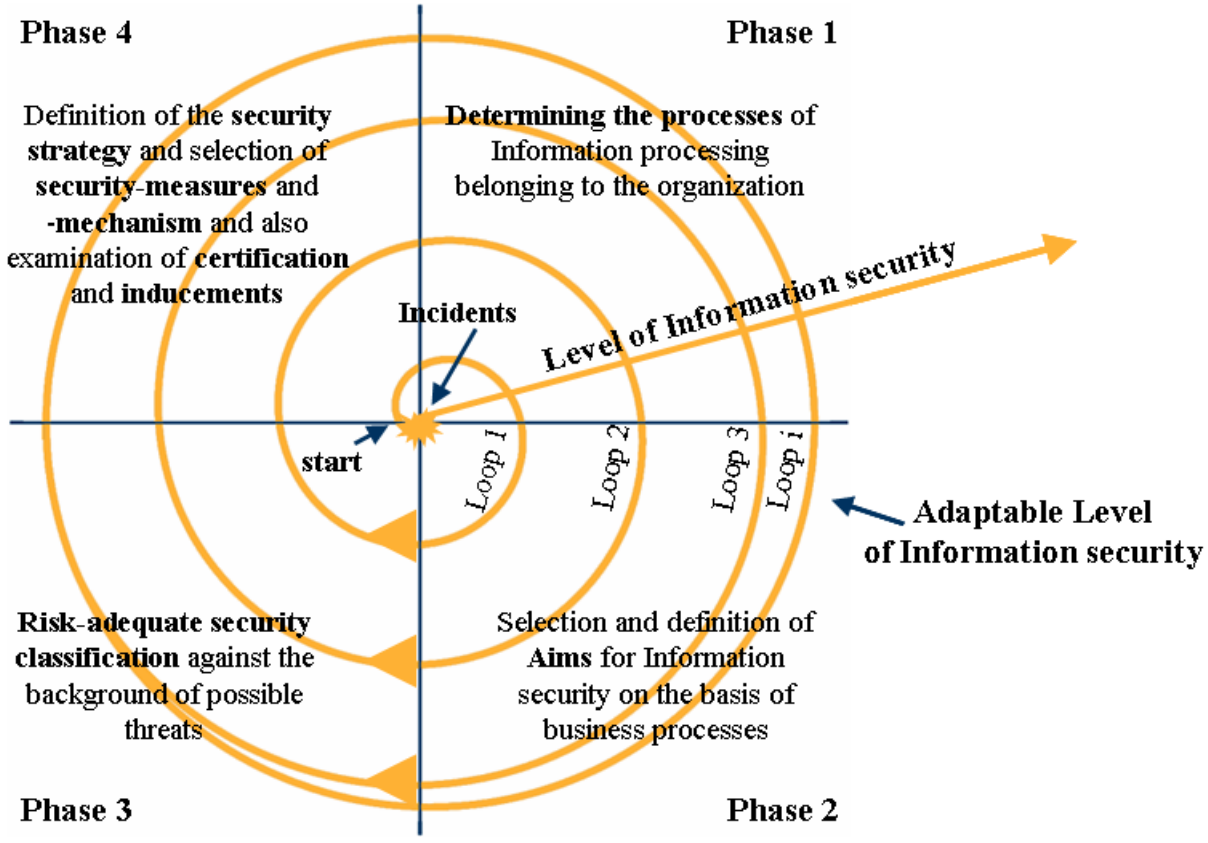
IWI Discussion Paper Series
 # 15 (May 5, 2005)[1]
ISSN 1612-3646

Strategic Management of Information Security in State-run Organizations

Robert Pomes[2] and Michael H. Breitner[3]



---

1 Copies or a PDF-file are available upon request: Institut für Wirtschaftsinformatik, Universität Hannover, Königsworther Platz 1, 30167 Hannover (www.iwi.uni-hannover.de).

2 Diplom-Ökonom and PhD Student (pomes@iwi.uni-hannover.de).
3 Full Professor for Information Systems Research and Business Administration (breitner@iwi.uni-hannover.de).

Table of Contents

Strategic Management of Information Security in State-run Organizations

Robert Pomes, Michael H. Breitner

Universität Hannover

Abstract: *Global processes of exchange information and communication between organizations are leading to significant weak points and increasing incidences concerning information security. This leads to the question, which aspects the strategic management of information security of state-run organizations should consider to make information fully accessible but secure at the same time. The strategic management of information security should lead into an integral and convergent security process, which would take into consideration the specific demands and conditions of state-run organizations. Within the framework of the security process, structural components, security aims and the demands of a state-run organization are analyzed, evaluated and modified to meet specific conditions. The aim of the strategic security process is the system-immanent and integral strategy preparation and implementation of an information security for a state-run organization.*

Keywords: Information security, state-run organizations, convergent security process, strategic management

1 Motivation and Aim

The importance of information against the background of globalization and increasing complexity of communication processes is unmistakable. The interest in information of state-run organizations is coming from members of staff, recipients of services, competitors, companies as well as the public.

