Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 1441–1447
DOI: 10.15439/2014F44
ACSIS, Vol. 2

# Information security in IT global sourcing models

Prof. Kazimierz Perechuda
Wroclaw University of Economics
ul. Komandorska 118/120
53-345 Wroclaw, Poland
Email:
kazimierz.perechuda@ue.wroc.pl

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

***Abstract*—In the dynamic environment, organizations are required to build their competitive advantage not only on own resources, but also on resources commissioned from external providers, accessed through various forms of sourcing, including the sourcing of IT services. This paper presents some of the aspects of information security, in the context of the modern implementation of new IT sourcing methods. IT sourcing solutions are presented, as employed by modern companies, together with potential benefits offered. The main focus is put on the determination of the most important risks involved in information sharing in IT sourcing relations, as well as minimization and reduction of such risks, with particular attention to various cloud computing services on offer.**

***Index Terms*—management, IT sourcing models, cloud computing, information security**

## I. Introduction

BUSINESSES are on the lookout for newer and more innovative ways to enhance competitiveness and get ahead of the growth curve. A new generation of advanced technologies – social, mobility, analytics and cloud – have taken the center-stage, promising to transform enterprises and help them do business better. Enterprises that embrace these technologies would be able to seamlessly redesign their business models, strategy, operations and processes to meet the new customer demands.

The business models employed by modern enterprises are increasingly more involved in problems related to the security and protection of information, data, and knowledge, particularly of the classified and undisclosed type.

In a sense, these business models can be viewed as based on knowledge and security. The classified knowledge (technical, technological, design, logistic, etc.) is one of the core competences of large network corporations, such as Renault, Mazda, Opel, Toyota, Deutsche Bank, and others.

The network structure of large corporations, while designed to provide competitive advantage in two areas, namely:

- outsourcing of ancillary functions, support functions, and even primary functions (as in the case of Opel assembly factory in Gliwice),
- centralized investment in R+D and new technologies (patents, inventions, improvements, copyrights),

may also increase the risk of uncontrolled 'leakage' of key undisclosed knowledge (technical, design, technological, financial, trade, etc.) to market competitors. This is a direct result of the increased access to core corporate knowledge offered to cooperating entities.

The most important aspect of this process is the natural outflow of hot knowledge, resulting from transmigration of knowledge agents (managers and long-term employees with unique competences and experience), in both the networked and non-networked systems.

## II. New Global Sourcing Models Of Business

In the modern, 'flat' model of economy, networked enterprises build their competitive advantage through careful selection of sourcing agents. One of the most important criteria for such selection is the perceived level of security with respect to uncontrolled and undesired outflow of data, information, and knowledge from organizations to other entities outside their network structure.

Sadly, this particular criterion is rarely perceived as mission-critical. Companies tend to prioritize the aspect of compatibility between core competences of the potential sourcing partner with key competences and resources of the mother company. The increased asymmetry of key competences between sourcing partners may result in the following trends (Fig. 1):

- departure (short-term contracts, rapid capturing of the partner's know-how),
- unification (strengthening the cooperation, balancing the symmetry of undisclosed knowledge, participation in future projects).

New needs of enterprises result in the emergence of new types of global sourcing models, where sourcing can be defined "as the act through which work is contracted or delegated to an external or internal entity that could be physically located anywhere" ([1], p. 2]. Sourcing can also be defined as a comprehensive organizational strategy for distribution of business processes and other functional areas of the enterprise among cooperating partners. For the purpose of this study, sourcing is defined as a notion of superior level to the notions of outsourcing and insourcing ([2], p.17). The main

