Volume 24 (2) October 2017 ISSN 0216-423X

JABM
JOURNAL of
ACCOUNTING - BUSINESS & MANAGEMENT

Journal of Accounting – Business & Management vol. 24 no. 2 (2017) 70-83

Determining the Factors and Their Relative Effect on Offshored Data Privacy: Client and Vendor Perspectives

Anupam K. Nath*

Abstract

Offshoring of services has become an inevitable part of business strategy. While businesses are deploying service offshoring for quite some time now, 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-preservation of the offshored data and the 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 semi-structured interviews with the project managers of client organizations as well as from the project managers of vendor organizations to test the proposed model. The result of our study shows that the code of conduct set by the vendor organizations plays the most effective role in the privacy-preserving behavior of the vendors' employees.

Keywords: IT offshoring, data privacy, positivist case study.

I. INTRODUCTION

Offshoring of IT services has emerged as a practical strategic option for many Western firms. However, these firms looking to offshore their services face several risks (Polak & Wójcik, 2015). One of the most prominent risks of IT service offshore outsourcing is that it often involves transferring various sensitive and propriety data overseas and authorizing service providers located in different countries to access and use that data (Palvia, 2017). There have been several allegations that vendor's employees based in foreign countries have stolen data outsourced to the service providers.While such incidents are quite common, due to limitations related to enforcing privacy laws in foreign countries' courts, privacy has always been a major concern in offshore outsourcing decisions (Barwick, 2011). Offshore outsourcing might cause political, reputation, and even financial risks because of the misuse of the offshored data (Bank Technology News, 2014). For example, recently a US-based organization's breach took place through the employee(s) of its outsourcing partner in an offshore law firm (Zelijka, 2017). Such incidents refer to the underlying importance of offshore vendors' employees' role in the 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.

While preserving the privacy of data is a major challenge for the offshoring practice, in the extant literature, we found diminutive instances of comprehensive empirical investigation of the factors that affect privacy preservation of behavior of the vendors' employees and overall privacy preservation, especially from both client and vendor's perspective in the same study. Our research primarily addresses this gap in the literature through the following research question that guides our research:

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

* Georgia Gwinnett College, Georgia, USA. E-mail: anupamknath@gmail.com.

In this research, based on the existing literature 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 Dubé and Paré (2003) and Shanks (2002) in conducting the positivist case study.

The findings of the research have practical implications. As we understand the relative effectiveness of different factors which affect the privacy preservation of the offshored data, we believe that based on our findings client company would be able to identify the vital factors in privacy preservation behavior of the offshore vendors and their employees. Subsequently, this can help them to make necessary adjustments in offshore arrangements. A vital and unique aspect of our research is that we study the effects of different factors from both clients' and vendors' perspective. Having both views give us an opportunity to attain a holistic picture of privacy preservation in offshoring arrangements.

II. THEORETICAL DEVELOPMENT AND PROPOSITIONS

Offshoring is a type of outsourcing. Offshoring simply means having the outsourced business functions done in another country (Nath & Bejou, 2012). In the extant literature, authors used different theoretical lenses to describe the offshoring phenomenon and various aspects of it. Among them, Institutional Theory is one of the most frequently used theoretical lenses (Tate et al., 2009). Institutional theory concerns the study of organizational isomorphism, i.e., the process by which specific procedures and 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 specific practices for legitimacy even in the absence of any financial benefit (Meyer & Rowan, 1977; DiMaggio & Powell, 1983). This premise is vital for our study as it helps to identify the factors outside the economic factors that can influence the behavior of the offshore vendors and their employees.

2.1. Conduct of the Clients' Employees and its Effect on Privacy Preservation of the Offshored Data

Illegal use of intellectual property, privacy violation, and breaches in security are widespread in current IT world. Hence, ethical issues are particularly important in today's business environment. 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. A recent FBI Cyber Security Report also reiterates the employee as a potential threat to data security (Comey, 2016). Moreover, in many IT projects people from different parts of the world who belong to different cultural dimensions are participating as the current state of IT service offshoring. Usually, a client company possesses no direct control over the privacy preservation behavior of vendor's workforce (Nath & Bejou, 2012). Consequently, how these employees themselves make their ethical judgment regarding issues like Intellectual Property Law or privacy preservation, and their following behavior is a critical factor in preserving the privacy of the data. Therefore, we posit that:

P_1: privacy-preserving conduct of the vendor employees positively affects the privacy-preservation of the offshored data.

