Offshored Data Privacy: Determining the Factors and their relative Effect

Anupam Nath
Business Admin, Elizabeth City State University, Elizabeth City, NC, United States., aknath@uncg.edu

Azam Bejou
Business Admin, Elizabeth City State University, Elizabeth City, NC, United States., ambejou@mail.ecsu.edu

Offshored Data Privacy: Determining the Factors and their relative Effect

Anupam Kumar Nath
Elizabeth City State University
aknath@mail.ecsu.edu

Azam Bejou
Elizabeth City State University
ambejou@mail.ecsu.edu

ABSTRACT

For many US based companies' offshoring, especially IT services, has become an inevitable part of business strategy. However, preserving the privacy of the sensitive information of offshored data remains as one of the major challenges and concerns. In this paper, we identify factors that affect the privacy preserving conduct of the offshore vendors and their employees towards clients' data. We deploy a positivist case study method to examine the proposed relationships. We collected qualitative data through interviews from the project managers of client organizations as well as from the project managers of vendor organizations to test our proposed model. The result shows that the code of conduct set by the vendor organizations plays the most effective role in privacy preserving behavior of the vendors' employees.

Keywords

IT offshoring, Data Privacy, Positivist case study

INTRODUCTION

IT offshoring has emerged as a viable strategic option for many Western firms. However, there are several risks that are faced by companies looking to offshore their services. One of the most prominent risks of IT offshore outsourcing is that it often involves transferring various sensitive and Proprietary data overseas and authorizing service providers located in different countries to access and use that data. A study by Gartner group indicated that offshore services, requiring the transfer of personal data, grew by 38 percent in the year 2002-2003(Swartz 2004a). However, there have been several allegations that employees based in foreign countries have stolen data outsourced to the service providers (Wugmeister and Titus, 2009). Due to difficulties related to enforcing privacy laws in foreign countries' courts, privacy has been a major concern in offshore outsourcings decisions (Barwick, 2011) and Even though preserving the privacy of data is a major challenge for the offshoring practice, in the extant literature, we found few instances of comprehensive empirical investigation on the factors that affect privacy preservation of the offshored data. In order to address this gap in the literature, our research is guided by the following research question:

What are the factors that affect the privacy preservation of the offshored data?

Offshore outsourcing might cause political, reputation related and even financial risks because of the misuse of the offshored data (Bank Technology News 2004). For example, a US based bank traced the leak and found that the breach took place through an employee of its outsourcing partner in an Eastern European call center (Lucas 2004). In another incident in 2004, a US based software company found that an employee of its Indian outsourcing partner was trying to sell its intellectual property to a competitor (Dobbs 2004). Such incidents refer to the underlying fact that there are two major aspects in the privacy preservation of the offshored data: first, the conduct of the employees who handle the offshored data; second, the overall privacy preservation of the offshored data. Hence, in this paper we essentially identify the factors that affect the conduct of the employees who handle the offshored data; second, the overall privacy preservation of the offshored data.

In our research, we develop a model by identifying the potential variables that affect privacy preservation of the offshored data. Then we adopt a qualitative positivist case study to confirm the relationship between different identified factors and the privacy preservation of the offshored data. We adopt the guidelines suggested by Dube and Pare (2003) and Shanks (2003) in conducting the positivist case study.

The findings of the research will help to understand the relative effectiveness of different factors which affect the privacy preservation of the offshored data. We believe that with our findings client company t would be able to identify the important factors in privacy preservation behavior of the offshore vendors and their employees. Consequently, this can help them to make necessary adjustments in offshore arrangements. An important aspect of our research is that we study the effects of different factors from both clients' and vendors' perspective. This gives us an opportunity to attain a holistic picture of privacy preservation in offshoring arrangements.

THEORETICAL DEVELOPMENT AND PROPOSITIONS

Offshoring is a type of outsourcing. Offshoring simply means having the outsourced business functions done in another country (Wugmeister and Titus, 2009). In the extant literature, authors used different theoretical lenses to describe the offshoring phenomenon and different aspects of it. One of the theories that has been used most frequently is Institutional Theory (Tate et al., 2009). Institutional theory concerns the study of organizational isomorphism, i.e. the process by which certain processes or routines are adopted by all organizations and therefore gradually attain legitimacy in that field. Unlike decision-making models that focus mainly on economic motivations, institutional theory hypothesizes that organizations might adopt certain practices for legitimacy even in the absence of any economic benefit (DiMaggio and Powell 1983; Meyer and Rowan 1983). This premise is important for our study as it helps us to find out the factors outside the economic factors that influence the behavior of the offshore vendors and their employees.

