IT Security Threats in Cloud Computing Sourcing Model

Artur Rot
Wroclaw University of Economics
ul. Komandorska 118/120
53-345 Wroclaw, Poland
Email: artur.rot@ue.wroc.pl

Malgorzata Sobinska
Wroclaw University of Economics
ul. Komandorska 118/120
53-345 Wroclaw, Poland
Email: malgorzata.sobinska@ue.wroc.pl

Abstract— **New information technologies have been developing nowadays at an amazing speed, affecting the functioning of organizations significantly. Due to the development of new technologies, especially mobile ones, borders in the functioning of modern organizations diminish and models of running business change. Almost all organizations are involved in some way in sourcing activities, and each of them develops a sourcing relationship that suits its particular needs. In this article different kinds of outsourcing models were discussed, which are applied in the contemporary management, with particular emphasis put on cloud computing.**

The main aim of this article is to present the most important risks related to the introduction of management models based on the most recent IT technologies, e.g. cloud computing, and emphasizing the role of appropriate IT security management in the times of globalization of organization virtualization.

I. Introduction

Information resources have nowadays strategic significance and have key influence on gaining the competitive advantage by all types of enterprises. Organizations are forced to look for still better and more effective IT solutions that enable for example: IT cost reduction, access to the best technology and best IT hardware and software experts, IT systems security etc. One of such new models referring to IT services is cloud computing.

Ongoing research projects investigate client and vendor capabilities required to successfully implement these sourcing models and initiatives, and how to manage knowledge and expertise in various sourcing contexts to improve efficiency and outcomes of sourcing engagements. Organizations are facing a large variety of possibilities to choose from when making sourcing decision. They should take into consideration a lot of factors (both positive and negative) to be able to make the right decision.

The London School of Economics's research regularly finds that firms that outsource give away too much of their technical capability. It is a challenge to retain skilled people in house paying them the market rate and offering them interesting, value-adding work. The alternative to such an "invest to save" HR approach is to put at risk the long-term health of the deal [4, p.10]. This can be especially true dealing with immature markets, such as cloud services.

In the next part of the paper we will discuss what makes cloud computing popular and what are the main risks of cloud computing sourcing model.

II. Evolution of sourcing models

Oshri, Kotlarsky and Willcocks, who have observed outsourcing market since years, notice that various types of global sourcing models have begun to emerge. The major difference between these models lies in whether the function is performed by a subsidiary business unit of the firm or an external vendor (or by both, as a joint effort), and also whether the function is performed on the firm's premises (i.e., on-site) or off-site, which can be onshore (in the country where the organization is located), nearshore (in a neighbor country), or in an offshore location [3, p. 25].

Insourcing means managing the provision of services internally, if needed- through buying in skills that are not available in-house, on temporary basis (for example by staff augmentation). Offshore or nearshore outsourcing means outsourcing contract with vendors situated in a different country from the client organization. Out-tasking- it is outsourcing on a small scale. It usually implies ongoing management of and support for selected packaged applications. Joint venture in the outsourcing or offshoring context – means a partnership between a client firm and offshore vendor whereby the parties contribute resources to the new deal/project Shared services- it is an operational approach of centralizing administrative and business processes that were once performing in separate divisions or locations- for example: finance, IT, human resources. In literature there are listed also the following sourcing models based on Internet delivery of products or services: cloud computing, software as a service, crowdsourcing, and microsourcing. Sourcing decisions should be made jointly by business and IT executives [4, p.11].

III. Attributes of cloud computing model

Although the idea of cloud computing has been around for quite some time, it is an emerging field of computer science. Cloud computing can be defined as a computing environment where computing needs by one party can be

978-1-4673-4471-5/$25.00 © 2013, IEEE

outsourced to another party and when need be arise to use the computing power or resources like database or emails, they can access them via Internet. Cloud computing is a recent trend in IT that moves computing and data away from desktop and portable PCs into large data centers.

During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location. Security, in particular, is one of the most argued-about issues in the cloud computing field. Comparison of the benefits and risks of cloud computing with those of the status quo are necessary for a full evaluation of the viability of cloud computing.

In Hauke's and Owoc's opinion facilities available via cloud computing are strictly determined by properties of this technology based on Internet resources [2, p. 125]. One can identify two essential concepts in "cloud" environment-abstraction and virtualization and several properties that can be expressed as secondary (such as scalability, flexibility, availability, measurability, efficiency, low costs of services, low barrier to entry, security).

Security – the most "sensitive" and disputable feature of CC. Theoretically all potential problems should disappear (all necessary tasks are performed by specialized partner). No doubts, problems with database recovery should be served professionally, however, a risk of data loosing or data leaking can occur [2, p.126].

