Business Continuity Challenges in Cloud Computing

Sashko Ristov, Marjan Gushev, Magdalena Kostoska, and Kiril Kiroski

Ss. Cyril and Methodius University / Faculty of Computer Science and Engineering,
Rugjer Boshkovik 16,
1000 Skopje, Macedonia
{sashko.ristov, marjan.gushev, magdalena.kostoska,
kiril.kjiroski}@finki.ukim.mk

Abstract. Cloud computing becomes the best offer in ICT for data storage and processing, offering flexible and scalable computing processing capacity. But, cloud computing may produce different risks with different impact to client company business than traditional IT solutions. Cloud service providers must implement effectively information security management to reduce the security risks improving the cloud customer business continuity. In this paper, we use high-level risk-based approach to address the risks of the security challenges in the cloud in order to improve the client company business continuity if migrates its services into cloud. The comparative analysis of main security benefits and detriments of the cloud that impacts the business continuity was not performed in the literature so far. In this paper we start analyzing the benefits that cloud computing offers to business continuity, in order to depreciate the risks to acceptable level.

Keywords: Cloud Computing Business Continuity, Cloud Computing Security Benefits, Cloud Computing Security Detriments, Cloud Computing Security Risk Assessment

1 Introduction

Cloud computing is relatively a new model defined as for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [12]. It enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing [8].

The process of globalization enforces companies not only to modernize their approach to the production process, but also to implement modern technologies, and to compete on a wider scale if they want to be successful. Cloud computing may lavishly help companies determined to be successful outside of their local boundaries, and managers become increasingly aware of its benefits [16].

Despite all of the benefits cloud computing offers, there are several open issues to be solved, such as service interoperability, performance, multiple server platforms, and segmented databases. However, since the data, and probably the applications, is outsourced from the company security perimeter to the third-party cloud computing

platforms, the most important issue is to retain minimum the same security level as before moving into cloud.

1.1 Security Challenges Moving into Cloud

The security objectives of a company are a key factor to make decision about outsourcing their IT services, especially data and applications to a public cloud computing environment [11]. But, in some cases, cloud computing offers enhanced security benefits to the companies; for small companies with limited qualified IT administrators and security officers, and lack of business growth, it provides opportunity for overall security improvement.

Many organizations aren't comfortable storing their data and applications on systems that reside outside of their on-premise datacenters [1]. This might be the single greatest fear of cloud clients.

One approach to security challenges in the cloud is technical approach. Thus, [2] focuses on technical security issues arising from the usage of cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations.

[11] provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organization should take when outsourcing data, applications, and infrastructure to a public cloud environment. The advantages and disadvantages (in the context of data security) of using a cloud computing environment are presented in [6]. It also analyzes the data security risks and vulnerabilities which are present in current cloud computing environments. [10] illustrates the unique issues of cloud computing that exacerbate security and privacy challenges in clouds and discusses various approaches to address these challenges and explore the future work needed to provide a trustworthy cloud computing environment. [3] makes a step forward and proposes to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques to alleviate much of today's fear of cloud computing.

We found nice high-level approach of security management in cloud computing in [7] where the authors provide an overall security perspective with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of cloud computing. Different cloud delivery and deployment models are matched up against some of the information security requirements.

However, so far there are no papers that analyze how cloud security vulnerabilities and threats impact to both the client's and provider's business continuity and it is our challenge and main topic in this paper.

1.2 Risk-based approach

Business managers know that risks exist in spite of all the benefits of every new technology or business model offers. Also, many issues like regulatory violation, security, trust and privacy appear. Thus, each company that dives ahead using the

benefits of cloud computing, should evaluate the risks found if moving into the cloud, as well as if stay to the traditional solutions.

The main challenge when moving into cloud is security. Outsourcing data and application, virtualization and hypervisors, heterogeneity, lost security perimeter are some of the issues that should be addressed at least. The client company should define risk assessment mechanism to define levels of risk and make it part of the system development life cycle. Without preparation of risk assessment, it would be impossible to evaluate whether company systems are candidates for operating in the cloud and to assess the potential cloud service providers for their risk management practices. When this process is accomplished, the company systems and projects can have their risk assessments mapped with the cloud service provider and a decision can be reached about whether moving into cloud is appropriate for the systems.