Conduct of the clients' employees and the privacy preservation of the offshored data

With widespread illegal use of intellectual property, violation of privacy, and breaches in security ethical issues are particularly important in IT today. Interestingly, according to the 2003 CSI/FBI Computer Crime and Security Survey report, employees ranked just below independent hackers and above competitors as likely sources of attack. Moreover, in current state of IT offshoring, in many IT projects people from different parts of the world who belong to different cultural dimensions are participating and a client company in most cases does not have direct control over the privacy preservation behavior of such workforce. Consequently, how these employees make their ethical judgment regarding issues like Intellectual Property Law or privacy preservation, and their consequent behavior are very important factors in preserving the privacy of the data. Therefore, we posit that:

P1: Privacy Preserving Conduct of the vendors' employees positively affects the privacy preservation of the offshored data.

Code of Conduct and Other Requirements Set By The Client

In an outsourcing arrangement, regulatory controls such as legal documents, policies, formal systems, standards and procedures establish the relationship between the client and the vendor as well as specify boundaries (Das and Teng 2001). One of the most important components of any outsourcing deal is the contract which describes the services that a vendor is to provide, discusses financial and legal issues, and essentially becomes the blueprint for the life span of an outsourcing arrangement (Tafti, 2005). One of the major steps that might affect the privacy preservation of the offshored data is the code of conduct set by the client on the vendors, mostly through these contracts. (Internet Business Law Service). The contracts with the vendors should and can include requirements mentioning that the offshore vendor adhere to policies and standards for protecting data to which the outsourcing firm is itself subject, procedures for the offshore provider to follow for notifying the outsourcing firm of privacy breaches, controls to help prevent certain employees and third parties from obtaining access to certain confidential customer data, and language requiring the vendor to conduct regular privacy audits and report the findings to the company. As per suggested by the Internet Business Law services, the agreement should require the vendor to educate employees about the outsourcing company's data-protection and privacy policies, and require the vendor to have employees with access to sensitive data sign confidentiality agreements. Moreover, as there is a trend of subcontracting projects in the several offshore clients to even cheaper location such contract should also include that the vendor may not subcontract in the absence of outsourcer approval of the subcontract, and should give the outsourcing company a right to have the subcontract terminated for inadequate privacy. According to a panel of Internet Business Law lawyers, these clauses in the contract will play an important role in the privacy preservation of the offshored client data.

Moreover, as suggested by Ferrell and Gresham (1981) the rule, regulations and/or guideline such as code of conducts is one of the major factors that affect ethical behavior of the employees. Hence, we posit:

P2a: Code of conducts and other requirements for data protection set by the clients positively affects the privacy preserving conducts of the offshore vendors' employees.

P2b: Code of conducts and other requirements for data protection set by the clients positively affects the privacy preservation of the offshored data.

Code of Conduct and Other Requirements Set by the Vendor Company

To justify the level of investment by both the vendor and the client in an offshoring arrangement, both parties will normally look towards a long term contract (Hoffman, 2006). Therefore, realizing privacy preservation of the offshored data is a major concern for the client company, the vendor companies place rules, regulations and code of conduct for their employees to preserve the privacy of the client data. These rules, regulations and code of conducts might include additional ones in addition to what is required by the client in the contract (Barney,___). Vendor companies have direct control over the people handling the client data and are the authority responsible for enforcing the rule, regulations and code of conducts to preserve the privacy of data. Therefore, we assert that a vendor company placed rules, regulations, code of conduct and other requirements will positively affect the privacy preserving behavior of the workforce.

P3a: Code of Conduct and other requirements for data protection set by the vendors positively affects the privacy preserving conducts of the offshore vendors' employees.

P3b: Code of Conduct and other requirements for data protection set by the vendors positively affects the privacy preservation of the offshored data.

