IT Risk Management –
A Causal Modeling Approach for
End-User Computing

daniel J. Hinz

IWI Jour fixe
Frankfurt/Main, February 14th, 2006
• Motivation and research history

• Theoretical foundation
  – IT infrastructure continues to be a hot topic for more than 15 years now
  – Surprisingly, research neglects the management of inherent infrastructure risks
  – Financial risk management theory suggests the use of causal modeling approaches

• Study design
  – A single case study was used to create a design-oriented artifact
  – For desktop availability, experts identified and estimated a Bayesian Belief Network (BBN)
  – The validation with historical loss data resulted in adaptations

• Key findings
  – Implications for decision making: user incidents are a sensitive figure
  – Findings can be efficiently communicated by a balanced scorecard

• Contributions, limitations, and further research
• Motivation and research history

• Theoretical foundation
  – IT infrastructure continues to be a hot topic for more than 15 years now
  – Surprisingly, research neglects the management of inherent infrastructure risks
  – Financial risk management theory suggests the use of causal modeling approaches

• Study design
  – A single case study was used to create a design-oriented artifact
  – For desktop availability, experts identified and estimated a Bayesian Belief
    Network (BBN)
  – The validation with historical loss data resulted in adaptations

• Key findings
  – Implications for decision making: user incidents are a sensitive figure
  – Findings can be efficiently communicated by a balanced scorecard

• Contributions, limitations, and further research
Situation

• An international logistics company has an outsourced IT infrastructure of end-user computers, servers, and network

• During contract renegotiation, end-user computers are hotly debated
  – Major structural changes are the foundation to improve reliability and to reduce costs
  – Corresponding tightened SLA figures and objectives were negotiated

• Currently, transformation still in progress and SLA figures are not fully met

Who is responsible?
Are fundamental assumptions of the new contract correct?
Main question

How can risks arising from IT infrastructure be effectively assessed and communicated?

Sub questions

Assessment

• How to identify IT risks in a structured way
• How to measure or predict the risk potential (e.g., downtime)
  – In steady state (normal operation)
  – In change scenarios (e.g., outsourcing, contract renegotiation)

Communication

• How to facilitate decision making by communicating IT risks and the potential effects of mitigation measures effectively
• How to control risk mitigation strategies through effective reporting
# Thesis Structure and Peer Review Plan

## Thesis Structure

<table>
<thead>
<tr>
<th>Module</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction/Motivation</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
</tr>
<tr>
<td>Theoretical foundation</td>
<td>Financial risk management domain, IT management theory, DSS</td>
</tr>
<tr>
<td>Causal modeling of IT risks</td>
<td>Development of classification model for operational risk, key risk drivers and dependencies, modelling of Bayesian Belief Network for PC desktop risks, empirical validation (single case study)</td>
</tr>
<tr>
<td>Application for IT managers</td>
<td>Communication and management of IT risks with BSC, risk mitigation strategies</td>
</tr>
<tr>
<td>Outlook and further research</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
</tr>
</tbody>
</table>

## Peer Review Plan

<table>
<thead>
<tr>
<th>Peer Review Plan</th>
<th>Part of Thesis</th>
<th>Accepted</th>
<th>Submitted/Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GITMA 06</strong>: &quot;IT Risks: Definition and Challenges&quot; (part of roof paper)</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>HICSS-38</strong>: &quot;High Severity IT Risks in Finance&quot;</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>ECIS 2006</strong>: &quot;Employing Bayesian Belief Networks for Measuring the Operational Risk of Information Systems&quot; (with H. Gewald)*</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>PACIS 2004</strong>: &quot;A Framework for Classifying the Operational Risks of Outsourcing&quot; (with H. Gewald)</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>WP</strong>: &quot;IT risk assessment – methods and application&quot; (with cluster 2: Pérez, Martinovic, Berbner, Steinmetz)</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>IRMA 2006</strong>: &quot;The Next Wave in IT Infrastructure Risk Management – A Causal Modeling Approach with BBNs&quot; (with H. Gewald)</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>(Journal): Empirical results</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>HICSS-39</strong>: &quot;Enhancing the Prognostic Power of IT Balanced Scorecards with Bayesian Belief Networks&quot; (with S. Blumenberg)**</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>EFLQ 3/2005</strong>: &quot;Management Communication of Complex Risk Assessment&quot; (with S. Blumenberg)*</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>ECIS 2006</strong>: &quot;An Integrated Approach to Assess and Communicate IT Risks&quot; (with Blumenberg, Weitzel)*</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>IRMA 2006</strong>: &quot;Mitigating Software Risk with Web Services&quot;</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>HICSS-39</strong>: &quot;Assessing the Risks of IT Infrastructure – A Personal Network Perspective&quot; (with J. Malinowski)</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /></td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