2.2. Code of Conduct and Other Requirements by the Client

An essential aspect of making an outsourcing arrangement requires including regulatory controls. Such regulatory controls can include but not limited to legal documents, policies, formal systems, standards, and procedures. These regulatory controls establish the relationship between the client and the vendor and also specify boundaries (Lee, 1996). One such vital mechanisms of any outsourcing deal are the contract between the client and the vendor. The contract serves as a blueprint for the lifespan of an outsourcing arrangement that includes the services that a vendor is to provide. It also discusses financial and legal issues of that arrangement (Lee, 1996).

According to Business Law Service, a significant step that can affect the offshored data's privacy- preservation is the code of conduct established by the client for the vendors. Such code is mostly implemented mostly through the contracts between vendor and client. The contracts with the vendors can include several requirements. This requirement usually mentions that the offshore vendor adheres to policies and standards required for protecting data to which the outsourcing firm is itself subject. In addition, the contract includes (a) procedures for the offshore provider to follow for notifying the outsourcing firm of privacy breaches, (b) controls to help prevent certain employees and third parties from obtaining access to certain confidential customer data, and (c) requirement that the vendor to conduct regular privacy audits and then the findings of the report to be shared with the client company. Internet Business Law services suggest that the contract between a client and vendor should include the requirement that the vendor needs to educate employees about the outsourcing company's data protection and privacy policies, and also requires that the vendor's employees with access to sensitive data have to sign confidentiality agreements. In the current offshoring state in the world, there is a trend of subcontracting of projects to an even cheaper location(s) by vendors. Hence, a contract between client and vendor should also include that the vendor may not subcontract in the absence of outsourcer approval of the subcontract, and give the outsourcing company a right to have the subcontract terminated for the lack of adequate privacy. According to a panel of Internet Business Law lawyers, the inclusion of such clauses in the contract can play a vital role in the privacy preservation of client data that has been offshored.

Moreover, as suggested by Ferrell and Gresham (1985), the rules, regulations or guidelines like a required code of conducts is one of the significant factors that affect the ethical behavior of the employees. Hence, we posit:

P_{2a}: code of conducts and other requirements for data protection set by the clients positively affects the privacy-preserving behaviors of the offshore vendors' employees.

P_{2b}: code of conducts and other requirements for data protection set by the clients positively affects the privacy preservation of the offshored data.

2.3. Requirements Set by the Vendor Company

An offshoring arrangement requires a considerable investment of resources from both the client and the vendor company. To justify the level of investment both parties usually look towards a long-term contract (Lee, 1996). In such arrangement data sharing is necessary and preserving the privacy of their data is a significant concern for the client company. Realizing this, the vendor companies place different types of rules, regulations for their employees to preserve the privacy of the client data. Such rules, regulations, and code of conducts include the ones required by the client as well as

might also include additional ones needed by themselves (Barney, 1991). Vendor companies are the one who assumes direct control over the people handling the client data. They are also 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.

P_{3a}: code of Conduct together with other data protection requirements by the vendors positively affects the privacy-preserving behaviors of the offshore vendor employees.

P_{3b}: code of Conduct together with other requirements for data protection by the vendors positively affects privacy preservation of the offshored data.

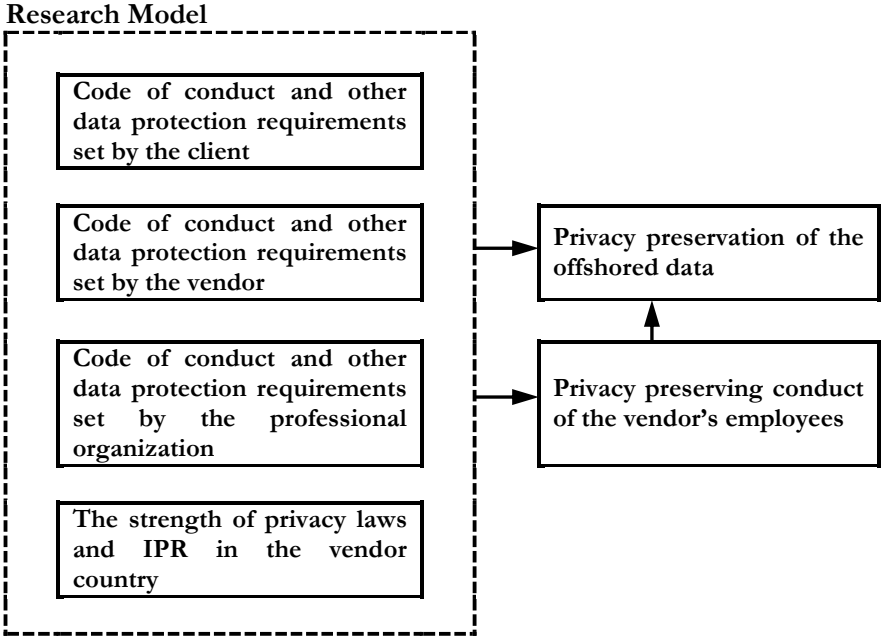
2.4. Requirements set by the Professional Association(s) in the Vendor Country