As a result the question arises, how information can be made fully available to authorized persons, but be protected from others. Extensive studies have been carried out on technical information security. However, the

problem of the security information[4] in a non-technical environment, particularly from a strategic perspective of information processing, have been insufficiently discussed.

It is predominantly the economic computing science, as an interdisciplinary field, situated in between business management and computing science, which should be encouraged to offer solutions concerning information security for all fields of information processing (IP) in organizations. For the majority of organizations, the increasing importance of the protection of the information systems (IS) and the information itself has priority over other matters. One reasons for this is the compact link of the IS with the core processes. Another reason is the demand for more transparency (e.g. KonTraG).

However, integral and complete security concepts are rarely or insufficiently translated into practice because of a lack in competence, commitment at management level of organizations and inadequate benefit and corresponding cost evaluations of necessary security concepts. During the course of this work, an extensive and sustained assessment of a strategic management of information security of state-run organizations will be developed. The tasks for the strategic management of information security will be based on a structured model procedure.

Furthermore, the "status quo" of the information security in state-run institutions will be described and the increasing numbers of security incidences discussed.

The findings will be used for to the preparation of a phase-oriented and therefore reciprocal model for a strategic management[5] of information security in organizations. In this context, advantages of certification and use of an integral view of the management of information security will also be presented.

---

4 The technical perspective itself does not offer an adequate basis on which all aspects of an organization can be judged. However, the investigation of the latest technical security solutions is indisputable.

5 In general a strategy can be understood as a measure to secure success of a business in the long term. [Compare Bea. F.X./Haas, J.: Management 1997, S.49]. Here, the term "strategic" also means giving high priority.

2 Foundations

2.1 Security of Information Systems and Information Management

An information system (IS) of an organization includes all technical and non-technical components of IP and therefore, includes all people, hard and software as well as their information and communication relationships in the organizational field [SDR98]. Picture 1 gives an example of possible components of IP.

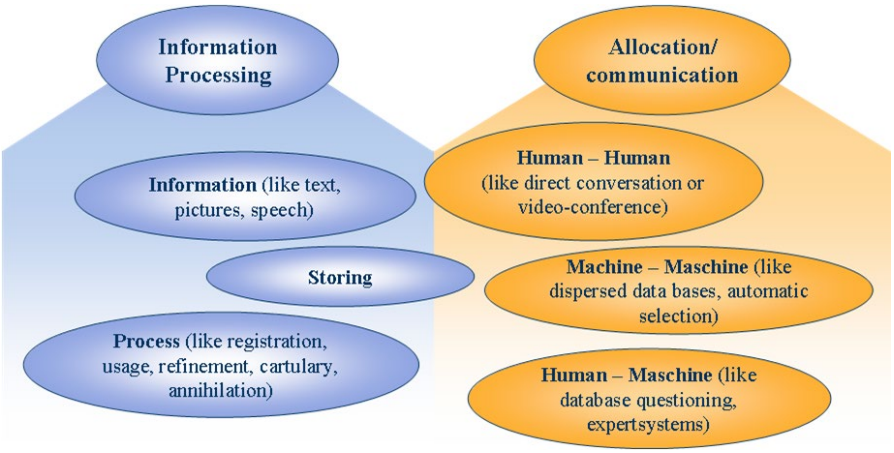


Figure 1: Components of an information system.

Source: Own representation following [Sto94].

The need for an information management (IM) primarily derives from the enhancement of information to a production and competition factor [Hüb96].

Information is seen as a strategic resource and regarded as a separate entity, which leads to the implementation of an IM in companies. [Bro92] The information management was established in the past two decades and is currently regarded as a basic factor of the management. [BP98] The term IM is interpreted in two ways: (1) the technical point of view emphasizes the creation of the IT-systems with the network, hard and software, databases etc, whereas (2) the economic point of view defines the tasks of the management of information and thus makes the creation and the operation of IS possible.

IM can be described as "die verantwortliche Gestaltung der betrieblichen Informationswirtschaft im weitesten Sinn von ihrer Konzeption im Sinn einer Unterstützung der Strategischen Unternehmensziele bis zur Realisation

unter den üblichen Effizienzgesichtspunkten, wie sie für alle betrieblichen Funktionen gelten" [Sch89].

