Abstract - 015-0344

Security risks in service offshoring/outsourcing: an assessment model based on the Failure Mode and Effect Analysis

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

POMS 21st Annual Conference
Vancouver, Canada
May 7 to May 10, 2010

Introduction

Companies are increasingly urged to rethink their sourcing strategies, choosing between in/out, domestic/international sourcing. Several motivations (e.g. cost reduction, flexibility, access to new technologies and skills, focus on core activities) are encouraging them to outsource and/or localize their (IT or business) processes in foreign countries (Embleton and Wright, 1998; Ghodeswar and Vaidyanathan, 2008). This choices determine also relevant risks, such as loss of control, poor service quality, vendor dependency, cost escalation, and security criticalities (Khalfan, 2004, Hoecht and Trott, 2006, Desouza, 2008). The last problem will be investigated in this work: obviously security issues occur also in domestic insourcing, but our focus is on the analysis of the security implications of outsourcing and/or offshoring choices. In fact the risks of confidential data loss and intellectual property violation increase when business activities are delegated to an external provider and/or delocalized in foreign countries characterized by different social, economic and political contexts (Colwill and Gray, 2007; Pai and Basu, 2007).

The security risks are thought to be very serious as they can strongly affect the success of the entire outsourcing/offshoring project: data or intellectual property breaches can result in long-lasting consequences with an indirect negative impact on the customers, suppliers, financial markets, and

business alliance relationships (Bojanc and Jerman-Blazic, 2008). The problem is wide and mainly involves three dimension: *organizational dimension*, that covers the decisions about which protection policies and procedures have to be implemented and about which safety requirements should be fulfilled by the company itself and its partners and suppliers (in case of outsourcing projects); *legal dimension*, concerning the legislative framework under which the company and its partners and/or suppliers operate; and *technical dimension*, that involves the company IT infrastructure providing IT tools for data protection (Karyda et al., 2006).

The literature so far developed is mostly focused on specific solutions (e.g. contractual terms, technical tools for data protection, etc.) of the security problem, while only few researches consider the combination of organizational, legal and technical protection tools. Moreover researchers often neglect the security implications of outsourcing and offshoring, focusing mainly within the organizational boundaries.

This study – based on a careful review of the literature and the analysis of some case studies (database of the Management Engineering Department of the University of Udine, Italy) – has attempted to develop an assessment framework useful to understand the main risks and tools for data and knowledge protection along the various steps of a offshoring/outsourcing project. The framework has been implemented and tested in a company in the Northwest of Italy, which operates in the iron and steel industry.

The paper is structured as follows. Next section introduces some clarifications about service outsourcing and offshoring, highlighting the various sourcing alternatives available to companies. The following section presents the main considerations emerged from the review of the literature on data and knowledge protection. After having summarized the research objectives and the methodology, the paper presents the assessment framework. The paper closes with some conclusions.

A premise: service outsourcing/offshoring

The literature fails to provide a widely shared definition of o*utsourcing* and *offshoring*: various authors (Monczka et al., 2005; Jagersma and Gorp, 2007; Elango, 2008, Manning et al., 2008) observe that the two terms are often confused and overlapped. Actually there is a clear difference: outsourcing refers to the ownership of productive assets (i.e. it determines the externalization to an independent provider of activities previously performed within the organisation) (De Boer et al., 2006; Ellram et al., 2008; Franceschini et al., 2003; Rebernik and Bradac, 2006), while offshoring[1] exhibits a geographic connotation (i.e. it refers to the localization of activities in a foreign country) (Bunyaratavej et al., 2008; Ellram et al., 2008; Grote and Täube, 2007; Manning et al., 2008).

Using both the asset ownership dimension (outsourcing) and the geographic dimension (offshoring), it is possible to find four options: domestic insourcing, domestic outsourcing, offshore (or international) insourcing, offshore (or international) outsourcing. In *domestic insourcing* the activities are directly controlled by the firm or by a subsidiary located in the home market (Jagersma and 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 and Pan, 2008). *Offshore outsourcing* involves an independent service provider based abroad (Ellram et al., 2008; Manning et al., 2008; Nicholson et al., 2006; Pai and Basu, 2007).

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

---

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

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

Considering instead the activities/processes destined to out and international sourcing it is possible to discern among *Information Technology Outsourcing* (ITO), *Business Process Outsourcing* (BPO) e *Knowledge Process Outsourcing* (KPO). ITO regards the externalization of processes associated to the technological infrastructure of the client firm (Bhalla et al., 2008; Ghodeswar and Vaidyanathan, 2008) (i.e. software development, web development, help desk). BPO refers to the partial or total outsourcing of support activities (Sen and Shiel, 2006) (i.e. Finance and Accounting, HR). KPO services involves highly complex, knowledge intensive and judgment-based processes (e.g. medical diagnostics, policy administration) (Currie et al., 2008; Sen and Shiel, 2006). 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 Finance and Accounting (Dossani and Kenney, 2007; Frost, 2000; Lewin and Peeters, 2006).

Estimates on the ITO, BPO and KPO market size indicate that outsourcing and offshoring nowadays represent an increasing phenomenon (Budhwar et al., 2006; Currie et al., 2008; Lacity et al., 2008).

The literature has also analyzed outsourcing/offshoring determinants and potential risks. Motivations can be classified according to four dimension: strategic, organizational, operational and economic. Main strategic reasons consist in focusing on core business, increasing strategic flexibility and competitiveness and accessing 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 quality improvement are the main operational reasons, while operating costs reduction, capital investments and cash infusion fall into economic motivations (Belcourt M., 2006; Bounfour, 1999; Bunyaratavej et al., 2008; Embleton and Wright, 1998; Ghodeswar and Vaidyanathan, 2008; Gonzalez et al., 2006; Kedia and Mukherjee, 2008; Lau and Zhang, 2006).

There are also potential risks associated to outsourcing choices, to the international location (offshoring), or both. 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 service outsourcing/offshoring focuses on IT services and/or IT-enabled services. Also political instability and laws in the host country can cause problems of business security and contract enforcement (Graf and Mudambi, 2005; Nicholson et al., 2006; Schniederjans and Zuckweiler, 2004; Stringfellow et al., 2008). There are then loss of control, poor service quality, vendor opportunistic behaviors, loss of in-house expertise, cost escalation, vendor dependency, service provider lack of necessary capabilities, loss of confidential data and violation of intellectual property rights (Bounfour, 1999; Ellram et al., 2008; Embleton and Wright, 1998; Gonzalez et al., 2006; Rebernik and Bradac, 2006). These last two risks, cited in the literature also as security risks, will be the focus of next sections.

Literature review : data and knowledge protection

The literature review is based on the examination of journals articles sourced from various electronic databases (JStore, ISI Web of Knowledge, Science Direct, Emerald, Cilea and Sabra), using the follwoing keywords: “Data protection/security”, “Information protection/security” and “knowledge protection/security”. The aim of the analysis was to capture a snapshot of the researches being conducted in the security field.

