Abstract - 011- 0373

IP protection in service offshoring: a self-assessment model

Daiana Dus, CASCC, Via Bogino 9, 10123 Torino, Italy
daianadus@libero.it, +39 348 7643665

Guido Nassimbeni, University of Udine, Via delle scienze 208, 33100 Udine, Italy
nassimbeni@uniud.it, +39 320 4366017

Marco Sartor, University of Udine, Via delle Scienze 208, 33100 Udine, Italy
sartor1@uniud.it , +39 328 2198896

POMS 20th Annual Conference
Orlando, Florida U.S.A.
May 1 to May 4, 2009

Abstract

Service offshoring (SO) nowadays represents an increasing phenomenon. There are several motivations that justify the location of (IT or business) processes in developing countries, but there are also several risks to consider.

The protection of intellectual property violations constitutes one of the most relevant issues in SO processes and may strongly affect their success.

The literature so far developed is mostly focused on single aspects (such as the contractual terms or the technical tools for data protection) of the problem, while only few researches consider the whole process in order to capture – beside the legal or technical aspects – also the managerial ones.

In this study we develop a model for the company's self-assessment of data and IP expropriation risks in service offshoring. The study – based on a careful review of the literature and the analysis of some case studies – is aimed at developing a self-assessment model useful to understand the main disruption risks and managerial tools for IP protection along the various steps of the offshoring process.

Introduction

Service outsourcing and offshoring represent increasing practices: companies outsource and delocalize their IT and business processes in order to gain competitive advantages by cutting costs, increasing flexibility, having access to new technologies and skills and focusing on core activities (Embleton & Wright, 1998; Ghodeswar & Vaidyanathan, 2008). There are also risk issues (e.g. loss of control, security issues, poor service quality, vendor dependency, cost escalation) to be considered (Ellram et al, 2008; Frost, 2000). Among these risks data security is thought to be one of the most serious (Khalfan, 2004). Many companies are reluctant to adopt outsourcing and offshoring because of the possible breach of their information assets (Karyda et al., 2006; Razvi Doomun, 2008; Weidenbaum, 2004). Since most of these information are stored, processed and communicated within information systems, each organization must be able to guarantee protection from a continuously increasing set of disruptions (Carey & Berry, 2002; Flowerday & von Solms, 2005).

There are several type of risks as denial of service attacks, hackers, viruses, warms, spyware, employee frauds, unauthorized access to system or networks, accidental or intentional disclosure, modification, loss or theft of intellectual property and natural disasters (Faisal et al., 2007; Andrijcic & Horowitz, 2006; Loch et al.,1992). Some of these can result in short-lived disruptions with immediate cost consequences, instead others can cause longer-lasting consequences with an indirect negative impact on the customer base, supplier partners, financial market, banks and business alliance relationships. Many authors agree in identifying IP loss as the main long-lasting disruption, and IP protection as the most difficult and potentially expensive information security problem (Andrijcic & Horowitz, 2006; Bojanc & Jerman-Blazic; 2008, Fenn et al., 2002; Stephenson, 2005).

Considering all this aspects in our study we first conduct a literature review on service offshoring/outsourcing and data protection topics and then we analyse more in depth the problem of IP protection. Alongside this literature review, we further analyse some firm experiences in the outsourcing/offshoring field, using a database (of the Management Engineering Department of the

University of Udine, Italy), in which are collected 18 case-studies concerning phases and problems of sourcing processes in China and India.

The objective has been to develop a model for a company self-assessment of security risks in service offshoring. The model, that will be further tested through some new case studies, consider the main disruptions and technological and managerial tools for protection among the whole service offshoring process.

The paper is structured as follows. Next section presents the main topics emerged from the review of the literature about service outsourcing/offshoring, data and IP protection. Then we describe the research methodology and the self-assessment model so far develop. The final section points out the conclusions and the future work.

Literature review

We reviewed 219 papers, of which 150 deal with service outsourcing/offshoring, 86 deals with data and IP protection and 17 intersect both of these issues. The analysis was conducted using the major databases (JStore, ISI Web of Knowledge, Science Direct, Emerald, Cilea and Sabra) and selecting other works from the references of the individualized papers.

It follows the review of the two investigated issues: service outsourcing/offshoring and data and IP protection.

Service outsourcing/offshoring

Many authors assess that *offshoring*[1] refers to the delocalization of activities in a foreign country (Bunyaratavej et al., 2008; Ellram et al., 2008; Grote & Täube, 2007; Manning et al., 2008), while outsourcing refers to the contracting with an independent service provider to handle services

[1] Often we find instead of *offshore*, *global* (Bhalla et al., 2008; Chandrasekhar & Jayati, 2006; Gonzalez et al., 2006), *internationa*l (Geishecker, 2008; Kedia & Lahiri, 2007; Schniederjans & Zuckweiler, 2004), *cross-border* (Jahns et al., 2006; Varadarajan, 2008), *overseas* (Aron & Singh, 2005; Burns, 2008; Dossani & Kenney, 2007; Graf & Mudambi, 2005), *far-shoring* (Carmel & Abbott, 2007; Gonzalez et al., 2006).

previously performed within the organization (Boer L. de et al., 2006; Ellram et al., 2008; Franceschini et al., 2003; Rebernik & Bradac, 2006).

Analyzing the relationship between outsourcing and offshoring is possible to find four options: domestic insourcing, domestic outsourcing, offshore insourcing, offshore outsourcing. In *domestic insourcing* the services are directly controlled by the firm or by a subsidiary located in the home market (Jagersma & Gorp, 2007). *Domestic outsourcing* involves contracting with a provider in the same onshore market (Manning et al., 2008). *Offshore insourcing*[2] refers to a practice where the organization source from an owned subsidiary located in a foreign market (Chua & Pan, 2008). *Offshore outsourcing* involves an independent service provider based abroad (Ellram et al., 2008; Manning et al., 2008; Nicholson et al., 2006; Pai & Basu, 2007).

To complete the offshoring scenario, in addition to the four options previously analyzed others alternatives emerges from the literature: *nearshoring*, that describes the process of offshoring in countries situated in the proximity of the local market (Carmel & Abbott, 2007; Ellram et al., 2008; Gonzalez et al., 2006; Lacity et al., 2008) and *rural sourcing* or *homeshoringTM* (Lacity et al., 2008; Metters, 2008) which refers to the practice of offshoring in remote areas of the same country.