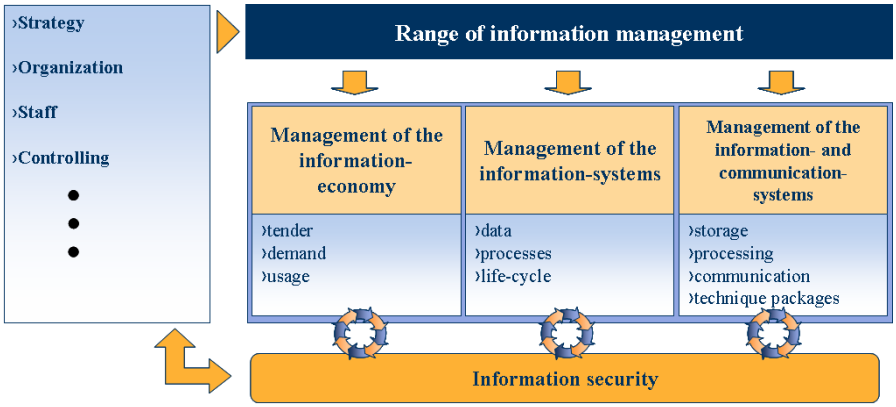


Figure 2: Information security as a cross-section task of the IM

Source: Own representation following [Krc2003, 46].

At present, information progressing (IP) is organized via the IM. With this is mind, it has to be remarked that information security is given only a minor role [Pfa97, Hei99, Sch98, KW93]. Publications tackle information security only as a secondary or third subdivision, which means it is a topic in which the focus is directed to the administrative as well as the operative field [Hil99, S. 135; Pfa97: Hei99; Sch98]. Information and communication are inseparable and require an integrated and integral assessment [Hei99], within which a trouble-free information processing can be guaranteed only with a high level of security. Because the IP is organized by the IM, information can not be protected independently of the IM, therefore, information security should rather be seen as a cross section task of the IM, as it is presented as an example in picture 2 [Kon98]. For further specification of information security, the tasks, which arise at the implementation and the use of the information system, have to be discussed.

Heinrich offers a generally accepted task-oriented theory for the IM, in which the tasks for the development and use of an information infrastructure are composed of the information function [Hei, 19]. Here, the information function is of particular importance as it occurs at the intersections of the basic functions as well as a cross section functions[6] and thus portrays the summary of all business tasks, referring to information and

[6] Basic functions are, for example, procuring, production, sales, and cross section functions such as personnel, finances and logistics.

communication [Hei99, S. 19]. The tasks of the information functions are to be placed at the strategic, administrative and the operative level.[7]

Strategic problems with the security of information can be revealed when the aims are being formulated, at the analysis of the situation and at the time when measures are being planned. These tasks will be explained below.

2.2 Strategic Areas of Responsibility of Information Security

2.2.1 Situation analysis

The main focus of the analysis is directed at the basis of the IS and in particular at the setting up and course of the structure, through which attacks and threats can not be detected and prevented efficiently [DKL93].

According to common understanding of system theory, a system is comprised of a number of certain elements, which are all interconnected. The definition of a system in relation to its environment, that means to surrounding systems, illustrates interfaces from which the analytical basis of an IS can be formed. The configuration of possible interfaces of an IS, is based on the structural aspect, that means the transformation of the input into the output and the consideration of the contents and connections within the IP.[8]

Feasible components, which relate to the setting up and the course of the structure of an IS are: (1) software, (2) hardware, (3) tasks and associated kinds of information, (4) faculties, institutions and central fields,[9] (5) business processes, as well as activities and procedure. Apart from the examination of structural aspects of an organization, business processes of the IP have to be considered. They will be described below in form of chains of processes driven by events (CPE), which, in particular, disclose weaknesses in information security. Its core elements are incidents, data objects and organization units as well as functions and combining opera-

---

7 Strategic tasks cover the long-term adjustment of IM at the company targets. Tasks for the realization and maintenance of the infrastructure, especially the entire system planning and development are called strategic tasks and converted strategic planning. Operational tasks designate the enterprise and the use of an existing information and communication infrastructure. [Krc03]

8 The definition of the analysis articles by the exclusive view of the input as well as the output would correspond to a "Black box process" and only rudimentary statements about contentwise connections would entail.

9 Especially their spatial distribution as well as their primary and secondary relations.

tors [SJ96]. Business processes can be analyzed, improved or organized anew by the formation of CPEs. Furthermore, a reduction in complexity of organization processes becomes possible, when the complex connection is divided into in single aspects (aspects of function, data and resources) [for further information Sch93].[10]

2.2.2 Security and Safety aims

The classification of aspects of the security of information, data and systems will be carried out with the terminology of availability, integrity, confidentiality, and reliability of the IP. Due to a possible threat to these aspects, security aims are formulated.

