INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 2(28) · 2013

ISSN 1507-3858

Artur Rot, Małgorzata Sobińska
Wroclaw University of Economics
e-mail: {artur.rot; malgorzata.sobinska}@ue.wroc.pl

IT SECURITY RISKS IN MODERN SOURCING MODELS – CLOUD COMPUTING. AN EXAMPLE

Abstract: Information technologies have been developing nowadays at an amazing speed, affecting the functioning of organizations. Almost all of these organisations are involved in some way in sourcing activities, and each of them develops a sourcing relationship that suits its particular needs. In the article, different kinds of outsourcing models were discussed, which are applied in the contemporary management, with particular emphasis put on cloud computing. Cloud computing has become an omnipresent and an increasingly important technology and new risk areas have appeared. The main aim of this article was 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 emphasize the role of appropriate IT security management.

Keywords: IT management, IT/IS security, IT risks, sourcing models, Cloud Computing.

1. Introduction

Information resources have nowadays a strategic significance and have a key influence on gaining 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 the best IT hardware and software experts, IT systems security etc. One of these new models referring to IT services is cloud computing (CC).

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 a 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' research regularly finds that firms that outsource give away too much of their technical capability. Recently, even the UK Government admitted that it, too, has lost too many skilled people to its outsourcing

partners − a problem that will take many years to fix. 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 [*Professional outsourcing* 2011, p. 10]. This can be especially true when dealing with immature markets, such as cloud services, that seem to be ubiquitous in the IT sphere of organisations.

There are numerous challenges facing organisations that are considering cloud computing.

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

2. Evolution of sourcing models

Oshri, Kotlarsky and Willcocks, who have observed the outsourcing market for 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), near-shore (in a neighbouring country), or in an offshore location [Oshri, Kotlarski, Willcocks 2011, p. 25].

Insourcing means managing the provision of services internally, if needed-through buying in skills that are not available in-house on a temporary basis (for example by staff augmentation).

Domestic outsourcing is contracting with the third party located in the same country as the client organization for the completion of a certain amount of work, for a specified length of time, at a certain cost and at a certain level of service. We can distinguish homesourcing and rural outsourcing that involves sending the work to lower-wage, usually rural, regions within the home country. Offshore or near-shore outsourcing means outsourcing contract with vendors situated in a different country from the client organization. Out-tasking is outsourcing on a small scale. It usually implies the ongoing management of and support for selected packaged applications. Out-tasking is popular with local suppliers, but it can be also provided by offshore vendors. Captive models mean a strategic choice to site organizational activities within a wholly owned subsidiary in another country (there are a few variants of captive model: basic, shared, hybrid and divested). Build-operate-transfer (BOT) models- in such models the client contacts with an offshore or near-shore vendor to do an outsourcing arrangement whereby the vendor will build and operate the service center (e.g. a call center) for an extended period of time. The client keeps the right to take over the operation under certain conditions and certain financial arrangements. 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. Many of the offshoring joint ventures have a BOT component inside the agreement. Shared services 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. A shared services center can be a captive center or outsourced to a third party.

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. There needs to be real clarity about what can and cannot be outsourced [*Professional outsourcing* 2011, p. 11].

3. Attributes of cloud computing model

Internet has changed the computing world in a drastic way. It has travelled from the concept of parallel computing to distributed computing, to grid computing, and recently to cloud computing. 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 the computing needs by one party can be outsourced to another party and when the need arises, 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.

Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. 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 expressed concern about critical issues (such as security) that appear with the widespread implementation of cloud computing. These types of concern 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. A 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.

There are many definitions of cloud computing. In common understanding, cloud computing can be identified with a service over the Internet on a utility basis [Hauke, Owoc 2011, p. 123].

Another definition says that cloud computing is a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet [Nowicki, Ziora 2011, p. 204].

In Hauke's and Owoc's opinion, facilities available via cloud computing are strictly determined by the properties of this technology based on Internet resources

[Hauke, Owoc 2011, p. 125]. One can identify two essential concepts in the "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).

Abstraction means that in cloud computing, details of system implementation are not specified in advance (for example, locations of data storage are unknown and the administration of systems in some way outsourced). Virtualization consists in pooling and sharing the resources of computer systems. Parts of system infrastructure can be provisioned as needed from the available computer infrastructure and resources are scalable in a smart way.

The features presented below can be considered as less or more crucial in different cloud computing types.

Scalability – using CC a user has access to the unlimited resources of the whole computer infrastructure. Therefore, companies do not need to plan additional resources assuming the growth of volume data processing. The available infrastructure can be gradually extended according to the user's requirements.