Many studies have attempted to classify security risks affecting the organisations intellectual capital. According to Loch et al. (1992), Tickle (2002), Posthumus and von Solms (2004) and Faisal et al. (2007) these risks can be broadly divided into two categories. The first includes those risks

that might occur internally (i.e. within the company boundaries), while the second include external risks (i.e. those risks that have the potential to impact an organisation from outside).

Moreover most of the analysed works (Haugen and Selin, 1999; Loch et al., 1992; Hinde, 2003; Posthumus and von Solms, 2004; Chang and Yeh, 2006; Bojanc and Jerman-Blazic, 2008) recognized that both internal and external risks can be further classify in human (i.e. those threats related to human acts) and non-human (i.e. associated with natural phenomena and technical failures), intentional and unintentional.

Among those threats the human (such as theft, loss or destruction of sensible information and intellectual property, unauthorized access to the network service, infection with malicious code, disclosure of someone's personal data and identity theft) are thought to be the most serious (Loch et al., 1992; Fenn et al., 2002; Hinde 2003; Chang and Yeh, 2006; Bojanc and Jerman-Blazic; 2008). The surveys of Loch et al., 1992 and Chang and Yeh, 2006 empirically find out that employee actions are ranked among the top security threats a company could face.

Another issue pointed out in the literature is the growth of external security risks because of the increasing phenomenon of outsourcing/offshoring. In fact as security move from being a 'domestic' issues to one that involves third parties (in some cases located in foreign countries) risks seem to increase: when a third party manages a process (outsourcing) and the related information are no longer in the hand of the enterprise, there is a loss of control while the provider and its possible sub-contractors can have access to sensible data (Peltier and Edison, 1996; Karyda et al., 2006; Hoecht and Trott, 2006; Faisal et al., 2007; Desouza, 2008; Doomun, 2008). Risks are even more relevant when processes are delocalized (offshoring) to offshore locations where the cultural and legal environment is less able to protect foreign investors (Kennedy and Clark, 2006; Colwill and Gray, 2007; Pai and Basu, 2007).

Motivated by the relevance of these issues in the last decades scholars developed and analysed different protection tools and practices to mitigate security risks, both internals and externals. Those tools ca be classified according to three dimensions (Figure 1): technical, legal and managerial.

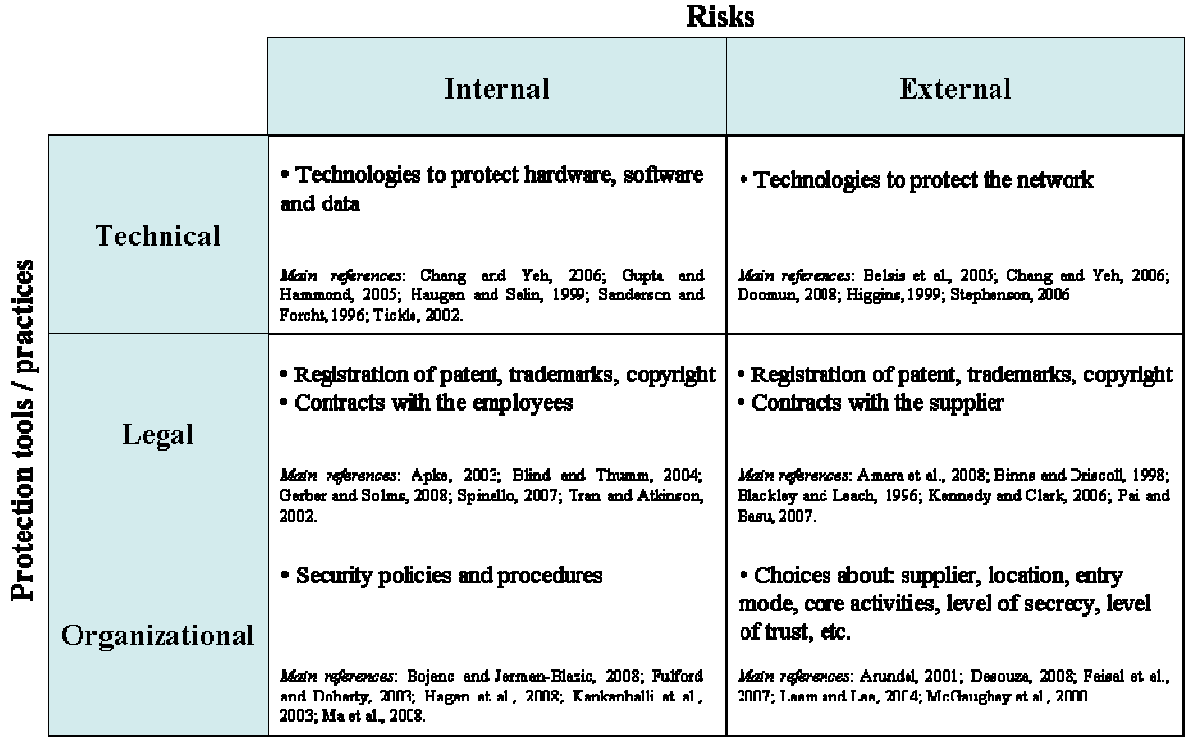

Figure 1 – Literature classification

Technical protection tools includes the (hardware and software) technologies implemented to ensure protection from (intentional or unintentional) attacks to the information system, such as encryption mechanism, authorisation schemes, digital signatures, passwords, firewalls, antivirus.

Moreover studies on legal protection tools have been widely developed. They mainly cover two areas: intellectual property (IP) rights and contracts. The registration of an IP right provides companies with the protection for their innovative knowledge: the holder of an IP right has the ownership over its creation in order to exclusively exploit it for a certain period of time. Contracts helps to protect (through specific clauses) data and knowledge that are shared with employees and eventual other parties (e.g. with a supplier in case of outsourcing).

Of course authors recognize that the protection given by legal tools is strongly influenced by the environment in which a company operates: data and intellectual property violations are more likely to occur in countries (e.g. China) with a weak legal system. For that reason they suggest to reinforce legal method using organizational measures.

Several studies have analysed the development of these organisational tools that involve the creation and implementation of security policies, procedures and controls within a company and the careful planning of eventual outsourcing/offshoring projects. On the latter point the literature suggests that security risks can be mitigated through a targeted selection of the activities (to be externalized or delocalized), of the host country (in case of offshoring), of the supplier (in case of outsourcing), the creation of a trusting relationship with him, its (and its employees) education in security issues, the exploitation of lead time advantages, of complementary capabilities and of the company experience in outsourcing/offshoring practices.

