Performance Measurement in Cross-Organizational Security Settings

7th International Workshop on Security Measurement and Metrics
Banff, Alberta

Lukas Demetz, Stefan Thalmann, Daniel Bachlechner, Ronald Maier
Overview

• Motivation
• Empirical Foundation
• Results
• Conclusion & Outlook
Motivation

What are suitable metrics for determining a service supplier’s level of security and compliance?
Empirical Foundation

- Two series of interviews with 28 information security professionals focusing on
  - Intra-organizational settings
  - Cross-organizational settings
- Interviews recorded, transcribed and qualitatively analyzed
Results

• Service Consumer
  – Quality of service supplier
    • # of security and compliance violations per service provider
  – Integration of existing landscape
  – Monitoring supplier
  – Skilled employees
    • # of employees able to integrate outsourced services
  – Trust for service providers
    • avg. probability of security incidents per supplier

• Service Supplier
  – Taking changes in technology into account
    • avg. time to plan for changes
  – Providing audit compliance
    • time/costs spent on audit activities
  – SLAs covering provided services
    • % of SLAs with assigned account manager
  – Cost of missing security
  – Customer satisfaction
Conclusion & Outlook

• Interviewees are able to judge whether processes are well performed, however, struggle to identify KPIs
• Interviewees face several challenges when trying to define suitable KPIs
• Based on the interviews and a thorough literature review exemplary KPIs could be proposed
• The evaluation of the success of a software tool focusing on achieving and maintaining secure and compliant IT infrastructures will be based on the proposed KPIs
Acknowledgments

The research leading to these results was partially funded by the European Union 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129) and through the COSEMA project which is sponsored by the Tyrolean business development agency.

http://www.posecco.eu

http://www.cosema.org/en
Contact

Lukas Demetz
Lukas.Demetz@uibk.ac.at

Stefan Thalmann
Stefan.Thalmann@uibk.ac.at

University of Innsbruck
School of Management
Information Systems I
Universitätsstraße 15
6020 Innsbruck, Austria
## KPIs – Service Consumer

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quality of service supplier</strong></td>
<td># of security and compliance violations per service provider</td>
</tr>
<tr>
<td><strong>Integration of existing landscape</strong></td>
<td>avg. time to realize changes of the existing IT landscape</td>
</tr>
<tr>
<td></td>
<td>avg. costs to realize changes of the existing IT landscape</td>
</tr>
<tr>
<td><strong>Monitoring supplier</strong></td>
<td>avg. time needed for auditing an (outsourced) service</td>
</tr>
<tr>
<td></td>
<td>avg. costs needed for auditing an (outsourced) service</td>
</tr>
<tr>
<td></td>
<td>% of service providers meeting defined security, compliance requirements and SLAs</td>
</tr>
<tr>
<td><strong>Skilled employees</strong></td>
<td># of employees able to integrate outsourced services</td>
</tr>
<tr>
<td></td>
<td># of employees able to negotiate technical details</td>
</tr>
<tr>
<td></td>
<td># of employees being able to monitor service provider</td>
</tr>
<tr>
<td><strong>Trust for service providers</strong></td>
<td>avg. probability of security incidents per supplier</td>
</tr>
<tr>
<td>KPIs – Service Supplier</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Taking changes in technology into account</strong></td>
<td></td>
</tr>
<tr>
<td>avg. time to plan for changes</td>
<td></td>
</tr>
<tr>
<td>avg. costs of change implementation</td>
<td></td>
</tr>
<tr>
<td><strong>Providing audit compliance</strong></td>
<td></td>
</tr>
<tr>
<td>time/costs spent on audit activities</td>
<td></td>
</tr>
<tr>
<td># of audits successfully completed</td>
<td></td>
</tr>
<tr>
<td>% of systems with security certifications</td>
<td></td>
</tr>
<tr>
<td><strong>SLAs covering provided services</strong></td>
<td></td>
</tr>
<tr>
<td># of SLAs per service</td>
<td></td>
</tr>
<tr>
<td>% of service levels that are measured</td>
<td></td>
</tr>
<tr>
<td>% of SLAs with assigned account manager</td>
<td></td>
</tr>
<tr>
<td><strong>Cost of missing security</strong></td>
<td></td>
</tr>
<tr>
<td>cost of security incidents per service</td>
<td></td>
</tr>
<tr>
<td><strong>Customer satisfaction</strong></td>
<td></td>
</tr>
<tr>
<td>% of stakeholders satisfied with quality of IT security</td>
<td></td>
</tr>
</tbody>
</table>
Study Procedure

Two Interview Series

12

Intra-organization Interviews

16

Cross-organization Interviews

Data analysis

Literature Review

Problems when measuring security

Exemplary KPIs
Open Questions

• How would you proceed to measure security in a cross-organizational security setting?
• Have you already done something similar?
• Do you have any recommendations?
• Do you know any best practices in this domain?