Considering services being outsourced/offshored it is possible to discern among *Information Technology Outsourcing* (ITO), *Business Process Outsourcing* (BPO) e *Knowledge Process Outsourcing* (KPO). ITO is the externalization of processes associated to the technological infrastructure of the client firm (Bhalla et al., 2008; Ghodeswar & Vaidyanathan, 2008) (i.e. software development, web development, help desk). BPO refers to the partial or total outsourcing of support activities (Sen & Shiel, 2006) (i.e. F&A, HR). KPO services involves high complexity processes characterized by higher knowledge intensity and judgement-based (i.e. medical diagnostics, IP research, policy administration) (Currie et al., 2008; Sen & Shiel, 2006).

[2] Several authors (Bunyaratavej et al., 2008; Elango , 2008; Jahns et al., 2006; Kedia & Lahiri, 2007) use the terms *captive offshoring* and *captive shared services* like synonyms.

Some authors denote that companies usually start with the outsourcing/offshoring of IT functions and continue, if the previous operations are successful, with the outsourcing/offshoring of more complex processes, such as F&A (Dossani & Kenney, 2007; Frost, 2000; Lewin & Peeters, 2006).

Estimates on the ITO market size indicate that this will reach about $200-250 billion by 2007 while BPO and KPO will reach respectively $350 billion and $16-25 billion by 2010 (Budhwar et al., 2006; Currie et al., 2008; Lacity et al., 2008).

Outsourcing/offshoring presents both potential benefits and potential risks. It is possible to classify the *determinants* through four dimensions: strategic, organizational, operational and economic. Main strategic reasons consist in focusing on core business, strategic flexibility, increase competitiveness and access to new markets. Organizational reasons include reduction of internal complexity and the management of a well defined cost center. Access to skills/ knowledge and lead-technologies and improving quality are the main operational reasons cited, while reducing operating costs, capital investments and cash infusion fall into economic motivations (Belcourt M., 2006; Bounfour, 1999; Bunyaratavej et al., 2008; Embleton & Wright, 1998; Ghodeswar & Vaidyanathan, 2008; Gonzalez et al., 2006; Kedia & Mukherjee, 2008; Lau K. H. & Zhang J., 2006).

The achievement of the potential benefits previously mentioned is not always immediate and simple because of several obstacles/barriers that affects (especially) offshoring projects. Among these, linguistic and cultural differences in the host country often prevent a good client-vendor interaction through communication mismatches and mutual needs misunderstandings. Geographical distance can instead be considered as both an obstacle (especially during problem solving in which immediate feedback is essential) and a determinant (to ensure a 24/7 customer support). Moreover, infrastructure availability/quality and cost can represent a challenge as the service outsourcing/offshoring focuses on IT services and/or IT-enabled services. Finally, political instability and laws in the host country can cause problems of business security and contract enforcement (Graf & Mudambi, 2005; Nicholson et al., 2006; Schniederjans & Zuckweiler, 2004; Stringfellow et al., 2008).

Obstacles/barriers are not the only issues companies handle in outsourcing/offshoring: usually they also have to deal with several risks that can strongly affect the success of the project. The most common in the literature are loss of control, poor service quality, opportunistic behavior by the vendor, loss of in-house expertise, cost escalation, vendor dependency, service provider's lack of necessary capabilities and, especially in the offshoring, turnover in the host country and loss of IP and confidentiality (Bounfour, 1999; Ellram et al., 2008; Embleton & Wright, 1998; Gonzalez et al., 2006; Rebernik & Bradac, 2006). These last two will be the risks on which we will focus in the following section.

Data and IP protection

Information security (IS) is "the process of controlling and securing information from inadvertent or malicious changes and deletions or unauthorized disclosure"(Gerber et al., 2001). It concerns mainly the attainment and preservation of the following attributes:

- confidentiality to assure that private or confidential information are not disclosed to unauthorised or unwanted individuals (Tickle, 2002; Khalfan, 2004).
- integrity to guarantee that data has not been maliciously altered (Tickle, 2002; Khalfan, 2004).
- availability to assure that authorized users have access to information when and where they need it (Tickle, 2002; Khalfan, 2004).

In order to protect data, different information security management (ISM) practices have been proposed and developed by both researchers and practitioners (Ma et al., 2008).

A common practice is the risk management assessment. Information security risk management involves the analysis of risks to which the company is subjected, the assessment of the consequent business losses and the identification of actions to mitigate the risk to an acceptable level (Bojanc & Jerman-Blazic, 2008; Flowerday & von Solms, 2005).

These actions include the implementation of both technical (e.g. physical protection of people and systems, encryption techniques, digital signature, password, firewall, antivirus, system back-up) and

organizational (e.g. security policy, procedures and control, awareness programs for employee) measures.

Most enterprise still attempt to solve security related problems using technical measures alone, and focusing on technical rather than managerial controls (Chang & Yeh, 2006). Similarly much of the literature focuses mainly on technical issues. However, there is a growing tendency to recognize the key role of non-technological tools. The survey's findings of Dlamini et al. (2009); Ma et al., (2008), Hagen et al.(2008), Chang & Yeh, (2006) show that most of today's security challenges are to a greater extent related to human and organisational aspects, rather than pure technical ones.

Information breaches can be caused by software or system failures, or non-technical malfunctions such as administrative problems or human error. The effectiveness of information security can be obtained by implementing both organizational and technical measures (Thomson & von Solms, 1998).

Belsis et al. (2005) argues that "the actual effectiveness of security issues has been seriously questioned, as the volume of security related incidents and consequent financial losses continue to increase in magnitude, as well as in severity". An explanation may be that lot of companies that relay on protection technology doesn't have appropriate organizational practices, such as awareness program for the employees. It is important to train and educate the users in information security issues to reduce human error and to assure they are aware of their responsibilities. Furthermore regular and irregular audits can help in lowering the probability of human theft, fraud or misuse. (Peltier & Edison, 1996; Chang & Yeh, 2006).

The organizational aspects has achieved major importance with the evolution of information security from minor and short lasting breaches to longer lasting risks with a huge impact on the organization (Dlamini et al., 2009). Intellectual property theft is one of that long lasting risks.

Intellectual property (IP) refers to all the creations of human mind, as inventions, literary and artistic works, and symbol, names, images and designs used in commerce, and intellectual property rights (IPRs) aim to protect such creations (Wang, 2004). Copyright gives to an author the right of

dissemination and economic exploitation of its creative work (Spinello, 2007). Patent protection refers to a product or process and gives the right to exploit the invention in a specific period and territory in order to prevent others from making, using or selling that invention without permission. A trademark protects the right to commercial identity. It represents any sign or combination of signs, including personal names, letters, numbers, designs and combinations of colours, capable of distinguishing the good or services of a company from those of others (Doyle, 1995). A trade secret includes information that can be used in the operation of an enterprise to guarantee a real or potential advantage over competitors, so long its secrecy is maintained (Spinello, 2007).

