

RESEARCH

Tobias Ackermann

IT Security Risk Management

Perceived IT Security Risks in
the Context of Cloud Computing



Springer Gabler

IT Security Risk Management

Tobias Ackermann

IT Security Risk Management

Perceived IT Security Risks
in the Context of Cloud Computing

 Springer Gabler

Tobias Ackermann
Fachgebiet Wirtschaftsinformatik
TU Darmstadt
Darmstadt, Germany

Dissertation Technische Universität Darmstadt, 2012

D 17

ISBN 978-3-658-01114-7
DOI 10.1007/978-3-658-01115-4

ISBN 978-3-658-01115-4 (eBook)

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Library of Congress Control Number: 2012955651

Springer Gabler

© Springer Fachmedien Wiesbaden 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use. While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer Gabler is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-gabler.de

Foreword

Since many years, IT outsourcing is a widespread and actively used opportunity to transfer IT functions to third parties and thereby reduce costs. In recent years, the current trend in the form of Cloud Computing, i. e., the sourcing of applications, computing power and storage space over the Internet, is increasingly discussed by scientists and practitioners. However, the promised benefits of Cloud Computing are accompanied by a growing number of IT security incidents that are, on the one hand, a problem for the users, as they may not be able to access and use the service or because the confidentiality of their customer data may be compromised. On the other hand, such security incidents are also a problem for the service providers as they may jeopardize their reputation and may lose customers.

Therefore, the research objective of this thesis is to analyze the perception and effect of IT security risks of Cloud Computing in detail. First, the relevant IT security risks of Cloud Computing are identified and systematized in a structured process, in order to later use them as a part of an empirical survey. A quantitative empirical survey is used to examine how potential users perceive IT security risks as well as how these risk estimations affect the adoption of Cloud Computing. At the end, using a mathematical model specifically designed for the characteristics of Cloud Computing scenarios, it is investigated how parameters of a scenario affect the distribution of potential losses.

This thesis's first part addresses the analysis of the various IT security risks of Cloud Computing and their perception. In order to identify the individual components of the concept "IT security", Mr. Ackermann first presents a structured literature review. The iterative refinement of search results and the following process of extracting all relevant individual risks and clustering them to risk dimensions are thoroughly described. Mr. Ackermann uses the Q-sort method to systematically evaluate the resulting taxonomy. In order to further refine and evaluate the individual risk descriptions, he conducts qualitative interviews with 24 IT security

experts. Thereby, the exhaustiveness of the list of risks is ensured and it is possible to discover five previously not published individual risks. Subsequently, the formal specification of the latent construct “Perceived IT Security Risk” is described and the relationships and effects between the individual constituting dimensions and their risks is discussed. Finally, after describing the setup of the quantitative empirical survey, the validation of the developed scale is presented. In addition to traditional tests of the goodness of fit and the validity and reliability of indicators and constructs, the scale is also tested using more advanced tests, such as known-groups comparison or tests for nomological and multidimensional validity.

Mr. Ackermann makes several significant contributions to information systems science: In addition to the developed scale, the analysis of the effects of the perceived IT security risks on the potential users’ adoption decisions contributes to information systems literature. Based on the theory of reasoned action and previous studies, he derives hypotheses about the decision processes of IT executives. The hypotheses are analyzed in the form of structured equation models and their validity is confirmed using the responses of the quantitative study. The results show that the perceived IT security risk has a double detrimental effect on Cloud Computing adoption decisions.

In this thesis’s second part, Mr. Ackermann develops a mathematical risk quantification framework which can be used to support the IT risk management process for Cloud Computing scenarios. He describes methods with which it is possible to identify the individual risk or component that introduces the biggest share of the overall aggregated risk distribution. The results of the sensitivity analysis indicate that scenarios are more sensitive to changes in the amount of the potential losses, while changes to the occurrence probabilities or the number of risks have a smaller effect on the resulting distribution. Moreover, the framework is applied to an existing e-commerce system where two alternative security levels are compared to each other in order to find the most economically reasonable countermeasures. Additionally, the cost drivers of the scenario are identified with the help of the presented methods.

The entire scale development process as well as the mathematical model’s analysis show a great degree of methodological rigor and provide many interesting results. This thesis will be valuable to readers in both, academia and practice, as it suggests concrete recommended actions for users and providers of Cloud Computing services that can be applied during IT risk management. Therefore, I wish this thesis a widespread distribution.