For a country with"weak" rule of law, it can be inferred that the existing institutions might not be effective enough. Subsequently, those institutions do not 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 a code of conducts placed by a higher authority, can affect the conduct of the employees of the vendors and overall privacy of the clients' data. One such example is the National Association of Software and Services Companies (NASSCOM) from India. NASSCOM is a trade association of Indian Information Technology and Business Process Outsourcing industry. It is one of the most recognized and vocal trade organizations in the information technology (IT) software and services industry in India. There have been increasing concerns around data security and privacy in India. To address this issue and to sustain the growth, NASSCOM has inaugurated several measures to address data security and privacy concerns regarding service provider employees. Many of NASSCOM's roles to an extent reflects India's weak regulatory environment. (Trombly & Yu, 2006). As India does not have a strong law in place requiring the protection of personal data, NASSCOM has implemented "assessment and certification" programs for the new employees. This effort essentially is in an attempt to fill the regulatory lacking as well as to discourage illegal and unethical behaviors (The Economist, 2006). Together with these efforts, NASSCOM has also established a self-regulatory agency in the early 2000s. The goal of this agency is to improve privacy and data protection standards for the country's offshore IT services and BPO clients. Subsequently, Kshetri & Dholakia (2009) suggested that in a country with "weak" rule of law, a professional associations can become very effective in shaping the members' behavior. The effectiveness and the *"success"* of India's NASSCOM in preserving the privacy of the offshored data in India is an example of such phenomenon. Hence, we posit the following:

P_{4a}: code of conducts and other requirements for data protection suggested by the professional associations in the vendor country will positively affect the privacy-preserving behaviors of the offshore vendors' employees.

P_{4b}: 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 1
Research Model



2.5. The Strength of Privacy Laws and IPR in the Vendor Country

Every country governs Intellectual property and privacy of Data based on own distinct national law. These laws vary from one country to another. Many US and Europe-based companies are concerned about privacy preservation of the offshored data as in many of those countries there is a weak legislative environment and it is challenging to enforce privacy (Engardio et al., 2004; Ravindran, 2004). In outsourcing, North America's privacy legislation is more lenient in comparison to European Union (E. U.) regulations. North American privacy protection effectively ends at the border and places the obligation directly and solely on the shoulders of the client companies. If there is any privacy breach offshore, client organization and their home country are responsible for taking any necessary action. However, European consumers have considerably greater protection by an E. U. law. As per E. U. law, an organization can send personal data to offshore only to selected countries in which privacy laws are perceived to provide equivalent privacy protection. E. U. law also requires the vendor's country to have strong law enforcement capabilities. Such requirement by E. U. law essentially reflects that the Privacy Protection law and Intellectual property law in the vendors' country will help to protect the privacy of the offshored data. Hence, we posit:

P_{5a}: the strength of Privacy preservation law in the vendor country positively affects the privacy-preserving conduct of the vendor's employees.

P_{5b}: the vendor country's Privacy preservation law strength positively affects the privacy preservation of the offshored data.

III. RESEARCH APPROACH AND METHODOLOGY

A positivist case study research can be used to test theory(s). To use case study research in testing theories, the first step is to specify a set of theoretical propositions derived from existing theory, and based on those related propositions that are testable. After the data collection and analysis, the findings are used to compare the case study findings with the expected outcomes as predicted in 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. 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 the proposition. Falsified propositions might need to be refined based on the reasons for falsification and subjected to further empirical testing (Shank, 2002).