Code of Conduct and Other Requirements Set by the Professional Organizations

If the vendor country does not have "strong" rule of law then it could be inferred that the existing institutions are not effective enough to implement and exercise laws like Intellectual Property Right effectively to ensure the protection of the foreign clients' data. In that scenario, formal rules, regulations, guidelines as well as code of conducts placed by a higher authority will affect the conduct of the employees of the vendors and overall privacy of the clients' data. As there is increasing concerns around data security and privacy in India NASSCOM, one of the most recognized and vocal trade organizations in the information technology (IT) software and services industry in India, has put in place several measures to address data security concerns regarding service provider employees. Many of NASSCOM's roles to an extent reflects India's weak regulatory environment. (Trombly, 2006; Trombly and Yu, 2006). India does not have strong law in place requiring the protections of personal data. Therefore, NASSCOM has introduced "assessment and certification" programs for the new employees in an attempt to fill the regulatory lacking and to discourage illegal and unethical behaviors (The Economist, 2006). In addition to these efforts, NASSCOM has also launched an independent self-regulatory agency to improve privacy and data protection standards for the country's offshore IT services and BPO clients (Precision Marketing, 2006).

Kshetri (2008) suggested that in a developing country where rule of law is "week" or "ignored with impunities" (Bratton, 2007), the professional associations can become more effective in shaping the members' behavior. The effectiveness and the *"success"* of India's National Associations of Software and Service Companies (NASSCOM) in preserving the privacy of the offshored data in India is example of such phenomenon.

Hence, we posit the following:

P4a: Code of conducts and other requirements for data protection suggested by the professional associations in the vendor country will positively affect the privacy preserving conducts of the offshore vendors' employees.

P4b: Code of conducts and other requirements for data protection suggested by the professional associations in the vendor country will positively affect the privacy preservation of the offshored data.

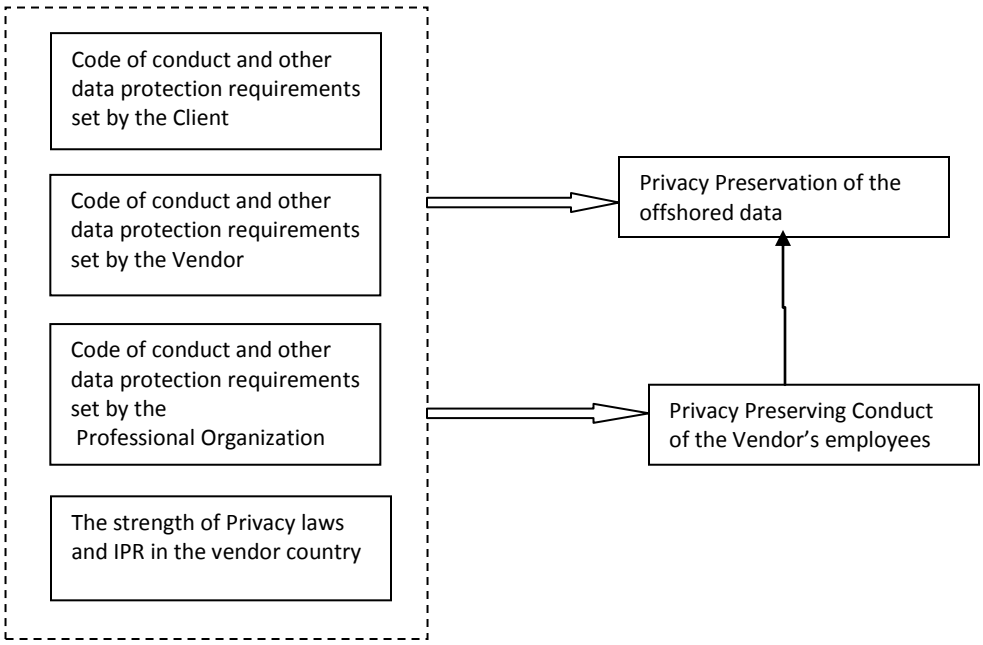

Figure: Research Model

The Strength of Privacy Laws and IPR in the Vendor Country

Intellectual property and privacy of Data are governed by its own distinct national law, which varies from one country to another. Many US and European companies are concerned about privacy preservation of the offshored data as in many of those countries there is weak legislative environment and it difficult to enforce privacy (Engardio et al., 2004; Ravindran, 2004). In outsourcing, U.S. privacy legislation is quite lenient relative to European Union regulations. U.S. privacy protections effectively end at the border, placing the obligation directly and solely on the shoulders of the U.S. client company if there is any privacy breach offshore. However, European consumers are afforded considerably greater protection by an EU law that permits personal data to be sent offshore only to countries whose privacy laws are perceived to provide equivalent privacy protection and that have been found to have strong enforcement capabilities. Essentially as perceived by the EU law, the Privacy protection law and Intellectual property law in the vendors' country will help them to protect the privacy of the offshored data. Hence, we posit:

P5a: The strength of Privacy preservation law in the vendor country will positively affect the privacy preserving conducts of the offshore vendors' employees.

