Secure Outsourcing: An Investigation of the Fit between Clients and Providers

Gurpreet Dhillon, Romilla Chowdhuri, Filipe De Sá-Soares

Secure Outsourcing: an investigation of the fit between clients and providers

Gurpreet Dhillon[1], Romilla Chowdhuri[1], Filipe de Sá-Soares[2]

[1]Virginia Commonwealth University, Richmond, USA
{gdhillon, syedr2}@vcu.edu
[1]Universidade do Minho, Portugal
fss@dsi.uminho.pt

Abstract. In this paper we present an analysis of top security issues related to IT outsourcing. Identification of top issues is important since there is a limited understanding of security in outsourcing relationships. Such an analysis will help decision makers in appropriate strategic planning for secure outsourcing. Our analysis is conducted through a two-phase approach. First, a Delphi study is undertaken to identify the top issues. Second, an intensive study of phase one results is undertaken to better understand the reasons for the different perceptions.

Keywords. Secure outsourcing, congruence, client vendor fit, Delphi study

1 Introduction

Information security is a significant sticking point in establishing a relationship between Information Technology (IT) outsourcing vendors and clients. While statistics related to outsourcing risks and failures are abound, there has been a limited emphasis on understanding information security related reasons for outsourcing problems. We believe that many of the problems stem from a lack of fit between what IT outsourcing vendors consider to be the key success factors and what outsourcing clients perceive to be critical for the success of the relationship. It is important to undertake such an investigation because of two primary reasons. First, majority of IT outsourcing projects fail because of a lack of appreciation as to what matters to the clients and the vendors [2], [14]. Second, several IT outsourcing projects fall victim to security breaches because of a range of issues – broken processes, failure to appreciate client requirements [10], among others. If strategic

alignment between IT outsourcing vendors and clients is maintained, many of the security challenges could be overcome.

A first step in ensuring a strategic fit with respect to information security is to identify as to what is important for the vendors and the clients respectively. In this paper we undertake an extensive Delphi study to identify information security issues related to both the vendors and the clients. This is followed up by an intensive analysis of the issues through in depth interviews with several client and vendor firms.

2 Informing Literature

In recent years there have been several security breaches where privacy and confidentiality of data has been compromised largely because there was a lack of control over the remote sites. In 2011 an Irish hospital reported breach of patient information related to transcription services in the Philippines. Recently US Government Accounting office survey reported that at least 40 percent of federal contractors and state Medicare agencies experienced a privacy breach (see GAO-06-676)[1]. While it is mandatory for the contractor to report breaches, there is limited oversight. Given the challenges, many corporations have begun implementing a range of technical controls to ensure security of their own infrastructures rather than rely on the vendors.

In addressing the security challenges in outsourcing relationships or for that matter any kind of a risk, management of client-vendor relationship has been argued as important. Earlier studies on outsourcing have mainly discussed different phases of client-vendor relationships and the relevant issues in each of the phases [7]. For example, *Relationship Structuring* involves issues deemed important when the outsourcing contract is being prepared, *Relationship Building* involves issues that contribute to the strengthening of relationship between client and vendor, and *Relationship Management* involves issues that are relevant to drive the relationship in the right direction. Another study lists 25 independent variables that can impact the relationship between outsourcing client and vendor [18]. The most cited factors include effective knowledge sharing, cultural distance, trust, prior relationship status, and communication.

[1] http://www.gao.gov/assets/260/251282.pdf. Accessed January 29, 2013

Studies related to secure outsourcing have been few and far between. In majority of the cases the emphasis has been on contractual aspects of the relationship between the client and the vendor. And many researchers have made calls for clarity in contracts as well as selective outsourcing [17]. Managing the IT function as a value center [36] has also been proposed as a way for ensuring success of outsourcing arrangements. There is no doubt that prior research has made significant contribution to the manner in which advantages can be achieved from outsourcing relationships, however there has been limited contribution with respect to management of security and privacy.