We deploy a qualitative positivist case-study approach to test the propositions. Our adoption of positivism is consistent with the views that are held by scholars in the fields of organizational studies (Eisenhardt, 1989), and information systems (Lee, 1989; Orlikowski & Baroudi, 1991; and Sarkar & Lee, 2002) and follows a similar path. "hypothetico-deductive logic" is central to the world of positivist research today (Lee, 1989), which necessarily is a synthesis of three traditions: empiricist, rationalist, and critical rationalist (Sarker & Lee, 2002). There is an empiricist influence in our positivist approach that is reflected in the rigor of our research process, drawing mainly on Yin (1994). The rationalist and the critical-rationalist traditions are reflected in the use of pattern matching to deductively test falsifiable statements derived from the literature (Sarker & Lee, 2002).

As this research is principally positivist in nature, using clearly defined methodological guidelines we satisfy the four criteria of rigor (Shanks, 2002): construct validity, internal validity, external validity, and reliability (Lee, 1989; Yin, 1994). In the following table, we summarize how we address the requirements of the positivist case-study method.

Table 1

Plan to Achieve Rigor of the Study as per Positivist Case

Steps to Achieve Rigor of the Study as Per Qualitative Case-Research Criteria	
Rigor Criterion	Guidelines to achieve rigor based on Lee (1989), Yin (1994), and Sarker & Lee (2002)
Construct validity	Use of multiple sources of evidence. Review of the report by the key informants. Chain of evidence.
Internal validity	Pattern matching
Reliability	Case-study database (consists of case-study notes, documents, and narratives) creation and maintenance. Case-study protocol.
External validity	Increased degree of freedom. Replication logic

Based on this plan, we collect data to test the proposed propositions.

3.1. Case Selection and Brief Description of the Selected Organizations and the Interviewees

Case selection is a critical aspect of conducting a case study. Not only does the population define the set of entities from which the research sample is to be drawn, but the selection of an appropriate population also controls extraneous variation and helps to define the limits for generalizing the findings (Eisenhardt, 1989). According to the recommendations by George and McKeown (1985), Eisenhardt (1989) and Yin (2003)

we based the case selection for our study on two factors - theoretical background and feasibility.

The first factor includes theoretical relevance, purpose, similarities, and differences across data sources with regard to the data sources' appropriateness for the study. In our case, we want to study uses and effects of Web 2.0 based KM at the group levels. Hence, we selected two organizations which have been part of the offshore arrangement for a sufficient length of time to identify and understand the effects of different factors related to privacy preservation of data. Both organizations are leading firms in their respective fields in the IT industry and have branches or offices in many countries. However, they are different regarding the role they play in an offshoring arrangement. While organization A is offshore vendor dealing with client data, organization C is the client. The second factor, feasibility, was largely determined by each organization's willingness to participate in the study and to provide the required information. In our research, the organizations we selected had to be willing to provide us the necessary information and share their experience so that we could study the effects of different factors regarding privacy preservation.

Organization A is India based company that provides information technology services. The company has 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 is recognized 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 United States based multinational corporation. Organization C's primary business is to design, manufacture, and sell consumer electronics, networking and communications technology and services. It has more than 65,000 employees at different levels and annual revenue of more than 36 billion dollars. Even though North America based, C has establishments in more than 160 countries in the world.

Organizations A and C are in many IT services offshoring arrangements. Organization C has been a client of organization A for more than fifteen years.

We interviewed three managerial level persons from organization C. The interviewed managers have been overseeing IT offshored projects for several years. Moreover, they have worked extensively with the vendor organization C in India. While one of the interviewees no longer is responsible for overseeing offshore projects because of his recent promotion and change in job description, others are still managing and supervising more than one ongoing offshored projects with Indian vendors.

On the vendor side, we could also include three managerial level individuals from organization A. All of them are involved in managing US-based clients' IT projects and have worked on such project in different capacities. The interviewees have worked on various sorts of offshored IT projects such as product development, testing, and sales management.

3.2. Data Collection and Analysis

Semi-structured interviews are the principal data collection method of our study. Each of these interviews was about 25-50 minutes. We recorded the interviews whenever possible. After completion of the interviews, we transcribed the recordings before starting the data analysis. In next step to enhance the validity of the answers, we cross-checked the summaries of the significant findings with the interviewee after the

end of each interview session. Additionally, to ensure consistency and reliability, we developed a structured interview guide. We used that guide for all the conducted interviews. In our interview guide, we included several open format questions based on our research model. However, as we wanted to allow the participants flexibility in their responses, our questions were open-ended.