Security – the most "sensitive" and disputable feature of CC. Theoretically all potential problems should disappear (all necessary tasks are performed by specialized partner). Undoubtedly, problems with database recovery should be served professionally, however, a risk of data loss or data leaking can occur [Hauke, Owoc 2011, p. 126].

Cloud computing solutions are offered by such large organizations as IBM, Microsoft, Amazon, Google and others. They can provide 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 [Willcocks, Lacity 2012, pp. 290-296]:

- weighing up the security and legal risks;
- defining the relationship through contracting;
- the lock-in dilemma;
- managing the cloud.

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

The problem of cloud computing risks will be more widely discussed in the next part of the article.

4. New challenges for IT security management

The existence of a company in cyberspace and the opportunity to communicate with it via electronic media is often a minimum condition for a company to be perceived as a reliable and solid partner. Unfortunately, the development of information technologies, e-commerce and new business models (including various kinds of IT

outsourcing) carries new risks apart from huge benefits. There are new threats, often incomprehensible and underestimated by the company management.

For example, few companies recognize the risk related to the fact that data leave easily the traditional 'company borders' and hence are much more prone to be disclosed. A lack of appropriate attitude towards the risk management process is an easy way to an accident, which may pose a serious threat to the further development and safety of an organization. Nowadays, organizations face a serious challenge of implementing an efficient safety security strategy, one of whose elements should be an appropriately performed risk management process.

The basic premise indicating the emergence of new kinds of risk accompanying the functioning of management IT systems include, e.g. the following facts and circumstances [*Information system*... 2003, pp. 11-13; Barczak, Sydoruk 2003, pp. 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,
- the 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 of the expansion of society's civilization development, which facilitates the development of cybercrime,
- most documents and information which have been dispersed so far, are now 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 may 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 new threats, since it is where you can easily find software for hacking IT systems security measures.

Nowadays, specialized institutions (e.g. CERT, Computer Security Institute, etc.) publish statistical data concerning the probability of occurrence of given kinds

of threats [see: http://www.cert.pl/raporty; http://gocsi.com/members/reports]. According to various statistics, they include intentional or unintentional actions of an organization's staff (negligence, lack of concentration, incompetence) and deliberate actions of dissatisfied or sacked employees.

It is worth discussing here the conclusions derived from the report 2011 TMT Global Security Study, prepared by the consulting 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's IT systems security. Another huge risk for the company's 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 consultants 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 an alarming 22%, only 18% of companies keep records of all suppliers processing the 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 (e.g. hackers) and activities of malicious software are relatively unlikely to happen. When assessing the frequency of the 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.

As can be concluded from the aforementioned research conducted by PwC, nearly half of the European respondents indicate that due to the increasing risk levels, ensuring safety is becoming more and more difficult due to insufficient financial means. Companies seek better ways of decreasing IT costs, optimizing resources and improving efficiency. This is why they decide to implement virtualization solutions, SOA (Service-Oriented) architectures, mobile networks, use cloud computing, which makes an organization face many new, yet unknown problems related to safety [Muszyński 2008].

Table 1. The classification of IT systems security threats

Criterion	Classification of threats	Examples of threats
Role of a man	Threats independent of human error	Atmospheric discharge, flood, fire, humidity etc.
	Threats dependent on human factor	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 so called 'social engineering, conscious transfer of data, etc.), informing workmates or third parties about security systems used in a company, sudden loss or resignation from work by the personnel (e.g. data security administrator, software developer, etc.) as well as a situation, when employees having access to confidential information start working for a competitor.
	Threats causing financial losses	Loss of clients and business partners, decrease in turnover and company share in the market, loss of technology, interruptions in the functioning of a business entity, the necessity to exchange the offered products (especially in the case of bank services), loss or damage of equipment and software, financial sanctions resulting from the binding legal regulations, increase of insurance premiums, decrease in process efficiency (longer customer service duration, longer time of obtaining reports necessary to make a decision, temporary lack of possibility to use IT systems, etc.) and activities carried out in a company (weak results of launched marketing campaign or low efficiency of adopted company strategy etc.), necessity to hire additional employees, costs of outsourcing, judicial costs, penalty interest for breaching agreements, terminating self-employment, etc.)
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, threat to human health or life, incorrect decisions made on the basis of falsified or incomplete data, etc.
	Threats independent of human factor	Atmospheric discharge, flood, fire, humidity etc.

Source: [Dziembek 2006; *Information Technologies*..., pp. 160-161].