Literature presents, however, some lacks. Firstly, despite various authors (Chang and Yeh, 2006; Faisal et al., 2007; Hagen et al., 2008; Amara et al., 2008) highlight how different tools/practices seems to be more effective if used jointly - most of the papers still concentrates only on single aspects of the security problem. Secondly, a large part of the studies on data and knowledge protection (e.g. Belsis et al., 2005; Hagen et al, 2008) analyse risks focusing only within the organisational boundaries, without considering the implications of the company external collaborations. Finally, although the literature on outsourcing/offshoring is widely developed, there are only few works (e.g. Blackley and Leach,1997; Khalfan, 2004; Doomun, 2008) that discuss these practices from a security perspective.

Our study want to fill these gaps by developing an approach that consider security issues among all the steps of the offshoring/outsourcing process (namely among the pre-contractual, contractual and post-contractual phases) and examining an holistic (managerial, legal and technical) perspective.

Objectives and methodology

The objective of the study is to develop an assessment framework able to:

- identify the security risk profile of companies engaged in outsourcing/offshoring projects, considering jointly technical, legal and managerial aspects.

- detect the causes of possible security failures and the related corrective and preventive actions on the base of the Failure Mode and Effect Analysis (FMEA) method.

The study is aimed at overcoming the current prevailing "narrow approach" to face and measure security problems, involving a project team composed by scholars with managerial, legal and technical (IT security) competencies (belonging to two Italian Universities).

The project steps are two:

1) assessment framework development;
2) assessment framework testing through a pilot-case.

Phase 1 has pointed out the main phases of an offshoring/outsourcing project and the related possible criticalities. To construct the assessment framework we have carefully examined the existing literature on data and knowledge protection and on service offshoring/outsourcing. We have also drawn on a previous work of one of the involved research units. Specifically, this data base includes 18 companies active in various manufacturing and service sectors that have already carried out outsourcing and offshoring projects. The examined experiences, even if heterogeneous, present common criticalities and allow us (through the integration with the literature) to propose a general framework that can be adapted to any outsourcing/offshoring project.

Phase 2 has involved the testing of the model through a pilot-case (interviews have been developed with the persons in charge of the IT systems and the managers who follow the offshoring/outsourcing processes).

The assessment framework

The literature (Handley and Benton, 2008; Lacity et al., 2008) and the experiences we have collected (database of the research group) show that the absence of a planned strategy is often the main cause of companies difficulties in outsourcing/offshoring projects. From a security perspective data and knowledge protection issues could be better addressed if organizations consider them since

the planning phase: the security needs should lead some of the choices that characterized the outsourcing and/or offshoring processes.

According to these considerations, in this section we propose a framework that describes the main security issues that should be addressed during the preparation and implementation of an outsourcing and/or offshoring project.

The framework also intend to have a double value:

- *Ex ante*: anticipating potential risks and identifying corrective actions;
- *Ex post*: going back to the causes when a problem occurs.

The strategic path of the outsourcing/offshoring experiences we have collected and analysed can be organized through the model of Monczka *et al.* (2005), which theorizes the succession of three phases:

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

Starting from this scheme we have analyzed in detail the security criticalities, highlighting the possible causes of data and intellectual property breaches that may affect each phase and sub-phase of the process (Figure 2).

Obviously (as we will clarify) although most of the causes regard both outsourcing and offshoring, there are some implications that interest only outsourcing processes (such as in the choices concerning the supplier selection).

Moreover, beyond the analyzed causes affecting each phase of an outsourcing/offshoring project, there are also some "transverse causes" influencing the whole project, such as the company lack of competences, skills, resources, infrastructures, etc.

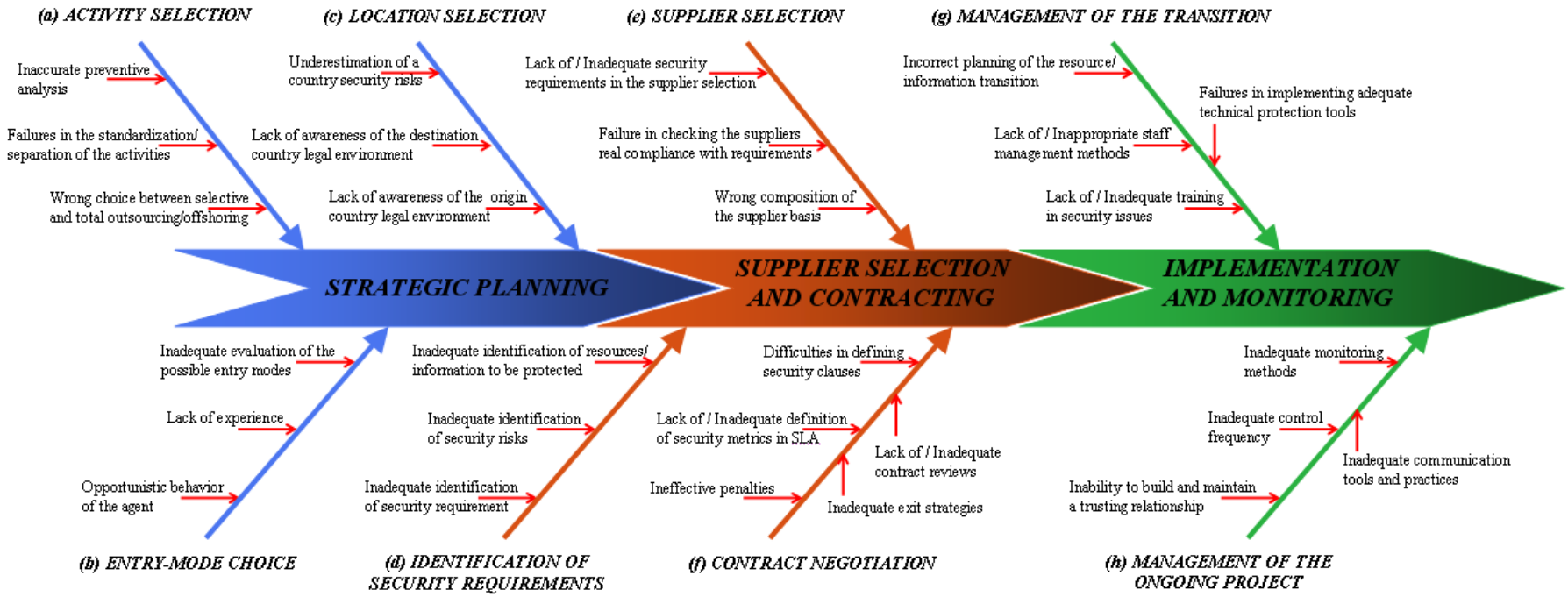

Figure. 2 Possible causes of data and intellectual property breaches

1. Strategic planning

(a) *Activity selection*

This phase involves the definition of the offshoring and/or outsourcing goals and the analysis of the business activities in order to promote standardization and to identify those more adapted to be outsourced and/or delocalized (Franceschini et al., 2003; Leach and Zergo, 1995).