Many countries lack adequate laws to protect data and intellectual property, so security risk increases when a company decide to localize its activities abroad, especially if there is no awareness of the political, economical and legal environment of the selected country (Pai & Basu, 2007). Moreover, when a third party manages a process and the related information are no longer in the hand of the enterprise, security risks increase due to the access to such information by the provider itself, its employee and its possible sub-contractors (Peltier & Edison, 1996).

All the above issues must be correctly addressed in the outsourcing/offshoring contract, that represents one of the most important protection tools against opportunistic behaviour by third parties (Tafti, 2005). Security polices and procedures should be negotiated within the contract in order to assure that IS security objectives will be fulfilled at the vendor site at the same level as it was in the customer's site (Razvi Doomun, 2008; Blackley & Leach, 1996). The ownership of intellectual property rights should be considered, with the distinction between 'foreground rights' (intellectual property developed during the costumer-vendor relationship) and 'background rights' (owned, or able to be accessed independently, by each party) (Binns & Driscoll, 1998; Kennedy & Clark, 2006). These and other (such as non-disclosure agreements, employee contracts, service level agreements etc.) contractual aspects represent the main research line of the literature. However the weak rule of law and the poor institutional environment of many offshore outsourcing destinations,

creates difficulties with the contract enforcement (Kshetri, 2007) and rises the needs of different protection measures.

Many researchers and practitioners therefore analyse and developed the so called 'informal' methods of protection (e.g. creation of a trust relationship with the provider, employee education, lead time advantage over competitors, complementary capabilities).

There are different opinion regarding the relationship between contractual-legal methods and informal measures of protection. Lee (1996) asserts that a tight contract is the only way to guarantee the fulfilment of all the company expectations, instead McGaughey et al. (2000) case-study research shows that the main role of trusting relationship and firm-specific resources and capabilities as protection mechanisms. Most authors sustain that the different protection measures are not mutually exclusive, but have to be used jointly: Amara et al.(2008) and Anton and Yao (2004) suggested that informal protection can be used to reinforce legal methods, especially in countries where legal institutions offer only limited protection; Yang (2005) argues that a contract is more important at the early stage of collaboration, while once a trust collaboration is established the vendor-customer relationship will become more a reciprocal obligation rather than a contractual commitment; according to Faisal et al. (2007) to create an effective risk mitigation policy it is necessary not only to understand the available protection methods, but also the mutual relationships among them.

Despite authors recognize the effectiveness of a combined use of protection methods, most of paper concentrate only on single aspects of the security problem. On one hand some studies analyse the information risks only focusing within the organisational boundaries, without taking account of the implications of collaboration between companies in an international context. On the other hand, although many researcher focus on various outsourcing/offshoring issues, there are only few works that discuss these issues from a security perspective. Furthermore, if only few studies in the literature address the interconnection between the data and IP protection and outsourcing, even less are those that consider interconnection with offshoring. We want to fill this gap building a model that consider the security issues among all the steps of the offshoring process, namely among the

pre-contractual, contractual and post-contractual phases. Furthermore, the model want to have an holistic perspective, assembling all the main protection methods emerged from the literature and the analysed case-studies, and considering both technological and managerial aspects of the security problem.

Objective and methodology

The main research objectives are the followings:

- identify and analyse the major security risks (concerning data, sensible information, intellectual property) that affect an offshoring project of a company that decide to localize some of its activities/processes in a foreign country;
- identify the solutions that can be used to mitigate security risks and assure an adequate protection.

The goal is to construct a model considering each stage of the offshoring process, which generally involves decisions that affect the firm security level and its vulnerability to data and IP infringement.

The method adopted is a case study research since it is most appropriate for exploratory and explanatory research and it provides an in-depth qualitative analysis of individual experiences. We want to conduct several interviews using a semi-structured questionnaire.

The check-list, designed to obtain a comprehensive view of security issues companies experienced in offshoring, is divided in four sections:

1. *General information about the company*. This section will collect data such as legal form, turnover, number of employees, organizational structure, etc..
2. *Strategic planning*. Information collected here will regard the methods to select the activities that can be outsourced (without causing a loss of key competencies for the company) and the relationships between the security level and the choices regarding the entry mode and the selection of the foreign country.

3. *Supplier selection and contracting*. This section will collect information regarding the security aspects to be considered in the selection of parameters to evaluate the supplier and the contractual measures for information and intellectual property protection.
4. *Implementation and monitoring*. Information collected here will consider the risks associated with the transfer of resources and processes, training activities on security aspects, and monitoring methods of the supplier security performances.

We have currently identified and contacted several companies with a multi-year experience in sourcing activities in China and India. The choice of companies operating within these countries is due to the fact that nowadays the centre of service offshoring is represented by the Asian area, with China and India ahead. Moreover India and especially China represent developing countries where various companies have experienced episodes of data and IP infringement.

The research want to focus on the offshoring of IT and business processes services, through the selection of firms operating in different sectors such as managerial consultancy, banking, industrial automation, pharmaceutical, and others. This choice allow us to analyse a wide range of processes to be delocalized in order to derive a general model, independent of the specific offshoring form, that can be adopted by any company that want to delocalize its activities. As a result, there can be some adjustments and specific criticalities, which go beyond this work, and that should then be considered depending on the company type and/or the sector in which it operates.

Moreover, the sample has been chosen to include firms of different sizes in order to obtain a general framework even as regards this aspect and to investigate the possible effects of the size variable on security issues.

Discussion of results

In the following sections we will describe the main aspects of the study so far developed. As the model want to have a general validity, we considered the phases of a typical offshoring process (Monczka et al., 2005):

1. Strategic planning
2. Supplier selection and contracting
3. Implementation and monitoring

Below we will analyse critical security elements and at the end of each section we will draft a checklist that allow to asses the security level of the company considered. We then present a scheme to analyse the causes of IP and data breaches, that will be the starting point to capture the potential risk profile of the offshoring project considered. Our intention is to use the individualized causes within a tool like FMEA (Failure Mode and Effect Analysis), which allow to highlight not only the major risks that affect the project but also the technological and managerial tools to mitigate these risks.

