An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security

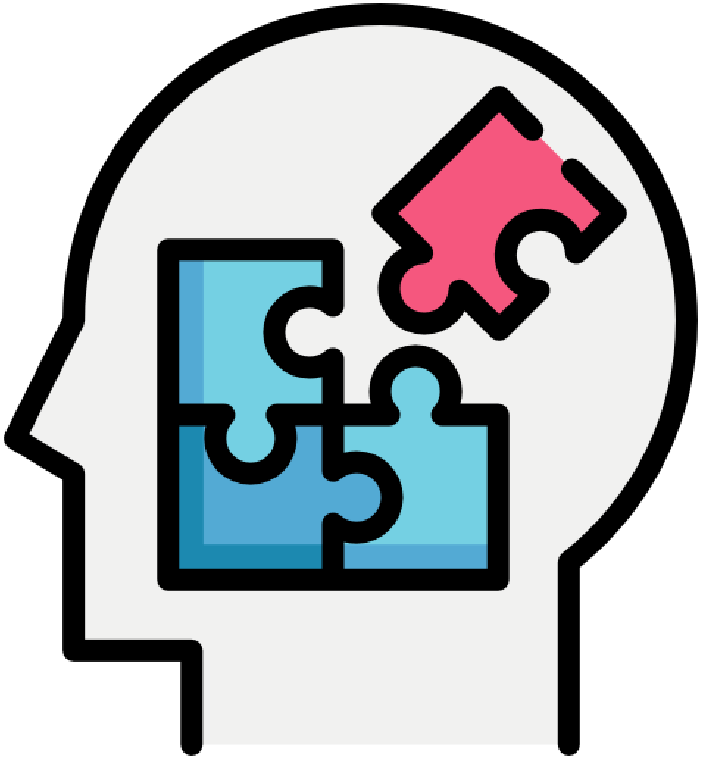
Sebastian Pape and Jelena Stankovic

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt

September 26th 2019 SPOSE Luxemburg

Agenda

- Introduction
- Methodology
  - Respondents
- Findings
- Discussion
- Conclusion



Introduction

- Cloud Computing / Outsourcing is broadly used.
- RQ1: ”What role does security play in CP selection?”
  - Expected:
    - to verify the importance of security.

      → CSPs invest in security

      → CSPs invest in quality/security assurance methods (lemon market)

- RQ2: „How are the providers’ security measures verified?“

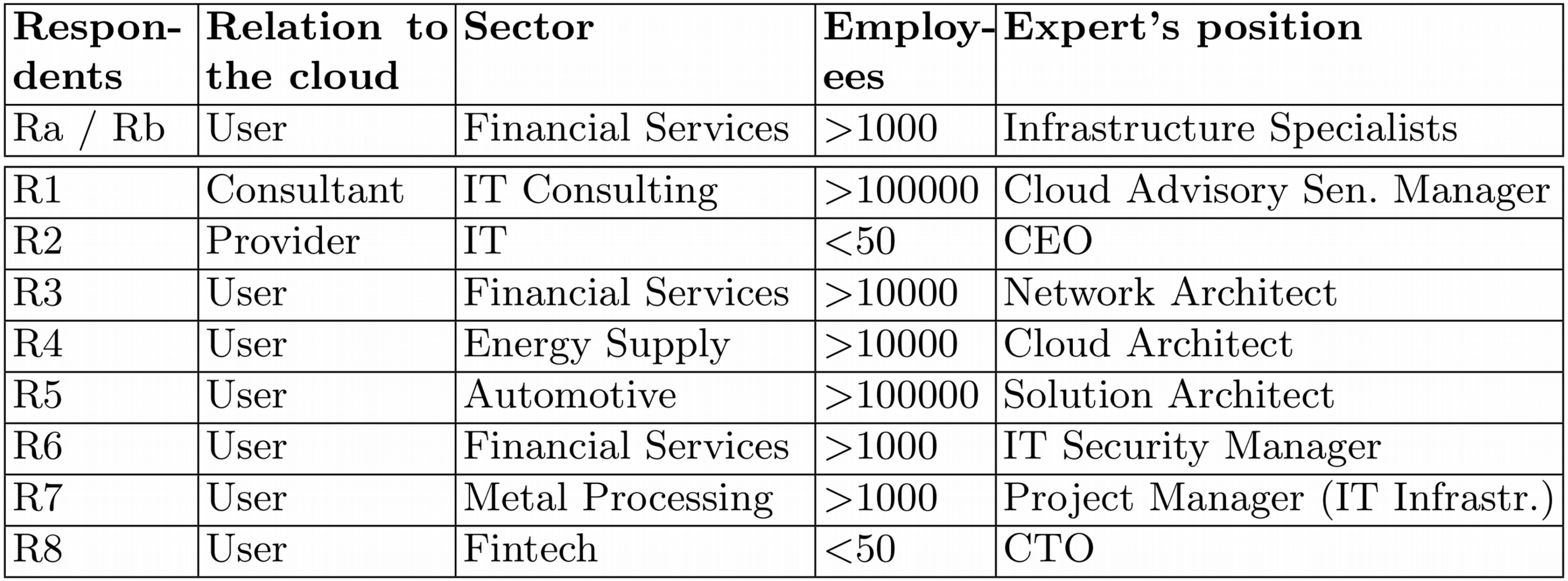
  alternatively:

