Selected Issues of IT Risk Management in the Cloud Computing Model. Theory and Practice

Artur ROT
Department of Information Systems, Wroclaw University of Economics
Wroclaw, Poland

ABSTRACT

Cloud computing transforms the way IT is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand [9]. However, as the cloud computing is developing rapidly, the legal, economic, service quality, interoperability and especially security and privacy issues pose significant challenges [13]. The risk connected with the wide application of this technology in business grows together with the increase of organization's correlation from its customers, business partners and outsourced operations. Technological progress generates dependencies which evoke growth of diversities, complexity, non-descriptiveness and quantity of risk factors. In insufficient investments on information security the issue of IT risk management becomes more significant, concentrating on searching optimal proportion between threats and costs of IT systems protections. In such a dynamic development of Information Technologies, especially Cloud Computing, the time needed for appropriate reaction on risk is decidedly shortened. Failure to ensure appropriate security protection when using cloud services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing. This article outlines the issue of IT risk in the cloud computing model, it describes various risks in cyberspace, identifying major challenges for cloud computing. In particular, the paper discusses IT security risk management as critical challenge in cloud computing. These issues were presented both in their theoretical aspect and in the light of selected empirical research studies.

Keywords: Cloud Computing, Risk Management, IT Security, Risk Avoidance, Disaster Recovery, Business Continuity Management.

1. INTRODUCTION

In recent years business, and in particular the applied information technologies, have seen a radical change, including the appearance of three aspects of their development which completely reshape the traditional approach to managing the risk of IT systems. These three new phenomena include cloud computing, mobile solutions and social media. Each of these areas has its own specificity and changes the paradigm of security, which seems not to be noticed by both business owners and users, and the providers of IT solutions [18].

As new technologies develop, in particular those related to cloud computing, boundaries between the operations of nowadays firms become even more blurred. The fast changing modern technologies offer huge advantages for organizations, but – unfortunately – they also entail new forms of risk, making the traditional approach to security inadequate for the current situation. All the time new types of threats are created, which are often not understood an d remain underestimated by the senior management of an organization. Organizations today face a serious challenge of implementing an effective security strategy, which should include an adequate risk management process, while the current comprehensive approach is becoming out of date. An essential prerequisite is the knowledge of threats, as well as the evaluation if and to which extent they influence our security.

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [13]. The rules presented in this article should be implemented and supported with expertise, software and hardware. The purpose of this article is to outline the issue of IT risk in the cloud computing model and presenting the most essential aspects of cloud computing security. The article shows these issues both in their theoretical aspect and in the light of selected empirical research studies.

2. SOURCES OF RISK IN CYBERSPACE

The key reasons for the development of new types of risk which accompany the operation of contemporary IT systems such as cloud computing, are, among others, the following facts and circumstances [2]:

- information has become one of the most required goods on the market, which results in the increase of its price, thus raising the risk of its unauthorized acquisition,

- relentless pursuit of information, particularly in the business area,
- common availability of IT systems, which also facilitates the development of computer-related crime,
- most of the information, which has so far been dispersed, is now stored in one location, i.e. in the cloud, which makes it easily available,
- the technological complexity of corporate IT systems and their security, resulting in an average user not being able to use them rationally in order to minimize all possible threats,
- widespread ignorance or unawareness of threats to IT systems, which results in failure to comply with adequate requirements, procedures, etc.
- data collected in the IT systems (particularly those operating within the cloud computing model) are controlled by the administrators of these systems, which causes that there are several individuals having access to the relevant data and being able to modify them while remaining unnoticed,
- security systems designed to counter cyber threats are very expensive and therefore easily overlooked in favour of the unit's performance,
- companies offering IT security are often not certified and therefore their products are unreliable,
- new threats are being created by the Internet, which provides an easy access to IT security circumvention software.

The threats to IT systems are no longer the exclusive interest of specialists in IT security and the latest information technologies, as their consequences affect a substantial number of companies and their clients. Each existing list of incidents, included those related to cloud computing, is certainly incomplete. It is hard to determine, which organizations are being infiltrated, since many of them are not aware of having been attacked, whereas others are reluctant to disclose information about the cases of breaking into their systems due to fear of e.g. losing their reputation. All around the world such incidents take place almost every day.

The global number of detected cyber security incidents has risen by 38%, as compared to the previous year, which is indicated in the research study "The Global State of Information Security Survey 2016" carried out by PwC. Polish research study, which was conducted in the course of this report, showed that this proportion was even higher and stood at 46% [12].