Strategic planning

This phase involves the definition of offshoring goals followed by the analysis of business activities in order to promote standardization and to identify the activities more adapted to be delocalized (Franceschini et al., 2003; Leach & Zergo, 1995). Companies should plan the offshoring process considering all the risks that occurs when one activity or process is entrusted to a foreign provider. The aim of the strategic planning is to identify activities that can be outsourced without causing a loss of key competences for the company, namely activities that are not critical for the establishment and maintenance of the competitive advantage (Aron & Singh, 2005). Therefore a first basic protection method is to separate core and non-core activities in order to maintain internally the control of the core business. Moreover a company should break down activities into basic tasks in order to isolate those more easy to be transferred and with a lower intellectual content (May, 1998).

The strategic planning phase also includes choices concerning the entry mode and the foreign basin. Of course, this choices have a strong impact on the security level: the selection of a provider located in a country geographically and culturally far from the one of the customer-company will determine

greater risks due to different political and legal environment, different social behaviour and rules, different industrial practices, and so on.

It seems important to fully understand which legal instrument a country offer to protect from data and IP infringements and what level of enforcement can be reach through the institutional system (Kennedy & Clark, 2006). Companies are also called to comply with the laws of the home country, since there are often legal and contractual restrictions that prevent the relocation of activities in certain countries (Kshetri, 2007).

The security level a firm want to achieve impact heavily on the entry mode choice. Many authors have investigated this relationship. The surveys findings of Oxley (1999) and Javorcik (2004) shows that firms adopt more hierarchical governance solutions in countries where legal protection is weak. The reason is that the security risks increase with the shift from WOFE (Wholly owned foreign enterprise) to joint venture to contract-based alliances. In fact the control exerted by the company decrease and it is therefore more difficult to protect information and IP rights as they are transferred and created.

With the entry mode decision the company has to evaluate which entry modes the country offers and how to implement an agreement that respects foreign legal system (Kennedy & Clark, 2006).

Another issue is the company experience in offshoring practices. Companies with no experience comes across greater difficulties in defining a set of policies, procedures and measures to ensure the protection of corporate tangible and intangible resources in an international context. It is therefore advisable for these companies to start with the delocalization of simple and standardized activities using short term agreements in order to limit risks while gaining awareness of the new local context (Jandhyala, 2008; Javorcik, 2004).

Table 1. Check list of the Strategic planning phase

Strategic planning
Activity selection
- How the preventive activities/function analysis is conducted? Which are the planned steps?
- How core and no-core activities are distinguished?
- Which characteristics are required for activities to be delocalized?
- Do you usually make a selective or total outsourcing/offshoring for the selected activity/function?
- Which is and which characteristic presents the staff involved at this stage (e.g. is it a cross-functional team; is it a

team dedicated to that project)?
- Once the activity/function is selected, how the separation from the others business activities is performed? Shall the activity be standardized? How?

Entry mode choice
- How the activity complexity affect the entry mode choice?
- If the security risks are higher, the choice move from contract-based alliances towards jont-venture and WOFE? Why?
- How the company experience in the outsourcing/offshoring field affect the choice? Which security risks entail a lack of experience?
- Which security advantages and disadvantages arise from the involvement of an agent?
- Who is involved in the entry mode choice?

Location selection
- In the location choice do you focus more on attainable opportunities or on possible risks? Which importance is given to security issues in the choice?
- How do you look for information about the destination country legal environment (e.g. privacy law, data protection law, IP protection laws)? Who is involved in this task? Do you entrust to a legal advisor?
- Do the destination-country laws and enforcement methods affect the choice? How?
- Are you aware of the legal constrains (about data security) that your country exercise on the delocalization of certain activities? Which are that constrains and how strongly they affect the choice?

Supplier selection and contracting

The supplier selection generally involves the definition of some requirements that the provider shall satisfy, the draft of a list of potential suppliers and the choice of the one that better fulfils the requirements. Usually the assessment criteria and their weights depend on the activity considered. Criteria can include the price, the provider skills, experience and organization, the technical evaluation of the offered service and so on (Kakouris et al., 2006).

However the aspects previously indicated are necessary but not sufficient to address security issues when selecting a provider. According to Razvi Doomun (2008), “information system security is now among the most important factors in selecting an outsourcing partner ahead of financial strength, business stability and reputation”.

Before selecting the supplier, it is important to perform a security risk assessment to determine what are the risk for data and IP that the delocalization choice involves, how these risks can be mitigated and whether the organization wishes to accept the eventual residual risk associated with offshoring (Blackley & Leach, 1996; Broderick, 2001). In particular the company should identify which valuable assets have to be protected, to which risks those assets are subjected and which security objectives must be achieved. The security level required will increased with the asset value (high

for activities involving intellectual property and sensible information) and the likelihood and gravity of risks (Flowerday & von Solms, 2005; Bojanc & Jerman-Blazic, 2008). A company should therefore select the suppliers that can guarantee the requested security level, ensuring some (technical, organizational, legal) protection measures in line with the measures taken in-house before delocalization (Fink, 1994; Blackley & Leach, 1996; Razvi Doomun, 2008).

A clear definition of the security requirements is important not only for the supplier selection but also for the next contracting phase in which companies proceed with the drafting of a detailed agreement. Through a written contract it is possible to formalize the security requirements in order to obtain a tool for the management and control of the relationship: the contract allow to individualize responsibilities and obtain an adequate compensation if information or IP breaches occur (Platz & Temponi, 2007). For that reasons, among other contractual aspects, also security issues must be adequately addressed through some clauses that usually cover responsibility assignment, protection of intellectual property (both 'background' and 'foreground' rights), confidentiality and data protection, mechanism of control of the supplier staff, business recovery, auditing and access to premises and facilities (Blackley & Leach, 1996; Binns & Driscoll, 1998; Fenn et al., 2002; Currie et al., 2008).

Table 2. Check-list of the Supplier selection and Contracting phase

Supplier selection and contracting
Identification of the security requirements
- Did you identify the valuable resources/information (involved in the delocalized activity/function) that have to be protected? How? Who is involved in this task?
- Did you analyse the risks to which this information are subject? Which risk assessment methods are used? Who is involved in this task?
- Usually which are the main risks? Which are the occurrence probabilities and their gravities? Which are the tools to foresee and manage these risks?
- After the risk assessment how the security requirements are formulated? What these requirements involve (e.g. physical, logical, organizational security, business continuity plans)? Who is responsible of this task?
Supplier selection
- Are security requirements used in the supplier selection? Which importance is given to factors such as the pertinence of the supplier information security system, eventual supplier certifications, the supplier membership to trade/professional institution, use of subcontractors, staff turnover, awareness of the client economic-cultural environment, and experience in the offshoring field?
- Are there other security requirements considered in the selection?
- Who is involved in the supplier selection?
- Are there methods to check the requirements asserted by the supplier? Which are these methods?
- If the supplier does not meet exactly the security requirements, are there some measures to support him? Which are these measures?
- Does security risks affect the number of suppliers choice? How?