The experiences we gathered, aligned with the literature (Blumberg, 1998; Baden-Fuller et al., 2000; Franceschini et al., 2003; Aron and Singh, 2005), show that one of the main causes of loss of know-how and core competencies is an *inaccurate preventive analysis*. The analysis should in fact support the selection of those activities that are not critical for the competitive advantage. It is important to analyse and redefine business processes (Business Process Reengineering) to reach a thorough knowledge of each activity and its importance compared to the core business. However the distinction core/non-core is often insufficient and it seems necessary to further analyse activities in order to determine their level of outsourcing propensity (i.e. level of tacit knowledge, level of separability, comparison of internal and external performance etc.) and offshoring propensity (i.e. need of proximity between buyer and supplier, need of linguistic competencies, contractual/legal restraints etc.) (Franceschini et al., 2003; Bahli and Rivard, 2005; Nicholson et al., 2006; Grote and Täube, 2007; Youngdahl and Ramaswamy, 2008; Lacity et al., 2008; Stratman, 2008). In fact not all the candidate activities are suitable for outsourcing and/or offshoring since they can be complicated or difficult to separate from other activities or require a continuous managerial control and so on. *Failures in the standardization/separation of the activities* can therefore be another cause of potential security problems: the literature (May, 1998; Bounfour, 1999; Gonzalez e al., 2005) shows that it is useful to break down activities into basic tasks in order to isolate those more easy to be transferred.

Another problem emerged is in fact the *wrong choice between selective and total outsourcing/offshoring*. This choice requires a careful evaluation of advantages and disadvantages

of the two alternatives: on one hand the use of total outsourcing/offshoring can create difficulties in maintaining the necessary know-how on the transferred function; on the other hand selective outsourcing/offshoring require to further breakdown activities in sub-tasks leading to the previous cited problems of standardization and separation from other functions (Cullen e al., 2005; Gonzalez e al., 2005; Tafti, 2005).

(b) *Entry mode choice*

Once activities have been analyzed and selected it is possible to proceed with other choices. The entry mode choice refers to the mode by which the company makes available its offer to a selected country and/or move in that country some of its activities (Bertoli and Valdani; 2006). Basically, the choice range from the maintenance of activities within the company (in-house or in a captive foreign unit) to their externalization in the domestic (domestic outsourcing) or international (offshore outsourcing) market.

The entry mode choice impact heavily on the security level a firm want to achieve and many authors have investigated this relationship. The surveys findings of Oxley (1999) and Javorcik (2004) show 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 decreases and it is more difficult to protect information and IP rights as they are transferred and created. It is therefore clear that an *inadequate evaluation of the possible entry modes* may lead to a risky loss of control. Also the collected experiences show us that core activities or activities that require special skills should not be outsourced and the choice involves entry modes (such as captive offshoring) that can guarantee a higher level of control (and therefore security).

Moreover, closely linked to the loss of control there is a set of criticalities in the management of the entry-mode that can be attributed to a *lack of experience* in outsourcing/offshoring. Companies with no experience come across greater difficulties in defining a set of policies, procedures and measures

to ensure the protection of corporate tangible and intangible resources especially in offshore locations. 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).

A possible alternative is the use of an intermediary (= third party that mediates between the two actors (i.e. supplier and costumer) at the ends of a transaction) that can provide to the costumer company expertise and support in managing the outsourcing process. These benefits has however to be commensurate with risks coming from possible brokerage difficulties and from the impossibility to interact directly with the supplier (Gonzalez e al., 2006; Simmonds e Gibson, 2008): sometimes security violations has been caused by *opportunistic behaviour of the agent*.

(c) *Location choice*

The *underestimation of a country security risks* can increase the vulnerability of a sourcing project: the selection of a host country geographically and culturally far will determine greater risks due to different political and legal environment, different social behaviour and rules, different industrial practices, and so on (Lee, 1996; Belcourt, 2006).

It seems important to fully understand (possibly consulting a legal expert) which legal instruments a country offers to protect from data and intellectual property infringements and what level of enforcement can be reached through the institutional system (Kennedy and Clark, 2006). As highlighted by the analysed experiences and the literature, behind security criticalities encountered in offshore locations there is often a *lack of awareness of the destination country legal environment*.

Moreover also a *lack of awareness of the origin country legal environment* can cause problems: companies are called to comply with the laws of the home country, since there are often legal and contractual restrictions that prevent the relocation of activities (Kshetri, 2007).

2. Supplier selection and contracting:

(d) *Identification of security requirements*

After selecting the entry mode and choosing the destination country it is useful to perform a security risk assessment to determine what are the risk for data and knowledge that the outsourcing and/or offshoring choice may involve, how these risks can be mitigated and whether the organization wishes to accept the eventual residual risk (Blackley and Leach, 1996; Broderick, 2001). In particular the literature (Broderick, 2001; Norman, 2001; Gerber and von Solms, 2008) suggests to identify which valuable assets have to be protected, to which risks those assets are subjected and which security objectives must be achieved. Of course, the security level required will increase with the asset value (higher for activities involving intellectual property and sensible information) and the likelihood and gravity of risks (Flowerday and von Solms, 2005; Bojanc and Jerman-Blazic, 2008). An *inadequate identification of resource/information to be protected*, *of security risks* and *security requirements* can cause a lack of awareness of security issues with the consequent selection of ineffective protection methods (such as ineffective contractual clauses or inadequate security technologies).

(e) *Supplier selection*

This phase obviously intervenes only if the selected activities are transferred to an independent supplier, that is when an outsourcing choice has taken place.

The supplier selection generally involves the definition of some requirements that he 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 considered activity. Criteria can include the price, the provider skills, experience and organization, the technical evaluation of the offered service and so on (Antonucci et al., 1998; Belcourt, 2006; Blumberg, 1998; Pai and Basu, 2007; Razzaque and Sheng, 1998; Rebernik and Bradac, 2006). However these aspects are necessary but not sufficient to address security issues when selecting a provider: a *lack*

of/inadequate security requirements in the supplier selection can affect heavily the protection level of the outsourcing project.

According to 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". The literature points out that in selecting a supplier that can guarantee the requested security level some particularly appreciated characteristics are: the alignment with the client protection measures (Fink, 1994; Blackley and Leach, 1996; Doomun, 2008), the security certifications (Embleton and Wright, 1998; Razzaque and Sheng, 1998; Wright, 2005), the membership in trade and professional associations, the previous experience (Fenn et al., 2002; Pai and Basu, 2007), and the no use of subcontracting (Pai and Basu, 2007).

Moreover problems can occur because of *failures in checking the suppliers real compliance with requirements*, since often they don't provide entirely truthful information.

Considering now the number of suppliers, a *wrong composition of the supplier basis* can increase security risks. Some studies (Cullen e al., 2005; Franceschini e al., 2003) have confirmed that using only one supplier is more risky than using multiple suppliers especially when assets are very specific. The multi-sourcing allows to distribute various tasks among different suppliers in order not to reveal the underlying know-how. However, the multi-sourcing creates also higher transaction costs as well as problems in the management and coordination of the relationships. Some authors (Franceschini et al., 2003; Lacity et al., 2008) argues that it is enough to maintain at least two providers in order to ensure a simple management and, at the same time, reduce security risks.

