43

"Comprehensive Information Technology Security":
A New Approach to Respond Ethical and Social Issues Surrounding Information Security in the 21st Century

Anja Hartmann*

German Information Security Agency (GISA)
Department of Scientific Fundamentals, Certification, Accreditation
Division for Technology Assessment
P O Box 200363, 53133 Bonn, Germany

1 Introduction

Up to now, the information technology security (IT-security) has been seen as a mainly technical problem. Organizational and legal questions have been discussed and (sometimes) solved as a necessary and annoying evil. Nearly nobody has been thinking about the social and ethical dimension of IT-Security.
One of the reasons may be, that for a long time, information security as well as information technology security has been a theme concerning only a small group of applications (e.g. secret services or secret documents).
But times are changing. The increasing use of information technology in all fields together with growing economic problems in many countries result in industrial espionage as well as in social misuse. Security is no longer an issue for engineers only. In an extreme case, every person can be affected by wide-range or long-term damages in case of technical failures, manipulation attempts, operating errors or failures caused by various disasters. In addition, every person will be confronted with sensitive data and must learn to handle it. That is why we need a different perception of "information technology security" - a comprehensive one.

In the following we will discuss some items as well as some experiences leading us to such a kind of perception. The second step will be to summarize the most elementary issues and to work out an approach called "comprehensive information technology security". The aim is to show potential solutions to the arising questions.

* This paper reflects the opinion of the author only.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

2 Problems and Demands concerning the Growing Importance of Information Technology Security

The problems and demands on the growing importance of information technology security will be described with help of

- a different view of the issue
- a discussion of ethical questions
- a case study concerning IT-security and technology assessment.

2.1 Information Technology Security and its Relations to other Items

In a first step we address the problem of IT-security itself. Starting point of the discussion has to be the traditional concept of IT-security. This concept is based on the exclusion or reduction of threats (1) and focusses on technical problems like operating errors, technical failures, failures caused by various types of disasters or manipulation attempts. But - as we all know from experience - the main technical demands like availability (prevention of the unauthorised withholding of information), integrity (prevention of the unauthorised modification of information) and confidentiality (prevention of the unauthorised disclosure of information) (2) are not broad enough. The interactions between technology and society, technology and law, technology and economy and technology and organizations necessitate that a more comprehensive concept of IT-security should be taken as a basis.

The following examination levels have to be included:

- technical and technological elements of IT-security, i.e. availability, integrity and confidentiality,
- organizational elements,
- legal and economical elements, i.e. questions of legal compatibility and efficiency, as well as
- social and ecological elements, i.e. questions of social vulnerability and dependence on workable information technology.

2.2 Information Technology Security: Technology Influenced by Ethics

Because societies depending on information technology have become more and more vulnerable in many ways, we have to look for solutions not only in technical, organizational, legal, social, economical and ecological but as well in ethical dimensions. But what is the meaning of this? Very often not even philosophers agree on this question. How could engineers handle it? (3) The

answer seems to be easy: we have to try out new avenues - and some of the steps are already well known.
First there are some expressions like responsibility, professional ethics, values and each of us has some ideas what this could mean. Other professions can help us to improve these ideas and to work out some concepts. (4)

Falling back on various discussions we resume that the aim of ethical questions is to protect nature and people from damages. That means that every person must act responsibly in every situation. It is not at all sufficient meeting legal demands. The question is whether additional values should be taken into consideration. There are a lot of various values and engineers must think about a range: is economy more important than security? Or does it depend on the level of security, on the technological application, on the economic situation or on the potential number of damaged persons?
On the other hand we have to discuss the concept "responsibility". What is it? And who is responsible in which case? Who is responsible for information technology security? The engineers, the designers, the organizations, the users?