This risk assessment should not be a static one, but a dynamic, in order to meet the latest standards and trends. Both the cloud client and provider should evaluate the risks for the cloud services according the provider's cloud design and the user's service risk assessment. Also, hypothetically and eventually "leaving the cloud", that is, moving back to the traditional solutions, should be covered in the risk assessment.

It is often possible for cloud clients to "transfer" the risks to the cloud provider, if applicable. However, neither always nor all risks can be transferred to the provider. If some risk leads to the incident scenario with business failure, serious damage to reputation or legal implications, it is hard or even impossible for any other party to compensate for this damage. Ultimately, you can outsource responsibility but you can't outsource accountability [5].

Therefore, the motivation of this research is to address the main security challenges in the cloud, especially those that can be disastrous to the cloud client business, and have impact to the business continuity.

In this paper we analyze the security challenges in the cloud and the risk of incident scenario and their impact to cloud client business continuity. We also present benefits of the cloud in order to help the business managers in preparing the plans, such as Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) before moving the services into the cloud.

In the Section 2 we present the information security risk management process used to define, assess, treat and evaluate the risk acceptance, to compare the risk of staying with traditional in-house solution and the risk of moving the services into cloud. In Section 3 we address several main security benefits in the cloud that impact to the client's business continuity. The last two sections are dedicated to conclusion derived from our research, and plans for future work, respectively.

2 Information Security Risk Management

Cloud features, such as scalability and flexibility, impacts both positive and negative to the security [5]. The massive concentrations of data, applications, servers and resources in the cloud provoke the hacker efforts to attack, but on the other hand, cloud-based defenses can be more robust, scalable, etc, offering better protection as

the cost for traditional solutions defenses. Therefore, both the client and provider should perform the information security management.

The potential cloud clients should establish metrics and standards for measuring performance and effectiveness of information security management before moving into the cloud. Therefore, the risks of using cloud computing should be assessed and compared to the risks of staying with in-house solutions [5]. Cloud service providers should also include metrics to assist customers in implementing their Information Risk Management requirements. The potential cloud clients should understand their current metrics and how they will change when operations are moved into the cloud, where a provider may use different (potentially incompatible) metrics [8].

A formal risk assessment process, as a part of the security risk management process, should be established that allocates security resources linked to client's business continuity and to compare the risks of using cloud computing with the risks of staying with traditional solutions.

2.1 Risk Assessment Process

Security risk assessment is activity where the risks are identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization. This activity should be the main sub process during the Security Risk Management, because all the assets in cloud are exposed neither to the same risks, nor to the same risk level as before moving into cloud. The same assumption can be made in the eventually reverse process, which is, moving back from the cloud to the traditional solutions.

Security risk assessment is critical process which helps the company identifying, selecting / excluding security controls during the process of establishing the ISMS for ISO 27000 certification candidates, or during the processes of reviewing ISMS and its improvement. Lack of attention in risk assessment when migrating into cloud, can increase the information security audit findings. Even more, some of the risks can be unidentified or remain untreated. This motivated us to deeper explore the effects of risk in business continuity when moving into cloud.

Besides the protection of information assets, detailed and technical security risk assessments in the form of threat modeling should be applied to applications and infrastructure as well, due to their outsourcing.

The risk evaluation is the next activity after the risk identification and estimation [13]. For each asset, the relevant vulnerabilities and their corresponding threats should be considered, and if there is vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but precaution should be taken if the situation is changed eventually).

Also, other important issue is the business impact of the incident, as well as the likelihood to happen. [9] provides needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies.

A matrix for risk quantification to successful risk measurement in a scale of 0-8 is defined in [13], annex E. The risks are rated as low (scale 0-2), medium (scale 3-5) and high risk (scale 6-8) as shown on Fig. 1.

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Fig. 1. The risk level as a function of the business impact and probability of incident scenario

With these rating, business managers can evaluate the risks before and after eventually moving into cloud, and they can measure whether the risks are acceptable and treated as planned.

3 Business Continuity Challenges

In previous sections we analyzed existing research on risk assessment when moving into cloud and pointed that business continuity challenges were not analyzed systematically so far. Therefore, in this Section we point the security benefits that impact to the cloud client business continuity.