(f) *Contract negotiation*

The next step involves the contract drafting which provides the formalization of the security requirements previously settled. The contractual instrument is used to regulate both the relationships with independent providers (in case of outsourcing) and those with subsidiaries located in foreign countries (in case of captive offshoring). Of course, the legal protection should be

stricter in the first case since (as we have highlighted previously) the level of direct control over the activities will be lower.

Contract is considered the main legal protection tool as it allows to individualize responsibilities and obtain an adequate compensation if information or intellectual property breaches occur (Platz and 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 (or subsidiary) staff, business recovery, auditing and access to premises and facilities (Blackley and Leach, 1996; Binns and Driscoll, 1998; Fenn et al., 2002; Currie et al., 2008). Often *difficulties in defining security clauses* can lead to incomplete contracts as regards the protection from data and intellectual property breaches.

A contractual instrument, commonly cited in the literature (Pepper, 1996; Fenn e al., 2002; Karabulut e al., 2007; Desouza, 2008) is the Service Level Agreement (SLA) which may include, among different quality metrics, also security issues related to the quality of data protection during the transmission and the processing at the provider (or at the subsidiary). The goal is to formulate metrics that are actually representative of the service and its quality (measuring properly the customer expectations and the supplier performance): the *lack of/inadequate definition of security metrics in SLA* may lead to gaps in the identification and achievement of protection requirements.

Another issue regards the determination of penalties to be applied if the contractual terms are not respected. The risk is to formulate *ineffective penalties* not proportional to potential security violations: some factors affecting penalties dimensioning are the provider (or subsidiary) role, the information he can access and the potential losses that a data or IP violation can cause to the company (Peltier e Edison, 1996; Platz e Temponi, 2007; Tafti, 2005).

Moreover the need to review and include in the contract any change over time requires flexibility of the contract itself. The *lack of/inadequate contract reviews* may nullify all efforts to provide

protection as new threats arise constantly and new technologies are gradually made available (Blackley e Leach, 1996; Pai e Basu, 2007).

Finally the analyzed outsourcing experiences show that particular attention should be placed in drafting provisions for the contract termination, whether in advance (e.g if violations or other problems occur) or in the agreed terms (Blackley and Leach, 1996). In fact *inadequate exit strategies* may lead to a loss of sensitive information and know-how when the activities retransfer back to the company or to another provider takes place. Thus the importance of having agreed with the provider appropriate procedures to regulate the retransfer (Allen and Chandrashekar, 2000; Lee, 1996; Platz and Temponi, 2007).

3. Implementation and monitoring

(g) *Management of the transition*

The transition of business process and the related infrastructures, data and eventual personnel interests both outsourcing and offshoring since both practices impact on the organizational structure. The literature, as well as the analyzed experiences, show the importance of planning and managing carefully the transfer (possibly setting up a pilot project). An *incorrect planning of the resources/information transition* may determine losses, changes and/or damages of data, information, possible software and hardware and elements of the transferred infrastructure (Fenn et al., 2002).

Moreover the transaction can also involve personnel transfer and/or dismissal with recognized (Allen and Chandrashekar, 2000; Embleton and Wright, 1998; Pemble, 2004) negative consequences on personnel confidence and motivation. It follows that the *lack of/inappropriate staff management methods* can affect heavily the company turnover, causing a loss of key employees and know-how (Kakabadse and Kakabadse, 2000; Pemble, 2004; Gonzalez et al., 2005b). The literature, rich in publications on this topic (Embleton and Wright, 1998; Allen and Chandrashekar, 2000;

Kakabadse and Kakabadse, 2000; Zhu et al., 2001; Power et al., 2004; Budhwar et al., 2006) primarily suggests the formulation of a communication plan to better prepare the staff for the transition and the implementation of staff retention practices (e.g. team meetings, focus group).

The transition may also involve awareness programs, that are considered by several studies (Spurling, 1995; Thomson and von Solms, 1998; Siponen 2000; Hagen et al., 2008) an essential tool for the mitigation of security risks (especially in offshore destination characterized by a different cultural context). By educating employees on the limitations in the use of data and on the obligations in the protection of intellectual property, it is possible to facilitate the creation of a culture that recognize the importance of security issues (Thomson and von Solms, 1998). Consequently a *lack of/inadequate training in security issues* may determine a lack of awareness facilitating opportunistic behaviours.

During the starting phase of an outsourcing/offshoring project is finally important to implement all the technologies (hardware and software) to ensure protection from (intentional or unintentional) attacks to the information system. In fact the new link with the provider or the subsidiary network can increase security risks. *Failures in implementing adequate technical protection tools* can result in unauthorized accesses to sensitive information stored in the company information system. Several authors (Higgins, 1999; Apke, 2003; Belsis et al., 2005; Gupta and Hammond, 2005; Chang and Yeh, 2006; Doomun, 2008; Ma et al., 2008) suggest the use of tools such as passwords, firewalls, connectivity security technologies, cryptography to ensure that the provider or the subsidiary can only access settled information.

(h) *Management of the ongoing project*

Once the transition phase is over, the company has to deal with the management of the ongoing outsourcing/offshoring project. The costumer company activities involve the suppliers (in case of outsourcing) or the subsidiaries (in case of captive offshoring) monitoring in order to check, at regular intervals, that they continue to meet security requirements over time (Pepper, 1996;

Sherwood, 1997; Stephenson, 2006). It may happen that the providers or the subsidiaries no longer satisfy requirements because of the emergence of new technologies and protection methods or because they have changed some of its security measures (Broderick, 2001). Therefore problems of compliance with security requirements over time can occur because of *inadequate monitoring methods* or *inadequate control frequency*.

Finally, another protection method emerged from the analyzed outsourcing experiences 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 legal enforcement system. For that reasons the study has revealed that the *inability to build and maintain a trusting relationship* and the use of *inadequate communication tools and practices* can increase the company vulnerability hindering problems resolution and risks mitigation (Faisal et al., 2007; Yang, 2005).

Failure Mode and Effect Analysis (FMEA) applied to service security risk management

The consideration presented above have been organized, through the FMEA methodology.

The FMEA approach allows the construction of the outsourcing/offshoring project risk profile. This technique creates a hierarchy of risks through the Risk Priority Number[3] (RPN), as well as highlighting relations between risks, causes, effects and possible corrective actions (Chiarini and Vicenza, 2004). Starting from the causes scheme in Figure 2, we have classify the possible risks, causes, effects and corrective actions for the "strategic planning", the "supplier selection and contracting" and "the implementation and monitoring" phases. (Table 1-2-3).

[3] A numeric assessment of risk assigned to each failure mode obtained quantifying likelihood of occurrence, likelihood of detection, and severity of impact (Chiarini and Vicenza, 2004).