P5b: The strength of Privacy preservation law in the vendor country will positively affect the privacy preservation of the offshored data.

RESEARCH APPROACH AND METHODOLOGY

The use of case study research to test theory requires the specification of theoretical propositions and related testable propositions derived from an existing theory. The results of case study data collection and analysis are used to compare the case study findings with the expected outcomes predicted by the hypothesis (Cavaye, 1996).

The positivist studies are epistemologically premised on the existence of prior fixed relationships within phenomena which could be identified and tested using "*hypothetico-deductive*" logic and analysis (Dubé & Paré, 2003).

Propositions are tested by comparing their predictions with observed data. In order to test the propositions through deductive testing, as per suggestion by Lee (1989), we look for observations that confirm a prediction to establish the truth of a proposition as well as we involve looking for disconfirming evidence to falsify proposition. Falsified propositions are might need to be refined based on the reasons for falsification and subjected to further empirical testing (Shank, 2002).

Our research is positivist in nature and therefore it is very important that we satisfy the four criteria of rigor in positivist study: Construct validity, Internal validity, External validity and Reliability (Shanks, 2002). Validity and reliability in positivist case study research involves using clearly defined methodological guidelines to ensure construct validity, internal validity, reliability and external validity (Lee 1989; Yin 1994). In addition, as per suggestion by Sarker and Lee (2003), we adopt a ‘‘realist’’ ontology in our positivist case study.

Brief Description of the Selected Organizations and the Interviewees

Organization A is an information technology Services Company in India with more than 100 thousand professionals. It has offices in 22 countries and development centers in India, China, Australia, UK, Canada and Japan. In 2009, organization A has been identified as one of the best performing and innovative companies in the software and services sector in the world by Forbes and Business Week.

Organization C is an American multinational corporation that designs and sells consumer electronics, networking and communications technology and services. C has more than 65,000 employees and annual revenue of more than 36 billion dollars. C has more than 190 branches worldwide.

Organizations A and C are in different offshoring arrangements for various IT services, C as client and A as offshore vendor, for more than a decade.

We interviewed 3 managerial level persons from organization C. All these managers have been overseeing IT offshored projects for several years and working extensively with the vendor organizations in India. While one of them no longer are responsible for overseeing offshore projects because of his recent promotion and change in job description, others are still managing and overseeing more than one ongoing offshored projects with Indian vendors.

On the vendor side, we were able to conduct 3 managerial level individuals from organization A. All of them are involved in managing US clients’ IT projects and have worked on such project in different capacities. The interviewees have worked on different sorts of offshored IT projects such as product development, testing and sales management.

Data Collection and Analysis

Our principal data collection method is semi-structured interviews. Each of the interviews lasted around 25-50 minutes on an average. We recorded the interviews whenever possible and transcribed before starting the data analysis. To enhance the validity of the answers, wherever possible, we verified summaries of the major findings with the interviewee after the end of each interview session. Furthermore, to ensure consistency and reliability, we used structured interview guides for all interviews. The interview guide includes several open format questions based on our research model which is based on existing literature. However, to allow the participants flexibility in their responses, we used open ended questions.

PROPOSITIONS TESTING RESULTS AND DISCUSSION

The results of propositions testing have been presented in the following section and summary of the results has been presented in table1.

P1: Conduct of the Vendors' Employees and the Privacy Preservation of the Offshored Data.

Even though this proposition is intuitively "obvious" to an extent, we wanted to confirm the relationship empirically. Interestingly, while we found support for this hypothesis, it was not as strong as we anticipated. We identified two reasons for that.

First, the vendor organization's management perceives that with the proper technology in place it is easy to keep track of employees' action and to restrict what an employee is allowed to do with data.

We have noticed similar sort of response from the client organization's management. They also emphasized the importance of the relationship and the trust in the vendor. As in our sample, both the client and the vendor organizations have a quite a long history of working together in offshoring arrangement, apparently the client organization trust more on the vendor organization and its management rather than being too much concerned about the individual employee working on a project. For most of the offshoring arrangements, there is a person from vendor organization who serves as the local project manager. In most cases, the project manager in client organization, who is project manager of the overall project too, communicates through that local project manager. Unless otherwise it becomes very necessary for certain projects and project situations, the client side project managers do not communicate with the offshore team members on day to day basis. A project manager from client organization describes,

I hardly ever interact with the offshore members in the project directly. Most of my communications are with the local project manager from A (i.e. pseudo name for the vendor organization). Sometimes I think the people working under him are not even sure whether he is working on a project with us or A.