- RQ3:Why is security not considered in CP selection?

Methodology: Interviews

- Literature Review on „security assurance“
  - Follow up on „Ardagnaet al.: From security to assurance in the cloud: A survey. ACM Comput. Surv. (2015)“
- Semi-structured interviews
  - With practitioners engaged in the selection of a CP
  - No financial compensation
  - Main question: „which criteria were considered when choosing a CP“?
    - If security mentioned: asked about possible assurance techniques
    - If security was not mentioned: asked about the importance of security
- Selection process
  - Cloud Expo Europe 2018
  - Personal network
- 1 Pilot interview
- 8 Interviews
  - from October to December 2018
  - average duration around 37 minutes

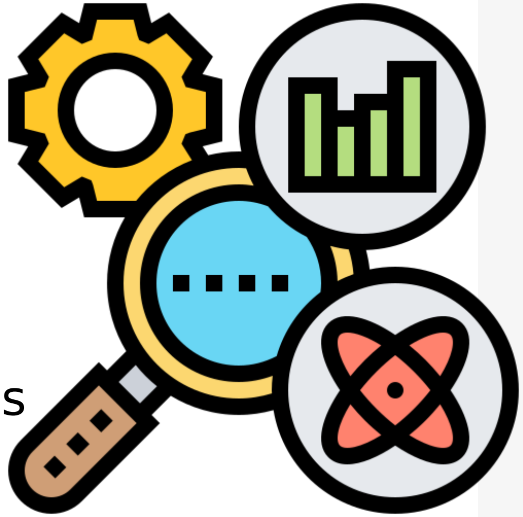
Respondents



Respondents	**Relation to the cloud**	**Sector**	**Employees**	**Expert's position**
Ra / Rb	User	Financial Services	>1000	Infrastructure Specialists
R1	Consultant	IT Consulting	>100000	Cloud Advisory Sen. Manager
R2	Provider	IT	<50	CEO
R3	User	Financial Services	>10000	Network Architect
R4	User	Energy Supply	>10000	Cloud Architect
R5	User	Automotive	>100000	Solution Architect
R6	User	Financial Services	>1000	IT Security Manager
R7	User	Metal Processing	>1000	Project Manager (IT Infrastr.)
R8	User	Fintech	<50	CTO

Methodology: Analysis

- Qualitative content analysis following Kuckartz (2016)
  - MAXQDA
- Steps:
  - Each interview was summarized
  - Master-coders chosen
    - deductively out of the interview questions
  - Coding all interviews with the master-codes
  - Grouped all passages coded with the same master-code
  - Inductively derived sub-codes for each master-code
  - Iterative approach



[Kuckartz, U.: Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung. Beltz Juventa (2016)]

Findings: The Role of Security in CP Selection

- Selection criteria
  - Costs (5), Size of provider (4), Ease of use (3)
  - Trust (3): Provider‘s reputation
  - Compliance (3)
  - Availability (3)
  - Multiple providers (2)
  - Hierarchy (2)
  - Confidentiality of their users’ data (2)
  - Convenience (4)

So many people shy away when they hear the name ”Google” considering them a ”data collector”

Basically the cloud risk process could have stopped the decision for the product.