978-83-60810-58-3/$25.00 © 2014, IEEE

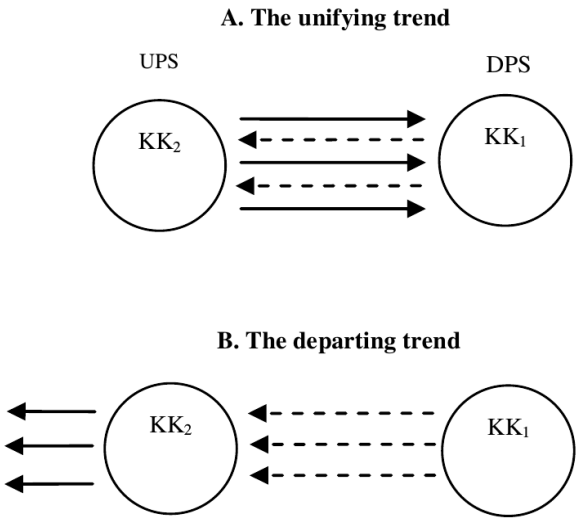


Fig 1. Trends in sourcing cooperation
Source: own research.

differences between sourcing models involve determination of the following factors:

- is the sourced function delegated to a dependent entity or an independent external supplier (or both), and
- is the sourced function performed on-site or off-site, is it performed onshore, nearshore (in a neighboring country) or offshore (in a remote location) ([1], p. 25).

A business model of IT sourcing may comprise the following types/models of sourcing cooperation/relation (own research, based on: [7], pp. 6-16; [1], pp. 26-42; [5], p. 1300; [6]]: facility management, selective outsourcing, tactical outsourcing, transformational outsourcing, transitional outsourcing, Business Process Outsourcing, joint ventures, benefit-based relationships, insourcing (staff augmentation), offshore outsourcing (foreign supplier), nearshore outsourcing (foreign supplier), onshore outsourcing (domestic supplier, "rural sourcing"), cosourcing, shared services, captive models and models based on Internet: cloud computing, software as a service, crowdsourcing and microsourcing. Figure 2 presents a graphic representation of a general model of IT sourcing.

A large number of modern organizations operate simultaneously in two business areas: the real and the virtual. The greater the availability of resources, the greater the potential impact. The more we expand the range of the network (new locations where functions/processes/services of an organization are implemented; greater number of sourcing providers; new areas of service delivery such as cloud computing), the greater the potential opportunities, but also the greater is the risk involved.

A decision to implement a particular sourcing model may be influences by the following factors:

Factors supporting the trends towards IT sourcing (own research, based [7], p.4):

- the global skills shortage,
- a more mobile workforce,
- the mounting cost of in-house developed software,
- the need to move fast, rapidly adopting new technologies and speeding up system development,
- the explosion of Internet technologies and services requiring a wide range of new skills and investments.

For the purpose of this study, the authors focus on the presentation and analysis of one of the most popular Web-based sourcing models – the cloud computing – without going into detailed analysis of other IT sourcing models in use.

Cloud computing allows users to access technology-enabled services on the Web, without having to know or understand the technology infrastructure that supports them. Nor do they have much control over it. It is an innovative new way to boost capacity and add capabilities in computing without spending money on new infrastructure, training new personnel or licensing software.

There are four basic types of clouds: private clouds (operated solely for the use of a single organization), community clouds (operated for a specific group that shares infrastructure), public clouds (which use cloud infrastructure available over a public network) and hybrid clouds (which combine the infrastructure of two or more clouds - public, community, and private).

The increased risk of cloud computing projects has to do with opening up the organization to a whole new space, which is not yet completely examined and "protected". The range of potential risk scenarios is impossible to predict at this moment, since they have yet to be observed in organizational practice. At the same time, the output and the use of the "new space-clouds" can increase the potential added value of using this type of sourcing, compared to more classical forms, such as the generic outsourcing and offshoring models.

New forms of contracting, and – consequently – new resource acquisition methods are required to help modern organizations survive in this age of innovation and strong competition. However, it should be noted that those new solutions, as any new ideas, come with new risks. Some of those risks will be discussed in the following chapters.

