Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2018 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2018

Cloud Users' Privacy Concerns in the Indian Healthcare Industry

Saman Nihal
Indian Institute of Technology Madras

Saji Mathew
Indian Institute of Technology Madras

R.K. Amit
Indian Institute of Technology Madras

Cloud Users' Privacy Concerns in the Indian Healthcare Industry

Saman Nihal[1]
Indian Institute of Technology Madras,
Madras, Tamil Nadu, India

Saji K. Mathew
Indian Institute of Technology Madras,
Madras, Tamil Nadu, India

R.K. Amit
Indian Institute of Technology Madras,
Madras, Tamil Nadu, India

ABSTRACT

The growing adoption of Cloud computing in various government and business domain makes it of importance for users to understand how their information is protected and accounted for in Cloud contracts especially in data sensitive domains such as healthcare. Prior studies have highlighted that contract terms for Cloud computing are evolving based on user's information privacy protective responses and liability is the most negotiated term. There is extant research on individual privacy but very few studies have addressed organizational privacy. This research inductively develops a framework using a multiple case study approach that addresses the following descriptive question- what dimensions constitute an organization's major privacy concerns when exchanging data in the Cloud. The findings from this research will have implications for managers while incorporating penalty clauses in Cloud contracts and informs government in forming privacy regulations suitable for the healthcare sector.

Keywords: Information Privacy, Cloud computing, Cloud contracts, privacy concerns, penalty clause, healthcare information protection.

[1] Corresponding author. Nihal.samann@gmail.com +91 9940184858

INTRODUCTION

Data collected from various sources is being used to drive management decisions. There is a widespread adoption of cloud computing in various business domains to store this data that result in several discrepancies that can be used to collect and utilize users' data. This puts the data at risk and has raised concerns about information privacy and its impact on the users of cloud. Therefore, information privacy is of significant interest to government regulators and business leaders. Recent reports also highlight that organizations experience pressure when adopting more technologies due to increased privacy concerns. (Casper, 2012, 2015). While prior studies have focused on individual level privacy, there are very few studies on organizational privacy (Smith et al. 2011, Belanger and Crossler 2011).

At an organizational level, cloud computing is being increasingly used for services such as Infrastructure as a Service (IaaS) and Software as a Service (SaaS). However, this requires sharing the data with the cloud service provider, thereby creating a dependency of user organizations on the cloud provider to protect their information. The degree of data protection varies based on the cloud delivery model and the nature of contract between the user and cloud service provider. Privacy, confidentiality and liability are the most negotiated terms in cloud contracts (Hon et al. 2012). Protection of information privacy has become an area of concern due to concerns about how customer data may be extracted (Kshetri, 2013). Against this backdrop, this research aims to answer the following descriptive question: what are the dimensions constitute an organization's privacy concerns. The target organizations are from the Indian healthcare industry. The findings of this study will aid managers in incorporating penalty clauses in cloud contracts and will inform government in forming privacy regulations in the healthcare sector.

LITERATURE REVIEW

Hui and Png (2006) have defined privacy as an individual's ability to control the collection and use of personal information. Organizational privacy has been defined as how organizations treat their customers' personally identifiable information (Greenaway and Chan 2005). Smith et al. (2011) conducted a review of information privacy research and identified that majority research focuses on predicting and explaining information privacy attitudes, practices and can be classified into three level of analysis: individual, group and organizational.

Information Privacy Measurement

Stewart and Segars (2002) have identified privacy as a multi-level construct, Concern for Information Privacy (CFIP). Internet Users Information Privacy Concerns (IUIPC) is a measurement scale which highlights that collection, control and awareness represent online consumers' concern for information privacy (Malhotra et al. 2011). While these studies highlight that privacy measurement at an individual level has been developed, there have not been similar studies on organizations' information privacy concerns to the best of our knowledge.

Organizational Information Privacy and Cloud Contracts

Organizational information privacy is centered on the data of its customers (Kshetri, 2013). Therefore, organizational information privacy is of significant importance to multiple stakeholders. However, there is little literature on organizational privacy. Studies have provided compelling explanations for firms' information privacy behavior (Chan and Greenaway 2005). Attili et al. (2018) find that business strategy and organizational activities reflect the level of importance of information privacy in organizations.