Findings: Reasons for Moderate Interest in Security

- Coping / managing risk:
  - Mitigation (4): Chosing large CSPs and/or located in EU
  - Responsibility (4): Shared between company and CSP
  - Encryption (4)
  - Data Criticality (2)
  - Trust (4): not / fully
  - Personal Responsibility (2)
  - Compliance (4)

When we provide the infrastructure only, encryption is mostly in the hands of the customer. But then he has to manage the keys, which represents an additional complexity he has to handle.

[…] when there is a service failure, it applies to everyone and one can say: ”Yes, you know it, AWS just had an outage”. So it’s the IBM effect: ”No one ever got fired for buying IBM”, applies to AWS nowadays.

Findings: Verification of Providers’ Security Measures

- Problems raised
  - Certification (5): mostly ISO 27001
  - Audits (5): rarely done, if so financial
  - Contracts (5):
    - Data location,
    - GDPR
    - Compensation
    - Visits to data center
  - Testing (2):
  - Risk assessment (1)
  - Questionnaire (1): based on CAIQ (CSA)

Exactly, it depends on what kind of auditor you get. [...] The only problem is that the ones who work conscientiously, are often those who are not well received and afterwards have trouble reselling. There is a slight conflict of interest.

If someone like you or me went there, what would we be supposed to see? If the door is not open somewhere or a cable hanging loosely, we would have no idea how secure this is [...]

Findings: Compliance and the GDPR

- GDPR
  - More attention
  - Companies waiting
- Location of CSP
  - Industry spionage from US

    → EU solution demanded
  - Lost importance: Looking at other companies
  - Does not compensate higher costs
  - German version missing features / tools
  - Customers in US
  - No trust in continuity of service
  - Telekom Cloud was mentioned (5)

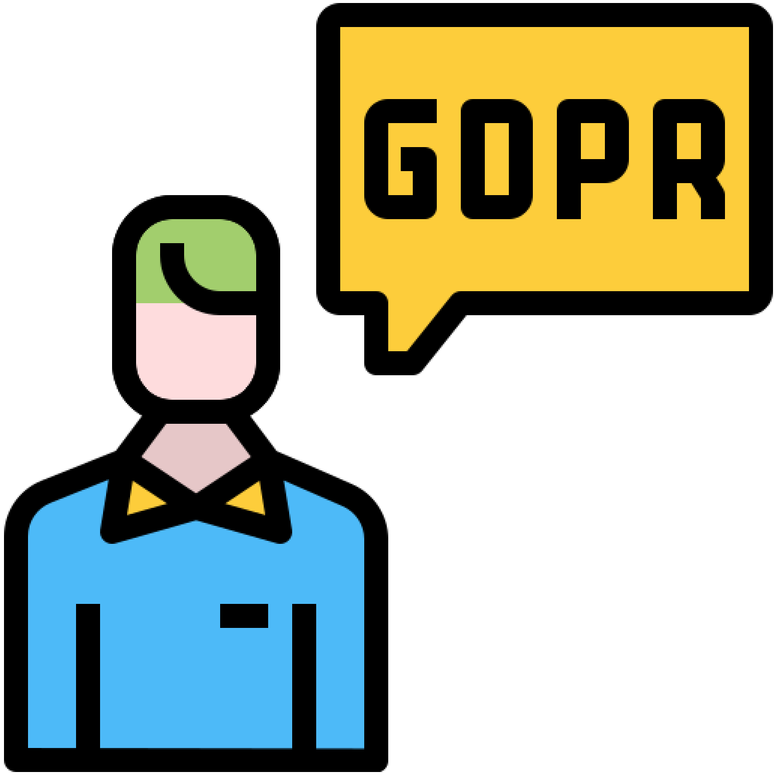
> *I believe that many (companies) still wait until the first penalties are issued, as surprisingly it (GDPR) did not have that many impact yet. [...] I think the first time something happens and jurisdiction is drawn, and a company really has to pay for it, many others will have a second awakening.*