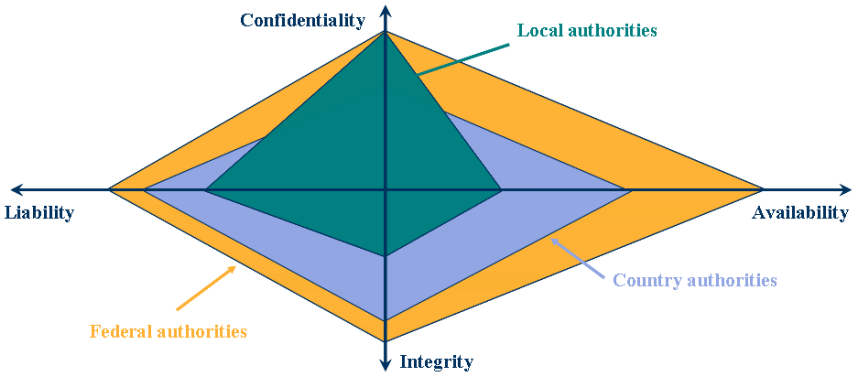


Figure 3: Classification of security aims in state-run organizations

Source: own depiction

As security aims, they have to be cumulative, and are described as so-called basic value of information security: (1) availability implicates that the practicality of the IS, is not impaired and that users have unrestricted access to its objects, (2) integrity means that all security relevant objects of the IP are complete, correct and unadulterated, (3) confidentiality means that only a selected number of users know about the contents and action of information, (4) reliability means that provability and authenticity

[10] Advantages of the modeling of the business processes by CPEs are: (1) condition changes of data objects as well as information flows are recognizable, (2) process-took part and organizational units are recognizable, (3) IT resources transparency as well as (4) information in connection with the business process set whereby its value become quantifiable [resuming Sch93].

are given [e.g. Krc03; Hei02].[11] The definition of security aims of state-run organizations is subject to the heterogeneous tasks of departments, which provide service, and will be shown in picture 3.

2.2.3 Requirements

The demand of the identification of weak points within a IS constitutes the formulation of security requirements, which define material or potential deviations from the specified condition. Against the background of a risk-fair security[12] classification the sensitivity of the objects involved in the IP and the entire organization have to be specified according to endangerments of information security. This classification takes place in four steps: (1) Determination of the relevance of information concerning their value for an organization. This necessity creates extraordinary problems for organizations, particularly for those run by the state.[13]

Figure 4: Objects of the threat

Source: Personal representation following [BMW04]

(2) As a result, the analysis of the information objects and -streams is indispensable, whereby threatened information during IP-processes should

---

[11] Further aspects of information security like correctness, originality, genuineness, trustworthiness, reliability are specified occasionally with equal standing and are usually only further broken down in its statement. [Kon98]

[12] Information uniformly on highest security level to protect is neither technically realizable nor economically justifiable, therefore security requirements should seize, where risks are not portable.

[13] In the operational surrounding field the value of information is usually determined at its contribution for the creation of value, their portion of furnishing innovation or their portion of attaining from competition advantages.

be located and examined in greater detail. (3) The effects and consequences that follow when information loses its availability, liability, integrity or confidentiality, have to be elaborated by chains of acting elements, and the tolerable endangerments of information have to be separated from the intolerable. Figure 4 gives an overview of potentially threatened objects. In step (4) existing security and control elements are to be examined concerning the security of information that has been determined as relevant [following Obe97; LG95].

This determined additional security then requires specific co-ordinated security precautions, which are represented exemplary in the following chapter.

2.2.4 Security precautions

A close relationship exists between measures and threats, whereby the measures are aimed at information security, in order to reach a condition, in which information is secured for loss, availability, integrity, liability as well as for confidentiality [DKL93]. This is followed by a systematization of security precautions belonging to the causal as well as the level model.

The causal model differentiates between cause and effect-related security precautions. Effect-related measures intend to minimize the latent power of endangerments. Cause-related security precautions avoid and/or reduce developing endangering occurrences in extenso [deepening Kon98, Ste93]. The level model differentiates between the physical, the logical, the legal-economical as well as the organizational-social level. The (1) physical level deals with physical and material fields of information security.[14] The (2) logical level concerns itself with logical and material aspects of securing information.[15] The field of the (3) legal-economical level is concerned with economic and legal aspects of information security,[16] whereas the (4) organizational-social level turns towards the reflection of the social dimension and also to the expiration and structure-

[14] For example hardware, structural measures and building, whereby security precautions can be the non removable disk reflection, admission control systems, the securing of energy or the air conditioning.

[15] Software, information as well as IP belong to this range. As measures like software protection functions such as passwords can be stated.