Internet Security has been considered as one of the technological risks [15], with data confidentiality, integrity and availability as the topmost concerns in an outsourcing arrangement [16]. While a few surveys report computer networks, regulations and personnel as the highest security threats to organizations [4], others recognize that not only technical, but also non-technical threats can be detrimental to an engagement [4], [8], and [28]. However, most of the work cited under the domain of IS outsourcing risks is generic and has a very limited focus on security [10], and [31]. Several researchers have provided frameworks to identify organizational assets at risk and to use financial metrics to determine priority of assets that need protection [3], and [27]. Research on security threats prevalent in an outsourcing or offshore environment and risk management models has also been undertaken [5]. The political, cultural and legal differences between supplier and provider environment are supposed to make the environment less favorable for operators. A multi-layer security model to mitigate the security risks, both at technical and nontechnical level, in outsourcing domains is presented by Doomun [9], where eleven steps in an outsourcing arrangement are divided across three layers of security: identification, monitoring and improvement, and measurement.

Wei and Blake [37] provide a comprehensive list of information security risk factors and corresponding safeguards for IT offshore outsourcing. More recently, Nassimbeni et al [23] categorized the security risks into three phases: strategic planning, supplier selection and contracting, implementation and monitoring. In both the studies the issues have mainly been borrowed from existing literature. Some of the researchers have also classified the risks as external and internal threats to an organization and human and non-human risks. Non-technical concerns such as employees, regulations, and trust have emerged to be

more severe than technological risks [21], [29], [34], and [35]. As such few studies are concerned with a specific type of security concern such as policies [11].

While the prevalent IT outsourcing research has certainly helped in better understanding the client-vendor relationships, an aspect that has largely remained unexplored is that of organizational *fit*. In the IT strategy domain organization fit has been explored in terms of alignment between IT strategy and business strategy [13]. In the strategy literature it has been studied in terms of the fit between an organization's structure and its strategy. Even though Livari [20] made a call for understanding organizational fit of information systems with the environment, little progress has been made to date.

With respect to IT outsourcing the notion of the fit between a client and vendor has also not been well studied. It is suggested that fit can be understood through the elements of congruence theory, which explains the interactions among organizational environment, values, structure, process and reaction-adjustment [24]. Based on congruence theory, an *outsourcing environment* thus can be defined as the existence of any condition such as culture, regulations, provider/supplier capabilities, security, and competence that can determine the success of an outsourcing arrangement. Organizational values determine the acceptable and unacceptable behavior. In this respect factors such as trust, transparency and ethics fall under the value system of an organization. Structure of an outsourcing arrangement defines the factors such as reporting hierarchy, ownership and processes for communication. Additionally reaction-adjustments are required, which entail the feedback and outcomes of an engagement and the related modifying strategy in response to the reactions of clients for a better strategic fit and alliance between outsourcing clients and vendors.

Clearly the existing literature on identification and mitigation of security risks is rich. The security risks at technical, human and regulatory levels are well identified; many of the studies highlight that non-technical risks are more severe than the technical ones. However, the literature is short of two perspectives: **First**, gap analysis of how outsourcing clients and outsourcing vendors perceive the security risks. **Second**, the existing literature does not discuss much about the congruence among different concepts in an outsourcing arrangement, particularly in the security domain. Hence to determine a fit between vendors and clients, we need to understand as to what security issues are im-

portant to each of them and then to establish a basis for their congruence.

3 Research Methodology

Given that the purpose of this study was to identify security concerns amongst outsourcing clients and vendors, a two-phased approach was adopted. In the first instance a Delphi study was undertaken. This helped us in identifying the major security issues as perceived by the clients and the vendors. In the second phase an in depth analysis of clients and vendors was undertaken. This helped us in understanding the reasons for significant differences in their perceptions.

3.1 Phase 1 – A Delphi Study

To ensure a reliable and validated list of issues that are of concern to the organizations, both from client and vendor perspective, a process to inquire and seek the divergent opinions of different experts is provisioned. A ranking method based on Schmidt's Delphi methodology, designed to elicit the opinions of panel of experts through controlled inquiry and feedback, is employed [32]. Delphi study allowed factors to converge to the ones that really are important in secure outsourcing.