Preface

This thesis was written during my work as a research assistant at the chair of Information Systems | Software Business & Information Management at the Technische Universität Darmstadt.

I am especially grateful for my supervisor Prof. Dr. Peter Buxmann, who greatly supported me and gave me many helpful suggestions. Likewise, I would like to thank my second referee Prof. Dr. Alexander Benlian for his valuable advises.

Furthermore, I thank the CASED graduate school for the granting of a PhD scholarship as well as numerous CASED postdocs and PhD students with whom I conducted the qualitative interviews.

My special thanks go to my friends and colleagues Alexander, André, André, André, Andreas, Anne, Anton, Björn, Christoph, Cornelia, Daniel, Eva, Florian, Golriz, Janina, Jasmin, Jin, Kerstin, Leonardo, Mark, Markus, Markus, Michael, Oliver, Omid, Patrick, Ruth, Sebastian, Sebastian, Sheikh, Sonja, Stefan, Sunil, Thomas, Thomas, Thorsten, Tobias und Tolga, whom I thank wholeheartedly for their support.

Darmstadt, September 2012

Tobias Ackermann

Contents

1	Introduction	1
1.1	Problem Description and Motivation	1
1.2	Objectives and Benefit	4
1.3	Structure of this Dissertation	8
2	Foundations	11
2.1	Cloud Computing	11
2.2	IT Risk Management	14
2.2.1	Risk-related Definitions	14
2.2.2	The Nature of Perceived Risk as Multi-Dimensional Construct	15
2.2.3	IT Risk Management Process	16
2.3	Risks in the Context of IT Outsourcing and Cloud Computing	22
3	Evaluation of Perceived IT Security Risks	27
3.1	Development of Measures Using a Structured Literature Review ..	29
3.1.1	Selection of Scientific Databases	29
3.1.2	Selection of Keywords	30
3.1.3	Search Filters	32
3.1.4	Successive Refinement of Risk Items	32
3.2	Scale Evaluation and Refinement Using the Q-Sort Method	37
3.3	Scale Evaluation and Refinement Using Qualitative Interviews among Security Researchers	40
3.4	Construct Conceptualization and Model Specification	42
3.4.1	Formal Measurement Specification	42
3.4.2	Descriptions of Security Risk Dimensions	44
3.5	Scale Assessment and Validation Using an Empirical Survey	49

- 3.5.1 Survey Development and Implementation 49
- 3.5.2 Methods of Validation 53
- 3.6 Analysis of Adoption Decisions 68
 - 3.6.1 Theoretical Perspective and Hypothesis Development 68
 - 3.6.2 Description of Measures 73
 - 3.6.3 Results of the Statistical Analysis 75
 - 3.6.4 Discussion of the Survey’s Results 82
- 4 Risk Quantification Framework 85**
 - 4.1 Model Description 85
 - 4.1.1 Parameter Descriptions 86
 - 4.1.2 Calculations of the Overall Risk Distribution 91
 - 4.1.3 Determination of Risk Measures 95
 - 4.2 Simulations 98
 - 4.2.1 Identification of Costs Drivers 98
 - 4.2.2 Sensitivity Analysis 101
 - 4.2.3 Trade-off: Accuracy and Performance 108
 - 4.3 Model Applications 114
 - 4.3.1 Dynamic Posted Pricing Service 114
 - 4.3.2 Decision Support System Prototype 123
- 5 Recommended Actions 127**
 - 5.1 Recommended Actions for Risk Identification 129
 - 5.2 Recommended Actions for Risk Quantification 131
 - 5.3 Recommended Actions for Risk Treatment 136
 - 5.4 Recommended Actions for Risk Review and Evaluation 138
 - 5.5 Recommended Actions for Cloud Computing Providers 139
- 6 Limitations, Summary, and Prospect 141**
 - 6.1 Limitations and Critical Assessment 141
 - 6.2 Summary 143
 - 6.2.1 Theoretical Contributions 143
 - 6.2.2 Practical Contributions 144
 - 6.2.3 Conclusion 145
 - 6.3 Recommendations for Future Work 148
- Appendix 151**
 - A.1 Sources for the Literature Review 152
 - A.2 Sources for each Risk Item 156
 - A.3 Q-Sort Statistics 158
 - A.4 Expert Interview Statistics 164

A.5 Questionnaire Items165

A.6 Survey Questionnaire167

A.7 Descriptive Sample Characteristics174

A.8 Results for Other Structural Equation Models176

References179