5. Threats related to virtualization and cloud computing

Ernst & Young conducted the 'Global Information Security Survey' in 2011 [*Into the cloud, out of the fog*... Ernst & Young 2011]. The study group consisted of 1700 organizations, including the largest and the most dynamic companies from 52 countries, from different activities (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. the identification of the most critical kinds of risk in the field of new IT technologies. As can be concluded from this study, the 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 greater and greater. 46% of organizations also recognize the increasing risk levels related to internal company threats. The Polish results are consistent with the global results as far as the assessment of the key threats is concerned. The study conducted by the company in 2010 [*The level of IT threats*… 2010] revealed that more than 64% of respondents found data safety to be one of the five key risk areas. This results directly from the fact that for 73% of Polish 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). IT systems' safety is nowadays so important for organizations because the consequences of, e.g. information leakage, are first of all related to the loss of reputation and brand weakening (according to 68% of respondents). Survey respondents also recognize threats related to the use of social networking sites by employees. As many as 86% of the surveyed (and 80% of Polish companies) are aware of the threats related to the use of these services, meanwhile 33% of respondents (and 20% of Polish companies) assess it as a significant or very significant problem. The study results indicate that in the light of the development of new technologies and an increase in the threat level, companies all around the world have to redefine their attitude to data safety.

An example of a technology which is developing very dynamically nowadays, is cloud computing, described in more detail in section 3 of this article. It is one of the most rapidly expanding sourcing trends of the recent years. Cloud computing is a phenomenon which will – according to specialists – dominate the IT market in forthcoming years. The number of services performed in the cloud and the number of its users is skyrocketing. The biggest problem for entrepreneurs interested in cloud services is issues related to the loss of data safety. According to the study conducted by the 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. The Eelastic-security.com portal also decided to analyze this topic and surveyed the suppliers of such services. The aim of the study was to check how suppliers and cloud users perceive safety

issues. The results show how divergent the expectations of these groups are. 69% out of the 127 surveyed suppliers claimed ensuring the safety of cloud services was the sole responsibility of users, who for their part thought the contrary. Most of them said that service providers are responsible for cloud safety or it is the result of suppliers' and users' action [Matuszewska 2011].

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 [*Cloud computing – bezpiecznie*... 2011]. 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 [Bieńkowski 2008].

Also the aforementioned study conducted by Ernst&Young 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.

Also Deloitte experts point out threats related to the use of new technologies. Nearly one third of the surveyed organizations indicated cloud computing as the main technological solution which will determine the future of information safety. 60% of the surveyed organizations think that third parties (e.g. organizations which they share information with or entrust it to) are a moderate or huge threat for data protection; nevertheless only 31% of companies verify their safety precautions in this field. According to Deloitte experts, companies should understand that they are more and more dependent on third parties in terms of IT systems safety. If an organization maintains high standards of information safety, then it should expect analogical precautions from external entities and cloud computing providers. According to the aforementioned research conducted by PwC, respondents indicated that the limited options of exacting the application of safety policies with technology providers is the largest risk related to cloud computing.

Nowadays, one of the key kinds of threats is APT (Advanced Persistent Threat), i.e. complex, long-term, wide-ranging and multi-level actions directed against concrete persons or companies. Increased ATP attack threat is also related to the growing popularity of mobile devices and social networking sites. Meanwhile only 37% of organizations all around the world have developed a safety strategy, which defines the rules of using mobile devices, and even fewer companies have a strategy concerning social media.

The materialization of the above kinds of risk is one of the greatest threats for organizations using modern technologies and IT systems. An organization can suffer tangible damage, which is measurable in financial terms, but also intangible, e.g. loss of envisaged profits, loss of reputation, prestige and image, decreased credibility in the eyes of clients and business partners. The consequence could be the loss of clients and business partners, decreased turnover and company's market share and the necessity to exchange the offered products (especially in terms of bank services).

Tangible damage of an organization may include damage of IT infrastructure (equipment, software) and loss of valuable data and hence the necessity to restore it. Another consequence could be the inaccessibility of IT systems, which may trigger financial losses, e.g. additional operational costs of an organization, 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, costs of court proceedings, etc. [Poniewierski 2008].

6. Conclusions

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 the development of IT and virtualization, become the fundament of a new perspective of the risk management process concerning IT systems' safety in organizations.

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. But as more and more information on individuals and companies is placed in the cloud, concerns have been growing about how safe the cloud environment is. Cloud computing provides tremendous benefits to organizations of all sizes. For small and mid-sized businesses, cloud computing allows time-constrained IT teams to operate more efficiently. For large enterprises, the cloud provides the ability to scale up or down to respond quickly to changing market conditions. Businesses of all sizes can leverage the cloud to increase innovation and collaboration. Yet many organizations are hesitant to fully leverage the benefits of the cloud, citing concerns regarding data loss and unauthorized access.

The example of cloud computing discussed in this article may – according to specialists – dominate the IT services market; however, it has several drawbacks. Cloud computing does not remove the need for a sound process [*Strategies To Improve*… 2010, p. 17].