Contract negotiation

- Do you use standard contracts?
- Do you contract short or medium-long agreements? Why?
- Who is involved in the contract drafting? Do you entrust to consultant or legal experts?
- Does the contract embraced all the following aspects: liabilities, IP protection (of both 'background' and 'foreground' rights, confidentiality and data protection, mechanism of control of the supplier staff, business recovery, auditing and access to premises and facilities?
- Do you include other security clauses?
- Which are the most critical issues to develop/define? Which are the most critical aspects to negotiate?
- Do you use Service Level Agreements also for security issue? How do you define security metrics?
- Which are the penalties/actions taken against the provider if data or IP infringement occurs?
- Is the contract flexibility considered an important aspect? How do you draw up a contract both flexible (to include future changes/evolutions) and exhaustive (to evaluate all possible contingencies)?
- Do you plan contract reviews? Who is involved in this task? How often?
- Which are the exit strategies? Do these strategies regard the transfer of resources/information?

Implementation and monitoring

The security issues here involve the management of risks related to the resources transfer and the contract enforcement (Platz & Temponi, 2007).

More specifically, there will be a transition phase in which the business process and the related infrastructures, data and eventual personnel are transferred to the provider (Kakouris et al., 2006). Companies should plan the transfer with their providers in order to insure that data, information, possible software and hardware and all elements of the transferred infrastructure do not undergo losses, changes and/or damages (Fenn et al., 2002). Moreover the transaction can also involve personnel transfer and/or dismissal with a consequent rise of uncertainty and loss of motivation among the remaining staff (Allen & Chandrashekar, 2000; Embleton & Wright, 1998; Pemble, 2004). These last aspects can influence the personnel turnover that is a factor enabling IP theft (Lu, 2007), so companies should implement personnel management procedures and, as suggest by some authors (Kakabadse & Kakabadse, 2002; Zhu et al., 2001), boost internal communication. Staff management may also involve awareness programs in order to facilitate the transition to the provider and its employee of a culture that recognizes the importance of security issues and to explain how to mange information while preserving their confidentiality (Thomson & von Solms, 1998).

Once the transition phase is over the company has to deal with the management of the ongoing relationship, which can affect the security level as this depends also from the customer ability to

closely monitor the supplier performances and to provide the necessary support if it is needed. Companies may verify the supplier fulfilment of the prescribed (in the contract) measures and may check, at regular intervals, that the provider continue to meet the requirements over time (Pepper, 1996; Sherwood, 1997; Stephenson, 2006). It may happen that the provider no longer satisfy requirements because of the emergence of new technologies and protection methods or because he has changed some of its security measures. (Broderick, 2001)

Finally, another protection method emerged from the study deals with the strengthening of the relationship with the provider over time. This informal measure is highly important as the contract, even though gives some guarantees, can not reduce risks to zero. Moreover, although the contract provides for penalties in case of failure in complying with the requirements, losses of time and resources can be substantial, especially in countries with a weak system of legal enforcement. For that reasons the study has revealed that it is advisable to build a trust based relationship between parties through a sharing of objectives, polices, culture and values. The alignment of this issues shall facilitate resolution of problems and therefore mitigate risks (Faisal et al., 2007; Yang, 2005).

Table 3. Check list of the Implementation and Monitoring

Implementation and monitoring
Management of the transition phase
- How the transition phase is planned? How risks (of data loss, damage and/or alteration) can be minimize during resource/information transfer?
- Who is involved in the transition phase?
- Do you train internal staff involved in the transition, control and provider monitoring? Who deals with the training?
- Do you implement awareness programs for the provider staff (in order to explain how to protect client data and IP)? Who deals with the training? Which security aspects are included in the program?
- Which actions are undertaken if the transition entail some problems?
- How the staff previously employed in the delocalized activity/function is managed? Which is their behaviour (e.g. uncertainty and loss of motivation)? How negative rebounds (as personal turnover) are managed?
Management of the ongoing relationship
- Which are the provider monitoring methods?
- Who is involved in the provider monitoring (e.g. in-house experts in order to maintain competencies on the delocalized activity)?
- Does the control frequency and accuracy decrease with time?
- Are SLA checks performed?
- Is the strengthening of the relationship considered as a protection method?
- Which measure do you use to strengthen the relationship and build trust?
- Which factors do you use to estimate the trust level you can put in the provider (e.g. supplier certifications, reputation, previous experiences)?
- Do you consider more effective (for data and IP protection) contractual-legal methods or informal ones (e.g. creation of a trust relationship)?
- Which are the main tools used to communicate and/or solve arising problems with the provider?
- How do you avoid the loss of in-house expertise related to the delocalized activity/function?