## III. Information and knowledge security in the IT sourcing models

Information security is one of the key factors to be taken into account in the context of sourcing decisions, particularly those which involve cooperation with external partners. Potential contractors may operate from remote locations, often

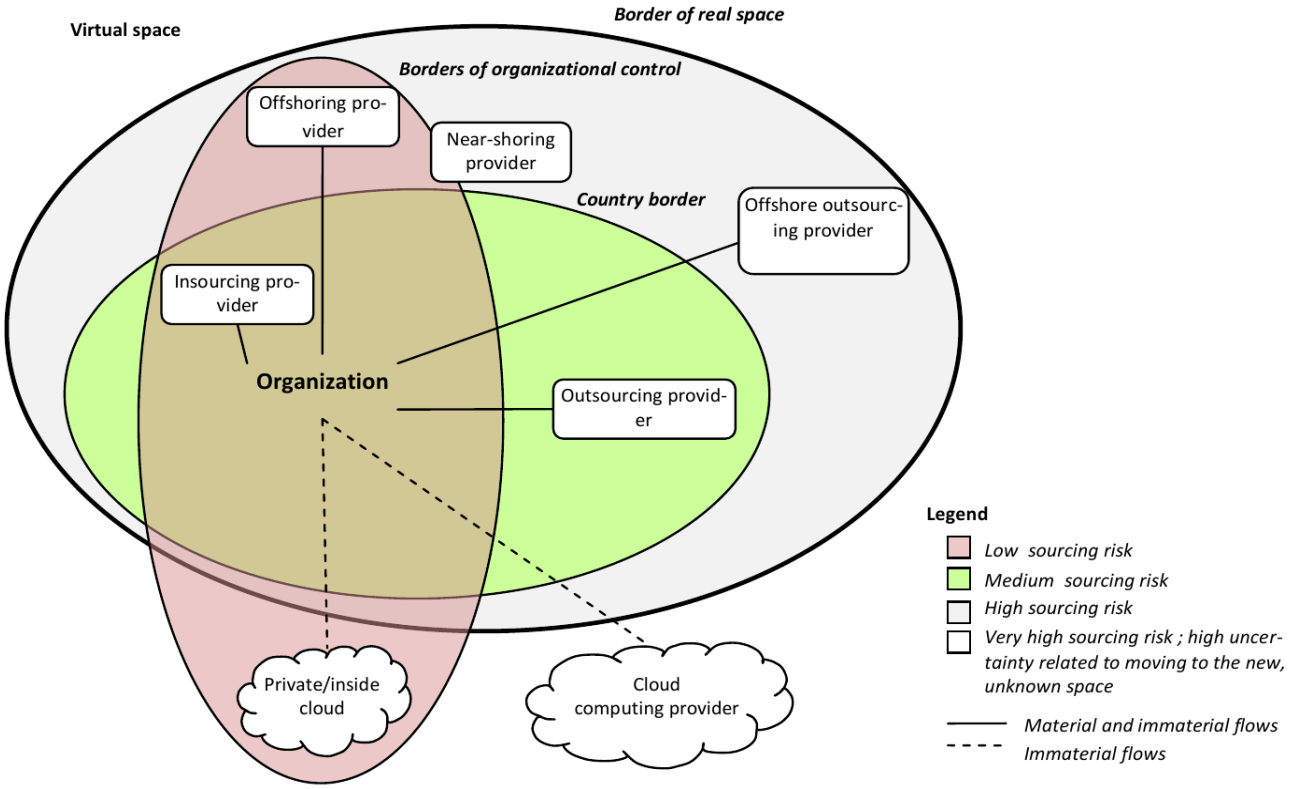


Fig. 2 A general model of IT sourcing
Source: Sobińska 2014

in diverse cultural, political, social, legal, and other settings. The problem of information security is also reported as one of the main concerns for potential cloud computing users and clients.