3. ARCHITECTURE OF CLOUD COMPUTING

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage [7]. Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers. It refers to applications delivered as services over the Internet as well as to the actual cloud infrastructure — namely, the hardware and systems software in data centers that provide these services [6]. Thanks to this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly [7]. From the perspective of service delivery, NIST has identified three basic types of cloud service offerings. These models are [1] [7]:

- Software as a service (SaaS) which offers renting application functionality from a service provider rather than buying, installing and running software by the user.
- Platform as a service (PaaS) which provides a platform in the cloud, upon which applications can be developed and executed.
- Infrastructure as a service (IaaS) in which the vendors offer computing power and storage space on demand.

Cloud integrators can play a vital role in determining the right cloud path for a specific organization [4]. Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are three main ways in which cloud services are deployed [13] [4]:

- Public clouds:
  - provided by a designated service provider,
  - may offer either a single tenant or multi-tenant operating environment with all the benefits and functionality of elasticity and the utility model of cloud,
  - the physical infrastructure is generally owned and managed by the designated service provider and located within the provider's data centers,
  - all customers share the same infrastructure pool with limited configuration, security protections, and availability variances,
  - one of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.
- Private clouds [13]:
  - provided by an organization or their designated services,
  - offer a single-tenant operating environment with all the benefits and functionality of elasticity and utility model of cloud,
  - the private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud.
  - there are two variants of private clouds [7]:
    (i) on-premise private cloud (also known as internal clouds) – hosted within one's own data center (this model provides a more standardized process and protection, but is limited in aspects of size and scalability).
    (ii) externally hosted private cloud – this type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy (this is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources).

- Hybrid Clouds [7]:
  - combine both public and private cloud models,
  - it can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud [5],
  - the cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and applications to be moved from one cloud to another one.

There are some of the considerable challenges associated with cloud computing, and although some of these may cause a exemption when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages [5]. The most important challenges certainly are security and privacy. These challenges surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. When considering a move to cloud computing, customers must have a clear understanding of potential benefits and security risks associated with cloud computing.

4. RISK MANAGEMENT IN THE NEW TECHNOLOGICAL AGE

Until recently, persons who were responsible for IT risk management assumed that managing such risk is possible only in the case of having full control over servers, storage media, applications and network links, i.e. everything which is related to corporate IT systems. Such an approach resulted in all the security and protection mechanisms being modelled with the assumption of a full control and ownership of the used resources. In the meantime, in consequence of the dynamic development of the Internet and IT solutions the classical security paradigm has lost its reason for being. Companies are not able to control fully their applications and data uploaded to the cloud or social media networks, which means that they are not able to manage their security according to the classical definition. For that reason managers should change their perception of risk and security issues in IT systems [11].

The key element of an IT security management system is risk management, whose aim is to control and maintain an acceptable level of risk. It is a level which guarantees the required security and simultaneously allows the effective use of resources, i.e. involves a compromise between the willingness to take risk and security. The cloud computing model entails specific types of risk, which results from the type of resources that can be threatened, as well as technologies. Unauthorized actions require expertise, hardware and software; they are usually difficult to identify for an average user. Therefore, they require an adequate response, including having at one's disposal adequate resources, which will enable to secure the network together with its computers and resources.

The key element of the risk management process is the risk analysis, which allows to identify system resources, localize their corresponding vulnerabilities and threats, as well as estimate the probability of their occurrence and the extent of potential losses. A crucial stage following the risk analysis consists in choosing the risk management procedure. Within this stage, one should:

- identify the methods, tools and means of risk reduction and transfer, as well as estimate their cost and effectiveness,
- implement the methods and means of risk reduction or transfer,
- determine the acceptable level of risk,
- establish the methods of risk avoidance.

Risk avoidance consists in adopting such IT management practices, which exclude the possibility of an increase in the level of risk. Risk avoidance means managing the activities (without the implementation of new security measures) in a way which allows for maintaining the lowest possible risk related to a given activity, or not performing this activity at all [16].

The risk can be reduced by the implementation of a security architecture, consisting of security measures procedures, regulations, etc. The undertaken action can lead to the elimination of risk or its reduction to an acceptable level. Measures aimed at the reduction of risk may go in two directions [14]:

- prevention, i.e. creating impact by controlling the vulnerability to threat materialization;
- minimization (reduction) of losses, i.e. influencing the result of threat materialization, with the aim of reducing the extent of potential losses.