We agree with the German philosopher Hans Lenk (5) in his meaning of responsibility: somebody must "answer" to his conscience, other people, God about the consequences of his actions. But taking into account the complexity of technical applications neither a single person nor a social group by itself can be responsible. There are so many actors involved, that there must be a new concept of responsibility: the "co-responsibility".
The co-responsibility concerning the developers on the one hand and the designers and users on the other hand. All actors who are involved in developing or using information technology (e.g. engineers, designers, organizers, users) but also politicians, trade unionists, persons who are responsible for data protection or data security are co-responsible. The extent of the co-responsibility depends on the potential influence each actor has. We have to differentiate between users (normally little influence and therefore not much co-responsibility) and e.g. engineers (quite a lot influence and therefore highly co-responsible). But regardless whether influence is high or not they all have to think about the risks and potential damages of technology and they all have to act responsibly. But how can they do that? Very often there is no chance at all for one single person to assess the consequences of new techniques. That is why we need a third sediment in our approach of "comprehensive information technology security": the technology assessment.

2.3 Technology Assessment in the Field of IT-Security

Technology Assessment (TA) is a sociological approach. Its aim is to assess the intended and not-intended, the short- and long-term consequences of new techniques and to look for options reducing risks. In interdisciplinary studies engineers, social scientists, psychologists, lawyers, users and other people affected examine, using different methods, chances and risks of new

technologies. They discuss suggestions for improvement and in a next step the different groups should correct the technique, looking for alternatives etc.
Unfortunately this approach is very seldom used for questions concerning IT-security. In the following we will use a German study to illustrate technology assessment as well as the new approach "comprehensive information technology security".

The German "Bundesamt für Sicherheit in der Informationstechnik (BSI)" was the first institution at all who initiated a TA-project to analyze questions concerning IT-security in important applications of information technology like traffic, health systems, monetary system or process control (6). The project was being carried out by two German institutions: the "Industrieanlagen-Betriebsgesellschaft (IABG)" Ottobrunn and the "Fraunhofer Institute for System Technology and Innovation Research (FhG-ISI)" Karlsruhe. It ended in July 1994. The objectives of the project were

- to show the various stages of technological development,
- to analyze questions of security and vulnerability,
- to point out advantages as well as risks,
- to sensitize the different parties and
- to work out possible actions.

The project was characterized by two very important approaches:
1. An interdisciplinary discourse among affected persons, engineers, data protectors, members of various associations and insurances, trade unionists, social scientists etc. was chosen to cope with the very complex task and to complement disciplinary knowledge.
2. Scenarios are to be developed to illustrate the main problems of different design options.

It has be seen that it may not possible to find answers to all of the arising questions. There are still a lot of different opinions concerning, the design options for exmple. And there are also concerned persons that do not like the use of techniques (e.g. patient cards) at all.

Within the limitation of a small and short discourse project two problems were tackled: all participants discussed together the pros and cons of various design options and a lot of unsolved questions arose (and for some of them there are suggested solutions). A next step would be to let all affected persons and actors know the results of this study and look for further solutions, political decisions and legal rules.

3 Comprehensive Information Technology Security

After discussing the problems and demands on information technology security, we are able to summarize - in our opinion - the most elementary issues for a new approach, the "comprehensive information technology security". To illustrate this approach, we make use of the above mentioned study and take the project "Chip Cards in Medicine" as an example.

The background of our example:
A "medical insurance card" has been introduced in Germany since 1994: each person is bound to submit the card in medical practices as well as in hospitals. This medical insurance card is a small card (similar to a credit or telephone cards) with a chip on it. The following data are stored on this chip card: the name of the insurance carrier, the name of the insured, his/her date of birth as well as his/her address, the insurance number of the policy holder, the beginning of the insurance coverage and, finally, the period of validity of the card. As matters stand at the moment two objectives are pursued with this card: the rationalization of administrative tasks in medical practices and in hospitals, and the proof of an insurance coverage of the patients (7,8). To exclude any misuse of the medical insurance card, the manufacturers are bound to technical specifications concerning the card and the card reader. One of the requirements is that only the insurances shall be able to write, change or delete data on the cards. The "Bundesamt fuer Sicherheit in der Informationstechnik (BSI)" is evaluating the cards and card readers in regard to their information technology security (IT-security), and upon the successful completion of the examination will award a certificate to the manufacturers. That is the status in 1995.