Cloud computing solutions are offered by such large organizations as IBM, Microsoft, Amazon, Google and others. They can give a lot of benefits but they have also some limitations. There are numerous challenges facing organizations when considering cloud computing. Willcocks and Lacity, in their analysis, focus on the four challenges which seem particularly critical in the development of cloud use within organizations: weighing up the security and legal risks, defining the relationship through contracting, the lock-in dilemma, managing the cloud [5, p.290-296].

Cloud represents a great opportunity, but there are also strong challenges to take if an organization wants to use its potential for business advantage.

IV. New Challenges for IT security management

The existence of a company in cyberspace and an opportunity to communicate with it via electronic media is often a minimum condition for the company to be perceived as a reliable and solid partner. Unfortunately, the development of IT, e-commerce and new business models (including various kind of IT sourcing) carries new risks apart from huge benefits. There are new threats, often incomprehensible and underestimated by company management. The basic premises indicating the emergence of new kinds of risk accompanying the functioning of management IT systems, include e.g. the following facts and circumstances [6, p. 11-13] [7, p. 80-82]:

- information has become one of the most important goods on the market, which hence increases its price, meanwhile generating a risk of its unauthorized interception,
- ruthless chase after information, which is especially typical of business and media environments, blurs the border between legal and illegal actions aimed at acquiring it,
- increasing the availability of IT systems, which are considered to be the condition of society civilization development expansion, which facilitates the development of cybercrime,
- most of documents and information, which were dispersed so far, now are stored in one place – in a computer, which makes them easily accessible, but in case of unauthorized access the scope of damage is extensive,
- technological complexity of company IT systems and their security, which makes it impossible for an average user to use them rationally in order to minimize all threats,
- common lack of knowledge or unawareness of information systems threats, which results in lack of compliance to certain requirements, procedures etc.,
- data gathered in IT systems remain under the supervision of system administrators, which results in the fact that a few people have an insight into very important data and can modify them practically without anybody noticing,
- security systems are expensive and happen to be neglected for the sake of efficient performance of an individual,
- companies offering security tools for IT systems are often uncertified, which makes their products fallible and often of low quality,
- companies developing various IT solutions often offer fallible systems, which are full of mistakes,
- the Internet brings in new threats, since it is where you can easily find software for hacking IT systems.

Nowadays specialized institutions (e.g. CERT, Computer Security Institute, etc.) publish statistical data concerning the probability of occurrence of given kinds of threats [see: 8, 9]. According to various statistics, intentional or unintentional actions of organization staff (negligence, lack of concentration, incompetence) and purposeful actions of dissatisfied or sacked employees.

It is worth discussing here conclusions derived from the report 2011 TMT Global Security Study, prepared by the counseling company Deloitte. According to this report, one fifth of companies from the technology, media and telecommunication sector (TMT) find personnel mistakes to be the major threat for the company IT security. Another huge risk for the company IT systems security is the use of mobile devices by employees (personal smartphones, tablets, laptops) at work. The risk is in this case related to data confidentiality, application popularization and IT support.

Similar conclusions can be derived from studies conducted by the counseling company PricewaterhouseCoopers (PwC). The 2012 Global State of Information Security Study was conducted in 2011 all over the world. The results were obtained on the basis of answers provided by more than 9600 managers, vice-presidents and IT and information security directors from 138 countries, including Poland. According to them, current or former employees are perceived by companies as the major source of risks for IT systems. However, respondents pay more and more attention to a different category of external risks: 17% of respondents indicate clients, and 15% - business partners and suppliers as the key risk sources. In Europe during the past two decades the percentage of companies which require that the suppliers adjust security policies to their requirements, dropped from 31% to alarming 22%; only 18% of companies keeps records of all suppliers processing personal data of customers of employees.

Threats which are less likely to occur include ICT networks and IT systems failures and natural disasters (fire, flood, hurricane and earthquake). Threats related to unauthorized access (of e.g. hackers) and activities of malicious software are relatively unlikely to happen. When assessing the frequency of occurrence of such risks, it is recommended to take into account the specificity of the given company and its environment. The basic classification of IT systems security threats is presented in table 1.