Several privacy issues arise when organizations use cloud services due to multi tenancy that could result in a loss of control. The users of cloud do not possess the technical mechanisms

that will allow them to control the secondary usage of their data which leads to significant risk to privacy. Therefore, they must rely on cloud contracts as a way to mitigate risk (Pearson and Benameur 2010). While current cloud contracts have well-defined confidentiality clauses and service level agreements, the penalty clauses that account for liability are not well defined as providers exclude or restrict liability (Hon et al. 2012). Governments have not provided a uniform policy that outlines a clear guidance regarding privacy breaches (Ker and Teng 2012).

Cloud Computing and Healthcare Industry

Previous studies have highlighted that privacy concerns vary with the business domain, with domains such as healthcare and banking adopting cloud less due to the sensitivity of the data (Pearson and Benameur 2010; Pearson and Charlesworth 2009). However, it is infeasible to store healthcare data in-house due to the size of healthcare datasets (Thorogood et al. 2014). Therefore, a cloud solution offers major economic advantage. However, risk of data breach continues to exist with consequences such as reputation loss and revenue loss (Wall et al. 2016). The economic impact of the breach of data and contract provisioning to manage such risks pose a major challenge to industry (Hon et al. 2012; Bradshaw et al. 2011).

In summary, prior privacy studies that focus on privacy measurement have largely addressed concerns at an individual level. Organizational level studies have focused on understanding firms' behavior in response to privacy breaches. In the specific context of cloud computing, while cloud contracts currently include confidentiality clauses, there are no clear guidelines for penalty clauses. In this paper, we use a case study approach to examine organizational privacy concerns when uploading data to the cloud and its relationship with cloud contracts, breaches and the business impact of these privacy concerns.

RESEARCH METHODOLOGY

This research adopts a qualitative case study approach based on grounded theory. We use a multiple site, multiple-case study approach. Case study research is employed when it is preferred to examine a phenomenon in its natural setting and the studies pertaining to the phenomenon are nascent (Strauss and Corbin 2008). Evidence from multiple –case studies is considered more cogent as sufficient theory emerges from the data collected to support the phenomena under study (Yin 2011). An inductive method has been adopted in our study that involves theory building without a priori theory. Through this inductive approach, we move from general observation to understanding the factors that emerge. This provides a rigorous approach to build a theory that is tightly connected to the data and the context of study.

The domain of our study was the healthcare Industry in India. The choice of this industry was due to the sensitivity of data. The organizations were selected based on suitability to study privacy in cloud and accessibility to key executives. This includes hospitals, diagnostic labs and healthcare technology providers. In order to achieve analytical generalizability, we replicated the study across the organizations studied as suggested by Yin (2011).

Data Collection

Data was collected using interview method with consenting key informants with expert knowledge in privacy and cloud. We conducted nine interviews with informants who held key positions in healthcare organizations over a period of 4 months in 2017. A semi-structured questionnaire was used as the interview protocol and the questions for the interview were designed keeping the scope of the study in mind. Table 1 shows the different organizations that participated in the study and individual profiles of the participants involved in the study.

Data Analysis

In the data analysis stage, the audio records were transcribed manually and reviewed to identify concepts. These new concepts were included as critical dimensions of the phenomena under study. A two-step process was followed for coding the interview data wherein the transcriptions were imported into NVivo, a qualitative analysis tool and a first order analysis was performed with manual open coding, structuring data on a line-by-line basis with no a priori categorization. In the second order analysis, the items coded were carefully examined to include only text passages from the interviews that dealt with privacy, cloud, contracts and healthcare as stand-alone words or in combination. During this axial coding phase, the categories were converted into themes. Lastly, selective coding was conducted that established relationships among the emergent categories and gave rise to a coherent theoretical framework. This process resulted in 4 dimensions, 9 themes and over 150 quotations. The transcripts were coded by another independent researcher and the inter-coder reliability was found to be 75% which established the reliability of the coding.

