.

3.3 Method used in assembling the results

As previously mentioned we have found that there is no need to present the actual interviews in detail. Rather it has
been our intention to find common points of view which bear high significance. This has been accomplished by numerous discussions of the material within the group.

The results will be presented in two ways. In section 4 the "down-to-the-earth" conclusions that are more or less easily drawn will be stated. Section 5 consists of our own opinions on security in EDP systems as they have developed out of this and earlier work in the field.
4. RESULTS OF THE INTERVIEWS

This section is divided into three parts. The first part presents the demands that were generally or fairly often agreed upon to be important during the interview. The second part deals with the fulfillment of these demands today and the expected improvements and changes within five years. The increasing use of EDP has strong effects not only on direct EDP environments but on the whole society as well. The effect on society might result both in new demands on EDP and in new laws or other changes that are not directly connected to computers. These effects are discussed in the third part of this section.

4.1 Requirements for protection regarding:

a) Investments

The security of hardware and storage media as physical entities is not stressed in this study. The techniques developed for other valuable installations and registers are valid here as well. Their implementation is just a matter of striking a balance between cost of protection and estimated cost and risk of destruction.

Investments in the development of programs and EDP systems are threatened by the rapid development of the EDP-field itself. Computers and computing techniques are fairly short-lived and when a new and better system is installed, sometimes nothing but the experience gained can be used from the old system. This has caused a demand for portability of programs, procedures and other subdivisions of an EDP-system. Preferrably a program or sub-routine written in a standardized computer language should be transportable to any computer without changes. In the same way every other interface should be standardized. The utter confusion of today in protocols and interfaces for peripherals and data communication links must be abolished and possibilities of connecting anything to any computer should be provided.
The preservation of investments in programs is sometimes also a question of protection from theft. This leads to demands on information security.

b) \_ \_ \_ \_ Computer\_reliability

It is completely self-evident that above all else an EDP-installation should do its work as well as possible with few breakdowns much of the time as possible. Not unexpectedly, security measures are most often found amiss in this area, where demands are strong and lack of security is very easily detected.

The most important factor is that the computer works at all, and that the inevitable occasional breakdowns do not mean a catastrophe. Thus there must be means to handle power failure, and secure as much as possible of what would normally disappear or survive in an erroneous state at such an event. Efficient techniques for taking back-up copies of files at exactly the right intervals must exist and logging of on-line transactions, in order to restore the system state after a breakdown, must be possible without costs in time or money that exceed the cost of losing the transactions. The overall logging of events during runtime should also be adjustable to producing any sorted, summed or subdivided list that might be needed.

Since systems often do work, though not in the expected way, there must be efficient ways to clearly state what should be done and equally efficient ways to control what is really done. This means that programming languages should be highly standardized, easily learned and easily used, realizable in efficient machine code, and crystal clear in all their concepts.

Testing of programs should be thorough and exhaustive without taking to much time and producing lists that are too big for any one to read. It should be possible to trace even single items down to register level during any period of a run without getting more information than the requested and without completely jamming the computer. It should also be possible to initialize some values used by a part of a program, run that
part, and then check the results for a possible error. Naturally there should be a specific testing milieu, where for example data base up-dating programs can be run at debugging without interfering with normal runs.

c) ___ Information

In most EDP-installations today, there is not much concern about the security of information. It is usually felt that the information within the system is totally uninteresting to anyone except those legally using the system. Files containing sensitive information on individuals are very rare in the small systems, which make up the majority of the installations. When it comes to the question of sabotage, villains are supposed to be more likely to use bombs than to learn the intricacies of a special system in order to do damage from within. Employers are normally trusted. However it is generally felt that this age of relative innocence can not last much longer and a sizable number of installations have passed it. As knowledge of data processing becomes more widely spread and more and more sensitive information is fed into and stored and processed within EDP-installations, special safe-guards for information must be established. The most prominent among these are four main features. First you should be able to compartmentalize the system rigidly and to control completely the flow of information between compartments. Then it should be possible to identify terminals positively as well as terminal operators and computers. There should also be controls for access to data bases and other shared resources, and last it should be possible to encrypt especially sensitive information both on communication lines and on storage media. The basic insecurity in most existing operating systems, caused by their improper functioning at unpredictable moments in unpredictable areas, is felt as a major threat to computer security as a whole and to safeguards and controls in particular. Operating systems must be better built, better controlled and tested, and less prone to break down completely whenever an error is triggered in any part of the system.
d) Data_quality