Preventive measures include such activities as: security of access to hardware, software, data, access to the Internet as well as other internal/external networks, systems for malware detection and elimination, internal control procedures, as well as audit and the selection and training of personnel.

The measures reducing the consequences of negative events include [18]:

- emergency plans aimed at disaster recovery as well as maintaining the continuity of business operations,
- technical architecture considering redundant systems and operation centers,
- response procedures to incidents,
- backup devices.

The basic tools for minimizing the consequences of negative events are disaster recovery plans (or DRP) and business continuity plans (or BCP). In terms of finance, reserves are created and insurance against some types of risk is arranged [8]. DRP and BCP are expensive and should be applied only there where they are indispensable. Their essentiality can be determined based on the analysis of risk and defined critical processes. The critical processes are those which decide about the core activity of an organization. BCP include adequate

procedures and usually a second set of hardware resources, along with a copy of data, which is stored in secure locations. It allows a reconstruction of infrastructure and maintaining the continuity of organization's operations.

The transfer of risk consists in ceding the consequences of damage occurrence or the financial liabilities resulting from it on another entity. The fundamental rule of such an operation is transferring the abovementioned consequences or liabilities on an entity which is able to manage its risk better than the entity which wants to eliminate this risk or reduce it. The forms of risk transfer in organizations include outsourcing (i.e. using specialized external services) or insurance.

The necessity to change the approach to security has been perfectly highlighted by the rise of cloud computing, and particularly by 'infrastructure as a service' offers (or IaaS). The users do not purchase any application or physical discs or servers which need to be protected, but they are recipients of a service which involves a remote access to an application or a disc space. Access management is transferred to a third party under an agreement, whereas the decisions related to risk management remain entirely beyond the company, which needs to support itself with the collected data, contractual provisions and, if necessary, additional insurance coverage [18].

A change in terms of costs is also essential: the company does not incur expenses for IT infrastructure, but it pays its subcontractor for the access to resources and software, as well as for the protection of data stored on remote servers. Both risk management and cost structure undergo a radical change. The fundamental change in terms of security involves the transfer of risk from internal (i.e. own) IT to an external provider [11].

Risk acceptance means coming to terms with possible consequences and giving up further action. According to the fundamental rules of risk management, it means that the owner conducted an analysis and accepted the existing threats as well as the available methods of their reduction. However, in the case of new technologies only a small percentage of users are aware of the necessity to accept risk, whereas the rest trivialize the process of such acceptance [11].

5. THE SECURITY ASPECTS OF CLOUD COMPUTING

Cloud computing has been one of the fastest growing trends of the recent years. Cloud computing is a phenomenon which, according to experts, will dominate the IT market in the coming years. The philosophy of cloud computing consists in transferring all the burden of providing IT services (data, software or processing power) to the provider's server and providing a permanent access via client computers. Owing to this, the security does not depend on what occurs to the client computer, and the processing speed results from the processing power of the server. Cloud computing consists in providing solutions, in which a part of the IT system is located beyond its infrastructure.

Data is at the core of IT security concerns for any organization, whatever the form of infrastructure that is used. Cloud computing does not change this, but brings an added focus because of the distributed nature of the cloud computing infrastructure and the shared responsibilities that it involves. Essentially, the questions relating to data for cloud computing are about various forms of risk: risk of theft or unauthorized disclosure of data, risk of tampering or unauthorized modification of data, risk of loss or of unavailability of data [17].

The main risks related to cloud computing services refer to the issues of authorization, data security and privacy, interfaces with internal systems, system availability, continuity of system operation, as well as its content and other legal requirements. Among all these risk factors the security and privacy are the most crucial area, since the related data is stored outside the premises of the organization. Before the implementation of cloud computing solutions, numerous security-related issues should be taken into account, including [15]:

- Risk management in an enterprise – is related to the organization and requires control and supervision over actions and services taking place in the cloud. In particular it refers to these issues, in which the employees of the cloud computing provider are involved, such as the standards of application development, design, monitoring and implementation. The migration of processes to the cloud requires special attention to risk management, which is a consequence of new types of business models.
- Compliance with the provisions of law – the cyberspace is regulated by a number of norms and legal provisions, and the cloud computing providers are obliged to comply with them. By deciding to use the cloud computing solutions, one should be aware that e.g. transferring personal data outside its country of origin is subject to strict regulations and a decision must be taken on where the data processing is going to take place, so that there is no infringement of the relevant provisions of law.
- Resource sharing – this issue raises a challenge to the protection of user data from unauthorized access by another users carrying out processes on the same physical servers. Resource sharing may also foster a more rapid dissemination of malware.
- Information management and data security – includes the identification and control of data. The data is protected by the network security measures, in terms of both virtual and physical data integrity, as well as data segregation, creating backup copies and data encryption. This field should also include the protection of data from unauthorized access and prevent the loss of data during their migration in the cloud. Particular importance in the cloud computing model should be given to the following areas of information management [15]:

- Authorization and credibility of the acquired information – within the cloud infrastructure there is data which can be altered without the owner's consent.
- Data segregation – using the cloud computing platform involves technology sharing, therefore the stored information and data should be adequately separated in order to ensure that each client has only the access to the essential information and does not have influence on another clients' data.
- Data retrieval – losing data is a serious security problem within the cloud. Cloud service providers should ensure that adequate data retrieval systems are implemented, and the clients need to know what happens with their data in case of a disaster. One of the security requirements that has to be fulfilled is the replication of data and the reliability of storage media.
- Identification and access management – the process of taking decisions concerning access authorization, processes and data stored in the cloud.

Another issue threatening the security of the data are the standards of cloud computing services. In order to achieve the interoperability between clouds and increase their stability and security, it is essential to introduce unified standards. The data storage services offered by one cloud provider may be in contradiction with the interest of another service provider. Currently there is a large number of diverse standards representing entities with different interests, e.g. IEEE Cloud Computing Standard Study Group (IEEE CCSSG), ITU Cloud Computing Focus Group, or Cloud Security Alliance (CSA). In order to raise interoperability and free flow of data between clouds, common standards must be developed in such areas like network architecture, data format, measurement and settlement, service quality, resource assignment, security, identity management and privacy [15].

6. THE PRACTICAL RISKS OF CLOUD COMPUTING

Both the number of services provided in the cloud and the number of its users are growing dynamically. The largest problem of entrepreneurs who are interested in the cloud services are the issues related to the data security risk. A research study conducted by Harris Interactive shows that as many as 91% of respondents are afraid about the security of public clouds, and about 50% indicate that the issues of security pose the largest obstacle to the dissemination of cloud solutions. The Eelastic-security.com also decided to analyze this problem by carrying out a survey among cloud service providers. The aim of the survey was to determine how the security issues are perceived by the providers and the users of cloud computing services. The survey results show the discrepancies between the expectations of each of these groups. 69% of the 127 surveyed cloud providers placed the responsibility for the security of using cloud services their users, whereas the users expressed an opposite opinion. The majority believe that the responsibility for the security in cloud should be assigned to the service provider or that it is jointly shared by the provider and the recipient [10].

Even though cloud computing has been known for several years, for most users it still remains a mysterious technology, and therefore it seems to carry significant risk. As the Gartner Group analysts highlight in their report "Assessing the security risks of cloud computing", processing data outside the company entails risk, therefore in order to minimize it, the firm should decide to use only the proven and best solutions [3].

The Deloitte experts also stress the threats related to the use of new technologies. Almost one third of the surveyed organizations indicated cloud computing as the main technological solution which will decide about the future of information security. 60% of the responding organizations believe that third parties (e.g. organizations, with whom they exchange information or to whom they entrust it) are a moderate or major threat for the protection of data, yet only 31% check their corresponding security measures. The experts believe that companies should understand that the security of their IT systems is increasingly more dependent on the third parties. If an organization applies high standards with regard to information security, similar security standards should be required from external entities and cloud computing providers. According to the abovementioned PwC's research, the most significant risk related to cloud computing, in the respondents' opinion, results from the limited possibility to enforce the application of security policies on the providers of this technology.

7. CONCLUSIONS

Cloud computing offers a viable alternative to the current traditional model of IT management. It must be stressed that from the security perspective, this model involves a transfer of risk from the company's internal (own) IT on an external provider. However, the decision to use the external provider should be well considered and based on rink analysis. The most significant forms of risk related to the use of cloud computing include risks within three categories: availability, data security and compatibility.

As numerous research studies show, companies notice the trends related to new forms of risk even more frequently, as well as the fact that the level of risk related to the development of new technologies, including cloud computing is increasing. Managing IT risks is a crucial subject for many areas of IT departments, yet it does not remain the exclusive domain of IT specialists. The risks related to running a business in the cyberspace, such as the risk of losing reputation, financial losses, interruption

in the business activity (sales, providing services), consequences for innovation, research and development, or regulatory penalties are crucial areas of interest for the entire organization. That is why they should be placed on the map of the key areas of risk to be monitored by the adequate company departments.