Panel Demographics

To account for varying experiences, and role of experts, both outsourcing vendors or providers and outsourcing clients or suppliers were chosen as the target panelists. A total of 11 panelists were drawn from the pool of 21 prospective participants. We identified senior IS executives from major corporations and asked them to identify the most useful and experienced people to participate in the survey. The participants were divided into two groups –*Outsourcing Providers (5)* and *Outsourcing Suppliers (6)*. The panelists had impressive and varied experiences in IT outsourcing and management. The number of panelists suffices the requirement of eliciting diverse opinions and prevents the panelists from being intimidated with the volume of feedback [32]. Moreover, the comparative size of the two panels is irrelevant since it doesn't have any impact on response analysis. For detecting statistically significant results, the group size is dependent on the group dynamics rather than the number of participants; therefore, 10 to 11 experts is a good sample size [26].

Data Collection

The data collection phase is informed by Schmidt's method, which divides the study into three major phases [32]. The first round - brainstorming or blank sheet round - was conducted to elicit as many issues as possible from each panelist. Each participant was asked to provide at least 6 issues along with a short description. The authors collated the issues by removing duplicates. The combined list was sent to panelists explaining why certain items were removed and further asked the panelists for their opinion on the integrity and uniformity of the list. In the second round we asked each panelist to pare down the list to most important issues. A total of 26 issues were identified which were sent to the panelists for further evaluation, addition, deletions and /or verification. This is to ensure that a common set of issues is provided for the panelists to rank in subsequent rounds. Ranking of the final 26 issues was done in phase 3. During this phase each panelist was required to rank the issues in order of importance with 1 being the most important security issue and 26 being the least important security issue in outsourcing. The panelists were restricted to have the ties between two or more issues.

Multiple ranking rounds were conducted until a consensus was achieved. To avoid bias a randomly ordered set of issues was sent to each panelist in the first ranking round. For the subsequent rounds, the lists were ordered by average ranks. In this study we used Kendall's Coefficient of Concordance *W* to evaluate the level of agreement among respondents' opinions in a given round. According to Schmidt [32], 'W' can range between 0.1 (very weak agreement) and 0.9 (unusually strong agreement). Moreover, Spearman's Rank Correlation Coefficient *rho* is used to evaluate the level of stability of the panel's opinion between two successive rounds and between two different groups of respondents in a given round. The value of *rho* can range between -1 (perfect negative correlation) and 1 (perfect positive correlation) Subsequent ranking rounds are stopped either if Kendall's Coefficient of Concordance *W* indicated a strong consensus (>0.7) or if the level of consensus leveled off in two successive rounds.

At the end of every ranking round, five important pieces of feedback were sent to panelists: (1) mean rank for each issue; (2) level of agreement in terms of Kendall's *W*; (3) Spearman correlation *rho*; (4) P-value; (5) relevant comments by the panelists

Data Analysis
The analysis of the results was performed in two parts: First, an analysis of aggregated Delphi study treats all respondents as a global panel and thus presents the unified ranking results. Second, an analysis of partitioned Delphi study presents the ranking results based on respondents group, i.e. outsourcing providers and outsourcing clients.

3.2 Phase 2 - Probing for Congruence

The second round of data collection was based on two workshops with representatives from Fortune 500 companies. There were 11 individuals with an average of 8 years of work experience who participated in these workshops. The workshops were conducted from May 2012 to July 2012. In the first workshop, each participant was required to answer three questions for all 26 issues. Suitable probes were added following each question. This helped in developing a rich insight. The probes were:

1. What do you think about the issue?
2. Why do you think it is important for outsourcing provider?
3. Why do you think it is important for outsourcing client?

The second workshop was concentrated to achieve congruence between outsourcing suppliers and outsourcing providers. Different ranks assigned by clients and vendors to particular issues were highlighted. The participants were asked to answer two questions so as to elicit their opinions on the gaps identified in the ranking sought by clients and providers for the issues.

1. Explain what do you think is the reason for assigning different ranks by outsourcing clients and outsourcing providers?
2. Explain what can be done to resolve the difference in order to seek a common ground of understanding between clients and providers?

4 Findings from the Delphi Study

For phase one, the results were analyzed from a global or aggregated view and partitioned or client vs. vendor view. The global panel reached a weak consensus by third ranking round (see table 1).

Table 1 – Global Consensus

Round	W (Clients * Provider)	Rho
1	0.342(p<0.001)	
2	0.279(p<0.001)	0.568 (p<0.01)
3	0.102(p<0.727)	0.497 (p=0.01)

On the other hand, by the third ranking round, Clients had fair agreement whereas vendors had very weak agreement. Moreover, a weak positive correlation exists between round 2 and round 3 in global ranking as well as between clients and providers by round 3 (see table 2).