This is a notion that is swiftly gaining in importance. It has for a long time been pointed out by DP-specialists that input can be checked to a much greater extent in computers than in manual files. It is also well-known that the absence of elementary controls in automated systems can have almost unbelievable effects. Since data quality, however, is not only a matter of direct errors in stored information but also the question of what exactly any given item designates, what accuracy it has etc, the present development enhances this concept very much. Three new features all contribute to produce situations where data quality is not self-evident or manageable by instinct and feeling alone. Those features are huge shared data bases, where the complexity of the data base management system makes it impossible for any human being to know where and how all the data are stored, centralized data collection, where the collector cannot foresee every use that the data might be put to, and new trends in system design, where the whole process and its goals rather than the details are emphasized. Hence new tools are needed. There should be new and better ways to indicate what information a data item actually contains, and what is its source. Methods for thorough documentation of the purpose of a system will also be necessary. There will be an increased demand for data retrieval languages where you can easily and comprehensively state exactly what information you want to be fetched etc.

The basic checks on validity of data can also be improved by techniques for more efficient and sophisticated controls, which have mainly became feasible because of fast and random access to data.

e) Social_integrity

The extensive collection of all kinds of information by government agencies and others for computerized files is regarded as a major threat to privacy and personal ability to decide on one’s own life. There is rather much general concern that information, more or less voluntarily given to one agency, might
crop up in some quite unexpected place and cause some action by another agency. This possibility is all the more disconcerting because of the fact that information might have been given with the explicit purpose of having excellent quality for the given usage, and that might render the quality for the new and unknown usage intolerably bad. Since it is only with the help of computers that any extensive exchange and use of personal information is possible laws aimed at controlling the information flow should come now. The Swedish Data Act is a good start, but there should also be strict controls on the exchange of information on individuals between government agencies as well as rules stating that any one collecting information on individuals, voluntarily given or otherwise, for computerized files should inform the subject on the use, that will be made of the information, and to what third party the information might be passed.

4.2 Level of fulfillment of requirements, today and within five years

a) Investments

Building regulations, fire protection recommendations etc are fairly advanced today and will be further developed. These areas cause little theoretical problem.

Portability is often completely lacking today, mostly because of the extensive use of assembly languages in older systems as well as the absence of any ordered structure with well-defined interfaces which might have allowed the substitution of parts of the system. Since high-level languages are more and more used today, portability will automatically improve. The new trends towards "structured programming", in any sense of that term, and towards well-defined interfaces both in software and hardware will also help. New products from the same manufacturer are mostly designed to be compatible with old models built for similar tasks. However, improvement does not necessarily mean perfection. Faster computers, efficient implementation of high-level languages, and the ensuing
lack of need for tricky programming etc might make assembly languages obsolete, but the task of creating good high-level languages for such areas as data communication and data base handling is not an easy one, and the lack of standardization does not improve on that condition. Even more so, the competition between manufacturers tends to increase the number of partly incompatible versions of languages, I/O-techniques etc, since differences and refinements are tools in the competition. Hence, portability is poor today, sometimes even between different computers and peripherals from the same manufacturer. It will improve in certain areas, but far from as much as is possible.