Therefore, apparently it is very important that the client and the client side project managers have a good level of trust on the offshore vendor's project manager rather than each individual person in the offshore team. In fact, there is a very interesting comment made by one of the client side project managers:

Even though I am the project manager and the team lead, due to the nature of the project he (the vendor side project manager) has access to more sensitive data than me.

Hence, how that vendor side manager deals with the client data is very important to preserve the privacy of the offshored data rather than each individual team member.

P2: Guidelines and Code of Conducts Set by the Client and Privacy Preservation of Offshored Data

We have some interesting conflicting findings on these propositions. While from the client's perspective we have found strong support for this proposition, we did not get ample support from the vendors' point of view. The managers of the client organizations think that the requirements such as code of conducts for employees they impose on the vendor side through the contact they sign with the vendors plays the most important part in protecting their data from any sort of misuse when they offshore them. The managers identified three major aspects of any contract that they thought plays the most important role in protecting their data. They are:

First, as per the contract, if a vendor organization fails to protect client organization's data then the vendor will pay a large monetary penalty to the client organization. A project manager from client organization mentions:

If somehow they (the vendor organization) fail to meet the requirements mentioned on the contract, they have to pay us (the client organization) a huge amount of fine.

Second, the client organization ultimately has the authority to decide who will work on the project and who from the vendor organization will have access to the data. As a project manager mentions,

Contract requires them (i.e. vendor organization) to have clearance for every employee they use in my project from me.

Third, most of the contracts are short term. Hence, in order to keep on renewing the contract, the vendor organization has to keep the client data safe which is one of the requirements of the clients. A project manager mentions,

Most of our contracts are only 3 months long initially. The contract gets renewed for another 3-6 months based on the performance in those 3 months. So if I am not convinced with the safety of my data then I will not renew the contract.

On the other hand, the management of vendor organization thought that the aspects mentioned by the clients are important. But what matters most is the guidelines, code of conduct, rules and regulations they have in place to protect any sensitive data. Interestingly, it appeared to us that the managers from the client organization felt almost offended when we emphasized the importance of clients' suggested guidelines and code of conducts for protecting data.. According to the vendor organization, they have enough sensitive data of their own and they need to protect that from competitors or any other unauthorized users and uses. Hence, to protect data, they make sure all the employees working for them abide by the code of conduct and other rules and regulations. As a manager explains,

We have to eat our own dog food you know. We have those data security and privacy measures in place for our information too as we need to protect the sensitive information from the outsiders.

They also thought that their employees do not interact with the client organizations' representatives frequently enough to be driven by their code of conducts. However, they admitted that the manager who is working on behalf of the vendor organization might take extra effort to convince the clients about the integrity of their (client's) data. To do so, as one of the managers from client side has described, it can become *"sand is hotter than the sun"* scenario. One of the examples a manager provided is like this-

When one of the employees working with client's data ran a query who is not supposed to run by mistake, that employee got fired immediately. Finding no other way, that employee contacted the manager from the client organization, describing the scenario and how he did it by mistake and not with any bad intention. Under the circumstances, the manager from the client company thought it was little "too harsh" and recommended giving back his job.

Examples like these let us to conclude that while guidelines and code of conduct set by a client are important for the vendor organization to an extent; however, they are not the most influential factor in privacy preserving behavior of the employees as the client organizations do not and/or cannot implement those directly in most cases.

P3: Guidelines and Code of Conducts Set by the Vendors and Privacy Preservation of Offshored Data.

We have found the strongest support for this set of propositions. Both client and vendor organizations thought that code of conducts set by the vendor organizations are the most influential factor. From vendor's point of view, they thought as they are the party who are responsible for enforcing any code of conduct as well as rules and regulations, they are the most influential factor no matter whether those rules have been proposed by a client or a professional organization or vendor country. They emphasized that in most cases their employees are not aware or concerned about from whom the guideline, code of conduct or rules and regulations have been originated. What matters to them most is that in order to work for that vendor organization (and in some cases in certain projects), they have to abide by those rules, regulations and code of conducts; otherwise, they see job loss or other sort of punishment carried out by the organization they are working for i.e. the vendor organization as the immediate effect.