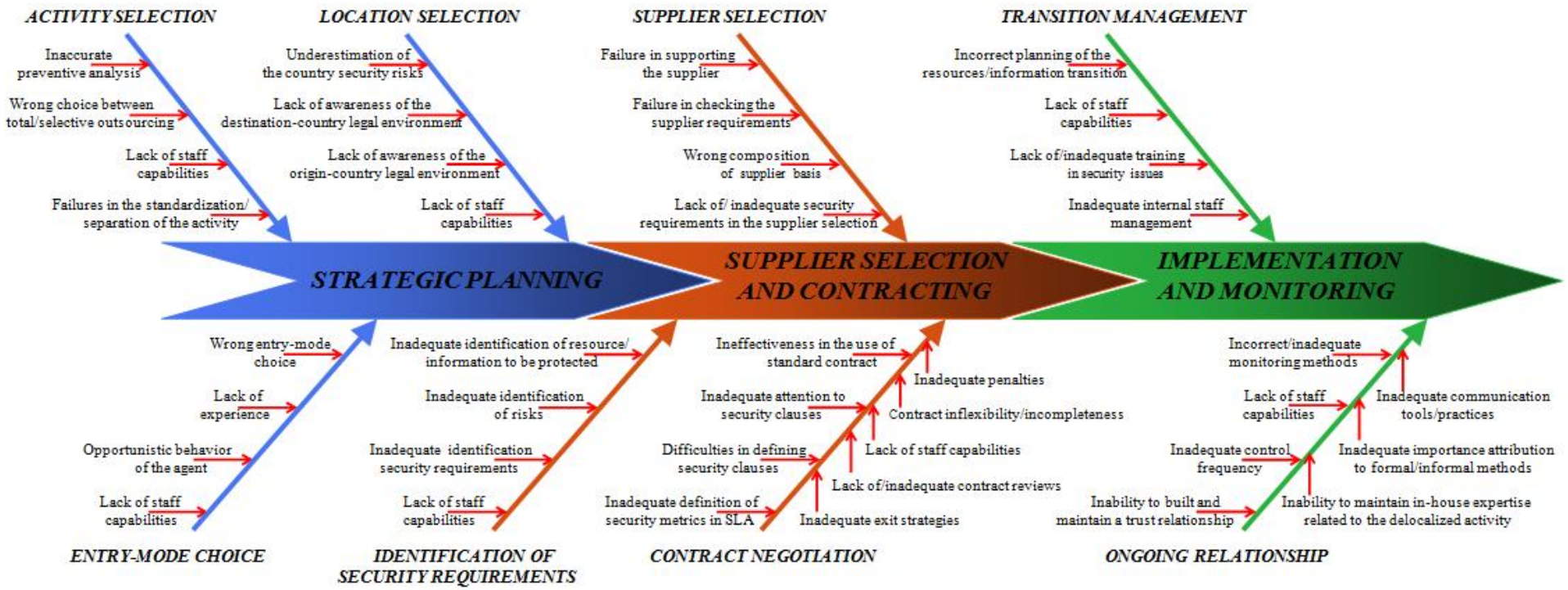

Figure. 1 Causes scheme

Cause scheme

Considering the previous check-lists we propose a scheme (Fig.1) of the causes of data and IP breaches that may affect an offshoring process. The biggest arrows represent the main phases of the process, which can be further divided into sub-phases represented by middle-size arrows. This sub-phases can be affected by some security risks, whose causes are identified by the smallest arrows. As we can note none step, of the process is free of security concerns, so a good level of protection may be achieved successfully planning and managing every stage.

Once risks and causes are identified, it seems necessary to quantify the severity of disruptions in order to build the risks profile of the selected offshoring project and to individualize the best technical or managerial tools to lower these risks. A future research directions will be the creation of a company risks profile: we will analyse the selected firms using a tool like FMEA, calculating risks severity by multiplying the gravity by the occurrence probability.

Conclusions and future work

This article proposes a model for evaluating risks associated with data and IP infringements among the offshoring process and the related tools for managing those risks. The study helps to fill a literature gap: there are only few papers dealing with offshoring according to a security perspective. In addition they usually cover only single aspects (e.g. contractual protection, informal protection methods) of the problem. The study here developed instead aim to analyses data and IP protection among all the steps of the offshoring process, from a company decision to offshore some of its activities/processes to the management of the ongoing relationship with the provider.

The first version of the model, we presented in this article, has been constructed intersecting the literature on service offshoring/outsourcing and on data and IP protection, and analysing a database containing several case-studies of outsourcing/offshoring projects in China and India. The study highlighted, among other things, the main steps of the offshoring process and the related risks including the loss of sensible information and intellectual property violations, which represents

often a big obstacle for companies who want to outsource and/or delocalize certain business functions. The analysis has also suggests some protection measures in order to follow the security best practices.

The model have to be further tested through other case-studies. This step may help to understand the validity of the model and may highlight new issues and/or managerial tools and practices. Companies involved in the study belong to different sectors and are committed in the offshoring of different IT and business processes services. This choice will permit to obtain a general framework.

References

Allen S. & Chandrashekar A. , 2000, "Outsourcing Services: The Contract Is Just the Beginning"; *Business Horizons*, Vol. 43, No. 2, pp. 25-34

Amara N., Landry R., Traorè N., 2008, "Managing the protection of innovations in knowledge-intensive business services"; *Research Policy*, Vol. 37, No. 9, pp. 1530-1547

Andrijcic E., Horowitz B., 2006, "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property "; *Risk Analysis*, Vol. 26, No. 4, pp. 907-923

Anton J.J., Yao D.A., 2004, "Little patents and big secrets: managing intellectual property"; *RAND Journal of Economics*, Vol. 35, No. 1, pp. 1-22

Aron R. & Singh J. V., 2005, "Getting Offshoring Right"; *Harvard Business Review*, Vol. 83, No. 12, pp. 135-143

Belcourt M., 2006, "Outsourcing — The benefits and the risks"; *Human Resource Management Review*, Vol. 16, No. 2, pp. 269-279

Belsis P., Kokolakis S., Kiountouzis E., 2005, "Information system security from a knowledge management perspective"; *Information Management & Computer Security*, Vol. 13, No. 3, pp. 189-202

Bhalla A., Sodhi M. S., Son B., 2008, "Is more IT offshoring better?: An exploratory study of western companies offshoring to South East Asia"; *Journal of Operations Management*, Vol. 26, No. 2, pp. 322-335

Binns R., Driscoll B., 1998, "Intellectual property issues in R&D contracts"; *Pharmaceutical Science & Technology Today*, Vol. 1, No. 3, pp. 95-99

Blackley J. A. & Leach J., 1996, "Security Considerations In Outsourcing IT Services"; *Information Security Technical Report*, Vol. 1, No. 3, pp. 11-17

Boer L. de,Gaytan J., Arroyo P., 2006, “A satisficing model of outsourcing”; Supply Chain Management: An *International Journal*, Vol. 11, No. 5, pp. 444-455

Bojanc R., Jerman-Blazic B., 2008, “An economic modelling approach to information security risk management”; *International Journal of Information Management*, Vol. 28, No. 5, pp. 413-422

Bounfour A., 1999, “Is Outsourcing of Intangibles a Real Source of Competitive Advantage?”; *International Journal of Applied Quality Management*, Vol. 2, No. 2, pp. 127-151

Broderick J.S., 2001, “Information Security Risk Management – When Should It be Managed?”; *Information Security Technical Report*, Vol. 6, No. 3, pp. 12-18

Budhwar P. S., Luthar H. K., Bhatnagar J., 2006, “The Dynamics of HRM Systems in Indian BPO Firms”; Journal of *Labor Research*, Vol. 27, No. 3, pp. 339-360

Bunyaratavej K., Hahn E. D., Doh J. P., 2008, “Multinational investment and host country development: Location efficiencies for services offshoring”; *Journal of World Business*, Vol. 43, No. 2, pp. 227-242

Burns B., 2008, “Offshoring: secure or open to the praying mantis?”, *Strategic Outsourcing: An International Journal*, Vol. 1, No. 1, pp. 77-86

Carey P., Berry D., 2002, “Data security – the key to privacy”; *Computer Law & Security Report*, Vol. 18, No. 2, pp. 112-113

Carmel E. & Abbott P., 2007, “Why 'nearshore' means that distance matters”; *Communications of the ACM*, Vol. 50, No. 10, pp. 40-46

