Challenges in Cross-Organizational Security Management

Stefan Thalmann, Daniel Bachlechner, Lukas Demetz, Ronald Maier
Innsbruck University School of Management, Information Systems I
{firstname.lastname}@uibk.ac.at

Abstract

Many organizations hoping for cost savings and higher flexibility consider consuming services from service providers or combining such services with services offered organization-internally. Organizations, however, often renounce from the expected advantages due to security and compliance concerns. The key challenges leading to these security and compliance concerns in cross-organizational settings have not yet been discussed elaborately in scholarly literature. However, a thorough understanding of the underlying challenges is necessary in order to find ways to compensate them and, in consequence, tap into the full potential of the cloud computing model. This paper discusses challenges gathered by means of guideline-based interviews. The identified challenges comprise managing heterogeneity, auditing clouds, coordinating the parties involved in cross-organizational settings, managing their relationships, coping with the lack of security awareness, and localizing and migrating data. Potential research avenues are discussed for each challenge.

1. Introduction

Consuming services from service providers or combining these with services offered organization-internally becomes increasingly appealing for many organizations as this approach not only promises cost savings and higher flexibility, but also lets organizations focus on their core business [46]. Its adoption depends on the service providers' ability to achieve and maintain compliance with security requirements so that customers can trust them. The top concern with cloud computing is security [29, 41] which currently dampens the willingness of many organizations to adopt cloud computing as IT procurement model [13].

Accountable clouds would be beneficial for both service consumers and service providers [21]. Due to the involvement of several organizations in achieving and maintaining security requirements, respective security settings are called cross-organizational. These are neglected in both research and practice while there is much literature on organization-internal security. Organizations that take advantage of the cloud computing delivery model also need to provide justification that their IT is properly managed, e.g., with the help of audits. Goals of this paper are to elaborate on cross-organizational security settings and identify the most pressing challenges that hinder adoption of cloud computing in organizations.

One frequently mentioned challenge in this regard is the heterogeneity of technology applied in cloud computing and non-standardized interfaces [23, 46, 4]. Technical aspects and architectural guidelines are in the primary focus of the research on this challenge [29]. Related work considering management aspects of this challenge or specifically on the introduced scenario is scarce.

Liability and trust are other frequently mentioned challenges for cloud computing [28, 23]. Availability of services [4] and uncertainties regarding performance and scalability [4, 23, 42] are major issues as well as the definition and enforcement of service level agreements (SLA´s) [23, 46]. Provenance is a further issue comprising object identification, determination of responsibilities and provenance reliability [42, 28, 4].

The paper investigates challenges in cross-organizational security management identified in a series of semi-structured interviews and related literature. We recommend solutions that address these challenges. Finally, we show promising research avenues towards a research agenda for secure cloud computing.

Section 2 outlines the design of our empirical study. Section 3 describes a cross-organizational security setting as found in the study. After presenting the identified challenges in section 4, we discuss them in section 5 and give recommendations on how to overcome them. Section 6 concludes the paper including a research agenda for cross-organizational security management.

2. Study design

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.148

The primary goals of our study were (1) to investigate cross-organizational security settings, (2) to extract the key challenges employees involved in cross-organizational security settings face and (3) to elicit and describe approaches to overcome these challenges. The study followed an explorative approach and was intended to portray challenges with original voice rather than to be representative. The study comprised three phases:

Desk study on roles: Literature related to the roles involved in cross-organizational security management and to the challenges faced by them was analyzed with the study goals in mind. The result was a list of about 80 roles relevant for the investigated setting as well as a basic understanding of general challenges faced by service providers and auditors.

Key informant interviews: Two key informants were interviewed in a convenience sample who worked for a service provider and an auditor, respectively. The roles identified in the desk study were discussed with the key informants focusing on how they were involved in activities in cross-organizational security management. The result was a refined list of key roles important for at least one of the two types of organizations. Due to the large number and considerable variety of roles and the explorative nature of the study, it was decided to focus on these most important roles. A convenience sample of people holding at least one of these roles was identified whom key informants regarded as having sufficient experience with the topic in order to provide valuable feedback.

Informant interviews: Fourteen semi-structured informant interviews were conducted with interviewees representing eight organizations in the first quarter of 2011. The interviewees were from Australia (1), Austria (1), France (4), Germany (7), Switzerland (1) and the US (2). At least one individual was interviewed per identified role. Although the focus was put on their current position, the interviewees were free to also report from roles they had assumed in the past, if they were considered relevant regarding the focus of our research. The structure of the informant interviews addressing the responsibilities of the interviewees, the activities they were involved in and the challenges they faced were adapted based on the results of the key informant interviews.

While the key informant interviews were conducted face-to-face and took approximately 120 minutes each, the informant interviews were conducted by telephone and took approximately 60 minutes each. The interview guideline was slightly adapted after one face-to-face pre-test interview and sent to the interviewees before the interviews. 12 informant interviews were recorded and transcribed. In case of two informant interviews, the interviewers took notes and produced a written summary right after conducting the interviews.