Table 2 – Client and Vendor Consensus

Round	Clients' W	Providers' W	Rho
1	0.349(p=0.0121)	0.522(p<0.001)	0.374
2	0.486(p<0.001)	0.266(p=0.0297)	0.479
3	0.569(p=0.287)	0.100(p=0.94)	0.119

The weak consensus in global ranking clearly suggests that outsourcing clients and outsourcing vendors have conflict of interest. Moreover, the weak consensus within vendors indicates that not all vendors perceive the importance of security at same level. And finally the difference between ranks assigned to each issue by clients and vendors further highlights the conflict of interest between the two. Table 3 presents a comparison of the ranks from client and vendor perspectives and shows a significant divide between the two groups. The issues are sorted compositely; however, given the significant difference for most of the issues, the composite rank is irrelevant. For this paper we assume a difference of more than three, between the ranks sought by client and vendors, as significant. Thereby, a total of 16 issues out of 26 show significant difference between the rankings of two groups

Table 3 – Comparison of Client and Vendor ranks (only significant issue are presented)

Rank of the issue	Issue Description	Client Rank	Vendor Rank
2	Comprehensiveness of information security outsourcing decision analysis	7	2
3	Information security competency of outsourcing vendor	8	1
5	Ability of outsourcing vendor to comply with client's security policies, standards and processes	2	10
7	Dissipation of outsourcing vendor's knowledge	10	3
8	Technical complexity of outsourcing client's information security operations	13	5
9	Trust that outsourcing vendor applies appropriate security controls	1	20
10	Diversity of jurisdictions and laws	4	17
12	Information security credibility of outsourcing vendor	15	9
13	Quality of outsourcing vendor's staff	18	6
14	Legal and judicial framework of outsourcing vendor's environment	9	16
15	Inability to redevelop competencies on information security	19	11
17	Audit of outsourcing vendor staffing process	20	12
18	Inability to change information security requirements	12	22
20	Transparency of outsourcing vendor billing	14	24
21	Audit of outsourced information security operations	25	14

5 Reviewing Congruence Amongst Issues

It is interesting to note that there is a significant difference in the client and vendor perspectives of the top secure outsourcing issues. In this section we explore these issues further to develop a better understanding. In terms of managing security of outsourcing it makes sense to develop a fit between what the clients and the vendors consider important.

Two issues that seem to be of significant concern for both the clients and the vendors is of *diversity of laws* and the *legal and judicial framework of the vendor's environment.* Both these concerns are indeed noteworthy. Our discussions with a CIO of a major bank in the US, which has outsourced significant amount of IT services to India, suggest jurisdictional issues to be a major concern. The CIO noted:

> I can say with absolute certainty that our outsourcing experience has been very positive. We found significantly high level of competence in our vendor. However there are constant challenges of dealing with the regulatory environment. Laws in the US are rather strict in terms of disclosure and we feel that to be an impediment to getting our work done.

The literature has reported similar concerns, albeit with respect to mainstream outsourcing issues rather than security. It has been argued that there are issues of conformance and contractual violations, which

can have a detrimental impact on outsourcing relationships [28]. It is interesting to note though that both issues 10 and 14 rank higher amongst the clients than the vendors. It seems that regulatory compliance and prevalence of a judicial framework is more of a concern to the outsourcing clients than the vendors. Another IT manager in our study commented:

> Increased transparency regarding the laws governing the vendor may mitigate the risk for the client. However, the burden is on the vendor to reassure the client that the risk is minimal. Therefore the vendor should be supplying as much information to reassure the client that they are working under the same legal context and that their legal agreements are mutually beneficial.

In the literature several calls have been made that suggest clarity of legal and regulatory frameworks (e.g. [30]). Beyond clarity however there is a need to work on aligning the legal and regulatory frameworks at a national level. Country specific institutions shall play a critical role ensuring such alignment (e.g. NASSCOM in India). To better mitigate the risks and to ensure that the interest of both parties is secure, increased transparency in legal structure is required. The burden lies on the provider though. Therefore the vendor should be making available as much information to reassure the client that they are working under the same legal context and that their legal agreements are mutually beneficial. As a principle we therefore propose:

Principle 1 - Reducing the diversity of laws and ensuring congruence of legislative controls ensure security in outsourcing.