* Part of T-Systems agenda  ** Best paper nomination
• Motivation and research history

• Theoretical foundation
  – IT infrastructure continues to be a hot topic for more than 15 years now
  – Surprisingly, research neglects the management of inherent infrastructure risks
  – Financial risk management theory suggests the use of causal modeling approaches

• Study design
  – A single case study was used to create a design-oriented artifact
  – For desktop availability, experts identified and estimated a Bayesian Belief Network (BBN)
  – The validation with historical loss data resulted in adaptations

• Key findings
  – Implications for decision making: user incidents are a sensitive figure
  – Findings can be efficiently communicated by a balanced scorecard

• Contributions, limitations, and further research
IT INFRASTRUCTURE CONTINUES TO BE A HOT TOPIC FOR MORE THAN 15 YEARS NOW

SIM survey

- Survey to identify the most critical issues in IS management
- Conducted regularly by the Society for Information Management (SIM), supported by the MIS Research Center (MISRC)
- Among their members consisting of top executives as well as IS researchers

1990
"IT infrastructure" appears for the first time in the top 10 issues identified by the survey

1995
"Building a responsive infrastructure" was ranked number one challenge

2000
"IT infrastructure management" ranked third in these two informal surveys

2001

2003
"Infrastructure developments" ranked second in the category of top application and technology developments

### Main viewpoints on IT infrastructure

<table>
<thead>
<tr>
<th>IT architecture</th>
<th>Main research questions</th>
<th>Main answers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• What are requirements and features of a good IT infrastructure?</td>
<td>• Flexibility</td>
</tr>
<tr>
<td></td>
<td>• What is the enabling technology?</td>
<td>• Standardization</td>
</tr>
<tr>
<td></td>
<td>• How can IT and business be aligned?</td>
<td>• Security</td>
</tr>
<tr>
<td></td>
<td>• What is the economic impact?</td>
<td>• Web Services</td>
</tr>
<tr>
<td></td>
<td>• What is a good management interface to the provider?</td>
<td>• SOA</td>
</tr>
<tr>
<td>(Internal) IT management processes</td>
<td>• Which internal support processes are needed?</td>
<td>• Risk assessment</td>
</tr>
<tr>
<td></td>
<td>• How can IT (risks) internally be managed?</td>
<td>• SLA management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Practical &quot;handbooks&quot; (ITIL)</td>
</tr>
</tbody>
</table>
FINANCIAL RISK MANAGEMENT THEORY SUGGESTS THE USE OF CAUSAL MODELING APPROACHES

<table>
<thead>
<tr>
<th>Generic (risk) management process</th>
<th>Assessment</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>Measurement</td>
<td>Decision making</td>
</tr>
<tr>
<td>• Systematically identify main sources of risk</td>
<td>• Estimate probabilities and loss to quantify risk</td>
<td>• Decide on mitigation measures</td>
</tr>
<tr>
<td>• Expert judgment</td>
<td>• Analysis of historical loss data</td>
<td>• Parallel consideration of prior analyses</td>
</tr>
</tbody>
</table>