But while the politicians are still looking to the problems of the introduction and use of these cards, the technical development of the medical insurance card is going on. Not only the manufacturers of chip cards and chip card readers, but also the health insurance companies, medical associations and scientists are thinking about further applications (9, 10). Depending on their different interests they plan to store various other types of data on the cards like treatment data (e.g. bills for medical treatment), emergency data (e.g. blood group, allergies, diseases), blood donor and/or organ donor data, vaccination data, diagnostic data (e.g. cancer, diabetis), therapy data (e.g. operations, cure) or prescription data.
Such an extension of the medical insurance card towards a **patient card** is - depending on the design - combined with both progress and risks.
The supporters are pointing out that

- further costs could be saved,
- duplicate examinations could be avoided,
- in case of emergency, lifesaving data would be available as quickly as possible,

- the patients would not have to repeat their anamnesis to each physician they are visiting anew,
- the patients could take care of their medical data themselves as the data is no longer stored in the different medical practices. (7)

On the other hand the antagonists are reminding again and again on the dangers:

- the flow of communication between physicians and patients could deteriorate,
- the quantity of medical treatments as well as the quality of diagnosis and therapy could deteriorate,
- forwarding of data could occur without knowledge and consent of the patients,
- a lot of questions concerning data protection and data security are not yet known and even less solved.

3.1 Elementary issues

First of all there is a need for a more *comprehensive interpretation of IT-security* and it follows from this that we have to put it into action in a new manner. It is not at all sufficient to implement "technical" IT-security. Rather organizational, legal, social, economical and ecological elements must be taken into consideration. In addition, we have to attach great importance to the information and qualification of all affected persons.

In our example "Chip Cards in Medicine" a more comprehensive interpretation of IT-security results in the following questions (6, 11):

- which are the main technical and technological potentials and risks of patient cards? Which problems concerning IT-security are combined with which individual configuration (e.g. the different combination of storage chip cards, processor cards, smart cards or optical cards with potential types of data stored on the card like treatment data, diagnostic data, therapy data or prescription data)? And: what can be done or which precautions are helpful to raise the security level?
- Who should be allowed to use the cards (e.g. doctors, patients, hospitals) and what has to be done to standardize the documentation, interpretation and use of the data on the patient cards?
- Are the legal conditions sufficient for storing data, processing data and forwarding data? Are there special laws concerning the electronical use of medical data and what does this mean for the technical IT-security of chip cards?
- Will all affected persons be able to handle the security precautions?
- ....

There are a lot of interactions between the different elements. That is why we suggest the following view of IT-security.

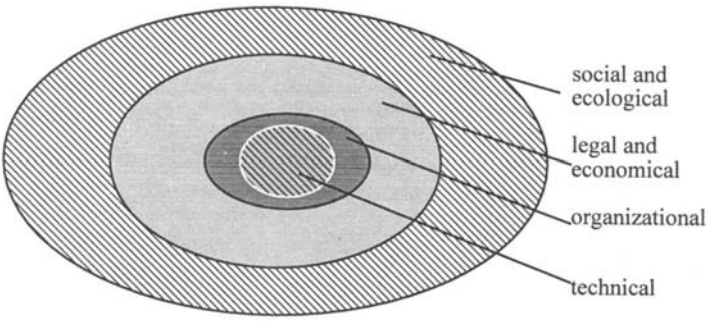

Figure 1. Elements of IT-security (11)

Secondly, the processes and results of *TA-studies* support us to assess the chances and risks of new information technologies as well as of new applications of well known technologies. Suggestions exist for a higher and more comprehensive security level.

> In the example "Chip Cards in Medicine" scenarios were developed to illustrate the main problems of different design options. Therefore the following questions were of elementary interest (6):
> - Which are the main technologies for the technical design of a patient card?
> - Which types of data in the health system are relevant for an electronical use?
> - Which actors are involved in the design, storing, forwarding or changing of data?
>
> The interweaving of the mentioned components resulted in a complex matrix of design options, which have been checked to see whether they are lawful or not. The resulting, very reduced matrix was then linked with the initial question: which problems concerning IT-security are combined with which individual configuration? And what can be done or which precautions are helpful to raise the security level?
> The discussed options are concerning technical, organizational, legal and social examination levels. (11). Suggested solutions, political decisions and legal rules have been discussed since the end of the project in July 1994 (i.e. according to the criteria in (12)).