The client organization to a large extent had similar opinion. They emphasized that while based on the nature of the project and the sensitivity of the data, they might want the offshore vendor to take additional measures to protect their data, the vendors are responsible for putting them in place. The representatives from client organizations also mention that the code of conduct for employees and other rules and regulations they want to be place are through contract they sign and in most cases they are not involved in the micro management of actually making sure they are implemented and followed properly. However, they have emphasized that it is largely because they have been working with a particular offshore vendor(s) for a long time and they have mostly positive experience up to that point. But, for an entirely unknown offshore vendor this scenario could be different.

P4: Rules and Regulations Imposed by the Professional Organizations and Privacy Preservation of the Offshored Data.

We have not found ample evidence to support Propositions H4a and H4b. Neither the client side nor the vendor organization thought that professional organizations have a very strong role to play in the privacy preservation in the current state of the offshoring arrangements between USA and India. Surprisingly, it has appeared to us that client

organization are very little aware of the role of the most prominent professional organization of India NASSCOM. They know that it is a there and it plays a certain role internally. However, interviewees from the client side did not think that professional organization would play a significant role in preserving privacy of their data. As a project manager from client organization mentions,

Yes. I know about NASSCOM. However, I am not so sure how effective they are in preserving the privacy of our data.

On the other hand, the interviewees from the vendor organization had interesting perspective. They thought professional organization like NASSCOM could play an important role in privacy preservation of the client data. However, they did not think it plays a significant role in affecting the privacy preserving behavior of their employees and their organization as they thought they have already strong rules and regulations to protect their data as well as client data.

The managers of vendor organizations provided examples regarding employee screening process and the behavioral guideline they have in place claiming that these processes are stronger than what a professional organization suggests. However, they thought it might help relatively newer organizations to shape up rules and regulations in a way that would help them to protect client data. Not only that, they thought for overall offshoring environment the professional organizations can play a very important role in protecting client data.

Propositions	**From Clients' Perspective**	**From Vendors' Perspective**
P1: Behavior of the vendors' employees	Moderate Support	Moderate Support
P2: Rules by Client	Supported	Moderate Support
P3: Rules by Vendor	Supported	Supported
P4: Rules by professional organization	Moderate Support	Moderate Support
P5: The strength of privacy preservation law in vendor's country	Moderate Support	Supported

Table1: Summary of the propositions testing

P5: The Strength of Privacy Preservation Law in the Vendor Country and Privacy Preservation of the Offshored Data.

We have found fairly strong support for this set of propositions. The client organization's management thought having a strong privacy preservation law will definitely affect the privacy preserving conducts of the offshore vendors and their employees. As mentioned by a project manager from client organization, *"It certainly makes us feel more comfortable if we know that there is strong privacy preservation law in that (i.e. vendor's) country"*. One thing was quite apparent that while the client organizations thought that having strong privacy preserving law would help and that was somewhat a concern in the beginning of the offshoring arrangements, over the time as they have worked with certain offshore vendor(s) and had mostly positive experience with the vendor(s), the strength of privacy preservation law in the vendor country has become less concern for them. A project manager from client organization mentions

…… over the time we have come to know some key persons in vendor organization and we rely on them.

On a similar note, we asked them about their Indian offshore vendor's practice of offshoring to China where arguably privacy preserving laws is weaker than India and whether that concerns them or not. Their response was that they trust their offshore vendor and rely on the contract that they have with them. So no matter to where their Indian offshore vendors send their works to get it done, they are the responsible party and will be held accountable for any sort of misuse of data. However, as per their contract, the offshore vendors have to get clearance from their

client for each of the team members who will have access to their sensitive data. Hence, if a vendor organization in India wants to involve team members from China then they have to get clearance from their clients. But as a project manager mentions,

Contract requires them (i.e. vendor organization) to have clearance for every employee they use in my project from me. However, in most cases it becomes merely a formality as I know him (i.e. the project manager/representative on vendor's side) and sort of think that he will make a right judgment. In any case, if anything goes wrong they would be held responsible.