Table 1. Characteristics of Organizations

Case No.	Type of Organization	Geographical Presence	Type of Data Stored on Cloud	Participant Role	Total Experience (in years)
1	Diagnostic center	National	Employee and Transactional data	CTO	21
2	Healthcare technology provider	National	Provides the cloud service	CFO	12
3	Hospital	Asia	Employee data	COO	16
4	Hospital	National	Does not exchange data on the cloud	Deputy General Manager-IT	18
5	Hospital	National	Employee data	CIO	19
6	Hospital	National	Employee data	Associate General Manager – IT	12
7	Hospital	National	Employee data	General Manager-IT	14

8	Diagnostic center	National	Software as a Service	CIO	21
9	Health Insurance	National	Does not exchange data on the cloud	CHCO	11

RESEARCH MODEL

In this section, we present our findings from the first and second order analyses of our qualitative data. The focus of the study was to identify concepts and themes relevant to privacy in cloud computing specific to the healthcare context. These themes serve as a foundation for our theoretical model for organizational privacy concerns presented in Figure 1. The first order constructs identified were categorized into four main dimensions- Antecedents, Privacy Concerns, Outcomes (which are reflected in the form of Business Impact to the organization in the event of a breach) and Breaches.

The antecedents to privacy concern refers to various aspects that act as drivers of information privacy concerns. It explains how individual privacy concerns can be shaped. They explain an organizations attitude towards privacy concerns prior to uploading data on the cloud. The antecedents identified in our study are (i) Credibility and (ii) Awareness of Privacy Rights.

Antecedents

Credibility of the Service Provider

This refers to the reliability and expertise of the service provider. Organizations enunciated on the necessity to work with reliable cloud providers who, due to their expertise, have stringent security checks in place to protect the data and regard privacy with seriousness.

"*So you check the credibility of the cloud provider, his practices, his maturity, his robustness, all of that have to be verified.*" - CIO, Case 5

"*Because Data storage in itself takes a lot of time to bring in clients. Someone opens it today; no one will come. Unless you have a history that you have been doing.*"- CFO, Case 2