Several key challenges were mentioned in the 14 informant and two key informant interviews. Due to the limited sample size, we do not claim the list of challenges presented in this paper to be complete. Even if completeness is not a primary concern of explorative procedures, comparing our findings with challenges already addressed in literature seems useful to compensate this point. Based on the results of a thorough literature review on security and compliance challenges in cloud computing, an initial coding scheme was developed to be used in a qualitative content analysis of the transcribed interviews as proposed by Dey [37]. The main idea was to support the data analysis focusing on challenges in cross-organizational security settings by considering related challenges mentioned in the literature. The chosen informed and inductive approach required questioning and adapting every initial code to the specifics of the analyzed data. Individual descriptions of challenges were merged into categories interpreted as the key challenges which represent individual challenges of at least three interviewees.

3. Cross-organizational security setting

Outsourcing of IT and business processes has a long history and started in the 1960s and 1970s [30]. With the advent of cheap minicomputers and PCs in the 1980s operating IT in-house became attractive [30]. However, in the following decades, companies started to gradually outsource (parts of) their IT, as well as their software, to professional IT and application service providers [2]. More recently, organizations adopted cloud computing [49] in which platforms and infrastructure are provided as a service besides software. The steadily increasing number of businesses consuming services out of the cloud is suggestive of this trend [27].

In our study, we identified a specific outsourcing constellation in which several organizations are involved, which we termed cross-organizational security setting. Figure 1 shows the relationships between organizations acting in this setting. In cloud computing, organizations abandon in-house IT and consume services provided by third parties. A supplier may offer specific services such as data archiving or signing of invoices, executed on an IT infrastructure operated and maintained at the supplier's site. The service orchestrator does not operate an own IT infrastructure at all, but consumes

services from different service providers and orchestrates the consumed services accordingly. Services of a network of suppliers, also comprising service orchestrators, may be combined to provide more comprehensive services.

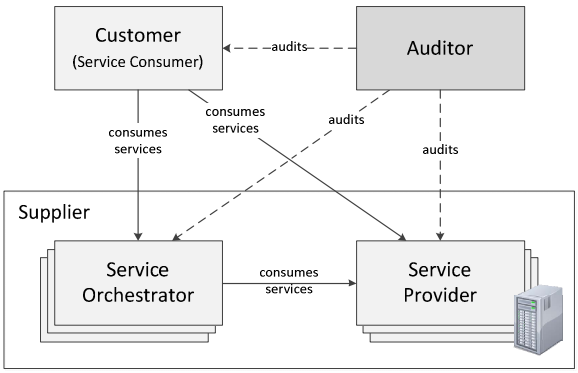

Figure 1 The cross-organizational security setting [48].

Most suppliers in a network such as the one presented in Figure 1 serve multiple customers and are thus faced with a myriad of individual security requirements they need to comply with. Satisfying these requirements, however, often is inefficient [18] and involves manual work which tends to be cost-intensive and error-prone. The costs of managing IT systems, including achieving and maintaining security compliance, soared over the last years [24]. Moreover, the increasing number of laws and regulations, e.g., HIPAA or SOX, exacerbates both the suppliers' and the customers' situations and raises the number and complexity of security requirements that need to be dealt with. Besides managerial difficulties, suppliers also face technical challenges, such as heterogeneity and incompatibilities of technology, privacy and data protection [46].

This way of operating IT also affects the work of auditors. They are faced with a different situation, as compared to auditing an organization with in-house IT services, since the auditee may not be able to provide all necessary information to the auditor. Thus, information needs to be requested from third parties and the audit depends on their willingness and capability to deliver relevant information. For services provided by a service orchestrator, the situation is even more complicated.

Depending on the number of outsourced services consumed by the customer and the type of suppliers, the complexity of showing compliance with security requirements increases. This in turn, prolongs the audit and increases its costs. In some cases, it may also be necessary to additionally audit the supplier. Showing compliance for a service orchestrator is more complex since it does not run any IT infrastructure and needs to show compliance of all suppliers it consumes services from. This, however, may often not be feasible, e.g., because the auditor has no right to enter the supplier's site. In such cases, the respective supplier could be audited by another auditor of the supplier's choice. If available, the supplier could also provide existing audit reports to the customer's auditor, indicating the effectiveness and efficiency of its controls and processes and the adherence to specific standards. Consequently, several people are involved in an audit of an organization outsourcing parts of its IT: (1) employees of the service consumer to be audited, i.e., the customer, (2) depending on the distribution of outsourced services, employees of several service providers which may be of different types, i.e., the suppliers, and (3) employees of the auditor.

4. Identified key challenges

In this section, the identified key challenges are presented and richly described by using original voice extracted from the interview transcripts. Each challenge is formulated deliberately close to original voice. An interpretation of the statements is given in section 5.