[16] These can be summarized as contractual regulations, material and immaterial goods, fundamental rights and right goods. As measures the data security and signature law can be specified.

organizational components of the organization [Ste93].[17] Security precautions can be completely structured by the causal and the level model, whereby the model can be taken as founded systematization to ensure information security in organizations.

3 Status Quo of Information Security in State-run Organizations

Today, without the use of IT systems, state-run organizations would not be manageable. Thus, information security increases in meaning in country-, federation- and local-authorities [Ros2003, 3].[18] Recent analyses confirm its necessity, as shown in table 1:

Year	Incidents	Difference	Vulnerabilities	Difference
1990	252	-	-	-
1995	2412	-	171	-
2000	21756	-	1090	-
2001	52658	142,04%	2437	123,58%
2002	82094	55,90%	4129	69,43%
2003	137529	67,53%	3784	-8,36%

Table 1: Security incidents and announced weak points of organizations.

Source: CERT/CC Statistics 1988-2004, http://www.cert.org/stats

As a concrete case, we would like to describe below one example of information security at universities and present their heterogeneous interfaces. Universities take on a responsible and indicative role with the development, the introduction and the employment of IS. The basis of a security strategy for universities is often seen in the qualified and competent support of the IT systems [Ros03]. It is postulated that success can only be achieved by an entire effort of "all", who are directly working in the field of information security. Within the framework of a co-operative

[17] On this level persons, organizational and administrative functions are settled. Security precautions are directed toward the identification of the co-workers with the relevance of information security and pointed to audits as classical and organizational measure.

[18] In a study to the IT trends 2004 the increasing meaning of the topic information security becomes clear. In a scale of 1 - 6 estimates approx.. 150 asked organizations the subject of information security 1,7. Whereupon ERP with 2,48, EAI with 2,96 as well as the topic of portals with 3,04. [Bettels, M/Jeschke, J, IT trend compares 2004 - new insights and prospects, Capgemini 2004]

concept of care, competent IT support persons are employed as well as IT security specialists who look after a faculty or a central institution.

The security of the information systems is usually classified by the universities as indispensable and understood as a joint task, carried out by everyone. In general, information security is supported, supervised and carried out directly by the university management. However, at universities, holistic and comprehensive strategies for information security are rarely to be found. Concepts to secure information dominate, which are interdependent due to their instances and respective adjustments. Thus, they are not goal-prominent.

Figure 5 explains exemplarily how different instances within the operational, administrative as well as strategic fields with tasks, responsibility, resources and authority overlap.

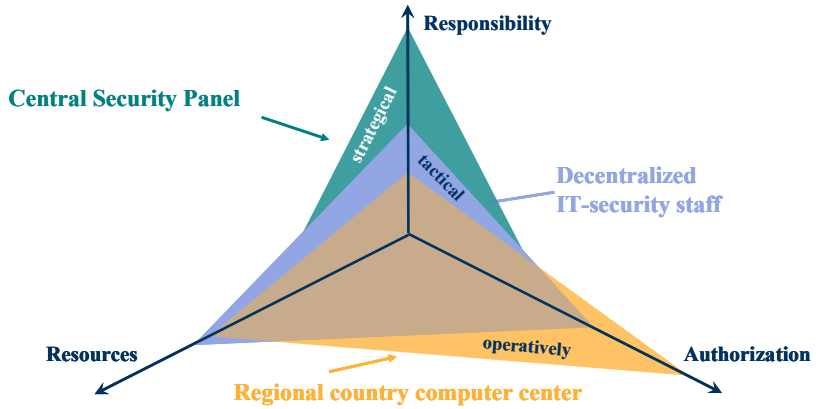


Figure 5: Heterogeneity of information security at universities

Source: Personal representation

Preceding representations illustrate the significant meaning of information security ascribed to universities in particular. Heterogeneous system landscapes and structures lead to special challenges in the university sector, which we will tackle with a holistic security process.

4 Long-Term Information Security with a Reciprocal Security Process

It is commonly believed that in national organizations strategic thinking and acting take place only in fields of fundamental and durable importance as well as pronounced complexity, which represent an organization-related total concept for information security. In this context, strategic guidance statements are to be formulated, conceptional defaults to be specified and

organizational basic conditions to be created, to ensure optimal and safe work.

4.1 Analysis of the Organization as a Constituent Part of the Security Process

The accurate and holistic statement of the strategic fields can only be ensured for the management of the information security of a complex IT group with a planned and gradual procedure of all who are involved. The initiative should proceed from the authority line, who is responsible for the entire process and who should actively accompany and support it. The procedure for the development of a founded security process is represented in detail in the following 4 phases:

Phase 1

In this phase the structure and expiration structure of the organization are determined, whereby interfaces to surrounding systems are determined. Subject of the view should also be the business processes of the IP through which, in particular, the weak points of information security will be uncovered.