Chandrasekhar C. P. & Jayati G., 2006, “IT-driven offshoring: The exaggerated ‘Development Opportunity’”; *Human Systems Management*, Vol. 25, No. 2, pp. 91-101

Chang A. J.-T., Yeh Q.-J., 2006, “On security preparations against possible IS threats across industries”; *Information Management & Computer Security*, Vol. 14, No. 4, pp. 343-360

Chua A. L. & Pan S. L., 2008, “Knowledge transfer and organizational learning in IS offshore sourcing”; *Omega*, Vol. 36, No. 2, pp. 267-281

Currie W. L., Michell V., Abanishe O., 2008, “Knowledge process outsourcing in financial services: The vendor perspective”; *European Management Journal*, Vol. 26, No. 2, pp. 94-104

Dlamini M.T., Eloff J.H.P., Eloff M.M., 2009, “Information Security: The moving target”; *Computers & Security*, Article in press

Dossani R. & Kenney M., 2007, "The Next Wave of Globalization: Relocating Service Provision to India"; *World Development*, Vol. 35, No. 5, pp. 772-791

Doyle S., 1995, "GATT TRIPS – a USA perspective"; *Computer Law & Security Report*, Vol. 11, No. 4, pp. 182-187

Elango B., 2008, "Using outsourcing for strategic competitiveness in small and medium-sized firms"; *Competitiveness Review: An International Business Journal incorporating Journal of Global Competitiveness*, Vol. 18, No. 4, pp. 322-332

Ellram L. M., Tate W. L., Billington C., 2008, "Offshore outsourcing of professional services: A transaction cost economics perspective"; *Journal of Operations Management*, Vol. 26, No. 2, pp. 148-163

Embleton P.R. & Wright P. C., 1998, "A practical guide to successful outsourcing"; *Empowerment in Organizations*, Vol. 6, No. 3, pp. 94-106

Faisal M.N., Banwet D.K., Shankar R., 2007, "Information risks management in supply chains: an assessment and mitigation framework"; *Journal of Enterprise Information Management*, Vol. 20, No. 6, pp. 677-699

Fenn C., Shooter R., Allan K., 2002, "How safe is your IT security?"; *Computer Law & Security Report*, Vol. 18, No. 2, pp. 109-111

Fink D., 1994, "A Security Framework for Information System Outsourcing"; *Information Management & Computer Security*, Vol. 2, No. 4, pp. 3-8

Flowerday S., von Solms R., 2005, "Real-time information integrity = system integrity + data integrity + continuous assurances"; *Computers & Security*, Vol. 24, No. 8, pp. 604-613

Franceschini F., Galetto M., Pignatelli A., Varetto M., 2003, "Outsourcing: guidelines for a structured approach"; *Benchmarking: An International Journal*, Vol. 10, No. 3, pp. 246-260

Frost C., 2000, "Outsourcing or increasing risks?"; *Balance Sheet*, Vol. 8, No. 2, pp. 34-37

Geishecker I., 2008, "The impact of international outsourcing on individual employment security: A micro-level analysis"; *Labour Economics*, Vol.15, No.3, pp. 291-314

Gerber M., von Solms R., Overbeek P., 2001, "Formalizing information security requirements"; *Information Management & Computer Security*, Vol. 9, No. 1, pp. 32-37

Ghodeswar B. & Vaidyanathan J., 2008, "Business process outsourcing: an approach to gain access to world-class capabilities"; *Business Process Management Journal*, Vol. 14, No. 1, pp. 23-38

Gonzalez R., Gasco J., Llopis J., 2006, "Information systems offshore outsourcing: A descriptive analysis"; *Industrial Management & Data Systems*, Vol. 106, No. 9, pp. 1233-12

Graf M. & Mudambi S. M., 2005, “The outsourcing of IT-enabled business processes: A conceptual model of the location decision”; *Journal of International Management*, Vol. 11, No. 2, pp. 253-268

Grote M. H. & Täube F. A., 2007, “When outsourcing is not an option: International relocation of investment bank research — Or isn't it?”; *Journal of International Management*, Vol. 13, No. 1, pp. 57-77

Hagen J.M., Albrechsten E., Hovden J., 2008, “Implementation and effectiveness of organizational information security measures”; *Information Management & Computer Security*, Vol. 16, No. 4, pp. 377-397

Jagersma P. K. & Gorp D. M. V., 2007, “Redefining the paradigm of global competition: offshoring of service firms”; *Business Strategy Series*, Vol. 8, No. 1, pp. 35-42

Jahns C., Hartmann E., Bals L., 2006, “Offshoring: Dimensions and diffusion of a new business concept”; *Journal of Purchasing and Supply Management*, Vol. 12, No. 4, pp. 218-231

Jandhyala S., 2008, “De facto property right protection and MNC location choices”; *Academy of Management Proceedings*, pp. 1-6

Javorcik B.S., 2004, “The composition of foreign direct investment and protection of intellectual property rights: Evidence from transition economies”; *European Economic Review*, Vol. 48, No. 1, pp. 39-62

Kakabadse N. & Kakabadse A., 2000, “Critical review – Outsourcing: a paradigm shift”; *Journal of Management Development*, Vol. 19, No. 8, pp. 670-728

Kakouris A. P., Polychronopoulos G., Binioris S., 2006, “Outsourcing decisions and the purchasing process: a systems-oriented approach”; *Marketing Intelligence & Planning*, Vol. 24, No. 7, pp. 708-729

Karyda M., Mitrou E., Quirchmayr G., 2006, “A framework for outsourcing IS/IT security services”; *Information Management & Computer Security*, Vol. 14, No. 5, pp. 402-415

Kedia B. L. & Lahiri S., 2007, “International outsourcing of services: A partnership model”; *Journal of International Management*, Vol. 13, No. 1, pp. 22-37

Kedia B. L. & Mukherjee D., 2008, “Understanding offshoring: A research framework based on disintegration, location and externalization advantages”; *Journal of World Business*

Kennedy G., Clark D., 2006, “Outsourcing to China – Risks and benefit”; *Computer Law & Security Report*, Vol. 22, No. 3, pp. 250-253

Khalfan A.M., 2004, “Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors”; *International Journal of Information Management*, Vol. 24, No. 1, pp. 29-42

Kshetri N., 2007, “Institutional factors affecting offshore business process and information technology outsourcing”; *Journal of International Management*, Vol. 13, No. 1, pp. 38-56