V. Threats related to virtualization and cloud computing

Ernst & Young company conducted the ‘Global Information Security Survey’ in 2011 [12]. The study group consisted of 1700 organizations, including the largest and the most dynamic companies from 52 countries, from different trades (banking, finance, insurance, motorization industry, public administration, transport, health service, trade). The company has been conducting such studies for 14 years, and their aim is e.g. identification of the most critical kinds of risk in the field of new IT technologies. As it can be concluded from this study, respondents recognize trends related to new kinds of risk, since more than 72% of them estimates that the level of risk related to the development of such technologies, as the aforementioned mobile devices, cloud computing and social networking sites, is larger and larger. 46% of organizations recognize also increasing risk levels related to internal company threats. Polish results are consistent with global results as far as the assessment of the key threats is concerned. The study conducted by the company in 2010 [12] revealed that more than 64% of respondents found data safety to be one of the five key risk areas. It results directly from the fact that for 73% of Polish

Table I.
Classification of IT systems security threats

Criterion	Classification of threats	Examples of threats
Role of a man	Threats independent on a man	Atmospheric discharge, flood, fire, humidity etc.
	Threats dependent on a man	Illegal modification of software or data, disclosure or deletion of data, illegal copying and installation of software, damage or deletion of software or data, stealing computer equipment or accessories, storage of resources prohibited by law, mistakes made due to the lack of knowledge, unintentional loss, damage, deletion or disclosure of data to unauthorized persons, etc.
Subject of influence	Threats related to computer systems	Interruptions in electric energy supply, intentional and unintentional human actions (e.g. mechanical damage, configuration errors, incompetent use or maintenance, etc.), unexpected failures of mechanical and electronic elements of computer equipment, etc.
	Threats related to software	Mistakes made by the software manufacturer, mistakes made intentionally or unintentionally by employees or third parties (e.g. incorrect installation, configuration, implementation, deletion or modification of software, introducing malicious programs, blocking correctly functioning applications, illegal access, illegal usage or copying of software, etc.
	Threats related to data	Unauthorized access to data, unauthorized modification of data (e.g. damage, change of content, deletion, etc.), unauthorized copying of data, monitoring (phishing) of data, introducing incorrect data, denying the reception/sending of data, etc.
	Threats related to ICT networks	Intentional or unintentional human actions (e.g. stealing network components, physical damage of a network, wrong configuration, partial or complete blockage of network activity, phishing or unauthorized use of a network, etc.), ICT network failures caused by external factors (e.g. atmospheric discharge, fire, etc.), unexpected damage of electronic elements of a network, etc.
	Threats related to people	Failing to keep business and trade secrets by economic entity personnel (e.g. unintentional release or transfer of data due to the so called ‘social engineering), informing workmates or third parties about security systems used in a company, sudden loss or resignation from work by the personnel as well as a situation, when employees having access to confidential information start working for a competitor.
	Threats causing financial losses	Loss of clients, business partners, decrease in turnover and company share in the market, interruptions in the functioning of a business entity, the necessity to exchange the offered products (especially in case of bank services), loss or damage of technology and software, financial sanctions, increase of insurance premiums, decrease in process efficiency and activities carried out in a company, necessity to hire additional employees, costs of outsourcing, judicial costs, penalty interest for breaching agreements)
Action results	Threats causing intangible damage	Loss of prestige and good name, loss of economic subject credibility in the eyes of clients and business partners (due to e.g. media interest in data safety breach), organizational chaos, loss of IT infrastructure efficiency, incorrect decisions made on the basis of falsified or incomplete data.
	Threats independent on a man	Atmospheric discharge, flood, fire, humidity etc.

Source: [16, p. 160-161]

respondents (and 53% of global respondents) the protection of brand and reputation is the most important aim of organizational safety policy, even more important than ensuring compliance with regulations in this field (60% of respondents in Poland and 56% around the world).

An example of a technology, which is developing very dynamically nowadays, is cloud computing, described in more details in point 3 of this article. The biggest problem for entrepreneurs interested in cloud services is issues related to the loss of data safety. According to the study conducted by Harris Interactive center, as many as 91% of respondents worry about the safety of public clouds, and approximately 50% of them indicate that safety issues are the largest obstacle in popularizing cloud solutions. Eelastic-security.com portal also decided to analyze this topic and surveyed suppliers of such services. The aim of the study was to check, how suppliers and cloud users perceive safety issues. The results how divergent the expectations of these groups are. 69% out of 127 surveyed suppliers claimed ensuring safety of cloud services was the sole responsibility of users, who thought the contrary. Most of them said that service providers are responsible for cloud safety or it is the resultant of suppliers' and users' action [13].

Although cloud computing has been known for a few years, it still remains a mysterious technology for most users, and hence it is perceived as highly risky [14]. As Gartner Group analysts confirm in their report entitled 'Safety risk assessment in cloud computing', processing data outside a company is related to a risk, therefore in order to minimize it, only checked solutions have to be applied [15]. Also the study conducted by E&Y explores the topic of cloud computing technology safety. 52% of respondents are concerned about data leakage, and 39% of them worry about the loss of control over information processed in a cloud.

Materialization of the above kinds of risk is one of the greatest threats for organizations using modern technologies. The consequence could be the loss of clients and business partners, decreased turnover and company's market share, the necessity to exchange the offered products.