Another issue, *dissipation of outsourcing vendors knowledge,* emerged to be significant. While this issue seems more critical for the vendors, there are some significant implications for client firms as well. Vendors believe that because of the untoward need to comply with the whims and fancies for the clients, there is usually a dissipation of the knowledge over a period of time. One of the members of our intensive study was the country head for a large Indian outsourcing vendor. When asked to comment of this issue, he said:

> The outsourcing industry has a serious problem. While we have our own business processes, we usually have to recreate or reconfigure them based on our client needs and wants. We are usually rather happy to do so. However in the process we lose our tacit knowledge. From our perspective it is important to ensure protection of this

> knowledge. Many of our security and privacy concerns would be managed if we get a little better in knowledge management.

Perhaps Willcocks et al [39] are among the few researchers who have studied the importance of protection of intellectual property. Most of the emphasis has however been on protecting loss of intellectual property – largely of the client firm. Management of knowledge to protect tacit knowledge has also been studied in the literature (e.g. see [1], [25]), though rarely in connection with outsourcing.

It goes without saying that poor knowledge management structures will disappoint the prospects of procuring of new contracts. In comparison, the clients seem to either assume that the provider has a sustainable structure that prevents or minimizes the loss of intellectual capital and ensures confidentiality, or the client is ready to bear the risk for the perceived potential benefits. Clients expect skilled resources as a contractual requirement. As the risk for clients is minimal, they rank this in less importance in comparison to the vendor. Existing literature mentions that for the better management of expectations, both clients and suppliers need to understand the utility of knowledge management, implications of loss and structural requirement [39]. This is also reflected in the comments of one of security assurance manager:

> Suppliers need to minimize staff turnover and find ways to ensure staff retention and knowledge sharing. There are many methods to achieve this; such as better wages, benefits, flex time, encouragement, knowledge repositories, education opportunities, etc. They should pair veteran staff member with new staff members to improve their understanding of confidentiality, integrity and availability.

As a principle we therefore propose:

Principle 2 Tacit knowledge management and ensuring the integrity of vendor business processes, is a pre-requisite for good and secure outsourcing.

Our research also found *information security competency of outsourcing vendor* as a significant issue. Many scholars have commented on the importance of vendor competence [12], [19], [38]. It is argued that value based outsourcing outcome should be generated and transferred from the vendor to the client [19]. However, as is indicative from our study, clients and vendors differ in their opinions on what is most important when selecting and promoting outsourcing security services.

While, vendors often believe that proving their competency through a large list of certifications, awards, and large clientele is important to have to prove their competency, the client's perspective is geared towards the application and utilization of supplier competency. One of the IT managers from a bank noted:

> The vendor is expected to be competent in their area of expertise, so the client needs to make clear to the vendor that a basic expectation should not be at the top of their list as there are more important factors that will be used to differentiate the vendors from one another.

As is rightly pointed out by the IT Manager, the issue with managing competence is not to present a baseline of what the vendor knows (i.e. the skill set), but a demonstration of the *know-that* (see [6]). Assessment of competence is outwardly driven and hence a presentation of some sort of maturity in security management is essential (e.g. ISO 21827). As a principle we propose:

Principle 3 - A competence in ensuring secure outsourcing is to develop an ability to define individual know-how and know-that.

Process is a formalized sequence of actions guided "informally" by the organization's structure and organization's value system. There is enough evidence in the literature about the impact of process standardization on outsourcing success [40]. However, the variations in the ranks of one of the issues identified - *ability of outsourcing vendor to comply with client's security policies, standards and processes* – is a cause of concern. The issue here is indicative of the need for facilitating communication and coordination required for the alignment of policies, standards and processes guiding information security in an outsourcing engagement. Clients certainly place high importance on its own policies and processes, giving this issue a higher rank. Meanwhile, providers view their policies, procedures, and standards as being best-in-class. Clearly the vendors seem to be ignorant of the fact that having a process framework that is not customizable to the individual requirements of different clients can be a potential hindrance. As one of the client notes:

> It is great that a company can claim they are competent in providing outsourced information security but it means nothing to the client unless the client perceives their specific policies as being effectively applied by the provider.