Main tasks

Classical source of information

Suggestions from financial theory

- Literature for operational risk management suggests causal modelling with **Bayesian Belief Networks** (BBN) [Alexander 2002]
  - To combine expert estimations with loss data
  - To identify key risk indicators and mitigation levers
  - To allow for upfront simulation

**Balanced Scorecard** (BSC) is a powerful and well-established method to communicate causal dependencies to top management [Van der Zee, De Jong 1999]
• Motivation and research history

• Theoretical foundation
  – IT infrastructure continues to be a hot topic for more than 15 years now
  – Surprisingly, research neglects the management of inherent infrastructure risks
  – Financial risk management theory suggests the use of causal modeling approaches

• Study design
  – A single case study was used to create a design-oriented artifact
  – For desktop availability, experts identified and estimated a Bayesian Belief Network (BBN)
  – The validation with historical loss data resulted in adaptations

• Key findings
  – Implications for decision making: user incidents are a sensitive figure
  – Findings can be efficiently communicated by a balanced scorecard

• Contributions, limitations, and further research
A SINGLE CASE STUDY WAS USED TO CREATE A DESIGN-ORIENTED ACTIFACT

Step 1: Model building and initialization based on expert estimation

- Two subject matter experts from leading IT consultancies
  - One with deep knowledge of company's IT and contract intentions
  - One with general knowledge of IT infrastructure
- No prior input from logistics company
- Iterative approach according to Eisenhardt and Yin

Typical process for construction of Bayesian Belief Networks

Resulting model

Step 2: Model adaption based on historical data

- Incident data from company's helpdesk systems during migration phase
- Enriched with individual configuration data for each system over time
- Key figures
  - App. 30,000 computers
  - 4 months of observation
  - Over 80,000 incidents
  - App. 120,000 aggregated data sets
FOR DESKTOP AVAILABILITY, EXPERTS IDENTIFIED AND ESTIMATED THE FOLLOWING BBN
THE VALIDATION WITH HISTORICAL LOSS DATA RESULTED IN ADAPTIONS

**Counter-intuitive findings**

- Notebook computers are as reliable as desktop computers
- Standardization has no effect on error resolution times
- Software image standardization and complexity obviously also drives number of user incidents

**Resulting adoptions**

- Edges connecting ostensibly independent nodes are kept in order to reflect the experts’ judgement
- New edges are added to incorporate newly identified dependencies
• **Motivation and research history**

• **Theoretical foundation**
  – IT infrastructure continues to be a hot topic for more than 15 years now
  – Surprisingly, research neglects the management of inherent infrastructure risks
  – Financial risk management theory suggests the use of causal modeling approaches

• **Study design**
  – A single case study was used to create a design-oriented artifact
  – For desktop availability, experts identified and estimated a Bayesian Belief Network (BBN)
  – The validation with historical loss data resulted in adaptations

• **Key findings**
  – Implications for decision making: user incidents are a sensitive figure
  – Findings can be efficiently communicated by a balanced scorecard

• **Contributions, limitations, and further research**
Only 8% of total measured downtime is due to user incidents and further reduction of TTR seems difficult …

… however, more than half of all incidents are user inquiries.

<table>
<thead>
<tr>
<th>Category</th>
<th>% of Total Downtime</th>
<th>% of Total Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other*</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Network*</td>
<td>17</td>
<td>9</td>
</tr>
<tr>
<td>Hardware</td>
<td>12</td>
<td>30</td>
</tr>
<tr>
<td>Software</td>
<td>61</td>
<td>52</td>
</tr>
<tr>
<td>User</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

Average TTR in days:

- Network*: 4,446 days
- Software: 4,229 days
- Other*: 3,354 days
- Hardware: 2,720 days
- User: 0,335 days

Special attention has to be given to user incidents, as impact on desktop uptime is minor, but number of user incidents is enormous. Further analyses (e.g., by benchmarking) may indicate, whether focus should be on reduction of incident volume instead of TTR.