Table 1: FMEA in the "strategic planning" phase

Phase	*Activity*		*Risks*	*Causes*	*Effects*	*Corrective actions*
Strategic planning	(a)	**Activity selection**	Selection of core activities	Inaccurate preventive analysis	Loss of core competencies and security	Form a staff that involves complementary competences and skills for a careful analysis of BPs
			Wrong scomposition of busines processes	Failures in the separation of the activities	Wrong results	Focus on re-engineering activities
			Wrong analalysis of the separability level of the activities	Inaccurate preventive analysis	Loss of core competencies and control on the activity	Analyse in-depth the individual tasks of the selected activity
	(b)	**Entry mode choice**	Wrong entry mode selection	Inadequate evaluation of the possible entry modes	Loss of control over the externalized/delocalized activities	Assess carefully the available sourcing forms
						Form a staff that involves complementary competences and skills
			Difficluties in managing the selected entry mode	Lack of experience	Loss of control over the externalized/delocalized activities	Initially choose short or medium term contracts to gain experience
			Inadvertent sharing of sensitive information with third parties	Opportunistic behaviour of the agent	Possible violations of sensitive data and intellectual property	Assess carefully the agent reliability
	(c)	**Location choice**	Selection of a risky country	Underestimation of the coutry security risks	Increase of the project security risks	Assign the appropriate weight to the security factor
						Form a staff that involves complementary competences and skills, possibly turning also to a legal
			Lack of legal protection in the destination country	Lack of awareness of the destination country legal environment	Increased vulnerability to data and intellectual property violations	Get in-depth information on laws and enforcement methods in the destination country
			Lack of legal protection in the origin country	Lack of awareness of the origin country legal environment	Increased vulnerability to data and intellectual property violations	Check any legal restrictions on the delocalization of the selected activity

The choice of FMEA as the proper method to frame our findings and to create an instrument for the company self-assessment of a ranking of security risks has been dictated by the following reasons:

- it can be used both ex-ante and ex-post
- the disassembling of the outsourcing/offshoring process in phases and sub-phases follows the logic of the FMEA process.

Table 2: FMEA in the "supplier selection and contracting" phase

Phase	*Activity*		*Risks*	*Causes*	*Effects*	*Corrective actions*
Supplier selection and contracting	(d)	**Identification of security requirements**	Unawareness of the resources/information to be protected	Inadequate identification of resources/information to be protected	Selection of inadequate protection tools	Identify carefully the sensitive information involved in the outsourcing/offshoring project
			Unawareness of the security risks of outsourcing/offshoring	Inadequate identification of security risks	Selection of inadequate protection tools	Assess in detail the risks to wich the information previously identified are subjected in case of
			Unawareness of the security requirements of the project	Inadequate identification of security requirements	Selection of inadequate protection tools	Identify carefully the security requirements of the project
						Form a staff that involves complementary competences and skills, possibly including an information system security
	(e)	**Supplier selection**	Selection of a provider that does not provide an adequate protection level	Lack of/Inadequate security requirements in the supplier selection	Inadequate protection of data/resources transferred to the provider	Include security (technical and organizational security requirements) in the selection
			Selection of a provider unable to meet the established security requirements	Failures in checking the suppliers real compliance with requirements	Inadequate protection of data/resources transferred to the provider	Conduct a check of the requirements established by the provider
			Increase in the contractual power and know-how of the suppliers	Wrong composition of the supplier basis	Increase vulnerability/Opportunistic behaviour	Assess the implications on security of a choice of single, dual or multi-sourcing
	(f)	**Contract negotiation**	Inadequate contractual coverage of security issues	Difficulties in defining security clauses	Lack of legal protection	Define carefully the following clauses: responsibility assignment, protection of intellectual property (both 'background' and 'foreground' rights), confidentiality and data protection, mechanism of control of the supplier (or subsidiary) staff, business
						Involve a legal expert/office
				Lack of/Inadequate definition of security	Lack of legal protection	Insert appropiate security metrics in SLA
			Contract not respected	Ineffective penalties	Opportunistic behaviour of third parties	Prepare penalties proportional to risks
			Underestimation of changes over time	Lack of/Inadequate contract reviews	Vulnerability to new threats/Failures in updating the	Prepare periodic review of the contract
			Problems in the activity (data, intellectual property, resources,etc.) retransfer	Inadequate exit strategies	Loss of know-how	Prepare appropiate procedures for the activity re-transfer inside the company or

In the tables for all the combinations of risk-cause three factors (Severity, Detection, Occurrence) should be estimated. The value to be attributed to each obviously depends on the context, industry, firm and kind of outsourcing/offshoring project. Each firm should therefore be able to create its ranking and individualize which risks require a priority intervention. Concerning the intervention point in the tables we suggest some possible corrective actions.

Table 3: FMEA in the "implementation and monitoring" phase

Phase	*Activity*		*Risks*	*Causes*	*Effects*	*Corrective actions*
Implementation and monitoring	(g)	**Management of the transition**	Problems in the activity (data, intellectual property, resources,etc.) transfer	Incorrect planning of the resource/information transition	Data loss, damage and/or change	Set up a detailed transfer plan and possibly launch a pilot
						Form a team that involve both the client and the supplier (or subsidiary) staff
			Morale lowering	Lack of/Inappropriate staff management methods	Increase in the staff turnover (→increased vulnerability)	Prepare suitable staff management methodologies
			Employees unawareness about the security/confidentiality aspects to be preserved when processing data	Lack of/Inadequate training in security issues	Opportunistic behaviour/Inadequate use of data	Plan the staff training on security issues
			Unauthorized accesses to sensitive information stored in the company information system	Failures in implementing adequate technical protection tools	Increased vulnerability to data and intellectual property violations	Use technical protection tools to ensure that the provider or the subsidiary can only access settled information
	(h)	**Management of the ongoing project**	Difficulties in the supplier (or subsidiary) monitoring	Inadequate monitoring methods	Failures in detecting the supplier (or subsidiary) mistakes	Use monitoring tools suitable for the measurement of the parameters to be monitored
						Assign competent employees to the activity control
			Failures in maintaining the security goals over time	Inadequate control frequecy	Vulnerability to new threats/Failures in updating the security systems	Perform the checks as planned in the contract and if necessary perform also
			Lack of cooperation	Inability to build and maintain a trusting relationship	Opportunistic behaviour of third parties	Create and maintain a trusting relationship with the other parties
			Misinterpretations/Misunderstandings	Inadequate communication tools and practices	Divergence between required and provided security goals	Provide accurate and unambiguous information to the other parties/Provide reporting techniques

The proposed model was implemented and tested on an Italian firm, which operates in the iron and steel industry. The managers who follow the outsourcing/offshoring processes and the persons in charge of the IT systems where interviewed through a questionnaire covering each point of the cause scheme (Figure 2). In addition the FMEA table was filled out by the responsibles of five offices. All the documents were then carefully examined to assess the model validity.