b) Computer reliability

The number of complaints about computer security that fall within this area is a good measure of both its importance and how much is yet to be done. Power failure safe-guards, possibilities of having duplicate equipment and automatic switching from a failing part to its duplicate etc already exist, even though they are not used everywhere. Sometimes they are too expensive, sometimes they cover only a part of what the customer regards as necessary, and sometimes they do not exist at all for some kind of equipment from some manufacturer. There are examples of operating systems, that cannot run if the data communication handler is not working in good order. The data communication handler cannot work if it is not in touch with the concentrator. The concentrator cannot work if the connection is broken on one of the opened lines. Hence a faulty telephone line can stop the central computer. This, however, is luckily enough not a typical example of how modern systems work. The idea of graceful degradation is generally acknowledged, and new systems are nowadays as a rule constructed to continue running on what is left when some part is no longer in a useable state. Naturally this philosophy has its limitations, and some parts are
really vital for the proper functioning. If you switch in a duplicate, there is always a chance that that part too will break down somehow. This means that recovery procedures are always needed. Recovery is not a new problem for computers, and these techniques have followed the general evolution. Saving copies of at least two generations of registers, saving transaction files for a while, checkpoint restart etc take care of these problems for batch-running even in multiprogramming environments. On-line transactions, however, are causing some problems, usually because simple duplication of transactions, before-looks etc on magnetic tape for example creates an unmanageable bulk of raw data in bigger systems, where data base files cannot be released for copying too often. Development of techniques that do the same amount of protection as duplication at lower costs, are badly needed but hardly a reality within five years.

Programmers tend to think that the advantages of the languages, that they first learned cannot be surpassed by the advantages in any other language. This peculiar tendency of human beings to stick to what they feel familiar with makes it extremely important to develop really good languages that can be taught to students and used everywhere, without drawbacks during the working career. Two of the most important factors are that the language should be adapted to the human way of solving problems and it should enforce clarity and the separation of different parts of the whole task rather than encourage completely intermingled, space-saving, time-saving and error-producing solutions. Most of the existing programming languages fall short on at least one of these points. Much research is done on better languages and some with fair emphasis on security are in existence. However, the cost of re-education, the desire to keep whatever portability there is, and the conservative mind of the programmer and his ex-programmer boss make it extremely unlikely that these languages will be fast in gaining ground. Nevertheless improvements
are bound to come eventually and in five years changes will be present even if they are not all that common. In the meanwhile the concept of structuring will do much to lessen the risks of unintended effects in programs. When it comes to the new areas of data bases and data communication, standardized languages and proper interfaces towards common high-level languages are still often missing. Customers do not expect much change there, partly because of the competition between suppliers and partly because it is felt to be too early to freeze the state of the art by imposing strict standards.

The problem of testing of programs is enjoying an increasing attention. Already most manufacturers or other software suppliers can offer some sort of debugging or tracing facilities. Special possibilities of running in normal or test mode and of having special data bases for testing and education are also often provided. Nevertheless tracing is often found to give too much information in addition to what you wanted, and debugging may mean that you can not continue the run after your checkpoints. What is really needed is a constant trace of all variables and registers under their names in the program with full possibilities of stopping the run at any specified point, checking on present values, altering them if needed and then continuing the run at that point. At the end of the run only requested parts of the trace would actually be listed. Today this is possible only at tremendous cost, but in five years we expect to be very much closer to good solutions at low cost.

c) Information

Information security is perfectly possible today to any degree below absolute security, which can never exist. In real life, however, information is mainly protected by the general ignorance of how any computer system works and especially how a presumptive target system works. Only in bigger systems with terminals more or less on-line can you expect to find more explicit measures for information security. However, demands for security are increasing and such measures as ex-
licit identification of users, terminals and computers and verification of the professed identity will be present in almost every system using remote terminals. Encryption will not be confined to classified military information and the like but will be used for all kinds of sensitive and valuable information. This will not only be caused by increasing concern about privacy but also by the growing awareness of the risks and costs of dissemination of trade secrets, introduction of extra transactions or alteration or destruction of valid transactions etc.

There are three kinds of demands on information security, which cannot be met without having an operating system with a good basic structure. These demands are in the areas of compartmentalization, possibilities of plugging in or leaving out standardized or own security measures (without giving the individual users any chance to bypass what is installed) and the basic question of operating system reliability. The present situation in all these three areas can hardly be changed for the better in most of the existing systems without replacing the old operating system with a new one. Such new ones exist, especially regarding the first two points. The question of reliability is still in the research stage, but so much has at least been done already that it is possible to find operating systems for sale that by far exceed their predecessors in basic security. However, since operating systems are expensive and not easily replaced by new ones, changes will be noticeable mostly in new installations.