Discussion

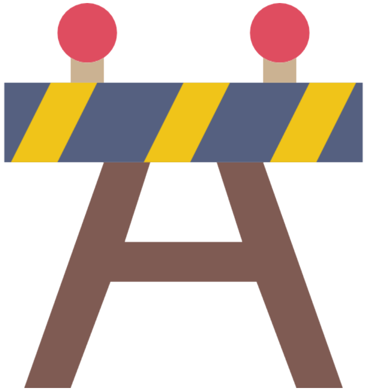
- Role of security
  - Security was never the first answer
  - Only vague security requirements mentioned
  - Sooner or later was present in all interviews
  - Systematic approach?
- Moderate interest in Security
  - Mitigation
  - Intrinsic motivation?
    - Compensation
    - Compliance
  - Trust
    - „IBM-Effect“

Discussion

- Security Assurance:
  - Certification, (audits), contractual agreements, testing
  - Does not seem to be cloud specific
- GDPR / Compliance:
  - Observe other companies



Limitations



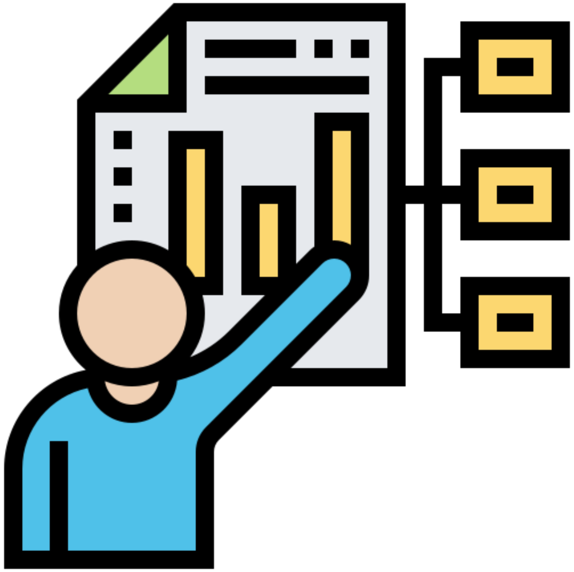
- Number of interviews
- Finding „good“ respondents
  - C-Level position
  - involved in cloud adoption
  - knowledgeable about processes in IT and security

    → hard to find
- More respondents from SME desirable
- Terms: Software-as-a-Service: Service vs. Provider Selection

Conclusion

- Security just one criteria out of many
- Research suggests elaborated (security) selection process
  - We could hardly find it in practise
  - Chosen based on vouchers, by chance , …
- Lift and Shift
  - ’first get into the cloud’
  - then optimise costs and (?) security
- Assurance: no elaborated models found
- Big companies trusted, no EU cloud