Existing outsourcing literature so far discussed only challenges and risks when outsourcing to service providers who operate their IT internally and do not have virtualization capabilities. However, cloud computing in a scenario such as the one introduced in section 3 is complex. Therefore, other and more sophisticated challenges are presented in the following.

Managing Heterogeneity

Interfaces between service providers are not yet standardized. Similar to the telecommunication sector, stronger standardization is needed.

A security manager said, "Especially if you try to map policies on standard configurations, it's a very challenging task." Similarly, a control manager remarked, "You come very quickly in a situation where you need to apply a lot of exceptions." It is important to find the right balance between complexity of processes and business reality. A security manager said, "As more complex and more complicated things are, the more bypasses are created by involved humans."

Computer centers differ with respect to systems and procedures. Furthermore, old or incompatible systems are frequently connected obscurely to productive systems. The level of security is usually measured at the weakest point. These legacy systems

are frequently the weak points of the security landscape.

In our setting, customers are different on the application layer and regarding their business processes. Frequently, organizational processes are performed differently, e.g., in different operational units or subsidiaries. In the context of cross-organizational security management, this is a huge challenge.

The challenge manifests, for instance, if services from different service providers should be orchestrated by in-house services but the interdependencies on the business layer as well as technical side effects are unknown.

Summing up, the challenge is to integrate different technologies effectively and in a way that they can be understood and hence are accepted by the users.

Auditing Clouds

According to the interviewees, the correct technical implementation of requirements is not difficult. The challenge, however, is to check if the outsourced services and their requirements fit to the business processes. In order to perform this task properly, auditors need an understanding of the current landscape taking all service outsourcing constructs into account, i.e., technical solutions which require much more time than in traditional settings. Due to the remarkable complexity of this task and the time constraints, it seems impossible to perform this task without proper tool support. In this regard, an IT auditor said, "The main challenge is to ensure that you are auditing the appropriate things."

Due to the complexity of the setting to be audited, the skills of people involved are crucial - skills of the auditing staff as well as the staff of the audited organization. A deep understanding of technical details and relationships is needed to verify whether a control is really implemented effectively by a technical component. Tool support and automation can be very beneficial, especially in the domain of documentation. The challenge in this regard is to make things easier so that the understanding of the IT infrastructure is not bound to the knowledge of a few employees. This can be achieved, for instance, by using tools or by a more standardized and homogeneous technology.

Since organizations differ with respect to business processes, their security and compliance requirements are different as well. In this respect, it is challenging to check the requirements from the client in an audit of the service provider. Furthermore, the significance of a general audit of a service provider seems questionable from the interviewees' point of view.

Due to the large number of involved components in cloud solutions, it is challenging to identify the critical ones which are tested in an audit. The danger is that the traditional audit sample size represents only a very small part of the IT infrastructure, more specifically such components that can be accessed easily in the organization. Hence, results of such a sampling are probably not meaningful.

Increased complexity and interwoven dependencies occur, for instance, if an organization orchestrates services flexibly according to their availability and additionally buys services from service orchestrators.

Summing up, the challenge is to understand complex IT infrastructures composed of services from different service providers, to select the relevant aspects for an audit and to test them in a way that the results are meaningful.

Coordinating Involved Parties

As in auditing clouds, it is essential to know the service providers and the services that support each business process. An IT professional said, "I want to see my business as a whole in a central view." Maintaining such an overview, however, is a huge challenge. Additionally, the communication of changed security and compliance requirements to all involved service providers is crucial. It becomes even harder if an organization has different security and compliance requirements in different business units.

The definition of proper rights management is a very challenging aspect. One compliance manger said, "I have even one layer [of suppliers] more and lose even more the overview." He suggests developing an easy and continuous rights management to overcome this point. The realization of such a proper rights management considering a service orchestrator, however, is a seriously difficult task.

For a service orchestrator, it is challenging to coordinate diverse customer requirements. An overview of current customer requirements and their realization by systems or service providers is needed. In addition to defining security and compliance requirements, also the knowledge about the customers' business processes and communication partners is highly relevant for fulfilling the expectations of the orchestrator's role between customer and other suppliers.

Service providers face this challenge, for instance, if the implementation of a requirement for one customer contradicts the fulfillment of requirements for another customer. This is particularly difficult for

service orchestrators which also have to ensure that their suppliers realized the requirements properly.

Summing up, the challenge is to fulfill all customer requirements properly and to maintain an overview of a customer's infrastructure and of all realized security and compliance requirements.

Managing Relationships

A service provider legally ensures to formulate contracts with all subcontracted service providers in such a manner that all customer requirements are fulfilled. However, service providers cannot inspect the contracts with subcontracted service providers.

It is difficult to detect violations of agreements with subcontracted service providers. An operations manager said, "It is very hard to determine if some services are temporarily subcontracted." Furthermore, it is necessary that all SLAs are synchronized through all levels of service provisioning. Due to limited access to the supplier's contracts, this is a very challenging task.