To eliminate the gap, processes and policies need to be comprehensive enough and the contracts need to emphasize the implications of non-compliance. For the sake of continued alliance, the responsibility lies more on vendor to ensure process compliance and governance. Another manager from a client organization commented:

> Clients are usually outsourcing to relieve their workload and performing a comprehensive analysis is viewed as adding to the existing workload they are trying to relieve. The more a potential supplier is willing to be an active partner and point out the pros and cons of their own proposals as well as the others, the smaller the gap will be.

As a principle, we propose:

Principle 4 - Establishing congruence between client and vendor security policies ensures protection of information resources and a good working arrangement between the client and the vendor.

If leveraging the core competency of suppliers is the main motive to outsource security operations, the lower ranking by clients for the issue - *audit of outsourced information security operations* - is justified. Clients expect competency of the outsourcing vendor to be in place. However, clients also seem to lack consensus on the need for continued monitoring and governance procedures. Auditing is one of the means for the client to verify whether the vendor is adhering to the security policies. Vendors by virtue of providing a higher rank in comparison to clients, appear to be aware of the importance of proving continued compliance with agreements. Providing audited or auditable information relating to the clients data and processes is a must for establishing trust. Much of the research in IS outsourcing has focused on different dimensions of governance procedures including contractual and non-contractual mechanisms of trust building [22]. Auditing and third party assurance, which leads to increased trust (see issues 4 and 9 in our study), typically do not seem to be touched upon.

A related issue (and also connected to principle 4 above) is that of a competence audit. Any audit of vendor operations must include several aspects including - overall competence in information security (issue 15 in our study) and quality of vendor staff (issue 13). Our research subjects reported several instances where there was a general loss of competence over a period of time. This usually occurs when either the ven-

dor organization gets too entrenched with one client and hence overlooking the needs of the other or when internal processes are patched and reconfigured in a reactive manner to ensure compliance with the expectations of a given client (refer to issue 5 in our study). One Chief Information Security Officer from a healthcare organization commented:

> There seems to be this half-life of a security competence. I have seen that after a contract has been signed, there is a somewhat exponential decay in quality.

In the literature there is some mention of such decay in quality, although not directly in relation to outsourcing (e.g. see [33]). It is found that in many of the quality improvement initiatives can interact with prevailing systems and routines to undercut commitment to continuous improvement. While our research does not suggest this to be the case in terms of secure outsourcing, the difference in opinions between the clients and the vendors seem indicative. As a principle we therefore propose:

Principle 5 - An internal audit of both client and vendor operations is critical to understand current weaknesses and potential problems there might be with respect to information security structures, procedures and capabilities.

Based on our research, two major constructs seem to emerge – *strategic context* of secure outsourcing and *organizational capability* in outsourcing (Fig.1). The strategic context is defined by legal/regulatory congruence and security policy alignment. In our research organizational capability is a function of knowledge management, competence and audit. Combined together, our constructs define security congruence. The level of congruence however can only be assessed through outcome measures (e.g. secure outsourcing). Such outcome measures could include reduced incidents of security breaches, high ranks from external vetting organizations etc.