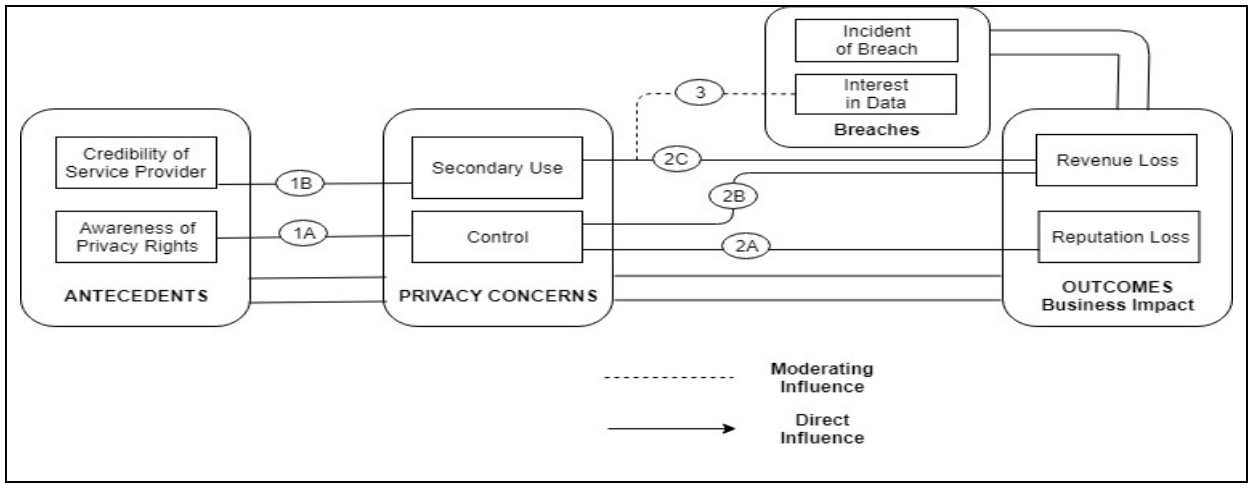

Figure 1. Emergent Research Model

Awareness of Privacy Rights

Awareness of privacy rights refers to the degree to which a consumer is aware about his or her organizational privacy practices. This includes not only organizations that are consumers of the cloud but also individual customers of an organization. Our sample data showed that in India, organizations that use cloud services are not very concerned with the privacy of their data and do not focus on privacy enhancing measures as generally their customers are not aware about privacy and do not demand it. Majority of the organizations agreed that awareness of privacy influences privacy concerns. This highlights the importance of awareness.

"We certainly understand privacy but it was a rude shocker when we came into services for Indian industry that our patients don't understand what privacy is, they don't know their rights from the privacy stand point. So that is when we decided that let us not change the industry right now [sic]"- CTO, Case 1

Privacy Concern

This construct characterizes an organization's major privacy concerns when uploading data to the cloud. Privacy concerns in the organizational context refer to perceptions about control over information and its secondary use. It also explains why organizations are hesitant to

upload data to the cloud. Respondents mention that organizations are worried when uploading data onto the cloud because as per the Medical Council of India (MCI) Code of Ethics Regulations (2002) healthcare data should not be shared with third parties (MCI India, 2002). However, the volume of information generated is very high and storing it in-house will incur significant storage and infrastructure costs which can otherwise be used for providing quality healthcare. Therefore, organizations currently upload employee and transactional data onto the cloud and store patient data in-house.

Control

This privacy concern refers to the degree to which an organization can monitor the usage, location and access to their data.

"That is a big pressure for you because you cannot expect what can be done with that data at a later stage because you don't have any control over that." - General Manager-IT, Case 7

"So, everybody not just this industry, any industry we build it (data servers) in-house itself, otherwise we cannot choose where it has to be [sic]." - Deputy General Manager-IT, Case 4

Secondary Use

This concern highlights the degree to which information collected for storage on the cloud can be utilized for a different purpose either internally from within the cloud provider's organization or externally due to breach or disclosure of data. The respondents emphasized that when working with credible cloud service providers, there are lesser chances of a breach that can lead to secondary use of data. This is because credible service providers invest more in reliable infrastructure and this safeguards the data.

"*So you want to safeguard yourself from all of this. You check the credibility of the cloud provider, his practices, his maturity, his robustness, all of that have to be verified [sic].*"- CIO, Case 5

"*I am a health care vendor, I cannot bring in all the securities which a cloud server would need because that is not my forte. That would be the forte of companies like Amazon or Microsoft. So for me to bring in confidence for a customer is , I sign up with these guys and say the data will be on their servers*." - CFO, Case 2

Based on the above support obtained from our case data we post the following proposition:

P1a: *Credibility of the service provider negatively influences secondary use of data.*

The respondents also mentioned that due to lack of laws around privacy there is reduced awareness which impacts an organizations privacy concerns. However, when the awareness of privacy rights increases, it will lead to a greater understanding of what data leakage entails and this in turn will lead to a demand for greater control over data.

"*The privacy measure should be so high I feel because patient data even if you want to show a presentation with clinical data, you can never show with patient name or patient UHID number. So that is the patient privacy which Indian healthcare industry does not know*" - General Manager IT, Case 7.

"*Privacy per se is not a subject which is demanded by the customers in today's Indian market in healthcare*" - CTO, Case 1

Therefore, we posit:

P1b: *Awareness of privacy rights will positively influence control over data*

Outcomes-Business Impact

This dimension explains the consequences of privacy concerns and breaches on the organization. The respondents indicated that due to data breach a healthcare organization might be viewed as unsafe by its customer base. This can be categorized as secondary use due to

reduced control over the data that has a consequence by loss of revenue to the organization. This financial impact occurs in the event of a breach through customer loss and reputational loss.