According to K. Liderman, information security comprises all forms (also verbal) associated with the exchange, storage, and processing of information. It represents the risks involved in information resource loss, as well as misinformation resulting from poor quality of information provided. It must be noted that Liderman makes a clear distinction between information security and 'security of information'. The latter, a subset of information security, is defined as "*justified trust (e.g. based on risk analysis and the adopted risk management procedures) that the organization will not face potential losses as a result of undesired (accidental or intentional) use of information stored, processed, and transmitted within the system, be it information disclosure, modification, removal, or rendering it unfit for processing purposes"* ([4], p. 22). The problem of information security, despite increased publicity in professional literature and media, is still trivialized by managers of many companies. And, while the managerial personnel declare their knowledge of risks involved in this area (as reported in many studies, see: ([11], p.19), in practice they tend to minimize their efforts with respect to information security. The main reasons for negligence are: the financial outlay, and the lack of competences. For instance, not many companies are able to perceive the risk associated with the fact that company information is no longer contained within the 'company perimeter'. Nowadays, information flows freely, and the risk of disclosure is far more pronounced. The lack of informed approach to the risk management process is a fast lane to disaster, since potential incidents may gravely affect the security or company development. *Modern organizations* face the serious challenge of implementing effective security strategies, with proper risk management as one of the main elements of the system [5].

In this context, outsourcing may be seen as a chance to improve information security (and the security of IT systems) by transferring the IT security responsibilities to an external provider with proper specialist knowledge and IT technologies. On the other hand, it may just as well add to the risk, by opening up sensitive company resources to external agents. Those resources may (unwillingly or intentionally) be used to detrimental effects.

Since cloud computing has become a hot topic in IT management, it may be useful to address some of the security issues involved in this form of cooperation. In terms of information security, the main difference between traditional IT structures and cloud solutions is the fact that cloud infrastructure is interspersed and shared among many users. In

addition, certain features of cloud computing, such as the need for continuous optimization, improved access, balancing the computing load across the nodes, etc., bring additional complications to the risk management process.

At present, three main categories of cloud computing solutions can be distinguished, namely: SaaS - Software as a Service, PaaS - Platform as a Service, and IaaS - Infrastructure as a Service. Factors of potential risk to information security include the following ([12], p. 230):

- IT system's resistance to intrusive attacks from outside,
- Resistance to internal attacks (with users able to access and capture information belonging to other users, by exploiting security holes and other vulnerabilities of the system),
- The security verification and encryption methods in use (whether the access codes and passwords are stored in secure, encrypted form, or stored and transmitted in open text).

Each of the above models of cloud computing (SaaS, PaaS, IaaS) employs a specific set of information security solutions ([12], pp.232-233):

- In the SaaS model, users rely on service provider in all matters concerning information security. The provider is responsible for restricting access to sensitive information, as well as supplying proper security measures to prevent intrusion or breakdown. The provider is also responsible for all matters concerning access verification and data encryption. However, the user is rarely able to examine the details of the security measures taken, to make sure that they are up to the desired standard of service.
- In the PaaS model, the service provider may choose to grant the software provider some control over the system security (for instance, the software provider may take on the responsibility of providing their own access verification and encryption systems), but any security issues beyond the application level, such as the security of host machines or network, come under the administration of the service provider. The provider may choose to pass on to the user selected details on the security measures in use.
- In the IaaS model, the software producer has a great deal of control over security mechanisms, since the cloud applications are run on virtual machines, independent and separated from virtual machines used by other users. However, applications in this model take longer to develop, and are decidedly more costly.

The majority of cloud computing service providers offer data backup solutions. This aspect is clearly important from the user's viewpoint, but it must be noted that data backup is not a 100% solution for all security concerns. The SaaS model, in particular, seems the most risky solution in the context of information security. In this model, both the software code and the data being processed are stored remotely (i.e. outside the subscriber's real machine). Consequently, the user has no access to computing operations, and is in no way able to modify it. SaaS offers the potential for server operator to modify the computing software or data processing procedures. Users must upload their data on the server for computing. The result is the spyware effect: the server operator receives user data freely and effortlessly, due to the character of the service rendered, and this gives him the unfair advantage (or even power) over the user. With the IaaS model, on the other hand, it is advisable to refrain from implementing needless functions on virtual machines, as well as making sure that all virtual machine images communicate over encrypted channels, so as to eliminate the risk of data capture on the network infrastructure level.