Thirdly, the concept of *co-responsibility* plays an important part. We have to think about our own roles, influence and power to increase the information technology security and to avoid risks and

damages. It is essential to discuss different values. This could be done in national and international associations as well as among various professional associations like engineers, philosophers, social scientists and politicians. There are already a few codes of ethics (13, 14, 15, 16, 17, 18) which could be taken as a basis.

As already mentioned above, responsibility means that somebody must "answer" to his conscience, other people or God about the consequences of his actions. In case of complex technical applications neither a single person nor one social group by itself can be responsible. There are so many actors involved, that there must be "co-responsibility". Here we have to differentiate between "causation responsibility" (persons who are involved in the development, design and implementation of a new technology) and "trustee responsibility" (users of a technological application). (4, 5).So various actors have to take the co-responsibility of a technique. But responsibility is not equally shared among all actors. It is rather dependent on the power and possible actions each actor has. Therefore there will never be a homogeneous measure for co-responsibility. Developers, TA-scientists, political decision-makers, pressure-groups, they all have different co-responsibility.
Example: In most cases, the participants of a TA-discourse have relatively little influence on the design of a new technique. The co-responsibility of other actors will increases, if they have (economic or political) influence and still do not use the results of the different TA-studies.

> In the example "Chip Cards in Medicine" all actors that use the patient cards could have co-responsibility: manufacturers of chip cards and chip card readers, health insurance companies and their associations, physicians and their associations, hospitals, drugstores, scientists, patients as well as political decision makers. In the end each inhabitant would have a bit of co-responsibility.
> Examples:
> - manufacturers have to consider the technical security precautions,
> - physicians, hospitals, drugstores and insurances have a special care responsibility, when they use the patient cards,
> - political decision makers have to establish the peripheral conditions for using the card,
> - patients have to take care of the card as well as of the relevance of the data.

Whether this concept of co-responsibility will work or not depends on our fourth elementary issue: the security culture.

Fourthly, the *security culture* is indispensable to complete the approach. Each person has an individual need for security. The more sensitive the data are the greater is this need. Out of this need of security various social groups develop different collective manners to handle insecurity, threats and risks.

> In the example "Chip Cards in Medicine" the need for security is extraordinary high for patients (because the risks for their health are very high), high for doctors (because they could lose patients if they did not consider the needs) and relatively low for a doctors' association (because their risks are reduced to legal questions).

The different collective manners of all social groups affected by a technique result in the so called security culture. In addition, the security culture is caused by social learning processes. It is expressed by a specific perception and coping with reality. So, security measures, instructions and norms as well as informal methods are signs of a security culture. In addition, the security culture with regard to a specific technique is embedded in a social, economic and legal surrounding. Therefore it is influenced by several experiences persons have. It is subjected to continous modification.

The management of IT-security will only be successful, if the development of a security culture is adequately supported. It would indicate that communication and cooperation potentials concerning IT-security are practiced. As a result we found the phenomenon that IT-security is dependent on the organization of an interculturel communication and cooperation process. the advantage from this point of view is that we have the chance to use security culture as a junction between the great demand of IT-security and its reality.

Finally, we must bring together the various results of the four issues "comprehensive interpretation of IT-security", "co-responsibility", "TA-studies" and "security culture". Therefore the *interdisciplinary, international and intercultural cooperation* should be strengthened and we have to try out new avenues concerning interdisciplinary discourse. The hereby suggested approach "comprehensive information technology security" is one potential avenue. The following figure illustrates this approach.