Phase 2

In this step, the classification of the security goals of the organization takes place. Here, an evaluation will be given according to the type of organization regarding integrity, availability, liability and confidentiality of the information in IS.

Phase 3

This phase determines classification requirements for information security. Here, the IP will be defined as well as the IP security requirements for risk-fair security classification, which are focused on potentially endangered objects and processes.

Phase 4

Finally, the requirements are categorized according to security precautions. Whereby we differentiate between a cause and effect-related model and logical, physical, organizational-social and legal-economical measures.

Figure 6 illustrates the methodology of the aforementioned points:

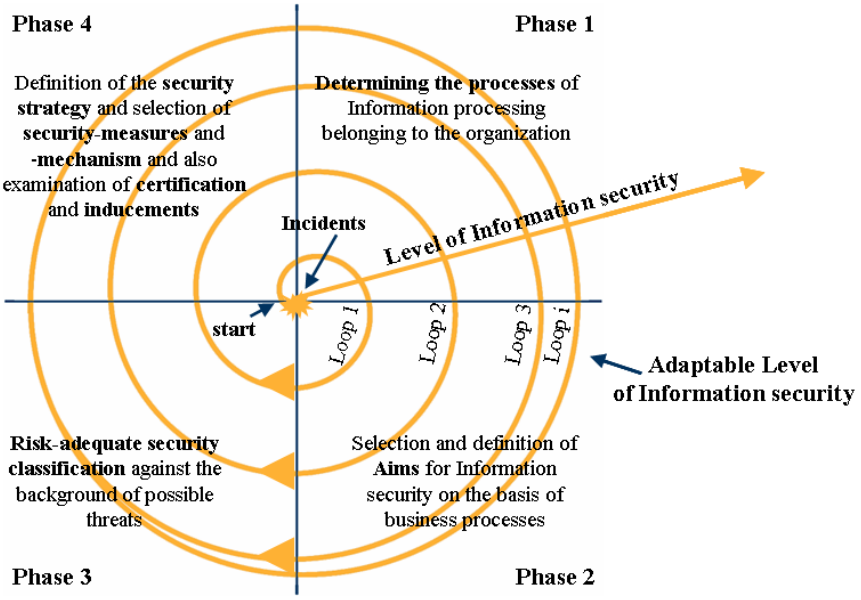


Figure 6: Strategic management of information security as a convergent spiral type model

Source: Personal representation

In phase 4, as a consequence of the 4 single phases, the security strategy of the organization is provided and examined in the following "Loop's" and adapted if necessary according to changing conditions. Whereupon defined security precautions are broken down to operational and administrative conditions and communicated in a manual for information security.

4.2 Certification of Organizations

Efforts to increase information security of organizations can form a basis from which the security standard of organization can be certified internationally. Certification designates thereby the examination and evaluation of products, persons or organizations according to uniform criteria such as standards, methods or best-practice beginnings [BSI03]. Preceding comments on the strategic management of information security can be used as an adequate basis, to certify an organization. Advantages result, such as the (1) international comparison and accessibility of IT systems and products. The (2) efforts concerning information security can be published and thus improve the reputation of the organization. (3) An objective third party reassured IT users and operators that the organization corresponds to the "state of the art". (4) Additionally, there is the possibility to define

oneself by an independent certification of other national organizations on a national and in particular on an international level.

4.3 Advantages of the Strategic Management of Information Security

Strong commitment to the security process, reciprocal in regular intervals, guarantees a permanent high level of information security.

Resulting costs of information security can be made transparent in national organizations as well, by the consistent adherence to the described phases (in particular phase 1).

Organizations can use their efforts for information security to achieve certification.

Concerted production, conversion and communication of a security strategy lead to identification and acceptance of information security on all levels of the organization.

Administrative and operational processes are subject to a total strategic concept for information security, i.e. they are not detached from the overall organization strategy.

Only the adequate classification of information security goals in national organizations permits an optimal and risk-fair definition of security requirements.