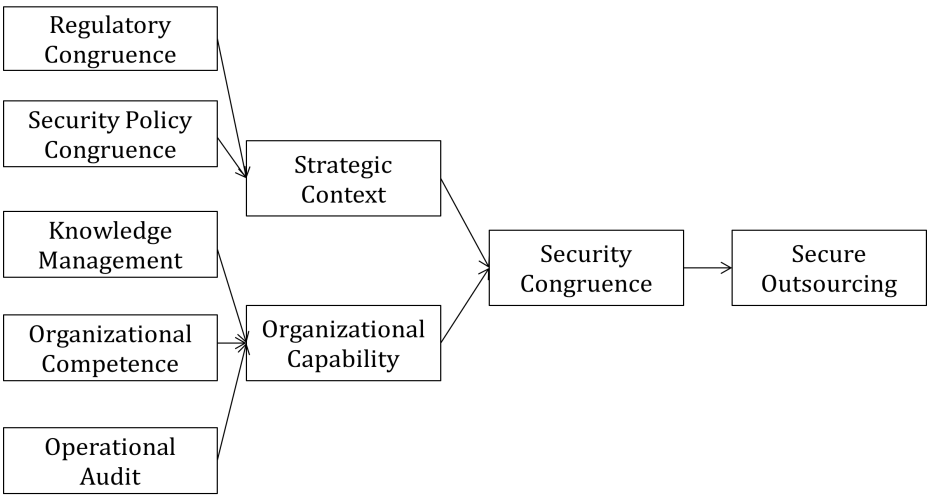

Fig. 1. Modeling security congruence

A central theme in organization strategy literature is that of "fit". Findings from our research seem to be in resonance with that body of work. For instance, and as noted previously, Nightingale and Toulouse [24] comment on the mutual interaction amongst values, structure, process, reaction-adjustment and environment leads to the congruent organization.

In the context of security of information resources, the need to develop a fit between outsourcing partners seems to be appropriate. Significant variations in the rankings on part of vendors raise some doubts: if they value the sensitivity of client data; if they ensure adequate protection of the assets; if the vendor is aware of the vulnerabilities in their processes. All these issues would also raise concern about the attitude of the client, particularly in relation to shunning responsibilities. This can indeed be a classic example of strife between factions of affordability and availability.

In order to achieve the congruence between clients and vendors, the discussion so far leads to the emergence of one main theme - *managing expectations*. In the purview of congruence theory this requires elimination of gaps between the two parties and eventually align the two organizations (in our case, around strategy and capability as per Fig.1). Fig.1 provides a conceptual design of such an aligned organization. For

better management of expectations, the supplier and vendor organizations need to communicate and coordinate their respective operations.

Both the organizations align to the required dimensions and in effect overtime the two organizations involved in an outsourcing contract appear to be one “virtual” organization, which has just one goal - delivering services in a secure manner (i.e. secure outsourcing). As long as a gap exists in processes, structure or values between the two organizations, the alignment is questionable. The time taken by the two organizations to align - *alignment latency* would be a critical success factor of a secured outsourcing engagement.

6 Conclusion

In this paper we have presented an in depth study of secure outsourcing. We argued that while several scholars have studied the relative success and failure of IT outsourcing, the emergent security issues have not been addressed adequately. Considering this gap in the literature we conducted a Delphi study to identify the top security outsourcing issues from both the clients and the vendors perspectives. Finally we engaged in an intensive study to understand why there was a significant difference in ranking of the issues by the vendors and the clients. This in depth understanding lead us to propose five principles that organizations should adhere to in order to ensure security of outsourcing relations. A model for security congruence is also proposed. While we believe there should be a positive correlation amongst the proposed constructs, clearly further research is necessary in this regard.

Secure outsourcing is an important aspiration for organizations to pursue. There is no doubt that many businesses thrive on getting part of their operations taken care of by a vendor. It not only makes business sense to do so, but it also allows enterprises to tap into the expertise that may reside elsewhere. Security then is simply a means to ensure smooth running of the business. And definition of the pertinent issues allows us to strategically plan secure outsourcing relationships.

References

[1] Arora, A. (1996). Contracting for tacit knowledge: the provision of technical services in technology licensing contracts. *Journal of Development Economics, 50*(2), 233-256.

[2] Barthelemy, J. (2001). The hidden costs of IT outsourcing. *MIT Sloan management review*, *42*(3), 60-69.

[3] Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413-422.

[4] Chang, A. J. T., & Yeh, Q. J. (2006). On security preparations against possible IS threats across industries. *Information management & computer security*, *14*(4), 343-360.

[5] Colwill, C., & Gray, A. (2007). Creating an effective security risk model for outsourcing decisions. *BT technology journal*, *25*(1), 79-87.

[6] Dhillon, G. (2008). Organizational competence in harnessing IT: a case study. *Information & Management, 45*(5), 297-303.

[7] Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information systems outsourcing: a survey and analysis of the literature. *ACM SIGMIS Database*, *35*(4), 6-102.

[8] Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *computers & security*, *28*(3), 189-198.

[9] Doomun, M. R. (2008). Multi-level information system security in outsourcing domain. *Business Process Management Journal*, *14*(6), 849-857.

[10] Earl, M. J. (1996). The risks of outsourcing IT. *Sloan Management Review*, *37*, 26-32.

[11] Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, *11*(3), 106-114.