**d) Data quality**

Checks on the credibility of data against limits and normal values are already widely employed and highly recommended in EDP literature. Checks against present values of the data item to be changed are also feasible today, due to the short access times to discs, drums, etc compared to magnetic tape. Even more sophisticated controls will probably become rather common in systems where accuracy is of highest importance. With new memory technology, it will be possible in five years to make extensive cross checks against various data items in the same time that a single check on one item would take today.

When it comes to documentation and the tagging of information on data items in data bases, not much has been done so far,
but with the ever-growing size and number of complicated data bases, new methods are bound to come within five years. Still the inertia of the industry is big enough to prevent any major break-trough in the use of such methods within that period.

**e) Social integrity**

This area depends on such unwieldy matters as politics, law, "common practice", etc. Hence changes are slow, strongly connected to other issues and prone to be rather much of patching up rules to take things back to where society was when something unexpectedly started to slip trough an unnoticed hole. The new awareness of computer issues tend to end this and one very tangible result in the Data Act. Rules for exchange of information between government agencies are still missing, but a committee, that is still at work, may come up with suggestions and these in turn might have been transformed to rules within five years. It is, however, not possible to know if the public anxiety about a "Big Brother" society will be calmed by what has been done by them.

**f) Alternatives**

All that has been said above about the future is founded upon the assumption that basic principles and feelings about computers will remain the same in five years. There are, however, the possibilities that either the computers will be subject to a campaign similar to that against nuclear power or that all fears and worries will disappear and no one will care about privacy any longer. The former situation is feared by many, even if they hope that it will never occur. Still it is generally felt that thorough education in what computers really are and what they do would do away with this risk entirely. If the situation should occur, no one is prepared to do away with his computer, since that would mean closing down the whole company, agency or whatever. Security measures would be in high demand, but it would mostly be a change in degree, not in structure. The change would probably be most prominent in the issuing of new laws and regulations concerning the actual use of informa-
If, in the other hand, all worrying about possible threats against privacy stops, even this would not have too much impact on new system designs. Some people do advocate today that in say five or ten years we will have learned to tolerate the fact that every one knows literally everything about us. It should however be noted that such views are put forward by highly educated, well-adjusted individuals who are confident in their ability to cope with most situations that might arise in our society. It cannot be expected that these views should be shared by people who regard themselves as inferior and who do things that they regret or can not take the consequences of. If, however, the "free information" society should arise, it will not have much impact on demands for data security. Investments, computer reliability and data quality of course remain vital, since the work must be done and done economically, efficiently and correctly. When it comes to information security, trade secrets still are trade secrets, sabotage still is possible and criminal financial gain is still possible, if there is no data protection. Moreover, there is an increasing awareness that information collection is expensive and hence information is a financial asset that should be protected. The absence of worries about social effects, however, is a prerequisite for the "free information" society. Hence almost no demands would remain in the area of social integrity.

4.3 EDP and the society

EDP has already had a tremendous impact on our society. That effect will probably not be diminished in the future, but it might be less apparent, as systems get more refined and adjusted to human needs instead of humans adjusting to computer routines. When punched cards appeared as a common form of bill for regular payments, everyone handling them could not avoid noticing the new demands that these signs of the budding computer era put on humans. "Do not fold, spindle, or mutilate" was written on them. Punched card bills were abandoned mainly
because people did fold, spindle or mutilate them, since they always had handled their bills in that way. Many effects of computers are the equivalents of this example. They appear because no one really thought about them, they are valid on for a while, because no one has acknowledged their significance yet, and they disappear, because someone in a deciding position suddenly realises that the situation is impossible. Other effects are more subtle and devious, but nevertheless of utmost importance. It is for example true that the present complexity of society could not exist without computers. Social security payments, wages and salaries in larger companies, transfers between banks etc would be very much delayed and very often incorrect, if they were not managed by computers. Thus computers are constantly reshaping society, but society is also constantly changing the conditions for computers, sometimes consciously and sometimes inadvertently.