"*And the last part I think is the fear of loss as in, we have redundancy systems in place but what happens if we can't recover the data that we put up there. Because unlike other settings, this is a patient sort of case history that over years will give you clues as to what we should do now and in the future. So if we lose this data it becomes a problem*." - COO, Case 3

These statements highlight the necessity for the organization to have control over the data that they upload onto the cloud in order to safeguard reputation.

P2a: *Control over data will positively impact a healthcare organization's reputation.*

Respondents also revealed that since data on the cloud is susceptible to breach and can lead to reputation loss and revenue loss that impacts business, majority organizations will choose to keep their data in-house so as to have greater control over the data.

"*It is basically a loss of revenue, I mean I would definitely consider it as loss of revenue because I don't know what this data is going to be used for and how much I am going to lose*"- Associate General Manager IT, Hospital 6

"*Whatever we give to the cloud backup solution, as an operational team member what I would will monitor is whether it is working properly. My audit perspective will be that my data should be safe in cloud*" - General Manager IT, Case 7

With support from the above quotes, we posit the following proposition:

P2b: *Control over data will negatively influence revenue loss of a healthcare organization.*

It is evident from Table 1 that majority of the organizations upload only employee data to the cloud and do not upload patient data in order to safeguard it. Respondents stressed although employee data is being not viewed as sensitive data, it can be used for strategic advantage.

"*My intellectual property, my customer information, my practice procedures, all of these are not stuff that you want to openly share. So, all of this can lead to the downfall of that business, individually or in combination. So you want to safeguard yourself from all of this*." - CIO, Case 5

Therefore,

P2c: *Secondary use of data will negatively influence an organization's revenue.*

Breach

Breach in this study emerged as a construct characterized by the incident of breach and interest in data. This construct indicates the potential occurrence of breach of data at the cloud level. However, in India, there haven't been major privacy breaches as sensitive information is not uploaded onto the cloud. . It was also found that interest in the data stored can only lead to a breach and the data can be used for strategic advantage.

"*No, there is no incidence. It cannot happen. Because see, the reason I am saying this is breach only is done if there is an interest. Amazon or Microsoft won't have an interest."*- Deputy General Manager-IT, Case 4

"*There is nothing which is called as impossible. There is nothing in this world which is 100% secure. The point which has to be understood is why someone should take it. If there is no motive behind it.*" - CFO, Case 2

P3: Interest in the data strengthens the relationship between Secondary use and loss of revenue.

DISCUSSION

Theoretical Implications

The main contribution of this study is the development of a theoretical framework to add to the body of knowledge in Information Systems specifically in the areas of cloud computing and privacy concerns. This framework brings out the privacy concerns at an organizational level

and signifies the inter-relations between privacy concerns, cloud contracts, breaches and their consequences using the broad canvas of the APCO model (Antecedents -> Privacy Concerns -> Outcomes) (Smith et al. 2011). Prior studies such as Malhotra et al. (2004) and Stewart and Segars (2002) have identified privacy concerns at an individual level. This study inductively develops privacy concern at an organizational level and identifies control over the data and secondary use of data during the event of a breach are an organization's major privacy concerns when exchanging data on the cloud. It was also identified that awareness of privacy rights and credibility of the service providers influences the degree of the privacy concerns of various user organizations. The degree of privacy concern leads to behavior which can have some business impact to the organization. These business impacts have also been captured in the study as outcomes of privacy concerns. This research thereby advances theory in the areas of organizational privacy concerns and cloud computing with a focus on the healthcare industry.

Theoretical Implications

Previous studies have reported that storing healthcare data in-house is infeasible due to the complexity and size of the data. It also incurs significant infrastructure costs to install and maintain data servers within the hospital. Therefore, using cloud services reduces IT infrastructure costs to healthcare providers due to the on-demand pricing of cloud services. The cost saved can also lead to investment in healthcare infrastructure that can improve healthcare services Therefore, uploading data to the cloud has significant economic advantage to the organization.