Many differences with respect to culture can be observed. People frequently have different attitudes towards rules in different cultural settings which could also apply to auditors. A control manager said, "People are the main challenge you have."

According to an operations manager one key question for a service orchestrator is, "Are all my service suppliers secure and confidential?" Trust to service suppliers typically bases not on occasionally performed audits, but rather on personal impressions of the suppliers' staff. Even high penalties in contracts are no guarantee that security and compliance requirements are fulfilled. The awareness of employees of service providers might decrease very quickly after contracting or customer visits. As humans make errors, the more humans are involved, the more challenging it becomes.

For instance, in the case of a service consumer with orchestrated services offered by many service providers, maintaining an overview and ensuring that security requirements are considered properly becomes more difficult with an increasing number of involved service providers.

Summing up, the challenge is to get confidence about the fulfillment of security and compliance requirements by service suppliers.

Coping with Lack of Security Awareness

A control manager said, "The most complex challenges are settings in which humans are involved." Humans are frequently not aware of security- and compliance-related issues in general. Due to the complexity and sensitivity of a cloud scenario, this aspect becomes even more relevant. All technical security mechanisms are worthless if they are bypassed by unaware users. This is not a primary issue for administrators and technicians, but rather for users. Especially in organizations with fewer restrictions, this aspect becomes highly relevant.

Furthermore, using consumer electronics, such as smart phones, and connecting them with the organizational infrastructure challenges compliance with security requirements. A control manager said, "The demand to access the organizational infrastructure with consumer electronics increases and such an access is important for user satisfaction and acceptance." However, such devices are typically designed for high convenience and not to fulfill high security requirements.

For instance, if an administrator of a service provider does not change default passwords, the system can be attacked easily. In such cases, the data of all customers and not only the data of the service provider are in danger.

Summing up, the challenge is to create awareness for security- and compliance-related issues.

Localizing and Migrating Data

It is quite important for customers to know and also to restrict the locations where their data are stored and handled.

Mobility is a crucial aspect and according to a customer relationship manager, questions like, "Where is the service consumed? Where are the data stored? Where are the data transferred to?", are relevant for customers. Furthermore, a big challenge is to verify the ownership structures of devices and data. Data of competitors may be computed or stored on the same systems, for example. Such situations can be unpleasant for customers and hence they want to know exactly how data separation, division of computation of division of storage is achieved.

For instance, it may be illegal for a German company to store data in the U.S. because European laws prohibit the storage of data in countries with lower data protection standards.

Summing up, the challenge is to maintain an overview of the current location of data and services and their ownership.

5. Discussion and Recommendations

The results presented in the previous section are discussed in this section taking the existing literature into account. Recommendations on how to overcome the challenges are given and avenues for future research presented.

Managing Heterogeneity

Challenge in related literature: Having different service providers offering incompatible services hinders users to change service providers. However, consumers of cloud computing services want to be able to switch cloud providers without substantial reimplementation. Additionally, they want to use the services of multiple cloud providers at once [16]. Yet, little interest in solving this problem has been signaled by cloud providers [25]. However, this is not only important for end users, but also for the ecosystems that evolve around cloud computing [16] as it would allow service providers to trade services more efficiently [10]. The challenges that are faced due to heterogeneous systems include, among others, addressing virtualized environments [7] and a lack of communication standards between clouds.

Recommendations: For dealing with the identified challenges, achieving and maintaining interoperability of service providers is crucial. Cloud interoperability is understood as the "customers' ability to use the same artifacts, such as management tools, virtual server images, and so on, with a variety of cloud computing providers and platforms" [15]. For interoperability, we need abstractions that efficiently utilize distributed infrastructures [25]. There are already several institutions, though, which aim at defining means for enhancing the interoperability between service providers, e.g., Computing Interoperability Forum or Open Cloud Consortium.

Research avenues: Interoperability between cloud providers can be increased via several avenues, e.g., by standardizing application programming interfaces [4, 16, 41]. Currently, users are not able to easily change the service provider without reimplementations. Cloud interoperability may also be achieved by common languages [20] and a standardization of protocols that govern the interactions between service providers [10]. In this respect, [7] proposes a blueprint for protocols and formats for cloud interoperability. Besides creating standards, agreed-upon programming frameworks and systems could help to manage the complexity of heterogeneous systems, e.g., the SAGA system [35], or the software framework Thrift [20].

However, management approaches are needed in case heterogeneity and interoperability problems cannot be eliminated. The adaptation of the information systems portfolio theory [34] to the specifics of the cloud seems suitable for this purpose. The portfolio approach helps deciders to maximize their benefits and to minimize their risks resulting from the heterogeneity.