3.1 Why Business Continuity and Disaster Recovery Planning is important?

The main goal of every company is to make the business growth. To achieve business growth, the company must have plans in place that will allow business continuity. The purpose of every business continuity / disaster recovery planning is to minimize the impact of any predictable / unpredictable interruption event on business processes. Business continuity and resiliency services helping businesses avoid, prepare for, and recover from a disruption.

The cloud client business continuity and disaster recovery plan should include scenarios for loss of the cloud provider's services, and even for the provider's loss of its third party services and third party-dependent capabilities [8]. In BCP, cloud client must determine who to contact if security incident occurs, or other events that require investigation, identification, notification, reaction, or even eventually legal actions. This plan should be tested periodically together with the cloud provider.

As the cloud provider becomes an external party the client relies, the cloud provider has to develop and approve BCP, mapped to the international standards, such as [13,14]. The cloud service provider must supply the client with provider's:

- Documentation for assets and resources are assessed and audited, as well as the frequency of the assessments and audits.
- Incident management, business continuity and disaster recovery plans, policies, and processes and procedures

- Review of co-location and back-up facilities, if applicable
- Providers critical services, key performance indicators (KPIs), and the way they are measured

In order to make a decision if the business migrate the services from traditional solutions to the cloud, business managers should complete and sustain the risk assessment, establish risk acceptance and measure the security risks in both solutions, especially the situation if they impact to the business continuity.

Table 1 as pointed out in [4] lists many events which could have impact to the cloud client business continuity, some of them potentially disastrous.

Table 1. Potentially Disastrous Events.

Avalanche	Flood	Shooting
Severe Weather (heat, cold, blizzard, etc.)	Natural Gas Leak	Fuel Shortage (usually associated with a loss of main electrical power)
Biological Hazard	Heating Ventilation or Air Conditioning Failure	Bomb Threat
Civil Disorder	Hostage Situation	Kidnapping
Telecom Outage	Acts of Terrorism	Theft
Robbery	Train Crash or Derailment	Lightning Strike
Computer/Software Failure, Virus or Destruction	Employee/Union strike	Acts of Vandalism
Pandemic	Picketing	Power Outage
Fire Damage	Water Damage	Radiological Hazard

3.2 Business Continuity Benefits from the Cloud

In this section we introduce a relatively complete survey of key factors for security aspects of moving into cloud for business continuity domain. Several papers [2,3,5,8,10,11] have mentioned many security vulnerabilities and threats, but this paper summarizes all relevant efforts and introduces another dimension.

Despite the security challenges and risks appeared to the business continuity if moving into cloud, we address several benefits that cloud computing has over traditional business continuity, as well. These benefits improve the client's BCP and depreciate the impact of the incidents to the client's business.

Eliminating downtime. SaaS offers advantages over traditional computing, for example, in the email services. Thus, SaaS ensures that email messages are never lost and makes the system outages virtually invisible to end users no matter what happens to your employees or infrastructure.

Better Network and Information Security Management. Company can outsource noncritical applications and its data to cloud, where they can run with better performance, which allows the company IT department to focus on critical applications. This also improves company network security and user access management.

Disaster Recovery – Backup Management. The successful recover from a disaster depends mainly of the quality and the frequency of backups. Cloud offers much better layered backup strategy. This feature offers to have a better Recovery Point Objective (RPO).

Disaster Recovery – Geographic Redundancy. Cloud Providers offer a built-in geographic redundancy in the form of regions and availability zones. This feature offers to decrease the Recovery Time Objective (RTO). We must note that many of the events in Table 1 are geographically related.

Avoid or eliminate disruption of operations. Some clouds expose a hash (Amazon S3 generate an MD5 hash) when store an object, thus eliminating the need for forensic image verification time.

Increased Availability. The scalability feature of cloud computing facilities allows for greater availability. Redundancy exists all over the cloud environments and on-demand resource capacity increases service availability.

DoS Attack Depreciation. Redundancy and on-demand resource scalability also provide better resilience when facing distributed denial of service attacks, as well as for quicker recovery from serious incidents.

4 Conclusion

Cloud computing offers a lot of benefits to the clients, but many security risks, as well. As cloud computing offers cost saving for the clients, they should reinvest the savings into the security, especially when they outsource into IaaS and PaaS, where they have a greater degree of control and responsibility, than the SaaS [8]. They should invest the savings into increased inspection of cloud service provider security management capabilities, security controls, and implement regular assessments and audits on cloud provider's BCP, DRP, processes and procedures.