Tangible damage of an organization may include damage of IT infrastructure, loss of valuable data and hence the necessity to restore it. Another consequence is the inaccessibility of IT systems, which may trigger financial losses, e.g. additional operational costs, loss of profits, claims of business partners, suppliers and clients for not performing services or performing them improperly, increased insurance premiums, claims under civil law resulting from torts, e.g. disclosing personal data, punishments imposed by public institutions, etc.

CONCLUSION

Nowadays, the dominant source of risk for an organization is the fallibility of IT systems, and one of the major sources – the level of data security. The presented studies confirm that new technologies, and with them – new business models/tools – generate new, so far nonexistent, threats, and are a source of new types of risks. Significant changes in the functioning of an organization – which result from ongoing globalization, increasing competition, automation, and in particular – development of IT and virtualization, become the fundament of a new perspective of the risk management process concerning IT security in organizations.

The cloud computing discussed in the paper may dominate IT services market; however, it has several drawbacks. Cloud computing does not remove the need for a sound process [1, p. 17]. As discussed in this paper, it may bring some opportunities, but even if organizations themselves feel "cloud ready" they must anticipate the capacity requirements in the cloud, be aware of new risks and manage IT security in accordance with new operation conditions.

REFERENCES

[1] *Strategies To Improve IT Efficiency In 2010.Using Predictive Analysis To Do More with Less*, April 13, 2010, A Forrester Consulting Thought Leadership Paper Commissioned By TeamQuest, http://www.teamquest.com/pdfs/whitepaper/forrester-it-efficiency-2010.pdf (Access: 18.04.2013).

[2] K. Hauke, M.L. Owoc, *Properties of cloud computing for small and medium sized enterprises*, [In:] Advanced Information Technologies for Management- AITM 2011, editors: J. Korczak, H. Dudycz, M. Dyczkowski, Wroclaw University of Economics Research Papers no 205, ISSN 1899-3192, Wroclaw 2011, p. 123-130.

[3] I. Oshri, J. Kotlarski, L.P. Willcocks, *The handbook of global outsourcing and offshoring*. Second edition, Palgrave Macmillan Ltd. – Houndmills Basingstoke Hampshire (UK) 2011.

[4] *Professional outsourcing*, Issue 7 Winter 2011, www.professionaloutsourcingmagazine.net (Access: 5.10.2012).

[5] L.P. Willcocks, M.C. Lacity, *The new IT outsourcing landscape. From innovation to cloud computing*, Palgrave Macmillan Ltd. – Houndmills Basingstoke Hampshire (UK) 2012

[6] J. Grzywacz J. (ed.) *Information systems security in banking institutions in Poland* (In Polish), Oficyna Wydawnicza SGH in Warsaw, Warsaw 2003, p. 11-13

[7] A. Barczak, T. Sydoruk *Management Information Systems Security* (In Polish), Dom Wydawniczy Bellona, Warsaw 2003, p. 80-82

[8] Online CERT security reports: http://www.cert.pl/raporty

[9] Online Computer Security Institute reports: http://gocsi.com/members/reports

[10] J. Muszynski *New Services, New Threats*, Networld of 15.12.2008, http://www.networld.pl/artykuly/329757/Nowe.uslugi.nowe.zagrozenia.html (Access: 18.09.2010)

[11] *Into the cloud, out of the fog - Ernst & Young's 2011 Global Information Security Survey*, http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011 GISS.pdf (Access: 21.02.2012)

[12] *The level of IT threats is rising in connection with the development of new technologies fog - Ernst & Young's 2010 Global Information Security Survey,* Feb. 2011, http://www.ey.com/PL/en/Newsroom/News-releases/PR11_Raport-GISS-2010 (Access: 24.02.2012)

[13] B. Matuszewska *Security in the cloud* (In Polish), Gazeta.pl 05.10.2011,http://komputerwfirmie.gazeta.pl/itbiznes/1,54790,10412168,Bezpiecznie_w_chmurze.html (Access:01.03.2012)

[14] *Cloud computing – Is It Secure In The Cloud?* (In Polish), 18.10.2011, http://internet-news.com.pl/cloud-computing-bezpiecznie-w-chmurze/ (Access: 10.03.2012)

[15] M. Bienkowski *Seven Threats for Cloud Computing Security* (Polish) http://webhosting.pl/Siedem.zagrozen.bezpieczenstwa.dla.komputerowych.chmur (Access: 29.01.2012)

[16] Nowicki A. Turek T. (ed.) Information Technologies for Economists. Tools. Applications (In Polish), Published by the University of Economics in Wroclaw, Wroclaw 2010, p. 160-161