Auditing Clouds

Challenge in related literature: The fundamental need for auditability follows from the complexity of multi-party trust considerations in the cloud [11]. The service consumer and its auditor are generally responsible for reviewing the overall IT infrastructure comprising the IT run internally and the services sourced from service providers. The service consumer can either define or implement internal controls to keep the service provider under surveillance or rely on the internal controls of the service provider. The service consumer, however, has no control of the outsourced data and the service provider's controls [51]. Third-party audit reports such as SAS 70 are usually of limited help as they only focus on a subset of controls and procedures that would normally be included in a comprehensive security audit. The difficulties for IT audits resulting from the use of cloud computing are widely recognized in the research community [5, 19, 22].

Auditability issues together with concerns regarding data confidentiality are ranked as the third most important obstacle to the growth of cloud computing [5]. Higher ranked are only concerns with respect to business continuity (i.e., availability) and the problem of data lock-in. Part of the problem is ascribed to the fact that the services are usually opaque and offer only little visibility into their underlying architectures and technologies and that such services cannot be audited without audit rights granted by the services provider [19]. Accountability is considered to be critical to address most of the challenges organizations using cloud services face [22]. Auditability was identified as one of the key technical requirements that accountable clouds have to meet. In this context, particularly the development of IT audit policies which are consistent with national and international regulations is considered an issue where further guidance is needed [33].

Recommendations: Several authors have proposed frameworks to overcome the challenges that auditing of cross-organizational security settings brings with it, e.g., a framework for secure cloud computing based on checklists [12] or an auditing scheme based on probabilistic sampling [52]. Attributes to be audited in cross-organizational security settings such as events and logs were investigated in [53].

The challenging aspects of auditing clouds found in the literature differ to some extent from the ones identified in our study. Aspects such as landscape documentation, audit scoping and skills have not yet been discussed elaborately in the context of cross-organizational security settings.

Research avenues: Since having an overview of the services and suppliers that make up processes is

crucial, a focus on modeling languages for IT landscapes seems sensible. Process documentation is also required for facilitating audit scoping by means of formal landscape descriptions. With respect to skills, it needs to be reconsidered if traditional certified public accountants are sufficiently qualified to perform IT audits in complex cross-organizational security settings. For a comprehensive security audit, thinking out-of-the-box may generally be more suitable than adhering to clearly defined checklists and procedures. However, at the same time, it is crucial to address the weaknesses of reports such as SAS 70 to reduce auditing efforts for service consumers as well as service providers.

The challenge-response protocol presented in [50] determines data correctness and locates possible errors in cloud environments. Similarly, [6] proposes a protocol to verify data possession in remote storages. Such protocols are crucial for auditing cloud environments and research in this area thus should be continued. The principal-agent theory as well as the usage control model may serve as good starting points for managing audit processes in clouds. Both have already been successfully applied in similar contexts [e.g., 45, 43].

Coordinating Involved Parties

Challenge in related literature: There is a substantial body of literature on the definition of SLAs [e.g., 23, 46]. This literature, however, does not or only partly considers the introduced scenario. Particularly the aspects of monitoring and enforcing SLAs are much more challenging in the scope of our scenario.

Recommendations: The reduction of complexity was frequently mentioned within the interviews. Maintaining only few, but trusted relationships facilitates their management. If services are outsourced to suppliers, it is important that a consumer trusts the supplier's suppliers since such a "transitive trust" is not given per se [26]. Furthermore, close relationships to customers and well-defined responsibilities for security and compliance requirements are necessary as well.

In analogy to business process management systems which standardize the representation of structures across business processes, users and organizations, a standardized representation of security and compliance-related requirements is needed [41]. A model based approach, as proposed in [8], seems promising. Having such a standardized representation, automated or at least semi-automated testing or creation of reports becomes feasible. Furthermore, the development of an automated detection of conflicts and decision support tools for resolving conflicts in security and compliance requirements also become feasible.

Research avenues: The standardization of languages to describe security and compliance requirements seems most promising. The same applies for the description of the implemented policies. Both enable automated checks whether requirements are implemented properly and also different overviews are provided. Both are crucial for organizations coping with the challenge of coordinating involved the parties. The declarative object-oriented language for specifying security and management policies for distributed systems presented in [14] seems appealing in this respect. Similar approaches are presented, for instance, in [3] and [47]. For mastering the complexity of policies, a tool such as PoliSeer [31] seems promising.

Guidelines and process descriptions should be developed for coordinating requirements of the many parties involved. Coordination theory [32] as well as transaction cost theory [2] could be valuable starting points for this purpose.

Managing Relationships

Challenge in related literature: Service providers use contracts to ensure the realization of their security requirements. However, the definition of compensations, measures, monitoring procedures or alternative procedures is currently very weak [41].

In this regard, reputation is a very important aspect which is difficult to establish and to maintain [4]. Reputation effects trust and trust in the service provider's ability to ensure security is very important [29]. Trust in the economic stability as well as in technical expertise is also demanded by customers [46]. Trust is mentioned as the "biggest concern facing cloud computing" [28].

