

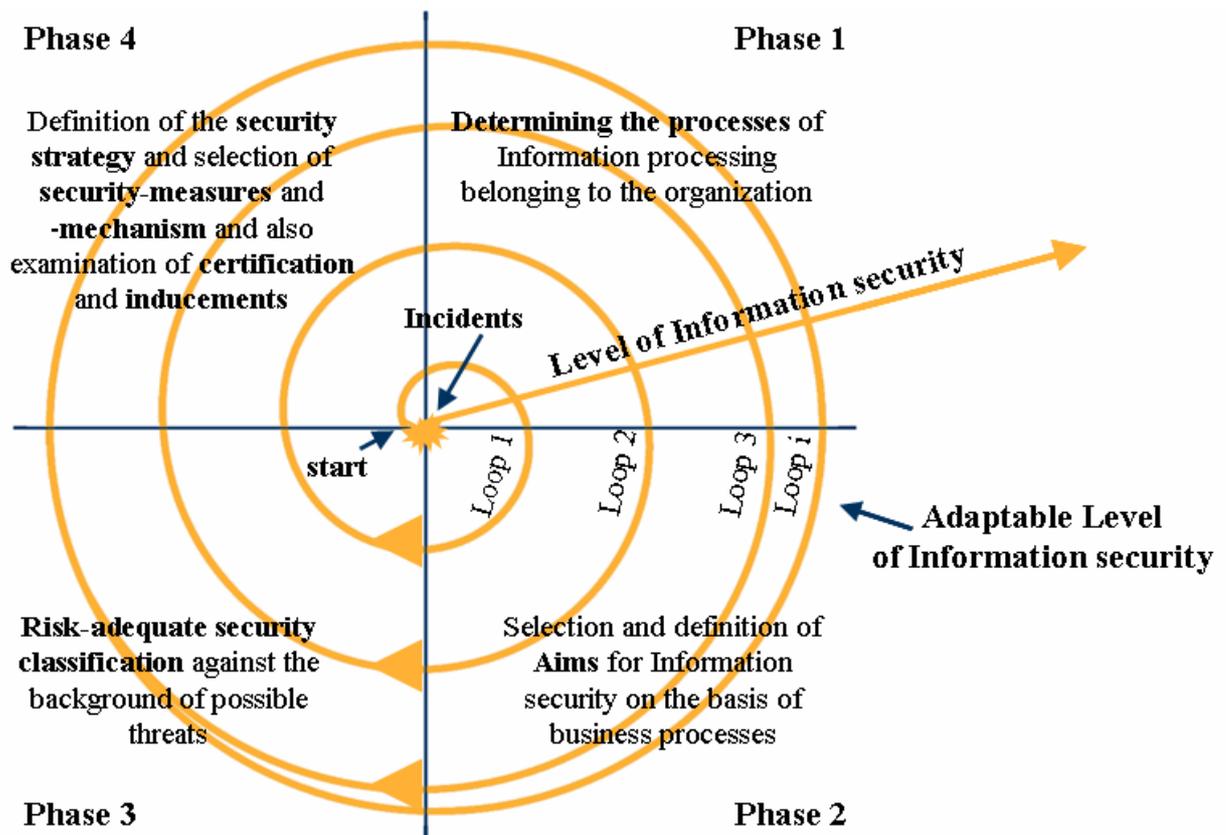
# IWI Discussion Paper Series # 15 (May 5, 2005)<sup>1</sup>



ISSN 1612-3646

## Strategic Management of Information Security in State-run Organizations

Robert Pomes<sup>2</sup> and Michael H. Breitner<sup>3</sup>



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

<sup>2</sup> Diplom-Ökonom and PhD Student ([pomes@iwi.uni-hannover.de](mailto:pomes@iwi.uni-hannover.de)).

<sup>3</sup> Full Professor for Information Systems Research and Business Administration ([breitner@iwi.uni-hannover.de](mailto:breitner@iwi.uni-hannover.de)).

## Table of Contents

<b>1</b>	<b>Motivation and Aim .....</b>	<b>1</b>
<b>2</b>	<b>Foundations.....</b>	<b>3</b>
2.1	Security of Information Systems and Information Management .....	3
2.2	Strategic Areas of Responsibility of Information Security.....	5
2.2.1	Situation analysis .....	5
2.2.2	Security and Safety aims .....	6
2.2.3	Requirements .....	7
2.2.4	Security precautions.....	8
<b>3</b>	<b>Status Quo of Information Security in State-run Organizations .....</b>	<b>9</b>
<b>4</b>	<b>Long-Term Information Security with a Reciprocal Security Process .....</b>	<b>10</b>
4.1	Analysis of the Organization as a Constituent Part of the Security Process .....	11
4.2	Certification of Organizations .....	12
4.3	Advantages of the Strategic Management of Information Security.....	13
<b>5</b>	<b>Conclusion and Outlook .....</b>	<b>13</b>
<b>6</b>	<b>References .....</b>	<b>14</b>

# 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<sup>4</sup> 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 reason 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<sup>5</sup> 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.

---

<sup>4</sup> 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.

<sup>5</sup> 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.

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.<sup>19</sup>

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.

---

<sup>19</sup> 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]

## 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.

Dorothee 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.