Lacity M.C., Willcocks L. P., Rottman J.W., 2008, “Global outsourcing of back office services: lessons, trends, and enduring challenges”; *Strategic Outsourcing: An International Journal*, Vol. 1, No. 1, pp. 13-34

Lau K. H. & Zhang J., 2006, “Drivers and obstacles of outsourcing practices in China”; *International Journal of Physical Distribution & Logistics Management*, Vol. 36, No. 10, pp. 776-792

Leach J. & Zergo C. B., 1995, ”Security Considerations of Network Outsourcing”; *Network Security*, Vol. 1995, No. 11, pp. 10-14

Lee K.O., 1996, “IT outsourcing contracts: practical issues for management”; *Industrial Management & Data Systems*, Vol. 96, No. 1, pp. 15-20

Lewin A. Y. & Peeters C., 2006, “Offshoring Work: Business Hype or the Onset of Fundamental Transformation?”; *Long Range Planning*, Vol. 39, No. 3, pp. 221-239

Loch K.D., Carr H.H., Warkentin M.E., 1992, “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding”; *MIS Quarterl*y, Vol. 16, No. 2, pp. 173-186

Lu L.Y.Y., 2007, “Protecting intellectual property rights”; *Research Technology Management*, Vol. 50, No. 2, pp. 51-56

Ma Q., Johnston A.C., Michael Pearson J., 2008, “Information security management objectives and practices: a parsimonious framework”; *Information Management & Computer Security*, Vol. 16, No. 3, pp. 251-270

Manning S., Massini S., Lewin A. Y., 2008, “A Dynamic Perspective on Next-Generation Offshoring: The Global Sourcing of Science and Engineering Talent”; *Academy of Management Perspectives*, Vol. 22, No. 3, pp. 35-54

May A. S., 1998, “Business process outsourcing: a new test of management competence”; *Career Development International*, Vol. 3, No. 4, pp. 136-141

McGaughey S.L., Liesch P.W., Poulson D., 2000, “An Unconventional Approach to Intellectual Property Protection: The case of an Australian Firm Transferring Shipbuilding Technologies to China”; *Journal of World Business*, Vol. 35, No. 1, pp. 1-20

Metters R., 2008, “A typology of offshoring and outsourcing in electronically transmitted services”; *Journal of Operations Management*, Vol. 26, No. 2, pp. 198-211

Monczka R.M., Carter J.R., Markham W.J., Blascovich J., Slaight T., 2005, “Outsourcing strategically for sustainable competitive advantage”, CAPS/AT Kearney in Nassimbeni G., Sartor M., 2006, “Approvvigionamenti in India. Opportunità e strategie nel paese del Service Offshoring”; Il Sole 24 Ore, Milano

Nicholson B., Jones J., Espenlaub S., 2006, “Transaction costs and control of outsourced accounting: Case evidence from India”; *Management Accounting Research*, Vol. 17, No. 3, pp. 238-258

Oxley J.E., 1999, “Institutional environment and the mechanisms of governance: the impact of intellectual property protection on the structure of inter-firm alliances”; *Journal of Economic Behaviour and Organization*, Vol. 38, No. 3, pp. 283-309

Pai A. K. & Basu S., 2007, “Offshore technology outsourcing: overview of management and legal issues”; *Business Process Management Journal*, Vol. 13, No. 1, pp. 21-46

Peltier T., Edison D., 1996, “The Risk Of Allowing Outside Staff Access To Your Information System”; *Information Security Technical Report*, Vol. 1, No. 3, pp. 18-28

Pemble M., 2004, “Transferring business and support functions: the information security risks of outsourcing and off-shoring: (A beginner's guide to avoiding the abrogation of responsibility)”; *Computer Fraud & Security*, Vol. 2004, No. 12, pp. 5-9

Pepper B., 1996, “Security Service Level Agreements For Outsourced Security Functions”; *Information Security Technical Report*, Vol. 1, No. 3, pp. 48-50

Platz L.A., Temponi C., 2007, “Defining the most desirable outsourcing contract between customer and vendor”; *Management Decision*, Vol. 45, No. 10, pp. 1656-1666

Razvi Doomun M., 2008, “Multi-level information system security in outsourcing domain”; *Business Process Management Journal*, Vol. 14, No. 6, pp. 849-857

Rebernik M & Bradac B., 2006, “Cooperation and opportunistic behaviour in transformational outsourcing”; *Kybernetes*, Vol. 35, No. 7/8, pp. 1005-1013

Schniederjans M.J. & Zuckweiler K. M., 2004, “A quantitative approach to the outsourcing-insourcing decision in an international context”; *Management Decision*, Vol. 42, No. 8, pp. 974-986

Sen F. & Shiel M., 2006, “From business process outsourcing (BPO) to knowledge process outsourcing (KPO): Some issues”; *Human Systems Management*, Vol. 25, No. 2, pp. 145-155

Sherwood J., 1997, “Managing Security for Outsourcing Contracts”; *Computers & Security*, Vol. 16, No. 7, pp. 603-609

Spinello R.A., 2007, “Intellectual property rights”; *Library Hi Tech*, Vol. 25, No. 1, pp. 12-22

Stephenson P., 2005, “Managing Intellectual Property”; *Computer Fraud & Security*, Vol. 2005, No. 4, pp. 14-16

Stephenson P., 2006, “Ensuring consistent security implementation within a distributed and federated environment”; *Computers & Security*, Vol. 2006, No. 11, pp. 12-14

Tafti M.H.A., 2005, “Risks factors associated with offshore IT outsourcing”; *Industrial Management & Data Systems*, Vol. 105, No. 5, pp. 549-560

Thomson M.E., von Solms R., 1998, “Information security awareness:: educating your users effectively”; *Information Management & Computer Security*, Vol. 6, No. 4, pp. 167-173

Tickle I., 2002, “Data Integrity Assurance in a Layered Security Strategy”; *Computer Fraud & Security*, Vol. 2002, No. 10, pp. 9-13

Varadarajan R., 2008, “Outsourcing: Think more expansively”; *Journal of Business Research*

Wang L., 2004, “Intellectual property protection in China”; *The International Information & Library Review*, Vol. 36, No. 3, pp. 253-261

Weidenbaum M., 2005, “Outsourcing: Pros and cons”; *Business Horizons*, Vol. 48, No. 4, pp. 311-315

Yang D., 2005, “Culture matters to multinationals’ intellectual property businesses”; *Journal of World Business*, Vol. 40, No. 3, pp. 281-301

Zhu Z., Hsu K., Lillie J., 2001, “Outsourcing – a strategic move: the process and the ingredients for success”; *Management Decision*, Vol. 39, No. 5, pp. 373-378