As a second data source, wherever possible, we also investigated the internal documents (e.g., draft of contracts) which the organizations use in an offshoring arrangement. Existing literature suggests that it is preferable to have multiple investigators in such case studies. Hence, wherever possible, we made sure that at least two researchers were present for the interviews. A significant characteristic of our research is the overlap of data analysis and collection, and we achieve this through field notes. Overall, we followed the same guidelines we followed in phase1 which was provided by Lee (1989), Yin (2003) and Sarker and Lee (2002) to achieve rigor in our case study.

IV. PROPOSITIONS TESTING RESULTS AND DISCUSSION

We present the results of propositions testing in the following section, and summary of the results in Table 1.

P_1: employee conduct and the privacy preservation of the offshored data.

In the beginning, we thought this proposition is to some extent intuitively "obvious." Still, we wanted to have empirical confirmation. Interestingly, while we found support for the proposition, it was not as strong as we anticipated. Based on our data analysis, we identified two possible reasons for that:

Firstly, the vendor organization's management believes that if the proper technology is in place, then it is possible to keep track of employees' action(s) and restrict what an employee can do with data.

We 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 the 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 the client organization who serves as the project manager of the overall project, make the necessary communications through the vendor assigned local project manager. Usually, the client-side project managers do not communicate with the offshore team members on day to day basis unless otherwise, it becomes vital for specific projects and project situations, As a project manager from client organization mentions,

> *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.*

Hence, it is imperative that the client-side project managers have a high level of trust on the offshore vendor's project manager rather than each member of the offshore team. There is an interesting comment made by one of the client-side project managers that further strengthens our finding:

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.

Henceforth, the manager of the vendor's perception towards client data and management of the client data play the more important role than each of his team members.

P_2: guidelines and code of conducts set by the client and privacy preservation of offshored data.

We have some exciting conflicting findings on these propositions. While we found strong support for this proposition from the client's perspective, we did not get ample support from the vendors' point of view. The managers of the client organizations thought that the requirements such as code of conducts for employees they impose on the vendor side through the contracts they sign with the vendors play the most important part in protecting sensitive data from any 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 significant 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 in the contract, they have to pay us (the client organization) a huge amount of fine.

Second, the client organization is the highest authority in almost all offshoring arrangements. They not only selects the project team members but also decides who will be given access to their data. A client-side project manager states,

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

Third, the contracts between a client and a vendor are mostly short term. Hence, for consistent renewal of the contracts, the vendor organization makes sure the client data is safe as that is one of the major requirements from the clients. As a project manager from the client mentions,

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

The vendor's management did not agree with the client's perspective entirely. They thought that the aspects mentioned by the clients are important. However, they felt that the guidelines, code of conduct, rules and regulations they have in place to protect any sensitive data play the most influential role. Remarkably, it appeared to us that the vendor side managers felt practically offended when during the interview we emphasized the importance of clients' suggested guidelines and code of conducts for data protection. According to the vendor management, they also have their own sensitive data that they need to protect that from any 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. A vendor-side manager states,

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 mentioned that their employees usually do not interact with the client organizations' managers or any other representative frequently enough to have any

significant impact. However, they admitted that the manager who is working on behalf of the vendor organization might take an extra effort to convince the clients about the integrity of the offshored data. Because of that, as one of the managers from client side has described, it can become *"sand is hotter than the sun"* scenario. An interviewee provides one such example:

> *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 lead us to conclude that 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 the privacy-preserving behavior of the employees because the client organizations do not or cannot implement those directly in most cases.

P_3: guidelines and code of conducts set by the vendors and privacy preservation of offshored data.

We found the most substantial support for this proposition. Both client and vendor organizations thought that code of conducts set by the vendor organizations is the most influential factor. From vendor's point of view, they thought they are the party who is responsible for enforcing any code of conduct as well as rules and regulations. Hence, 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 their employees mostly are not aware or concerned about the origin of the guideline, code of conduct or rules and regulations. What matters to them most is that to work for that vendor organization (and in some cases in specific projects), they have to abide by those rules, regulations, and code of conducts. Otherwise, the employee(s) sees job loss or another type of punishment carried out by the organization they are working for as the immediate effect.