5 Conclusion and Outlook

Nowadays State-run organizations mostly depend on the permanent availability and operability of there is. Taking into account the increasing attacks on IS of State-run organizations, security of information becomes more important. The clearly visible complexity and permanent development of information systems lead to the insight that only a global and systematically performed strategic management of information security can be successful in the context of an integrated security process. This process is to be co-ordinated and adapted thereby to the special requirements and conditions of national organizations. In terms of cost, a Panazee for the complete safeguard of information security would be unrealistic and inadequate. The convergent security process, however, represents a suitable

solution for permanent development, follow up and examination of the strategic information management for national organizations.[19]

Among other things, the consistent commitment to the individual phases of the security process always leads to a high and flexible information security level, the acceptance of the security strategy by the organization members as well as to higher transparency of costs for information security in national organizations. Apart from the presented advantages of a strategic management of information security, some insurmountable problems become apparent such as the non-transparency of costs or the insufficient documentation of business processes for national organizations. In addition to this, running costs are to be taken into account to make the initiated security process last.

The necessity for information security in organizations has gained significant public attention for quite some time. In this context, this essay points to the fact that operational and administrative tasks cannot be lastingly goal-prominent if detached from strategic implications.

Hence, the strategic management of information security has to be integrated into the politics of security of state-run organizations, as a cross-sectional task of the information management, and as a "conditio sine qua non".

6 References

[BMW4] Biethahn, J./Mucksch, H./Ruf, W.: Ganzheitliches Informationsmanagement, I, München 2004, 83.

[BP98] Brenner, W./Pörtig, F.: Informationsmanagement - eine ungeliebte unternehmerische Aufgabe. In: io-Management, 9/1998, 27-30.

[Bro92] Brockhaus, R.: Informationsmanagement als ganzheitliche, informationsorientierte Gestaltung von Unternehmen - organisatorische, personelle und technologische Aspekte, 41.

[BSI03] Bundesamt für Informationstechnik (BSI): Grundschutzhandbuch 2003, http://www.bsi.de/gshb.pdf.

[DKL93] Drews, H./Kassel, H./Leßenich, H.R.: Lexikon Datenschutz und Informationssicherheit - Juristische, organisatorische und technische Begriffe, 4 Edition, Berlin 1993, 230.

[19] The production of a strategy for information security is neither a temporarily limited project nor another unique procedure, but a still continuing process. [Hug84, S. 66]

[Hei99] Heinrich, L.J.: Informationsmanagement - Planung, Überwachung und Steuerung der Informationsinfrastruktur, 6. Edition, München, 1999.

[Hei02] Heinrich, L.J.: Informationsmanagement – Planung, Überwachung und Steuerung der Informationsinfrastruktur , 7. Edition, Wien 2002.

[Hil99] Hildebrand, K.: Informationsmanagement – Wettbewerbsorientierte Informationsverarbeitung, 1999.

[Hop92] Hopfenbeck, W.: Allgemeine Betriebswirtschaftslehre- und Managementlehre, 5. Edition, Landsberg am Lech 1987, 409.

[Hüb96] Hübner, H.: Informationsmanagement und strategische Unternehmensführung – Vom Informationsmarkt zur Innovation, München 1996.

[Hug84] Hughes, P.J.: Business Risk Analysis & Contingency Planning. In: Online Conferences, Systems Security the Key to Computer Integrity, Proceeding of the European Computer Systems Security Forum, London 1984, 61-74.

[Kon98] Konrad, P.: Geschäftsprozessorientierte Simulation der Informationssicherheit – Entwicklung und empirische Evaluierung eines Systems zur Unterstützung des Sicherheitsmanagements. In: Seibt, D./Derings, U./Mellis, W., Reihe Wirtschaftsinformatik, Edition 20, Köln 1998, 21.

[Krc03] Krcmar, H.: Informationsmanagement, 2003.

[KW93] Krallmann, H./Wiegmann, B.: Ganzheitliche Sicherheit betrieblicher Informations- und Kommunikationssysteme. In: Scheer, A.-W.: Handbuch Informationsmanagement - Aufgaben, Konzepte, Praxislösungen, Wiesbaden 1993, 697-711.

[LW95] Lessing, G./Weese, E.: Organizationsstrukturen des IV-Sicherheitsprozesses. In: Pohl, H./Weck, G., Hrsg.: Beiträge zur Informationssicherheit: Strategische Aspekte der Informationssicherheit und staatlichen Reglementierung, Oldenburg 1995.

[Obe97] Obenauf, J.: Qualitäts- und Sicherheitsmanagement - ein Ansatz zur Berücksichtigung funktionaler und qualitativer Sicherheitsanforderungen, Reihe Informatik Band 2, Weiden 1997, S. 11-24.

[Pfa97] Pfau, W.: Betriebliches Informationsmanagement, Wiesbaden, 1997.

[Ros03] Rossa, C.: IT-Sicherheit – was ist das. In: Rechenzentrum der Universität Würzburg, Inside – Juni 2003, Würzburg 2003, 3-4. http://www.rz.uni-wuerzburg.de/infos/publikationen/daten/inside_04.pdf

[Sch89] Schüler, W.: Informationsmanagement: Gegenstand und organisatorische Konsequenzen. In Spremann, K./Zur, E.: Informationstechnologie und strategische Führung, Wiesbaden 1989, 184.