8. REFERENCES

[1] Badger, L., Grance, T., Patt-Corner, R., & Voas, J., **Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146**. US Department of Commerce. May 2011. Available online at: http://csrc.nist.gov/publications/drafts/800-146/ Draft -NIST-SP800-146.pdf (accessed on: 11.05.2016).

[2] Barczak A., Sydoruk T., **Security of Management Information Systems**, Dom Wydawniczy Bellona, Warsaw 2003, s. 80-82.

[3] Bienkowski M., **Seven threats for cloud computing security** (In Polish), http://webhosting.pl/ (accessed on: 29.01.2012).

[4] **Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing CSA**, April 2009, https://cloudsecurityalliance.org/csaguide.pdf (accessed on: 17.12.2015).

[5] Dialogic, **Introduction to Cloud Computing**, White Paper, https://www.dialogic.com/~/media/products /docs/whitepapers/12023-cloud-computing-wp.pdf (accessed on: 04.11.2016).

[6] Dikaiakos M.D., Pallis G., Katsaros D., Mehra P., Vakali A., **Cloud Computing Distributed Internet Computing for IT and Scientific Research**, http://inf-server.inf.uth.gr/~dkatsar/papers/IEEE_ IC09dkmpv.pdf (accessed on: 18.11.2016).

[7] Harris T., **Cloud Computing – An Overview**, http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf (accessed on: 15.11.2016).

[8] Kapalczynski A., **Risk Management in Cyberspace in Uncertain World – Selected Issues**, Materials from an international academic conference „Socio-economic aspects of information society" 2013, http://www.myit.pl/2013-07-04-13-47-39/87-cyber, (accessed on: 30.11.2016).

[9] Leighton, T., **Akamai and Cloud Computing: A Perspective from the Edge of the Cloud**. White Paper. Akamai Technologies 2009, http://www.essextec.com/assets/cloud/akamai/cloudcomputing-perspective-wp.pdf (accessed on: November 20, 2012).

[10] Matuszewska B. **Safely in the Cloud,** Gazeta.pl web portal, 05.10.2011, (In Polish) http://komputerwfirmie.gazeta.pl/itbiznes/1,54790,10412168,Bezpiecznie_w_chmurze.html (accessed on: 01.03.2012).

[11] Poniewierski A. **New approach to IT security**, Harvard Business Review Polska no. 127, (September 2013), (In Polish), https://www.hbrp.pl/a/nowe-podejscie-do-bezpieczenstwa-it/36I9bAJw (accessed on: 10.11.2016).

[12] PwC: **The Global State of Information Security Survey 2015 – key conclusions from the results of the survey** http://www.pwc.pl/pl/publikacje/assets/gsiss_2015 _polska.pdf, 2015 (accessed on: 12.02.2016).

[13] Sen J. **Security and Privacy Issues in Cloud Computing**, Cornell University Library, https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf (accessed on: 30.10.2016).

[14] Szczepankiewicz E.I., Szczepankiewicz P., **Risk analysis in IT environment for the Purpose of Operational Risk Management. Part 3 – Strategies of Dealing the Operational Risk.** (In Polish), Monitor Rachunkowosci i Finansow no. 8/2006.

[15] Wojciechowska-Filipek S., **Selected issues of cloud computing security** [W:] Risk Management in Economy, Volume XVI, Part 3, ed. Raczkowski K., Wojciechowska-Filipek S., Spoleczna Akademia Nauk, Lodz-Warsaw 2015.

[16] Wolowski F., **IT security risk management.** (In Polish), [In:]. Information Systems Security, ed. Niemiec A., Nowak J.S., Grabara J.K, Polish Information Processing Society – Upper Silesian Division, Katowice 2006.

[17] Cloud Standards Customer Council, **Security for Cloud Computing. Ten Steps to Ensure Success. Version 2.0**, March 2015, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf (accessed on: 11.11.2016).

[18] Rot A. **Zarzadzanie ryzykiem w cyberprzestrzeni – wybrane zagadnienia teorii i praktyki** [In:] Projektowanie i realizacja systemow informatycznych zarzadzania. Wybrane aspekty, ed. Komorowski T.M., Swacha J., Polish Information Processing Society PTI, Warsaw 2016.