The client organization to a large extent had a similar opinion. The project managers 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, finally it is the vendors who are responsible for putting them in place. The client-side managers also mention that the code of conduct for employees and other rules and regulations they want in place are required through the contract they sign. In most cases, the client organization is not involved in the micro-management of the actual implementation of the policies. However, they have emphasized that it is because they have a long history of working with that specific offshore vendor(s) and they have mostly positive experience up to that point. But, for an entirely unknown offshore vendor, this scenario could be different.

P_4: rules and regulations imposed by the professional association and privacy preservation of the offshored data.

In our case study, we did not find sufficient evidence to support this proposition. Neither the client organization nor the vendor thought that professional associations have an influential role to play in the privacy preservation in the current state of the offshoring arrangements between USA and India. Surprisingly, it appeared to us that client organization has very little awareness of the role of the most prominent professional association of India NASSCOM. They know that it exists and also plays a

particular role internally. However, interviewees from the client side did not think that professional association would play a significant role in preserving the privacy of their data. As a project manager from client organization states,

> *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 an interesting perspective. They thought a professional association like NASSCOM could play an essential role in privacy preservation of the client data, especially in "weak" law country. 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 already had strong rules and regulations in place 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 had in place claiming that these are inherently stronger than what a professional association like NASSCOM 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 the professional associations could play a critical role in protecting client data.

Table 2
Summary of the Propositions Testing

Propositions	From Clients' Perspective	From Vendors' Perspective
P_1: behavior of the vendors' employees	Moderate support	Moderate support
P_2: rules by client	Supported	Moderate support
P_3: rules by vendor	Supported	Supported
P_4: rules by professional association	Moderate support	Moderate support
P_5: the strength of privacy preservation law in vendor's country	Moderate support	Supported

P_5: the strength of privacy preservation law in the vendor country and privacy preservation of the offshored data.

We found reasonably strong support for this proposition regarding the role of privacy preservation law. The client organization's management thought having a strong privacy preservation law strongly affects the privacy-preserving conducts of the vendors' employees. A project manager from client organization mentions,

> *"It certainly makes us feel more comfortable if we know that there is strong privacy preservation law in that (i.e., vendor's) country."*

It was very evident that the client organizations thought that having strong privacy preserving law would help and that was somewhat a concern at the beginning of the offshoring arrangements. However, over the time they had worked with the specific offshore vendor(s). With mostly positive experience with the vendor(s), the strength of privacy preservation law in the vendor country has become less critical. 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 the client management about their Indian offshore vendor's practice of offshoring to China. We wanted to know as China has arguably weaker privacy preserving laws in comparison to India if this practice is a concern for them or not. They responded that they trust their offshore vendor and rely on the contract that they had with them. Therefore, no matter to where their India based

offshore vendor sends their works, the primary vendor is the responsible party and is held accountable for any misuse of data. However, as per their contract, the offshore vendors' manager must get clearance from the client-side manager for each team member who will have access to their sensitive data. For example, if a vendor organization in India wants to involve team members from China, then they are required to get clearance from their clients. As a project manager mentions,

> *The 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 management thought that the existence of a strong privacy preservation law in their home country is a big help. Most of the employees in a vendor's organization have an indefinite or no idea about what conduct would be an invasion of privacy. The main reason behind this is that they grow up to earn their education in a society and system where sensitive things like intellectual property law and privacy preservation law either do not exist or not appropriately practiced. Therefore, the management of the vendor organization thought that it becomes a steep learning curve for the newly hired workforce to get accustomed to the all the new rules and regulations they should follow to preserve the integrity of any data they would handle. The vendor organization from India mention that they face the similar change when they hire people from China as they also grow up in a weaker "rule of law" country. Hence, having an environment where there is a strong "rule of law" to protect data or any intellectual property positively affects the privacy-preserving behavior of the people they would hire to work in projects and that in turn will increase the safety of data.

V. CONCLUSION

Offshore outsourcing certainly has its benefits. However, it comes with a risk of misuse of sensitive information. Different institutional factors might affect the privacy preservation of the offshored data. In this research, we identified and empirically tested different institutional factors that can affect the privacy preservation behavior of the vendor's employee. We considered and identified mimetic, coercive as well as normative institutional factors. The findings our research show that the offshore vendor's set code of conduct for their employees plays the most critical role. The second most factor based on our result is the code of conduct set by the clients followed by the strength of privacy preservation law in the vendor's country.