1. Strategic planning

Outsourcing/offshoring choices have characterized the company policy over the years involving various business functions (construction, design, software development). As the model points out a very critical phase concerns the activity selection (a): it seems important to conduct a careful analysis and rationalization of processes in order to individualize which activities can be better

transferred. Business process reengineering (BPR) methods are considered necessary to facilitate the process optimization and the distinction between core and non-core.

The company history is characterized by different outsourcing/offshoring projects: a first important externalization action has involved building activities with the aim of maintaining in-house the core business represented primarily by the design. In a second stage also this function has been further analysed and broken up to identify which sub-tasks should be maintained in-house (i.e. activities that contribute to the definition of the main equipment features, such as the dimensioning and the main components identification) and which to possibly delegate externally and/or delocalize (i.e. detailed design).

The same was done for the software development function: after defining a standard architecture on each of the three levels of the company software (namely level 1 – software for the machines monitoring; level 2 – software for the management and control of technological areas; level 3 – software for the coordination of the company activities), a disassembling of the software packages has been made in order to individualize the most technologically advanced packages to maintain in-house and those to externalize or delocalize. The company has therefore developed, within the design and software development functions, a selective choice of activities adapted to be transferred.

Another critical point concerns the entry-mode choice (b): it seems very important to careful analyse advantages and disadvantages of all the possible sourcing forms. The problem was strongly felt by the company that has in fact opted for captive offshoring in order to maintain an easier control and coordination of the transferred activities. Actually the firm has tried to implement some outsourcing projects, but pure outsourcing led to low-value results: the gained experience together with the need of more control have thus led to captive offshoring choices.

Considering now the location choice (c) the main criticism in the examined company seems to be related to the need of knowing in depth the destination country legal environment. As repeatedly stressed in the interview, the environment can strongly affect the success of the entire offshoring

project. Some of the criteria used to choose the destination country are the workforce characteristics (i.e. skills, cultural compatibility,…), the potential access to the local market, the future capacity of the local market, the costs; the security level.

2. Supplier selection and contracting

As we have seen the company has opted for captive offshoring delegating to the controlled units the tasks selected through the strategic planning phase. There are no service outsourcing projects in place: the firm source from independent vendors only the necessary components and then act as a system integrator (i.e. integrating different equipments according to the costumer requirements). So, this case (of service offshoring) doesn't involve point (e) of the scheme (supplier selection).

It appears instead important the analysis and identification of security requirements (d) concerning the delocated activities in order to determine the contractual requirements for the subsidiaries. In fact, although the companies with which the headquarter (HQ) operates are not independent suppliers, but controlled units it is still necessary to maintain the legal protection through the contract negotiation (f): the firm recognizes the contracts main role in formalizing collaborations and determining the obligations of the various parties. Moreover the interview highlights the importance of entrusting to a legal office the negotiation and management of the contract, especially when subsidiaries in foreign countries are involved.

Moreover, in this particular case, it has been highlighted the need of legal protection with the costumer, if he deals with the maintenance activity. The maintainer has in fact a global knowledge on the equipment and can therefore disclose confidential information. In these cases the company uses confidentiality agreements to assure that information on the equipment and the related software is used only inside the considered plant; the transfer of data externally is forbidden.

3. Implementation and monitoring

During the transition phase (g) the company goal is to reproduce in the subsidiaries the HQ *modus operandi* in order to allow an easier and more effective control on the activities execution as well as facilitate a share of values and organizational culture. The interviewed managers believe that such a sharing allow to mitigate security risks, especially in offshore destinations characterized by a culture that don't fully understand the importance of security. The suggested corrective action is an adequate training. According to this the company has in fact invested in the training activities: usually in each subsidiary it is provided the recruitment of 3-4 employees which become the local seniors. This personnel is transferred for a certain time to the HQ where it is trained to make him understand the policies and procedures with which the company operates. After the training period the staff is retransferred to the subsidiaries where it should apply the procedures learned and transmit (possibly through training) the HQ *modus operandi* and culture to local employees. Then the senior staff is also responsible of the monitoring of the activities conducted on the local site.

Finally the model suggests some consideration regarding the technical security tools to protect the firm information system: the risk of unauthorized accesses to sensitive information stored in the company information system is perceived as very critical. The managers explain that the need of information system security has suggested the choice of different technical protection tools. In particular the HQ can relay on two protection levels. Firstly the subsidiary employees can access only the information they need to do their tasks by using addresses and passwords that are renewed periodically. Secondly to gather these information they don't access the HQ information system, but a dedicated server (physically) external. In other words the communication between the HQ and the subsidiaries occurs on an external machine: the sender and the recipient of the communication can access to the dedicated server and exchange the necessary information without entering the central information system. In this way in addition to the protection guaranteed by the access controls tools, it is impossible for the foreign units to access directly the central system. Again the model has suggested a problem that (as confirmed by the interview) is consider particularly sensitive by the company.

Conclusions

In nowadays scenario companies are often led to rethink their sourcing strategies to achieve advantages such as cost reduction, flexibility, access to new technologies, and so on. In doing that, they have to manage some risks; one of them is security. This risk is so relevant that many companies are reluctant to adopt outsourcing and/or offshoring because of the possible breach of their information assets (Karyda et al., 2006; Doomun, 2008).

This work – based on a careful review of the literature and the analysis of some case studies (database of the Management Engineering Department of the University of Udine, Italy) – proposes an assessment model useful to understand the main risks and tools for data and knowledge protection. The study helps to fill a literature gap: there are only few papers dealing with outsourcing/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 analyse data and knowledge protection among all the steps of the outsourcing/offshoring process, combining (managerial, legal and technical) protection tools.

The framework was implemented and tested in a firm operating in the iron and steel industry. In brief, the use of the instrument has been useful for the following reasons:

- It has enabled the person in charge of the service outsourcing/offshoring decisions (together with the management of the firm) to have a better understanding of the security risks affecting each phase and sub-phase of the outsourcing and/or offshoring process;
- It has allowed a self-assessment of the risks perceived as priority with a consequent raise of the awareness about the greater security criticalities that the considered office has to face more carefully;
- The filled table can be examined by the management of the firm to verify that there is no understimation or an inadequate estimation of risks. Moreover if a problem occurs the table can enable to find the causes and identify the responsibilities quickly and easily.

The instrument has some limitations: it depends on the organisational and industrial context; surely there are security criticalities not considered in the model that can be applied to specific contexts. The implementation of the instrument should require time and the involvement of experts of various functions. Another limitation is that the effectiveness of the instrument strongly depends on the motivation of the staff. In filling the FMEA table there is a strong subjective component due to the fact that it is the company team who assigns the values to the parameters of severity, occurrence and detection.

However, the case study has demonstrated the instrument usefulness, since it can offer a structured assessment of security risks and show which are the greater criticalities where more attention should be paid. Further research could be conducted to apply the model in different sectors in order to check any significant variation and to develop further knowledge on the right mixture of (technical, managerial and legal) protection tools to manage security risks that arises from outsourcing/ offshoring projects.