According to A. Mateos and J. Rosenberg, the security of the cloud computing environment is comparable to that of most internally managed systems, because:

- Most of the potential (and known) risk problems can be eliminated by employing the existing technologies, such as data encryption and virtual local area networks (VLAN), as well as standard tools, such as firewalls and packet filtering (encrypted data stored on cloud may in fact be safer than non-encrypted data used locally);
- Cloud computing solutions may be supplemented by additional controlling and auditing functionality, layered outside the environment of the host. Such a solution offers the user greater security of cloud computing, far better than any locally implemented solution (since the latter require considerable outlay and design expertise);
- Many countries enforce security measures on SaaS service providers, requiring them to restrict transmission of data and other copyright content to the contractor's country of origin ([13], p. 104)

As aptly put by J. Viega, one of the fundamental benefits of a cloud solution is the fact that those structures are fairly unrewarding for willful intruders, since the code – i.e. the most vulnerable element that can be tested for security holes and exploited – is stored on server side, instead of being sent to the client browser ([12], p.230). Data centralization in cloud structures, as opposed to decentralized distribution of data within the company network, allows for vast reduction of leak risk, since users are less inclined to store sensitive resources on their real machines. Furthermore, the access to a centralized resource storage and actual data use can be monitored more closely.

The concern for security of information exchanged in the course of company relations with external service providers, although well-founded, must be examined against any potential benefits offered by this particular type of business model. And the actual informational risk may be largely minimized by employing proper principles of management with respect to relations with external providers – this applies also to knowledge management.

## IV. Ways to Reduce the Risk of Knowledge/Information Loss In It Sourcing Models

K. Liderman believes that information security can be enhanced by employing proper documentation of the security

system in use. This task serves the following purposes ([4], p. 120):

- to ensure proper level of protection with respect to information and to those elements of the system which are directly involved in data processing and storing;
- to track (and control) any changes introduced to the system;
- to satisfy the legal requirements that oblige companies to keep and produce on demand certain documents, such as 'security policy guidelines', 'safety instructions and procedures', etc. (the wording used in actual legal standards may vary).

The use of formal documents (information security policies or guidelines) may attest to the company's intent on keeping proper security standards in data protection. It may also help the organization build and maintain trust relations with customers and/or business partners. Lastly, it may also be used to stimulate the involvement of employees in all tasks and procedures related to data/information security.

With respect to basic technical security measures employed for the purpose of maintaining the informational stability of IT and telecommunication systems, Liderman provides the following classification of elements ([4], p. 158-159):

- data backup procedures;
- provision of independent backup power solutions;
- provision of backup solutions for data processing (or even for running the company business, if necessary), in a reasonably remote location from company HQs;
- doubling the key infrastructure: servers, routers, etc., to serve as backup;
- doubling the information packets;
- providing alternative transmission routes (doubling keys and operators);
- use of verified software offering suitable protection of transmitted and stored data (proper data transmission protocols, software-assisted verification of data integrity based on cryptographic methods, etc.);
- protecting the telecommunication and IT systems from unauthorized access – both physical (access to hardware and technical infrastructure) and logical (access to information resources);
- protection from intentional or accidental exposure to hazards (fire, flooding, strong electromagnetic impulses, etc.).