* Not significant (e.g., network mass problems not included)
CLASSICAL APPROACHES FOCUS ON "OFFICIAL" INCIDENTS, BUT THEY ARE ONLY ONE PART

Situation
Classical approaches measure mostly official incidents (e.g., helpdesk calls) [Niessink and Van Vliet, 2000]

Complication
- Not all incidents are reported but instead solved by asking co-workers or known experts
- How can those aspects be considered to get a more realistic number of incidents?
THE DENSITY OF THE SOCIAL NETWORK HAS AN INFLUENCE ON PROBLEM SOLVING

Based on expert interviews, two measures from Social Network Analysis (SNA) were chosen to influence problem solving.

**Socio-Centric Density (SCD)**

Of the network of co-workers [Barnes 1974]

\[
SCD = \frac{l}{n(n - 1)}
\]

**Ego-Centric Density (ECD)**

Of the helpdesk [Scott 2000]

\[
ECD = \frac{l}{n}
\]
SCD AND ECD CAN BE USED TO GET A MORE REALISTIC NUMBER OF USER INCIDENTS

The ratio of both densities can be used to predict the unknown number of total user incidents (UI) from the number of known incidents (CHD)

\[
UI = CHD \cdot \left(1 + \alpha \frac{SCD}{ECD}\right)
\]

**UI:** User incidents  
**CHD:** Calls that reach the helpdesk  
**α:** Scaling factor

Example

Calculation of user incidents:

\[
SCD = 0.68  
ECD = 0.80  
\Rightarrow UI = 185
\]
THE INITIAL MODEL HAS TO BE EXTENDED TO REFLECT THESE FINDINGS

Helpdesk quality and social network density now determine the user action upon an incident.
Balanced Scorecard (BSC)
Consists of entities (called figures), grouped within perspectives
Directed edges indicate causal relationships
Loops are allowed, but should be omitted to be compatible with BBNs

Bayesian Belief Networks (BBN)
Consists of entities (called nodes), may be grouped graphically
Directed edges describe causal relationships and are used to calculate conditional probabilities
Loops are not allowed (graphs has to be directed and acyclic)
FINDINGS CAN BE EFFICIENTLY COMMUNICATED BY A BALANCED SCORECARD

- Desktop infrastructure availability: Percentage of downtime
- Server availability: Percentage of downtime
- HW standardization: Percentage of standardized systems
- SW image complexity: Percentage of complex images
- SW standardization: Percentage of standardized systems
- User incidents: Number of calls
- Fieldservice TTR: Avg. time per call
- Helpdesk TTR: Avg. time per call
• **Motivation and research history**

• **Theoretical foundation**
  – IT infrastructure continues to be a hot topic for more than 15 years now
  – Surprisingly, research neglects the management of inherent infrastructure risks
  – Financial risk management theory suggests the use of causal modeling approaches

• **Study design**
  – A single case study was used to create a design-oriented artifact
  – For desktop availability, experts identified and estimated a Bayesian Belief Network (BBN)
  – The validation with historical loss data resulted in adaptations

• **Key findings**
  – Implications for decision making: user incidents are a sensitive figure
  – Findings can be efficiently communicated by a balanced scorecard

• **Contributions, limitations, and further research**
EX-ANTE SIMULATIONS ARE ONE OF THE MAJOR STRENGTHS OF THE APPROACH

Contributions to theory

• Causal modelling techniques can be applied to the assessment of IT infrastructure risks
• Bayesian Belief Networks and Balanced Scorecards can be combined to support a seamless and fully integrated risk management process
• Users seem to be a crucial point concerning risk, which are currently neglected by researchers and practitioners

Contributions to practice

• Simulations of the causal model help to identify most important risk mitigation levers
• In change scenarios like outsourcing negotiations, they may help to agree on key figures in the SLA
• The process itself of building and training the model improves risk understanding

Limitations and further research

• Further research has to show, whether this approach is actually better than others when applied in real world scenarios