The vendor organizations thought that having a strong privacy preservation law will definitely help. The managers of the vendor organizations thought that the most of the people they hire have a very vague or no idea about what conduct would be an invasion of privacy as they grow up in a society and gets education in system where sensitive things like intellectual property law and privacy preservation law either do not exist or not practiced properly. Therefore, the management of the vendor organization thought that it becomes a quite steep learning curve for the newly hired workforce to get accustomed to the all the new rules and regulations they have to follow to preserve the integrity of any data they would handle. The vendor organization from India thought they face the similar change when they hire people from China as they also grow up in a weaker "rule of law" country. So having an environment where there is a strong "Rule of Law" to protect data or any intellectual property will definitely positively affect the privacy preserving behavior of the people they would hire to work in projects and that in turn will increase the safety of data.

CONCLUSION AND FUTURE WORK

While offshore outsourcing certainly has its benefits, it comes with a risk of misuse of sensitive information. There are different institutional factors that might affect the privacy preservation of the offshored data. In our study, we have identified the mimetic, coercive, and normative institutional factors that would affect the privacy preservation of the sensitive offshored data and empirically tested their effectiveness. The findings show that the code of conduct set by the offshore vendors play the most important role followed by the code of conduct set by the clients and the strength of privacy preservation law in the vendor's country.

The findings of our research have shed light on an important aspect of the literature as we have included both client and vendor managements' perspective to verify the effects. However, one limitation of our finding is that the client and vendor organizations in our case study are industry leaders and very well reputed firms and have been in offshoring arrangement with each other for at least last 10 odd years. Hence, it has appeared to us that to a large extent the response from client management is based on the trust they have in the vendor organization and it might change if they get into an offshoring arrangement for a relatively new company. So in order to address this problem we intend to have more than one vendor organization with varied level of reputation in the market.

REFERENCE

Ackroyd, S& Hughes, J.A.,1992 Data Collection in Context, Longman, New York, 1992

Aubert, B. A., Rivard, S., & Patry, M. (2004). A transaction cost model of it outsourcing.

,Information & Management, 41(7), 921-932

Bender, D., 2007, Internet Law - Outsourcing Offshore May Pose Problems for Protecting Data, (http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1635)

Bommer, Michael, Clarence Gratto, Jerry Gravander, and Mark Tuttle. 1987. A Behavioral Model of Ethical and Unethical Decision Making., Journal of Business Ethics 6: 265-280

Bratton, M. ,2007, Formal versus informal institutions in Africa, Journal of Democracy 18(3): 96-110.

Culnan, Mary J. and Williams, Cynthia C.. 2009. How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches, MIS Quarterly, (33: 4) pp.673-687.

DiMaggio. J & Powell. W.1983, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, American Sociological Review, Vol. 48, No. 2, 147-160. Apr.,.

DiMaggio. J & Powell. W. (eds). 1991. The New Institutionalism in Organizational Analysis. Chicago: University of Chicago Press

Eisenhardt,K 1989, Building Theories From Case study Research, The Academy of Management Review, Vol. 14, No. 4. (Oct., 1989), pp. 532-550.

Engardio, P., Puliyenthuruthel, J., Kripalani, M., ,2004. Fortress India?, Business Week 3896, 42–43 (August 16)

Ferrell and Gresham, 1985, A contingency framework for understanding ethical decision making in marketing, Journal of Marketing, 49 (3), 87-96.

Gurbaxani, V. (2007), Information Systems Outsourcing Contracts: Theory and Evidence, Managing in the Information Economy: Current Research, (U. Apte, U. Karmarkar, eds), Kluwer

Haines, R. & Leonard , LNK Individual Characteristics And Ethical Decision-Making In An IT Context, Industrial Management & Data Systems, 2007

Haines, Russell and Lori Leonard. 2007. Situational Influences on Ethical Decision-Making in an IT Context., Information and Management, 44(3), 313-320.

Hunt SD, Chonko LB, 1984, Marketing and Machiavellianism, Journal of Marketing,

Hofstede, G. 1984,Culture's Consequences. Beverly Hills. Sage.

Hunt, SD & Vitell,S , 198 6, A General Theory of Marketing Ethics, Journal of Macro marketing

Jackson, D, Stern, A. 2006, Screening the Offshore Outsourcing Provider's Employees, FAO Today, May, 2006

Jose and Baruah, 2010, Indian IT players find China a profitable hub, The Financial Express,Feb 8, (http://www.financialexpress.com/printer/news/576833/)

Klaas, B.S., McClendon, J., and Gainey, T. (2001) 'Outsourcing HR: The impact of organizational characteristics' Human Resource Management, Vol. 40, Iss.2, pp 125

Koh, C., Soh, C., Markus, M.L. 2000,A process theory approach to analyzing ERP implementation and impacts: the case of Revel Asia, Journal of Information Technology Cases and Applications 2 (1), 2000, pp. 4–23.