Recommendations: Interviewees typically cope with this challenge by maintaining close relationships to their suppliers. This includes personal contacts and frequent visits. Furthermore, again the reduction of complexity by concentrating on main suppliers was suggested.

The maintenance of close relationships to service suppliers is a temporary solution to overcome the limitations of auditing and design of SLAs. A tool that makes the implementation of security and compliance requirements visible would be beneficial. Auditors could work much more efficiently which would increase the liability in their reports and would also be more traceable for customers.

Research avenues: One avenue could be the development of guidelines to support contract negotiations and the development of effective contract clauses. Apart from that, monitoring contract

enforcements is needed [46]. It was frequently mentioned that this instrument of coordination does not work efficiently. The principal agent theory [40] could be a starting point, in which relationships between two contract partners with asymmetric levels of information are explained and recommendations for the design of contracts are given.

Another avenue would be the design and the development of an IT solution providing more visibility of the implemented security and compliance requirements. This research avenue again requires a formal and standardized description of requirements as well as their implementation. Furthermore, trust on different layers could also be modeled and considered in such a system.

Coping with Lack of Security Awareness

Challenge in related literature: Organizations such as the ENISA or the NIST started addressing security awareness several years ago. One of the key achievements of ENISA in this context is a practice-oriented guide illustrating a sample strategy on how to plan, organize and run information security awareness-raising and training campaigns [17]. Similarly, NIST discussed the design and implementation of an information security awareness and training program [36]. Those and other guidelines are valuable resources when conducting security awareness campaigns and programs.

Recommendations: The approaches for raising security awareness in cloud scenarios do not differ from the ones applied in organizations which are not sourcing services from other organizations. However, it is critical in cross-organizational settings that the individuals from all involved parties recognize security concerns and respond accordingly.

Research avenues: One way to cope with the lack of security awareness is to enforce policies in an automated fashion as much as possible and thereby reduce the risk of human error. Focusing on automated policy enforcements seems particularly important in the context of organizations with open cultures. However, security awareness cannot completely be created by means of policies. Adapting the theory of planned behavior [1] and the theory of organizational culture [39] to the specifics of the introduced scenario seems suitable in this regard. The behavior of single actors can be investigated on the one hand and the influence of larger organizational factors on the other hand.

Localizing and Migrating Data

Challenge in related literature: Services can be located virtually everywhere, provided by everybody and replaced by other services in the cloud [4, 28]. This is one fundamental principle of cloud computing which renders localization of data more difficult. However, people do not trust the new paradigm and want information and assurance about the locations their data are stored and computed in. Uncertainties or no information about the location represent a main hurdle in using cloud computing [28].

Location is a concern particularly with respect to the laws and regulations of a specific jurisdiction, as data may become subject to the regulations of the jurisdiction where they or backup copies of them are stored [44]. At the same time, also verifying that data exists only at allowed locations is considered a difficult problem [38].

Traditional identification techniques based on hash values cannot provide unique object identifiers and hence cannot be applied properly [42]. Providing trusted localization information requires a reduction of the cloud computing paradigm. Instead of using any service available in the cloud, only services of few and certified suppliers are used. This enables localization, but limits the advantages of cloud computing, such as flexibility or cost efficiency.

Due to security concerns, some data are also stored locally. The handling and orchestration of these data with data stored in the cloud, their selection and differentiation is quite challenging [9].

Recommendations: It is crucial for localizing data that it can be assured that provenance data is not tampered and that auditors can check their integrity and correctness [42]. Currently, this implies a reduction of the number of potential suppliers.

The interviewees even go one step further. It is frequently not sufficient for deciders to have trusted localization data, they even want to see and inspect the location, i.e., the data center. Hence, arranging site visits for customers is recommended.

Research avenues: The research challenge in this regard is the development of localization mechanisms which allow the identification of locations in which data are stored or computed without restricting the flexibility demanded in cloud computing. Particularly the second aspect seems important for the efficient usage of cloud services. Combining proof of data possession with network geolocation technologies as proposed in [38] could be a promising avenue.

The users' need for localization data originates from a lack of trust in cloud computing. Hence, research investigating this lack of trust and focusing on measures to overcome it seems promising as well. Effective policies are needed in order to provide legal certainty to service providers and consumers. Applying the transaction cost theory [2] seems to be a valuable starting point to investigate the effect of

difficulties of data localization on the realization of outsourcing relationships.

6. Conclusion and Outlook

This paper described a cross-organizational security setting identified on the basis of a series of interviews. In the context of this setting, six key challenges were described, discussed in the context of the existing body of literature and potential research avenues were sketched for each challenge.

Concerns that security- and compliance-related issues are not handled properly in cross-organizational settings were recognized within the series of interviews. The aid of auditors and the presence of audit reports seem to be incapable to alleviate the skepticism regarding security and compliance of business partners. Only personal contacts and stable supplier relationships can alleviate these concerns. Since this contradicts the principles of cloud computing, this socio-technical phenomenon appears to be well worth further investigation.