[12] Goles, T. "The Impact of Client-Vendor Relationship on Outsourcing Success," University of Houston, Houston, TX, 2001.

[13] Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: leveraging information technology for transforming organisations. *IBM Systems Journal, 32*(1), 4-16.

[14] Kaiser, K. M., & Hawk, S. (2004). Evolution of offshore software development: From outsourcing to cosourcing. *MIS Quarterly Executive*, *3*(2), 69-81.

[15] Kern, T., Willcocks, L. P., & Lacity, M. C. (2002). Application service provision: Risk assessment and mitigation. *MIS Quarterly Executive*, *1*(2), 113-126.

[16] Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29-42.

[17] Lacity, M. C., & Willcocks, L. P. (1998). An Empirical Investigation of Information Technology Sourcing Practices: Lessons from Experience. *MIS Quarterly, 22*(3), 363-408.

[18] Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of information technology*, *25*(4), 395-433.

[19] Levina, N., & Ross, J. W. (2003). From the vendor's perspective: exploring the value proposition in information technology outsourcing. *MIS Quarterly*, 331-364.

[20] Livari, J. (1992). The organizational fit of information systems. *Information Systems Journal, 2*(1), 3-29.

[21] Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 173-186.

[22] Miranda, S. M., & Kavan, C. B. (2005). Moments of governance in IS outsourcing: conceptualizing effects of contracts on value capture and creation. *Journal of Information Technology*, 20(3), 152-169.

[23] Nassimbeni, G., Sartor, M., & Dus, D. (2012). Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems*, *112*(3), 4-4.

[24] Nightingale, D. V., & Toulouse, J. M. (1977). Toward a multilevel congruence theory of organization. *Administrative Science Quarterly*, 264-280.
[25] Norman, P. M. (2002). Protecting knowledge in strategic alliances: Resource and relational characteristics. *The Journal of High Technology Management Research, 13*(2), 177-202.
[26] Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management*, *42*(1), 15-29.
[27] Osei-Bryson, K.-M., & Ngwenyama, O.K. (2006). Managing risks in information systems outsourcing: an approach to analyzing outsourcing risks and structuring incentive contracts. *European Journal of Operational Research*, 174 (1), 245–264
[28] Pai, A. K., & Basu, S. (2007). Offshore technology outsourcing: overview of management and legal issues. *Business Process Management Journal*, *13*(1), 21-46.
[29] Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646.
[30] Raghu, T. (2009). *Cyber-security policies and legal frameworks governing Business Process and IT Outsourcing arrangements.* Paper presented at the Indo-US conference on cyber-security, cyber-crime & cyber forensics.
[31] Sakthivel, S. (2007). Managing risk in offshore systems development. *Communications of the ACM*, 50(4), 69–75
[32] Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences, 28*(3), 763-774.
[33] Sterman, J. D., Repenning, N. P., & Kofman, F. (1997). Unanticipated side effects of successful quality programs: Exploring a paradox of organizational improvement. *Management Science, 43*(4), 503-521.
[34] Tickle, I. (2002). Data integrity assurance in a layered security strategy. *Computer Fraud & Security*, *2002*(10), 9-13.
[35] Tran, E., & Atkinson, M. (2002). Security of personal data across national borders. *Information management & computer security*, *10*(5), 237-241.
[36] Venkatraman, N. (1997). Beyond outsourcing: managing IT resources as a value center. *Sloan Management Review, 38*(3), 51-64.
[37] Wei, Y., & Blake, M. (2010). Service-oriented computing and cloud computing: Challenges and opportunities. *Internet Computing, IEEE*, *14*(6), 72-75.
[38] Willcocks, L., and Lacity, M.C. "Relationships in IT Outsourcing: A Stakholder Perspective," in: Framing the Domains of IT Management, R. Zmud (ed.), Pinnaflex Inc., Ohio, 2000, pp. 355-384
[39] Willcocks, L., Hindle, J., Feeny, D., & Lacity, M. (2004). IT and business process outsourcing: The knowledge potential. *Information Systems Management*, *21*(3), 7-15.
[40] Wüllenweber, K., Beimborn, D., Weitzel, T., & König, W. (2008). The impact of process standardization on business process outsourcing success. *Information Systems Frontiers*, 10(2), 211-224.