In this paper we analyzed the opportunity to migrate company services from traditional solutions into the cloud with higher level of abstraction, that is, risk-based analysis, instead of using only technical security and control-based requirements.

We address cloud computing model security beneficial that improves the business continuity: eliminating downtime, better network and information security management, disaster recovery with both backup management and geographic redundancy. It also avoids or eliminates disruption of operations, increases service availability and DoS attack.

We are confident that our work can help the business managers in the information security risk management process, business continuity planning, disaster recovery planning, for both prior and post some or all the services migrating into the cloud. Also, we believe that they can assess the possible risks of the opposite process, which is, downgrading from the cloud to the traditional in-house solutions.

5 Future work

Probably not all cloud service providers neither offers all the specified benefits, nor offer or can guarantee some of the solutions to the specified security risks. Thus, it is our intention to evaluate the existing cloud computing solutions in the manner of security, both the benefits and detriments, and recommend the security improvements. We will also try to define relevant indicators for benchmarking and recommend addendums to known ISO 27K standards for cloud computing deployment.

Our intention is to emphasize not only the benefits the cloud computing offers, but the security benefits for a company as well. Also, cloud computing has a lot of security flaws, so we intend to propose solutions to the flaws as they can be minimized or become even a benefit in the manner to BCP, to offer the company business continuity better, instead of traditional solutions.

6 References

1. Chen, Y., Paxson, V., and Katz, R.: What's New About Cloud Computing Security?, Technical Report No. UCB/EECS-2010-5, EECS Dept., Univ. of California, Berkeley, (2010) http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html
2. Jensen, M. Schwenk, J. Gruschka, N. Iacono, L.L.: On Technical Security Issues in Cloud Computing.In: Cloud Computing, 2009. CLOUD '09. IEEE International Conference on, pp 109--116, (2009)
3. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling data in the cloud: outsourcing computation without outsourcing control. In: ACM Workshop on Cloud Computing Security (CCSW'09). pp. 85--90. ACM Press (2009)
4. Alexander, P.: Information security: a manager's guide to thwarting data thieves and hackers (2008). ISBN-13: 978-0-313-34558-6
5. Catteddu, D., Hogben, G.: Cloud computing risk assessment. European Network and Information Security Agency. (2009). http://www.enisa.europa.eu/publications/position-papers/position-papers-at-enisa/act/rm/files/deliverables/cloud-computing-risk-assessment
6. Sangroya, A., Kumar, S., Dhok, J., Varma, V.: Towards Analyzing Data Security Risks in Cloud Computing Environments. In: S.K. Prasad et al. (Eds.): ICISTM 2010, CCIS 54, pp. 255--265, 2010. Springer-Verlag Berlin Heidelberg (2010)
7. Ramgovind, S. Eloff, M.M. Smith, E.: The management of security in Cloud computing. In: Information Security for South Africa (ISSA), (2010)
8. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, https://cloudsecurityalliance.org/csaguide.pdf
9. Top Threats to Cloud Computing V1.0, http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
10. Takabi, H.; Joshi, J.B.D.; Ahn, G.: Security and Privacy Challenges in Cloud Computing Environments. J. of Security & Privacy, IEEE, Vol. 8, No 6, 24--31 (2010)
11. Jansen, W., Grance, T.,: Guidelines on Security and Privacy in Public Cloud Computing. Draft NIST Special Publication, National Institute of Standards and Technology, (2011)
12. Mell, P., Grance, T.: The NIST Definition of Cloud Computing, Version 15, (2009) http://csrc.nist.gov/groups/SNS/cloud-computing
13. ISO/IEC 27005:2008 Information technology - Security Techniques - Information security risk management; Annex E: Information security risks assessment approaches, (2008)

14. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2005), http://www.iso.org
15. Ristov, S., Tentov, A.: Security Based Performance Issues in Agent-based Web Services Integrating Legacy Information Systems. In: Proceedings of the WASA 2011, CEUR Workshop Proceedings, Vol. 752, pp. 45-51, ISSN 1613-0073, (2011)
16. Sonntagbauer, P., Gusev, M., Tomic Rotim, S., Stefanovic, N., Kiroski, K., and Kostoska M.: e-Government and e-Business in Western Balkans 2010, Proceedings of the 2nd ICT Innovations conference, Ohrid, Macedonia, 2010.