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

Antonucci Y. L., Lordi F. C., Tucker III J. J., 1998, "The Pros and Cons of IT Oursourcing"; *Journal of Accountancy*, Vol.185, No.6, pp.26-31

Apke T.M., 2003, "International protection of trade secrets when using Internet"; *Management Decision*, Vol. 41, No. 1, pp. 43-47

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

Arundel A., 2001, “The relative effectiveness of patents and secrecy for appropriation”; *Research Policy,* Vol.30, No.4, pp.611-624

Baden-Fuller C., Targett D., Hunt B., 2000, “Outsourcing to outmanoeuvre: Outsourcing re-defines competitive strategy and structure”; *European Management Journal*, Vol.18, No.3, pp.285-295

Bahli B., Rivard S., 2005, “Validating measures of information technology outsourcing risk factors”; *Omega*, Vol.33, No.2, pp.175-187

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 systems 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

Blind K., Thumm N., 2004, “Interrelation between patenting and standardisation strategies: empirical evidence and policy implications”; *Research Policy*, Vol.33, No.10, pp.1583-1598

Blumberg D. F., 1998, “Strategic assessment of outsourcing and downsizing in the service market”; *Managing Service Quality*, Vol.8, No.1, pp.5-18

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

Bond R.T., Audley H., Knyrim R.S., 2002, “Data protection – Third country transfer: Data transfer to third countries: standard contractual clauses of the European commission”; *Computer Law & Security Report*, Vol. 18, No. 3, pp. 187-190

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

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

Chiarini A., Vicenza M., 2004, *Strumenti statistici avanzati per la gestione della qualità. Affidabilità, FMEA, FTA,SPC,DOE*, Franco Angeli, Milano

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

Colwill C., Gray A., 2007, “Creating an effective security risk model for outsourcing decisions”; *BT Technology Journal*, Vol. 25, No. 1, pp. 79-87

Cullen S., Seddon P. B., Willcocks L. P., 2005, “IT outsourcing configuration: Research into defining and designing outsourcing arrangements”; *Journal of Strategic Information Systems*, Vol.14, No.4, pp.357-387

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

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

Desouza K. C., 2008, “The neglected dimension in strategic sourcing: security”; *Strategic Outsourcing: An International Journal*, Vol.1, No.3, pp.288-292

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

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

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, "IT Security outsourcing: 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

Fulford H., Doherty N.F., 2003, "The application of information security policies in large UK-based organizations: an exploratory investigation"; *Information Management & Computer Security*, Vol.11, No.3, pp.106-114

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., 2008, "Information security requirements – Interpreting the legal aspects"; *Computers & Security*, Vol. 27, No. 5-6, pp. 124-135

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.1233-1248

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

Gupta A., Hammond R., 2005, “Information systems security issues and decisions for small businesses: An empirical examination”; *Information Management & Computer Security*, Vol.13, No.4, pp.297-310

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

Handley S. M., Benton Jr. W.C., 2008, “Unlocking the Business Outsourcing Process Model”; *Journal of Operations Management*, Article in Press

Haugen S., Roger Selin J., 1999, “Identifying and controlling computer crime and employee fraud”; *Industrial Management & Data Systems*, Vol. 99, No. 8, pp. 340-344

Higgins H.N., 1999, “Corporate system security: towards an integrated management approach”; *Information Management & Computer Security*, Vol.7, No.5, pp.217-222

Hinde S., 2003, “The law, cybercrime, risk assessment and cyber protection”; *Computers & Security*, Vol.22, No.2, pp.90-95

Hoecht A., Trott P., 2006, “Outsourcing, information leakage and the risk of losing technology-based competencies”; *European Business Review*, Vol.18, No.5, pp.395-412

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

Kankanhalli A., Teo H.-H., Tan B.C.Y., Wei K.-K., 2003, "An integrative study of information systems security effectiveness"; *International Journal of Information Management*, Vol.23, No.2, pp.139-154

Karabulut Y., Kerschbaum F., Massacci F., Robinson P., Yautsiukhin A., 2007, "Security and Trust in IT Business Outsourcing: a Manifesto"; *Electronic Notes in Theoretical Computer Science*, Vol. 179, No. 6, pp. 47-58

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*, Vol.44, No.3, pp.250-261

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

Leem C. S., Lee H. J., 2004, “Development of certification and audit processes of application service provider for IT outsourcing”; *Technovation*, Vol.24, No.1, pp.63-71

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 Quarterly*, Vol. 16, No. 2, pp. 173-186

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", CASP/AT Kearney

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

Norman P.M., 2001, "Are your secrets safe? Knowledge protection in strategic alliances"; *Business Horizons*, Vol.44, No.6, pp.51-60

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

Posthumus S., von Solms R., 2004, “A framework for the governance of information security”; *Computers & Security*, Vol.23, No.8, pp.638-646

Power M., Bonifazi C., Desouza K.C., 2004, “The ten outsourcing traps to avoid”; *Journal of Business Strategy*, Vol.25, No.2, pp.37-42

Razzaque M. A., Sheng C. C., 1998, “Outsourcing of logistics functions: a literature survey”; *International Journal of Physical Distribution & Logistics Management*, Vol.28, No.2, pp.89-107

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

Sanderson E., Forcht K.A., 1996, “Information security in business environments”; *Information Management & Computer Security*, Vol. 4, No. 1, pp. 32-37

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

Simmonds D., Gibson R., 2008, "A model for outsourcing HRD"; *Journal of European Industrial Training*, Vol.32, No.1, pp.4-18

Siponen M.T., 2000, "A conceptual foundation for organizational information security awareness"; *Information Management & Computer Security*, Vol.8, No.1, pp. 31-41

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

Spurling P., 1995, "Promoting security awareness and commitment"; *Information Management & Computer Security*, Vol.3, No.2, pp. 20-26

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

Stratman J. K., 2008, "Facilitating offshoring with enterprise technologies: Reducing operational friction in the governance and production of services"; *Journal of Operations Management*, Vol.26, No.2, pp.275-287

Stringfellow A., Teagarden M. B., Nie W., 2008, "Invisible costs in offshoring services work"; *Journal of Operations Management*, Vol.26, No.2, pp.164-179

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

Tran E., Atkinson M., 2002, "Security of personal data across national borders"; *Information Management & Computer Security*, Vol. 10, No. 5, pp. 237-241

Varadarajan R., 2008, "Outsourcing: Think more expansively"; *Journal of Business Research*, Article in Press

Wright T., 2005, “Outsourcing – Financial Services Authority report on offshoring”; *Computer Law & Security Report*, Vol.21, No.6, pp.500-504

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

Youngdahl W., Ramaswamy K., 2008, “Offshoring knowledge and service work: A conceptual model and research agenda”; *Journal of Operations Management*, Vol.26, No.2, pp.212-221

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