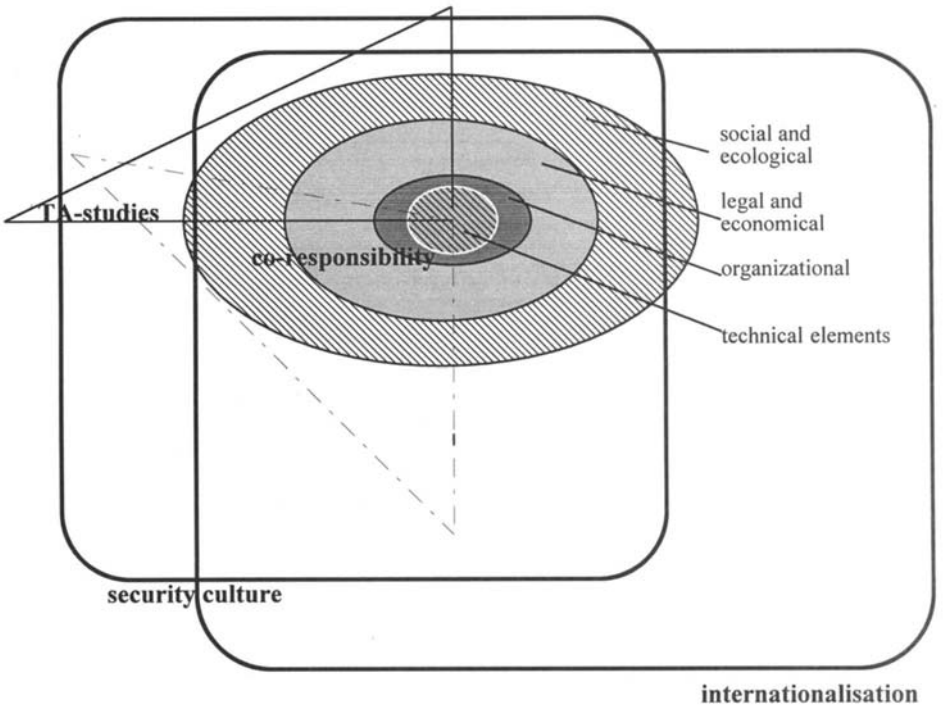

Figure 2. Comprehensive information technology security

This requirement is increasingly necessary the more the internationalisation of information techniques is continuing. Up to now more and more applications are used in an international context. That is why networking gets more important.

> In the example "Chip Cards in Medicine" there are some ideas to internationalize the application as follows:
> every physician as well as the medical assistants in hospitals all over Europe would be able to read the data and - if necessary - to store new data on the patient cards. A translation system translates the data into the corresponding languages (i.e. German-English, French-Spain, Italian-Portuguese). In case that not all relevant data is stored

on the card, the physicians would have the possibility to obtain the data via a medical network. Therefore the European Union is supporting the building up of such a medical network. IT-security in this case will only be possible, if the security precautions and the security culture as well as the behaviour of all concerned persons (i.e. co-responsibilty) is similiar in all of the European countries.

The example shows us, that there must be a harmonization in regard to the demands, the solutions and the way to use a technique. The worked out approach is one possibility in this direction.

3.2 Additional Requirements in Regard to a Comprehensive Approach

Obviously there are quite a lot of conditions necessary to realize the comprehensive information technology security approach. And there may also be some other elements we have to consider. That is why another very important question arises: what could be done to increase the probability for implementation?

A first step could be to *strengthen the discussions* concerning professional ethics both in professional associations and at universities (19, 20).

In addition, the associations must *enlighten the society* as well as their own members in regard to the importance of information security.

As well, the actors who are responsible for data security should take into consideration whether they can use the approach *"participative design"* and involve users in their work.
Wherever this is impossible, the actors should strive for *visibility of problems, chances, risks and processes*. Otherwise the concept of co-responsibility is not practical. Nobody can be responsible for unknown things (21).

Not least the *internationalization of demands, norms and solutions* is one of the most important requirements.
The approach "comprehensive information technology security" will be useful only if it is really comprehensive in regard to the issues, the process and the countries. Otherwise we cannot solve the problems - neither today nor in the 21st century!

4 Literature

(1) ITSEC: Information Technology Security Evaluation Criteria. Version 1.2. Provisional Harmonised Criteria, June 1991,

(2) Kersten, Heinrich, 1992: Die Kriterienwerke zur IT-Sicherheit - ihre Bedeutung für die Anwendungspraxis. In Wirtschaftsinformatik, No.4, 378-390.