The most advanced security measures used in cloud computing data centers include (own research, based on [13], pp. 104-114):

- physical security – modern centers are often located in unassuming locations and buildings (often in residential areas), with good security and skillful use of barriers (also natural). Security services cover both the immediate area and the access to actual data facilities, using modern CCTV solutions, intruder alert systems, etc. Servers are kept in fortified bunkers, protected by 5-level biometric scanners (hand geometry recognition), round-the-clock patrols and traps (caging intruders in case of unauthorized entry). Physical security is solely in the hands of the cloud computing service provider, and the above measures are required for certification purposes (the SAS 70 Statement on Auditing Standards No. 70).
- access control in public clouds – these apply to verification of users accessing the cloud. The initial registration of a user is a multi-layered procedure, consisting of several overlapping secret questions and answers (e.g. the user's credit card details). Other levels of security verification may include invoice address, call-back verification over the phone (the *out of band* mechanism, based on employing a different channel of communication), login and authorization (the password should be strong), access keys (a good practice here is to provide regular key substitution service), X.509 certificates, paired keys (the latter being the most important element of user verification when working in cloud environment instances)
- network security and protection of data in large clouds. Passing the task on to the experts employed by the cloud service provider seems the best approach, since it may be reasonably assumed that the provider will be faster to respond to a potential intrusion attempt, and that the response will be adequate to the risk at hand. System security in public cloud models is verified at many levels: at the level of the host's operating system, at the level of the virtual machine's operating environment or the host system, at the stateful firewall, and at the level of signed API calls (the cloud application programming interface), with each subsequent level supplementing the capacities of its immediate precursor.
- The role and the responsibilities of the application owner. Cloud users themselves are responsible for security at the level of their host machine accessing the virtual instance. Since the users have full admin control over their accounts, services, and applications, they are responsible for basic security measures, such as the use of strong passwords, safe storage of passwords and private keys, as well as regular key substitution. Data stored in clouds should also be sufficiently protected – for example, by encrypting the resources prior to uploading them to the cloud, to make sure they cannot be read or modified during transmission and storage.

Modern organizations – both the IT customers and IT service providers – should strive to identify and recognize all processes, services and resources considered mission-critical or of key importance from the information security viewpoint. They should also perform a reliable analysis of information risks, and take suitable measures and procedures to minimize the risk over the course of the cooperation with external partners. Thus, irrespective of the security solutions on offer by the service provider, they should employ their own, independent backup procedures with respect to sensitive data – such backup may be of great value if the company de-

cides to withdraw from the contract (in such cases, the provider may refuse access to data stored in their system) or if the provider goes bankrupt.

Companies unwilling to put their trust in external providers, despite numerous obvious benefits offered by cloud computing solutions, can always reach for other models, such as those based on insourcing or the private cloud model.

The insourcing solution is based on internal management of IT services. If need arises, the company may purchase the lacking skills on the market for a limited time, for example by contracting additional personnel for the task. In this model, the organization retains its internal IT personnel and infrastructure, trusting in its ability to free the latent potential of its employees for the purpose of improving its IT services and making them more effective. From the viewpoint of the insourcing model, the internal IT department is formally perceived as a provider of services.

In the case of private cloud solutions, the decision to adopt this particular business model is made on the basis of four fundamental factors: security, accessibility, the size of user population, and the effect of scale (Table 1).

TABLE 1. PREMISES FOR ADOPTING A PRIVATE CLOUD SOLUTION

| Factor | Description |
|---|---|
| Security | Applications require direct control and data protection, for confidentiality and safety reasons (for instance, governmental agencies use dedicated applications for processing of confidential and classified data – it is essential that they be kept from unauthorized access). |
| Accessibility | Applications require access to a predefined set of processing resources, and this type of access cannot be securely provided in a shared environment. |
| User population | The organization caters for many users, often in geographically remote locations, and they all require unrestricted access to computational processing resources (private clouds are used, for example, in large telecommunication corporation). |
| The effects of scale | Data centers and infrastructural resources are readily available, or can be expanded at minimum cost. |

Source: own research based on ([13], p.116).