[Sch93] Scheer, A.-W.: ARIS - Architektur integrierter Informationssysteme. In: Scheer, A.-W., Hrsg., Handbuch Informationsmanagement - Aufgaben, Konzepte, Praxislösungen, Wiesbaden 1993, 89.

[Sch98] Schwarze, J.: Informationsmanagement - Planung, Steuerung, Koordination und Kontrolle der Informationsversorgung im Unternehmen, Herne, 1998, 253f.

[SDR98] Schwinn, K./Dippold, R./Ringgenberg, A./Schnider, W.: Unternehmensweites Datenmanagement - Von der Datenbankadministration bis zum modernen Informationsmanagement. In: Fedtke, S.: Zielorientiertes Business Computing, Braunschweig 1998, 30-35.

[SH97] Stahlknecht, P./Hasenkamp, U.: Einführung in die Wirtschaftsinformatik, Berlin 1997.

[SJ96] Scheer, A.-W./Jost, W.: Geschäftsprozeßmodellierung innerhalb einer Unternehmensarchitektur. In: Vossen, G./Becker, J. et al., Geschäftsprozeßmodellierung und Workflow-Management, Bonn 1996, 35.

[Ste93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes System für die Risikoananlyse, Wiesbaden 1993, 23.

[Sto94] Stockar, D. v.: Informationssicherheit – Bedeutung und Durchsetzung von Sicherheitsstandards im Unternehmen. In Cyranek, G.; Bauknecht, K. et al.: Sicherheitsrisiko Informationstechnik – Analysen, Empfehlungen, Maßnahmen in Staat und Wirtschaft, DuD-Fachbeitrag 19, Vieweg Verlag, Braunschweig 1994, 81.

[Wit96] Wittman, W.: Unternehmung und unvollkommene Information, Köln, Opladen, 14.

IWI Discussion Paper Series

ISSN 1612-3646

Michael H. Breitner, Rufus Isaacs and the Early Years of Differential Games, 36 p., # 1, January 22, 2003.

Gabriela Hoppe, Michael H. Breitner, *Classification and Sustainability Analysis of e-Learning Applications*, 26 p., # 2, February 13, 2003.

Tobias Brüggemann, Michael H. Breitner, *Preisvergleichsdienste: Alternative Konzepte und Geschäftsmodelle*, 22 p., # 3, February 14, 2003.

Patrick Bartels, Michael H. Breitner, Automatic Extraction of Derivative Prices from Webpages using a Software Agent, 32 p., #4, May 20, 2003.

Michael H. Breitner and Oliver Kubertin, WARRANT-PRO-2: A GUI-Software for Easy Evaluation, Design and Visualization of European Double-Barrier Options, 35 p., #5, September 12, 2003.

Dorothée Bott, Gabriela Hoppe and Michael H. Breitner, *Nutzenanalyse im Rahmen der Evaluation von E-Learning Szenarien*, 14 p., #6, October 21, 2003.

Gabriela Hoppe and Michael H. Breitner, *Sustainable Business Models for E-Learning*, 20 p., #7, January 5, 2004.

Heiko Genath, Tobias Brüggemann and Michael H. Breitner, *Preisvergleichsdienste im internationalen Vergleich*, 40 p., #8, June 21, 2004.

Dennis Bode and Michael H. Breitner, Neues digitales BOS-Netz für Deutschland: Analyse der Probleme und mögliche Betriebskonzepte, 21 p., #9, July 5, 2004.

Caroline Neufert and Michael H. Breitner, *Mit Zertifizierungen in eine sicherere Informationsgesellschaft*, 19 p., #10, July 5, 2004.

Marcel Heese, Günter Wohlers and Michael H. Breitner, *Privacy Protection against RFID Spying: Challenges and Countermeasures*, 21 p., #11, July 5, 2004.

Liina Stotz, Gabriela Hoppe and Michael H. Breitner, *Interaktives Mobile(M)-Learning auf kleinen Endgeräten wie PDAs und Smartphones*, 28 p., #12, August 18, 2004.

Frank Köller and Michael H. Breitner, Optimierung von Warteschlangensystemen in Call Centern auf Basis von Kennzahlenapproximationen, 24 p., #13, January 10, 2005.

Phillip Maske, Patrick Bartels and Michael H. Breitner, *Interactive M(obile)-Learning with UbiLearn 0.2*, 21 p., #14, April 20, 2005.

Robert Pomes and Michael H. Breitner, Strategic Management of Information Security in State-run Organizations, 18 p., #15, May 5, 2005.