The famous Swedish Principle of Free Access to Public Records is actually getting into trouble in the computer age. It was designed to give any citizen the possibility of checking on any activity handled by civil servants. Thus bribery, incoherent decisions, etc would be very hard to conceal once they were suspected. One of the ensuing effects was that military and diplomatic secrets might be disclosed as well as highly private information on individuals who had had dealings with the authorities. To amend this without violating the basic principles the Secrecy Act was created. It states mainly what is exempt from the basic principle of free access. But the balance between these was established with regard to what could be harmful, and this decision was taken before computers were around and on-line requests were everyday routine tasks. What was once public and sensitive information, that was very hard to collect, at least in considerable quantities, is now just as public and sensitive but at least in theory extremely easy to collect especially in considerable quantities. At present this clash between free access and privacy concerns has led to decisions to remove some information from public EDP files, to applications for extensions of
the Secrecy Act, and other amendments. Since the situation is completely changed from the days when our laws were created a thorough revision is needed. A committee, OSK, is working on these problems. More public debate on these essential points would be welcome, since after all this is a matter of public opinion. How much privacy do we insist on? How dear to us is our right to review every action taken by the authorities? Because of computers one or the other might be severely and unintentionally restricted, if we do not look out.

On the other hand computers can be very much afflicted, not only by laws aimed at them and their misuses, but also by laws designed for completely unrelated purpose. The main reason for this effect is that a complete EDP system is normally a very rigid structure, where very few and small changes can be made without total restructuring at tremendous costs. For example new regulations for book-keeping might mean catastrophe for someone with a system that cannot be adjusted to these rules. To rebuild the system, that was recently constructed to adhere to the old rules, might be too expensive for the moment. In consequence great care must be taken both by people who design EDP systems and by people who design new laws and regulations. A permanent system must be well structured so as to lend itself as easily as possible to changes. New laws should be written with as keen an eye as possible on the effects on the information society of old ones, so as not to cause unnecessary dramatic changes in the daily routine of the law-abiding part of the society.
5. A PERSONAL POINT OF VIEW

During the research reported here we strongly felt that in our opinion some security problems in connection with information processing have been overlooked. In some cases the attention has been focused on relatively less important or less dangerous problems. We feel that it is appropriate here to express our opinion as researchers in the field of computer security. The suggestions made in this section are to be considered as rough ideas rather than final solutions.

We use the same structure as before and discuss the five groups of users' demands as listed in section 3.2.1. In addition to that we have some comments on the availability of computerized information.

5.1 Social integrity

The most discussed issue here is privacy. Many people feel a threat from the computerized society. They fear a situation like that in George Orwell's "1984" when everybody is controlled by "Big Brother". The privacy issue has led to demands on information security. We want to stress that even more important is a public knowledge of the principles of information processing.

The privacy discussion is mainly focused on the individual. In our opinion we must concentrate more on groups of individuals. Groups which may have the shape of the owners and employers of a company, an ethical group, inhabitants of a community etc. Group integrity deserves just as much attention as individual privacy. One example: There have been discussions about removing the identifying numbers from files with information intended for statistical purpose. When efficiently done, this may satisfy the privacy demands. Publication of statistics regarding a group of people may however be a threat to the group's integrity even if the individuals cannot be identified one by one.
The above problems, both privacy and group integrity, cannot be solved by information protection only. The data quality of the stored (and protected!) data is also important. This has been recognized but not fully appreciated. We discuss data quality below.

5.2 Security of investments

This problem is so similar to well-known issues that it has been thoroughly investigated and solved. We have no further comments.

5.3 Reliability

Reliability has been the concern of computer manufacturers ever since computers became publicly available. Still there is a tendency to blame the computer for mistakes and erroneous functioning. One reason might be that while the parts of an information processing system are sufficiently reliable, the total system has annoying errors like long delay when using a remote terminal. System reliability has to be better 1981.