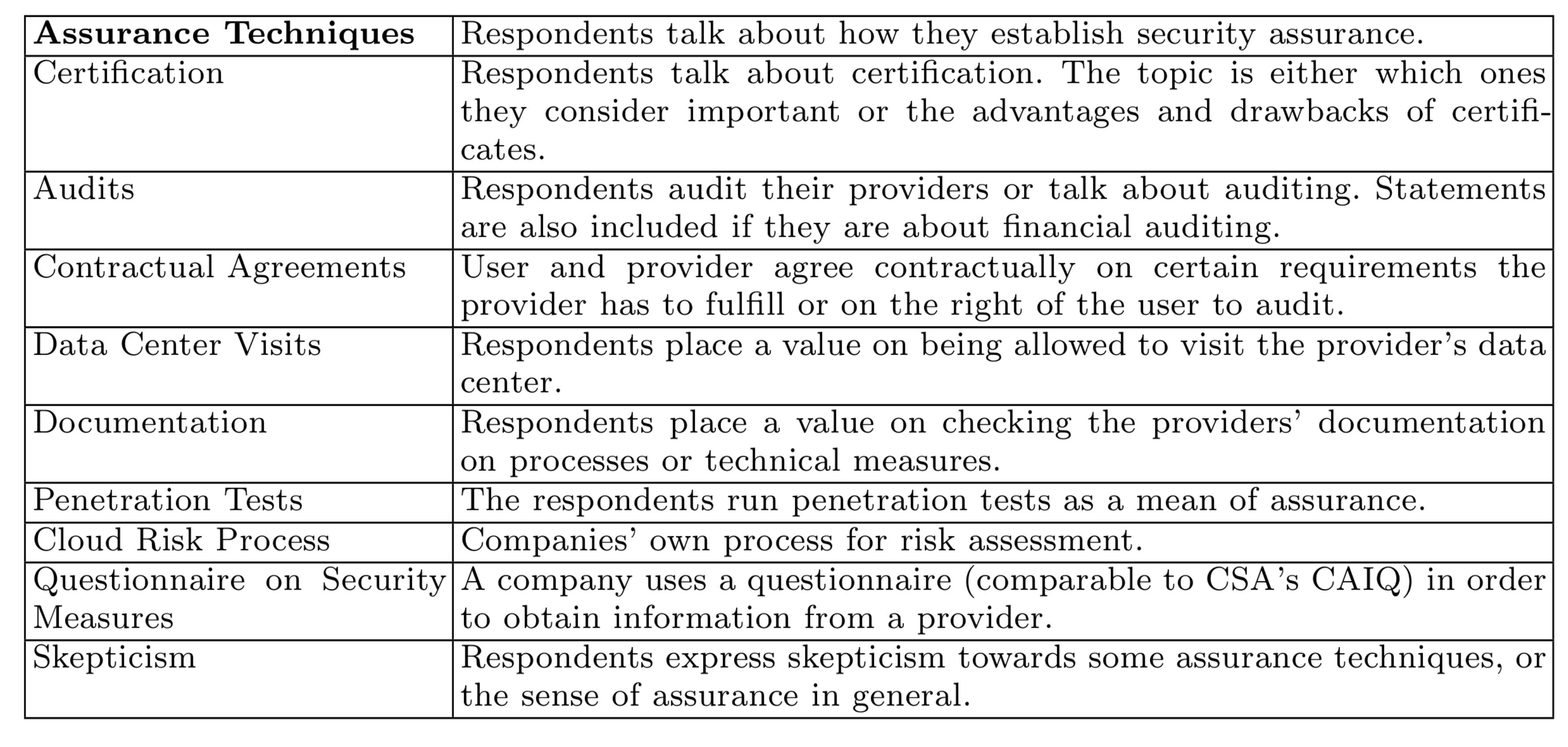
→ Gaps between research and pratice



Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de

Example Codes



Assurance Techniques	Respondents talk about how they establish security assurance.
Certification	Respondents talk about certification. The topic is either which ones they consider important or the advantages and drawbacks of certificates.
Audits	Respondents audit their providers or talk about auditing. Statements are also included if they are about financial auditing.
Contractual Agreements	User and provider agree contractually on certain requirements the provider has to fulfill or on the right of the user to audit.
Data Center Visits	Respondents place a value on being allowed to visit the provider's data center.
Documentation	Respondents place a value on checking the providers' documentation on processes or technical measures.
Penetration Tests	The respondents run penetration tests as a mean of assurance.
Cloud Risk Process	Companies' own process for risk assessment.
Questionnaire on Security Measures	A company uses a questionnaire (comparable to CSA's CAIQ) in order to obtain information from a provider.
Skepticism	Respondents express skepticism towards some assurance techniques, or the sense of assurance in general.