(3) Johnson, D.G. (ed.) 1991: Ethical Issues in Engineering, Englewood Cliffs, New Jersey 1991.

(4) Jonas, H. 1979: Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation, Frankfurt a.M. 1979.

(5) Lenk, Hans, 1988: Verantwortung in, für, durch Technik. In: Bungard, Walter / Lenk, Hans (Hrsg.): Technikbewertung. Philosophische und psychologische Perspektiven, Frankfurt, 685-688.

(6) Hartmann, Anja 1994: Chipkarten in der Medizin. In. Wolfinger, B. (ed.): Innovationen bei Rechen - und Kommunikationssystemen. Eine Herausforderung für die Informatik, Berlin, 1994, 258-266.

(7) Schaefer, O.P., 1993: Die Versichertenkarte - Auftakt zu neuen Kommunikationsstrukturen im Gesundheitswesen. In: Datenschutz und Datensicherung, No. 12, pp.685-688.

(8) Kilian, Wolfgang, 1992: Legal Issues in Relation to Medical Chipcards. In: Köhler, C.O. (ed.): Cards, Databases and Medical Communication. Fourth Global Congress on Patient Cards and Computerization of Health Records, Berlin, Newton, Mass.: Medical Records Institute, 1992, pp. 53-53xii..

(9) Waegemann, C. Peter, 1992: The State-of-the-Art of Patient Cards - A Global View of Developments in the Field of Patient Cards and Computerisation of Health Records. In. Köhler, C.O. (ed.): Cards, Databases and Medical Communication. Fourth Global Congress on Patient Cards and Computerization of Health Records, Berlin, Newton, Mass.: Medical Records Institute, 1992, pp. 78-78ix.

(10) Waegemann, Peter, 1993: Patient Card Technologies and Applications. In: Waegemann, Peter (ed.): Toward an Electronic Patient Record '93 - Ninth Annual International Symposium on the Computerization of Medical Records and North American Conference on Patient Cards, Newton, Mass., USA: Medical Record Institute, 1993, pp.175-178.

(11) Hartmann, Anja / Ulrich, Otto, 1994: Chip Cards in Medicine - Technology Assessment in the Field of IT-Security. International Association of Technology Assessment and Forecasting Institutions (ed): Technology Assessment in and for Developing Countries. 1st International Conference, Bergen, 2-8 May 1994

(12) Bizer, Johann, 1994: Rechtliche Möglichkeiten und Schranken der Patientenchipkarte. In: BSI 1994: Chipkarten in der Medizin. Dokumentation eines Fachdiskurses am 2. und 3. Dezember 1993 in Bad Aibling. BSI 7154. Bonn, pp.57-78.

(13) Association of Computing Machinery (ACM) 1992: ACM Code of Ethics and Professional Conduct. In: Communications of the ACM, No. 5 (1992) 94-99.

(14) Australian Computer Society (ACS) 1987: Code of Ethics, Darlinghurst 1987.

(15) The British Computer Society (BCS) 1992: Code of Conduct. In: IFIP-WG 9.2 1992, 26-33

(16) Canadian Information Processing Society (CIPS) 1985: Code of Ethics and Standards of Conduct, Toronto, January 1985.

(17) Dunlop, C. / Kling, R. (eds) 1991: Computerization and Controversy. Value Conflicts and Social Choices, Boston - San Diego - New York 1991.

(18) IFIP-WG 9.2 1992 - International Federation for Information Processing (IFIP), Working Group 9.2 (eds.): Ethics of Computing: Information Technology and Responsibility, Madrid 1992.

(19) Andersen, R.E. / Johnson, D.G. / Gotterbarn, D. / Perolle, J. 1993: Using the New ACM Code of Ethics in Decision Making. In: Communications of the ACM, No.2 (1993) 98-107.

(20) Coy, W. / Rödiger, K.-H. 1994: Initializing a Discourse on Professional Behaviour. In: (21), 29-32.

(21) Clement, A. / Robinson, M. / Suchman, L. / Wagner, I. (eds) 1994: Ethics and System Design. The Politics of Social Responsibility, Proceedings IFIP WG 9.1 Workshop, February 1994 in Havanna, Wien.