The development of a standardized approach to describe organizational security and compliance requirements as well as the description of their technical realization is considered useful to counter several of the identified challenges. An integrated tool focusing on security and compliance requirements, building on such standardized descriptions, is considered useful for organizations acting in scenarios similar to the one introduced in this paper.

7. Acknowledgments

The research leading to the presented 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.

8. References

[1] I. Ajzen, "The theory of planned behavior.", Organizational Behavior and Human Decision Processes, 50 (1991), pp. 179-211.

[2] S. Ang and D. W. Straub, "Production and Transaction Economies and IS Outsourcing: A Study of the U.S. Banking Industry", MIS Quarterly, 22 (1998), pp. 417-417.

[3] R. Anthony, "A versatile policy toolkit supporting run-time policy reconfiguration", Cluster Computing, 11 (2008), pp. 287-298.

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, S. I. and Z. M., *Above the Clouds: A Berkeley View of Cloud Computing*, *Technical Report*, University of California at Berkeley, 2009.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, S. Ion and Z. Matei, "A View of Cloud Computing", Communications of the ACM, 53 (2010), pp. 50-58.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, *Provable data possession at untrusted stores*, *Proceedings of the 14th ACM conference on Computer and communications security*, ACM, Alexandria, USA, 2007, pp. 598-609.

[7] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond and M. Morrow, *Blueprint for the Intercloud - Protocols and Formats for Cloud Computing Interoperability*, *Proceedings of the 4th International Conference on Internet and Web Applications and Services*, Venice, Italy 2009, pp. 328-336.

[8] R. Breu, M. Hafner, F. Innerhofer-Oberperfler and F. Wozak, *Model-Driven Security Engineering of Service Oriented Systems.* , *2nd International United Information System Conference, Uniscon 2008*, Springer, Klagenfurt, Austria, 2008, pp. 59-71.

[9] R. Buyya, R. Ranjan and R. N. Calheiros, *InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services*, *10th International Conference on Algorithms and Architectures for Parallel Processing*, Busan, Korea, 2010, pp. 13-31.

[10] R. Buyya, C. Yeo and S. Venugopal, *Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities*, *HPCC '08: Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications*, IEEE Computer Society, Dalian, China, 2008, pp. 5-13.

[11] Y. Chen, V. Paxson and R. H. Katz, *What's New About Cloud Computing Security?*, *Technical Report*, University of California at Berkeley, Berkeley, 2010.

[12] Z. Chen and J. Yoon, *IT Auditing to Assure a Secure Cloud Computing*, *6th World Congress on Services*, IEEE, 2010, pp. 253-259.

[13] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka and J. Molina, *Controlling data in the cloud: outsourcing computation without outsourcing control*, *Proceedings of the 2009 ACM workshop on Cloud computing security*, ACM, Chicago, USA, 2009, pp. 85-90.

[14] N. Damianou, N. Dulay, E. Lupu and M. Sloman, *The Ponder Policy Specification Language Policies for Distributed Systems and Networks*, in M. Sloman, E. Lupu and J. Lobo, eds., Springer, 2001, pp. 18-38.

[15] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research", IEEE Internet Computing, 13 (2009), pp. 10-13.

[16] F. Douglis, "Staring at Clouds", IEEE Internet Computing, 13 (2009), pp. 4-6.