As discussed in this paper, cloud computing 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

Barczak A., Sydoruk T., *Management Information Systems Security* (in Polish), Dom Wydawniczy Bellona, Warsaw 2003, pp. 80-82.

Bieńkowski M., *Seven Threats for Cloud Computing Security* (in Polish), 3.07.2008, http://webhosting.pl/Siedem.zagrozen.bezpieczenstwa.dla.komputerowych.chmur (29.01.2012).

Cloud computing – Is it Secure in the Cloud? (in Polish), 18.10.2011, http://internet-news.com.pl/cloud-computing-bezpiecznie-w-chmurze/ (10.03.2012).

Dziembek D., *Enterprise information systems security risk analysis and assessment* (in Polish), [in:] *Zarządzanie ryzykiem w działalności gospodarczej*, Part I, ed. E. Sitek, WZ PCz, Częstochowa 2006.

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

Into the cloud, out of the fog – Ernst & Young's 2011 Global Information Security Survey, Insights on IT risk Business briefing, Nov. 2011, http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf (21.02.2012).

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

Information Technologies for Economists. Tools. Applications (in Polish), eds. A. Nowicki, T. Turek, Published by the University of Economics in Wrocław, Wrocław 2010, pp. 160-161.

Matuszewska B., *Security in the cloud* (in Polish), Gazeta.pl, 5.10.2011, http://komputerwfirmie.gazeta.pl/itbiznes/1,54790,10412168,Bezpiecznie_w_chmurze.html. (1.03.2012).

Muszyński J., *New Services, New Threats* (in Polish), Networld, 15.12.2008, http://www.networld.pl/artykuly/329757/Nowe.uslugi.nowe.zagrozenia.html (18.09.2010).

Nowicki A., Ziora L., *Application of cloud computing solutions in enterprises. Review of selected foreign practical applications*, [in:] Advanced Information Technologies for Management − AITM 2011, *Information Systems in Business*, ed. J. Korczak, H. Dudycz, M. Dyczkowski, Wroclaw University of Economics Research Papers no 205, ISSN 1899-3192, Wrocław 2011, pp. 203-213.

Online CERT security reports, http://www.cert.pl/raporty.

Online Computer Security Institute reports, http://gocsi.com/members/reports.

Oshri I., Kotlarski J., Willcocks L.P., *The handbook of global outsourcing and offshoring*, second edition, Palgrave Macmillan Ltd., Houndmills Basingstoke Hampshire 2011.

Poniewierski A., *The Method of Assessing The Risks of Information Systems Security for The Insurance Companies* (in Polish), doctoral thesis, Academy of Economics in Poznań, Department of Computer Science and Electronic Economy, Poznań 2008, http://www.wbc.poznan.pl/dlibra/doccontent?id=110102&from=FBC (26.04.2012), p. 22.

Professional outsourcing, issue 7, Winter 2011, www.professionaloutsourcingmagazine.net (5.10.2012).

Sparrow E., *Successful IT Outourcing*, Springer, London 2003.

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 (18.04.2013).

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

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

Young G.O., *Synthetic structure of industrial plastics (Book style with paper title and editor),* [in:] *Plastics*, second edition, vol. 3, ed. J. Peters, McGraw-Hill, New York, 1964, pp. 15-64.

BEZPIECZEŃSTWO IT W NOWOCZESNYCH MODELACH SOURCINGOWYCH NA PRZYKŁADZIE CLOUD COMPUTINGU

Streszczenie: Nowe technologie informacyjne rozwijają się obecnie w zdumiewającym tempie, wpływając znacząco na sposób prowadzenia działalności organizacji. Większość przedsiębiorstw wykorzystuje, przynajmniej w pewnym zakresie, możliwości sourcingu i rozwija współpracę sourcingową, dopasowując ją do swoich potrzeb i możliwości. W artykule omówiono różne typy modeli sourcingowych, które pojawiają się we współczesnej praktyce zarządzania ze szczególnym uwzględnieniem cloud computingu. *Cloud computing,* nabierając coraz większego znaczenia i stając się wszechobecnie stosowanym rozwiązaniem technologicznym, niesie ze sobą nowe formy zagrożeń. Celem głównym artykułu było zaprezentowanie najważniejszych typów ryzyka związanych z wprowadzaniem modeli zarządzania, opartych na najnowszych technologiach IT, takich jak np. przetwarzanie w chmurze, i podkreślenie roli, jaką odgrywa właściwe zarządzanie bezpieczeństwem IT.

Słowa kluczowe: zarządzanie IT, bezpieczeństwo IT, ryzyko IT, modele sourcingowe, *cloud computing.*