The findings of our research shed light on an essential aspect of the literature. Moreover, the inclusion of both client and vendor managements' perspective adds a unique dimension to our study. A limitation of our findings is that both client and vendor organizations in our case study are very well reputed and industry-leading firms. Moreover, the organizations under study have been in offshoring arrangement with each other for at least last ten odd years. Hence, it appeared to us that the response from client management in many cases based on the level of trust they have in the vendor organization, and their response might get affected if they are in an offshoring arrangement with a relatively new company. Hence, to address this limitation, in a future extension of this research we intend to have more than one vendor organization with a varied level of reputation in the market.

REFERENCES

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120.

Cavaye, A. L. M. (1996). Case study research: A multi-faceted research approach for IS. *Information Systems Journal*, *6*, 227-242.

Comey, J. (2016). Audit of the federal bureau of investigation's cyber threat prioritization audit of the federal bureau of investigation's cyber threat prioritization. Retrieved May 10, 2017, from https://oig.justice.gov/reports/2016/a1620.pdf.

DiMaggio, J., & Powell, W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality organizational fields. *American Sociological Review*, *48*(2), 147-160.

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly*, *27*(4), 597-634.

Eisenhardt, K. (1989). Building theories from case study research. *The Academy of Management Review*, *1*(4), 532-550.

Engardio, P., Puliyenthuruthel, J., & Kripalani, M. (2004). Fortress India? *Business Week* (3896), 42-43.

Ferrell, O. C., & Gresham, G. L. (1985). A contingency framework for understanding ethical decision making in marketing. *Journal of Marketing*, *49*(3), 87-96.

George, A. L., & McKeown., T. J. (1985). Case studies and theories of organizational decision making. In *Advances in Information Processing in Organizations* (*2*, pp. 21-58). Greenwich, C. T.: JAI Press.

Kshetri, N., & 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*(2), 225-239.

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

Lee, M. (1996). IT outsourcing contracts: Practical issues for management. *Industrial Management & Data Systems, 96*(1), 15-20.

Meyer, J. W., & Rowan, B. (1977, September). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340-363.

Nath, A., & Bejou, A. (2012). *Offshored data privacy: Determining the factors and their relative effect*. Paper presented at the Proceedings of the 18th Americas Conference on Information Systems (AMCIS), Seattle, USA.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1-8

Palvia, S. C. J. (2017, April 11). Global sourcing of services: A two-stage model for selecting a vendor. *Global Sourcing of Services: Strategies, Issues, and Challenges* (vol. 11, pp. 407-449). Singapore: World Scientific-Now Publisher Series in Business.

Polak, J., & Wójcik, P. (2015, August). Knowledge management in IT outsourcing/offshoring projects (2nd ed.). *PM World Journal*, *4*(8), 1-10.

Ravindran, P. (2004). Factors that are worrisome for BPO sector. Business Line. Retrieved January 8, 2012, from https://www.thehindubusinessline.com/2004/04/03/stories/2004040302210300.htm.

Sarker, S., & Lee, A. S. (2002, January). Using a positivist case research methodology to test three competing theories-in-use of business process redesign. *Journal of the Association for Information Systems*, *2*(7), 1-72.

Shanks, G. (2002, November). Guidelines for conducting positivist case study research in information systems. *Australasian Journal of Information Systems*, *10*(1), 76-86.

Tate, W., Ellram, L., & Bals, L. (2009). Offshore outsourcing of services: An evolutionary perspective. *International Journal of Production Economics*, *120*(2), 512-524.

The Economist (2006, May 4th). Special report: Watch out India, outsourcing to China. *The Economist*, *379*(8476), 80. Retrieved August 20, 2012, from https://www.economist.com/node/6878397.

Trombly, M., & Yu, W. (2006). Outsourcing resilient in India. *Securities industry news*, *18*(26), 1-21.

Yin, R. K. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, C. A.: Sage.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, C. A.: Sage.

Zelijka (2017). Offshore law firm apple by confirms data breach. Retrieved January 20, 2018, from https://www.helpnetsecurity.com/2017/10/26/appleby-confirms-data-breach/.