[17] ENISA, *The new Users' Guide: How to Raise Information Security Awareness*, 2008.
[18] Forrester Research, *How To Manage Your Information Security Policy Framework*, 2006.
[19] M. Fratto, *Cloud Control*, *InformationWeek*, TechWeb, San Francisco, California, 2009, pp. 30-36.
[20] R. L. Grossman, "The Case for Cloud Computing", IT Professional, 11 (2009), pp. 23-27.
[21] A. Haeberlen, "A case for the accountable cloud", SIGOPS Oper. Syst. Rev., 44 (2010), pp. 52-57.
[22] A. Haeberlen, *A Case for the Accountable Cloud*, *3rd ACM SIGOPS International Workshop on Large-Scale Distributed Systems and Middleware*, 2009.
[23] P. Hofmann and D. Woods, "Cloud Computing: The Limits of Public Clouds for Business Applications", IEEE Internet Computing, 14 (2010), pp. 90-93.
[24] IBM, *Corporate Strategy Analysis of IDC Data*, 2007.
[25] S. Jha, A. Luckow, A. Merzky, M. Erdely and S. Sehgal, *Application-Level Interoperability Across Grids and Clouds*, in M. Cafaro and G. Aloisio, eds., *Grids, Clouds and Virtualization*, Springer, 2011, pp. 199-229.
[26] Y. Karabulut, F. Kerschbaum, F. Massacci, P. Robinson and A. Yautsiukhin, "Security and Trust in IT Business Outsourcing: a Manifesto", Electronic Notes in Theoretical Computer Science, 179 (2007), pp. 47-58.
[27] L. Kaufman, "Can Public-Cloud Security Meet Its Unique Challenges?", IEEE Security&Privacy, 8 (2010), pp. 55-57.
[28] L. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security and Privacy, 7 (2009), pp. 61-64.
[29] P. Koehler, A. Anandasivam, M. A. Dan and C. Weinhardt, *Customer Heterogeneity and Tariff Biases in Cloud Computing*, *International Conference on Information Systems (ICIS)*, St. Luis (USA), 2010.
[30] J.-N. Lee, M. Q. Huynh, R. C.-W. Kwok and S.-M. Pi, "IT Outsourcing Evolution--Past, Present, and Future", Communications of the ACM, 46 (2003), pp. 84-89.
[31] D. Lomsak and J. Ligatti, "PoliSeer: A Tool for Managing Complex Security Policies", Journal of Information Processing, 19 (2011), pp. 292-306.
[32] T. W. Malone and K. Crowston, "The Interdisciplinary Study of Coordination", ACM Computing Surveys, 26 (1994), pp. 87-119.
[33] S. Marston, Z. Li, S. Bandyopadhyay and A. Ghalsasi, *Cloud Computing – The Business Perspective*, *44th Hawaii International Conference on System Sciences*, IEEE, 2011.
[34] W. F. McFarlan, "Portfolio approach to information systems.", Harvard Business Review, 59 (1981), pp. 142-150.
[35] A. Merzky, K. Stamou and S. Jha, *Application Level Interoperability between Clouds and Grids*, *Proceedings of the 2009 Workshops at the Grid and Pervasive Computing Conference*, Geneva, Switzerland 2009, pp. 143-150.
[36] NIST, *Special Publication 800-50: Building an Information Technology Security Awareness and Training Program*, 2003.
[37] M. Q. Patton, *Qualitative Research & Evaluation Methods*, Sage, Thousand Oaks, 2002.
[38] Z. N. J. Peterson, M. Gondree and R. Beverly, *A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud*, *3rd USENIX Workshop on Hot Topics in Cloud Computing*, Portland, USA, 2011.
[39] A. M. Pettigrew, "On Studying Organizational Cultures", Administrative Science Quarterly, 24 (1979), pp. 570-581.
[40] R. Rees, "The Theory of Principal and Agent—Part I.", Bulletin of Economic Research, 37 (1985), pp. 3-26.
[41] B. P. Rimal, A. Jukan, D. Katsaros and Y. Goeleven, "Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach", Journal of Grid Computing 9 (2011), pp. 3-26.
[42] M. A. Sakka, B. Defude and J. Tellez, *Document Provenance in the Cloud: Constraints and Challenges EUNICE 2010 - Networked Services and Applications – Engineering, Control and Management*, Springer, Trondheim, Norway, 2010, pp. 107-117.
[43] R. Strausz, "Delegation of Monitoring in a Principal-Agent Relationship", The Review of Economic Studies, 64 (1997), pp. 337-357.
[44] D. Svantesson and R. Clarke, "Privacy and Consumer Risks in Cloud Computing", Computer Law and Security Review, 26 (2010), pp. 391-397.
[45] A. Syalim, T. Tabata and K. Sakurai, "Usage Control Model and Architecture for Data Confidentiality in a Database Service Provider", IPSJ Digital Courier, 2 (2006), pp. 39-44.
[46] H. Takabi, J. B. D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, Nov/Dec (2010), pp. 24-31.
[47] J. Tan and S. Poslad, "Dynamic security reconfiguration for the semantic web", Engineering Applications of Artificial Intelligence, 17 (2004), pp. 783-797.
[48] S. Thalmann, D. Bachlechner, R. Maier, M. Manhart and L. Demetz, *Key roles in cross-organisational security settings*, *Proceedings of the 2nd European Security Conference*, Örebro, Sweden, 2011.
[49] M. A. Vouk, "Cloud computing: Issues, research and implementations", Journal of Computing and Information Technology, 16 (2008), pp. 235-246.
[50] C. Wang, Q. Wang, K. Ren and W. Lou, *Ensuring Data Storage Security in Cloud Computing*, *Proceedings of the 17th International Workshop on Quality of Service*, IEEE, Charleston, South Carolina, 2009, pp. 1-9.
[51] C. Wang, Q. Wang, K. Ren and W. Lou, *Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing*, *Proceedings of the 2010 IEEE INFOCOM*, California, 2010, pp. 1-9.
[52] L. Wei, H. Zhu, Z. Cao, W. Jia and A. V. Vasilakos, *SecCloud: Bridging Secure Storage and Computation in Cloud*, *International Conference on Distributed Computing Systems Work*, IEEE, 2010, pp. 52-61.
[53] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, *Security and Privacy in Cloud Computing: A Survey*, *6th International Conference on Semantics, Knowledge and Grids*, IEEE, 2010, pp. 105-112.