Kundu, S.K., Jain, N.K., & Niederman, F. ,2007,Explaining propensity toward offshoring in information technology industry: A firm and country level analysis., Academy of International Business, Indianapolis,

Kshetri, N. 2007, Institutional factors affecting offshore business process and information technology outsourcing , Journal of International Management,

Kshetri, N. and Dholakia, N., 2009. Professional and trade associations in a nascent and formative sector of a developing economy: A case study of the NASSCOM effect on the Indian offshoring industry. Journal of International Management 15 225–239

Kundu, S.K., Jain, N.K., & Niederman, F. Explaining propensity toward offshoring in information technology industry: A firm and country level analysis. Academy of International Business, Indianapolis, 2007.

Lee,A. 1989, A scientific methodology for MIS case studies, MIS Quarterly 13 (1), 1989, pp. 33–50.

Mason, R. ,1986. Four ethical issues of the information age, MIS Quarterly, 10, pp. 5-12.

Milberg et al 2007, supra note 179.

Meyer, J. W., & Rowan, B. ,1983,. Institutionalized organizations: Formal structure as myth and ceremony. In W. Meyer, B. Rowan, & T. E. Deal (Eds.), Organizational environments ritual and rationality

(pp. 21–44). Beverly Hills, CA: Sage Publications

Moores, T. T. and Chang, J. C. J. 2006, Ethical Decision Making in Software Piracy: Initial Development and Test of a Four-Component Model. MIS Quarterly, Vol. 30, No. 1, 2006, pp. 167-180.

Orlikowski, W., 1993, CASE tools as organizational change: investigating incremental and radical changes in systemsdevelopment, MIS Quarterly 17, 1993, pp. 309–340.

Overby, S., 2010, Offshoring: The 25 Most Dangerous Cities for Outsourcing in 2010, CIO.com(http://www.cio.com/article/596533/Offshoring_The_25_Most_Dangerous_Cities_for_Outsourcing_in_2010)

Oxley,J & Yeung , B. 2001, E-commerce Readiness: Institutional Environment and International Competitiveness, Journal of International Business Studies, Vol. 32 No. 4

Palvia,P., King, R., Nemati, H." Offshoring control mechanism: Vendors' Perspective" Working paper

Ravindran, P., 2004. Factors that are worrisome for BPO sector. BusinessLine 1 (April 3)

Robin, DP& Reidenbach, RE Social Responsibility, Ethics, and Marketing Strategy: Closing the Gap between Concept and Application, Journal of Marketing, 1987

Roche,E & Palvia, P & Palvia, S, Global Information Technology and Electronic Commerce,2007

Roy,R. and Davidson, R., Technology trends to watch: 2011-2020, WiseTechnology (http://wistechnology.com/articles/8210/)

Sarker, S. & Lee, A. 2002 Using positivist case research methodology to test three competing theories-in-use of business process redesign, Journal of AIS 2 (7), 2002, pp. 1–72.

Swinyard, W. R., Rinne, H., & Kau, A. K. 1990. The morality of software piracy: a cross-cultural analysis. Journal of Business Ethics, 9(8), 655-664

Swartz, N.,2004, Offshoring Privacy, Information Management Journal, 38 (5) September/October, pp.24-26

Tate, W., Ellram, L. Bals, L.(2009) Offshore outsourcing of services: An evolutionary perspective, International Journal of Production Economics, Volume 120, Issue 2, August 2009, P512-524

The Economist, 2006. Special report: watch out, India — outsourcing to China. Outsourcing to China, 379 (8476), 80, May 6

Trombly, M., Yu, W., 2006. Outsourcing resilient in India, Securities Industry News 18 (26), 1–21 (July 10)

Van Maanen, J, 1988,Tales of the Field: On Writing Ethnography, University of Chicago Press, Chicago, 1988.

Vitell,S & Nwachukwu, SL & Barnes, JH, 1993,The effects of culture on ethical decision-making: An application of Hofstede's Typology , Journal of Business Ethics,

XMG, 2009, Outsourcing Year-end Revenue Forecast, Press Release by XMG,2009

Yin, R., 1994 Case Study Research: Design and Methods, Sage, Thousand Oaks, CA, 1994.

Zey-Ferrel, M. (ed.),1979, Readings on Dimensions of Organizations, San Francisco: Goodyear, pp. 59-82*Note:*