An even more important issue is the poor matching between the machines and the human beings trying to communicate via the machines. The design of information processing system with computers seems to start with a computer and then works it's way outwards. Thus the requirement of the machines has high priority when designing the interface between to human user. With the flexibility of today's hardware and software the obvious starting point of the design procedure should be the demands of the users. We then proceed by designing the appropriate manual and automatic information processing system. Of course, we have to compromise sometimes, but the first bid is always the user's. Man-oriented systems are possible today and even more so 1981.

Examples of features which would facilitate communication via EDP-systems: High-level languages with the capability to correct the most frequent errors made by the human users. Terminals which can print the same symbols as in ordinary human communication, for example small letters (not only capitals), drawings etc. A
standardized call (HELP) that results in a printout of a simple how-to-do instruction and a possibility to interact with the computer to solve any problem. Not just a reference to a 500 page instruction manual.

Computer security is most often interpreted as secrecy. Availability is of equal importance. If data stored in an EDP system has sufficient data quality (see section 3.2.1) for a specific problem, every legitimate user must have realistic possibility to process these data in order to solve the problem. We consider this to be an important reliability problem.

5.4 Information security

One area which has been largely overlooked is information security in connection with data communication. It must be observed that data networks contain information processing capability. (This by the way is also true for future communication networks in general). Today it is not clear who is responsible for security problems in data networks. This must be solved. Most data networks use transmission media (telephone lines etc) originally intended for telephone transmission. The character of this communication is such that it is less sensitive than data communication to loss, destruction or change of transmitted information. Hence data networks using telephone lines create information security problems. Transmitted data are best protected by encryption. In USA the National Bureau of Standards has proposed a standardized algorithm for data encryption. Integrated circuits with the hardware to perform the algorithm are said to be available during 1977 for approximately $100 each. Encryption is also an efficient method to protect sensitive data stored in an EDP system.

Proper identification of the transmitting and receiving part (for example the user and a specified file) in an information processing situation is a prerequisite to obtain high information security. This has been stressed in section 4 but we want to put it forward as the most important information security problem in an information processing system, manual and/or automatic.
Better operating systems are needed and can be constructed. One way to facilitate this is to use small dedicated EDP systems. The security requirements are the same, of course, but they are more easily satisfied in an dedicated system.

5.5 Data quality

This has been discussed a great deal but practically nothing is done to protect the quality. Data quality is discussed in section 3.2.1. The first problem is to get a widespread knowledge about data quality. The most important points here are that data quality cannot be expressed quantitatively and data quality is dependent on the decision to be made. Thus if data are collected for one purpose and have sufficient quality for that purpose, the quality for another purpose might be poor. Information processing has to be done carefully in order to preserve the quality of the data.

The only way to protect data quality is to compare the results obtained using EDP data with the results obtained from direct observation of the origin of the data. Another protection measure is to collect new data for each new purpose. In some cases we might find that these data coincide with previously collected and stored data.

5.6 The availability via EDP of public data

The celebrated Swedish "Principle of Free Access to Public Records" has a long tradition and ought to be preserved. With the increasing use of automatic information processing it becomes easier to access public records. This is an advantage as long as it is not misused. Data in public records are collected for a specified purpose. If for example, separate records are compiled (with EDP) for a purpose which was not originally intended, the quality of these data might be poor. To avoid misunderstandings and false decisions we want to control the access via EDP to public data. Still the Principle of Free Access has to be preserved.
One way out of this dilemma is to control the availability through EDP of public data. We suggest that public records are divided into two groups: one which is publicly accessible via EDP (for example via computer terminals in private homes) and one group which is only accessible by passing manual data handling. We call these groups EDP-accessible and non-EDP-accessible. EDP-accessible data may accessed from home terminals. Non-EDP-accessible data are obtained in the same way as today, for example via a telephone call to public authorities, personal visits etc. To facilitate the access to non-EDP-accessible public records computer terminals may be placed in public libraries and operated on request by the librarians.

5.7 The cost of computer security

One final point, which we want to stress, is that there is a tendency to compare the cost of security measures with the potential losses. Although this is relevant in many cases there are "losses" (of information, social integrity etc) which cannot be valued economically.
REFERENCES