Private clouds offer better control and assurance that the resources will not be used by other customers, since they are not shared in public space. However, as any other solution, the private cloud model has its own limitations, such as (own research, based on [13], pp.119-120):

- limited scale of operation, compared to public clouds,
- the problem of adopting old applications to the cloud structure requirements without redesigning the very architecture of the system,
- limited potential for optimization and innovation of the methods and elements of the system,
- larger operational outlay compared to the public cloud solutions.

Even if the organization does not anticipate any integration with external providers when choosing their outsourcing solution, it may be advisable to keep an open stance in this respect, so that it may smoothly transition to another model if need arises, and not be too restricted with their choice of a potential provider.

## V. CONCLUSIONS

New technologies, and the resulting new models and instruments for business, generate new and previously unforeseen risks and threats. Changes in company operating environment, brought about by globalization, increased competition, automation and – most of all – computerization, informatization and virtualization – require a new approach to information security in modern organizations.

As discussed in this paper, new IT sourcing models, especially cloud computing, offer some opportunities, but even if organizations themselves feel "cloud ready," they must anticipate the capacity requirements in the cloud. They must also be aware of new risks, and manage their IT security in accordance with the new operating conditions. The most important risk areas with respect to modern IT sourcing solutions (similarly to those observed in classical outsourcing models) include: the loss of control over the IT environment, inadequate protection of data, overdependence on external suppliers, the loss of potential to switch back to previous (self-contained) IT services, etc. A decision to adopt a particular IT sourcing solution should be based on such factors as: the size of the organization, the scale of operation, risk propensity, the adopted information security policy, the personnel strategy, and the budget.

It seems that migration to a cloud model is a good solution for companies intent on maximizing their profits (cloud computing services are decidedly more cost-effective) while at the same time retaining their high standards of security. What makes the cloud computing particularly attractive for business entities is the fact that they can pass most of the IT system security responsibilities on to the service provider. The providers of cloud computing services, being well aware of the fact that security concerns are the most important factor to restrain companies from choosing the cloud model, make huge investments in security solutions and infrastructure, as a way to emphasize their responsible approach to the security of their clients' resources. Companies which – for a number of reasons – are unable or unwilling to rely on external partners with their data, can reach for other sourcing models, such as the private cloud model or the insourcing model, to improve their IT effectiveness.

## REFERENCES

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

[2] Morgan, J.L., Bravard, R., 2010, *Inteligentny outsourcing. Sztuka skutecznej współpracy*, MT Biznes Sp. z o.o., Polska.

[3] Szpor, G., Wiewiórowski, W. R. (eds.), 2012, *Internet. Prawno – informatyczne problemy sieci, portali i e- usług*, Wydawnictwo C.H. Beck, Warszawa.

[4] Liderman, K., 2012, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa.
[5] Rot, A., Sobińska, M.*, IT Security Threats in Cloud Computing Sourcing Model*, Proceedings of the Federal Conference on Computer Science and Information Systems (2013 Federated Conference on Computer Science and Information Systems (FedCSIS),), pp. 1299 – 1303.
[6] Sobińska, M., *IT management business model - sourcing IT services,* a chapter in *Networking Models in Virtual Enterprises,* K. Perechuda (ed.) – in review (2014)
[7] Sparrow, E., 2003, *Successful IT Outourcing*. Springer, London.
[8] *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- accessed on 18.04.2013.
[9] Szpringer, W., 2008, *Wpływ wirtualizacji przedsiębiorstw na modele e-biznesu. Ujęcie instytucjonalne*, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa.
[10] Willcocks, L.P., Lacity, M.C., 2012, *The new IT outsourcing landscape. From innovation to cloud computing,* Palgrave Macmillan Ltd. – Houndmills Basingstoke Hampshire (UK).
[11] *Firmy lekceważą cyfrowe ataki*, Puls Biznesu, 27 Nov. 2013
[12] Viega J.*, 2010, Mity bezpieczeństwa IT. Czy na pewno nie masz się czego bać?*, Helion.
[13] Mateos , A., Rosenberg, J., 2011, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion, Gliwice.