The findings from this study have managerial implications to incorporate penalty clauses in cloud contracts. This study could further motivate organizations to the establishment of a method of valuating privacy in cloud contracts based on key factors pertaining to organizational

level privacy. The National Health Policy (2017) aims at the development of an integrated healthcare information system (Ministry of Health and Family Welfare, Government of India, 2017). This system, while useful for efficient healthcare service, is also easily accessible. However, the creation of a health information exchange platform also requires clear privacy laws that are currently not clearly defined in the policy. While organizations must take steps purposefully and consider their privacy practices, it is also important for the government to create mandates as to what constitutes privacy, what is sensitive information, who can have access to data and how will penalization take place in the event of a breach.

LIMITATIONS AND FUTURE RESEARCH

The objective of this study was to define a construct namely "Organizational Privacy Concern" in the context of the use of cloud services in the healthcare sector in India. A limitation of the study is the confinement of the sample to healthcare organizations in India. The findings of this study hold good when there are no well-defined privacy laws or a concrete method for privacy valuation. Furthermore, a qualitative approach was followed for theory building which limits the generalizability of the results until they are further tested and validated, analytically as well as quantitatively. Future research can extend this study by empirically testing the constructs and relationships identified, diversifying the geographies under study and can focus on privacy concern scale development at an organizational level.

REFERENCES

Attili, V. S., S. K. Mathew, & V. Sugumaran 2018. "Understanding Information Privacy Assimilation in IT Organizations using Multi-site Case Studies," Communications of the Association for Information Systems, (42:1), pp. 66-94.

Bélanger, F. and Crossler, R.E. 2011. "Privacy in the digital age: a review of information privacy research in information systems," MIS Quarterly, (35:4), pp.1017-1042.

Bradshaw, S., Millard, C. and Walden, I. 2011. "Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services," International Journal of Law and Information Technology, (19:3), pp.187-223.

Casper, C. 2012. "Predicts 2012 - new privacy laws bring change?" Gartner Report.

Casper, C. 2015. "Hype Cycle for Privacy," Gartner Report.

Corbin, J. and Strauss, A. 2008. "Basics of qualitative research: Techniques and procedures for developing grounded theory," SAGE Publications.

Greenaway, K. E. & Chan, Y. E. 2005. "Theoretical Explanations for Firms' Information Privacy Behaviors," Journal of the Association for Information Systems, (6:6), pp. 171-189

Hon, W.K., Millard, C. and Walden, I. 2012. "Negotiating cloud contracts: Looking at clouds from both sides now," Stan. Tech. L. Rev., (16:1), p.79-128.

Hui, K.-L. & Png, I. P. L. 2006. "Economics of Privacy," in Handbooks of Information Systems and Economics, Terry Hendershott, Elsevier, pp. 1-27.

Kerr, J. and Teng, K. 2012. "Cloud computing: legal and privacy issues," Journal of Legal Issues and Cases in Business, (1), pp. 1-11.

Kshetri, N. 2013. "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," Telecommunications Policy, (37:4), pp. 372-386.

Malhotra, N. K., Kim, S. S. & Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research, (15:1), pp. 336-355

Pearson, S. and Benameur, A. 2010. "Privacy, security and trust issues arising from cloud computing," in IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), Indianapolis, IN, pp. 693-702.

Pearson, S. and Charlesworth, A. 2009. "Accountability as a way forward for privacy protection in the cloud," in IEEE International Conference on Cloud Computing, Berlin, Heidelberg, Springer, pp. 131-144.

Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," Information Systems Research, (13:1), pp. 36-49.

Strauss, A. and Corbin, J. 1994. "Grounded theory methodology," Handbook of Qualitative Research, 17, pp.273-285.

Smith, H.J., Dinev, T. and Xu, H. 2011. "Information privacy research: an interdisciplinary review," MIS Quarterly, (35:4), pp.989-1016.

Thorogood, A., Simkevitz, H., Phillips, M., Dove, E.S. and Joly, Y. 2016. "Protecting the Privacy of Canadians' Health Information in the Cloud," Canadian Journal of Law and Technology, (14:1), pp. 173-213

Wall, J. D., Lowry, P. B. & Barlow, J. B. 2016. "Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess," Journal of the Association for Information Systems, (17:1), pp. 39-76.

Yin, R.K. 2011. "Applications of case study research". SAGE Publications.