The Information Privacy Concerns at the Organizational Level: An Exploratory Study in the Bank Sector

Emergent Research Forum papers

Gustavo Zimmermann Montesdioca
Universidade Federal do Rio Grande do Sul
gustavo.percio@ufrgs.br

Marcia Cassitas Hino
Fundação Getulio Vargas – São Paulo
marciahino@uol.com.br

Antonio Carlos Gastaud Maçada
Universidade Federal do Rio Grande do Sul
acgmacada@ea.ufrgs.br

Abstract

The leakage of private information in corporations continues to occur on a large scale, with loss of thousands of records. The information privacy concerns are one dimension that can help to define organizations' attitudes and initiatives regarding information privacy. Despite that, there is a reduced number of researches that investigate the antecedents and outcomes of information privacy concerns at the organizational level. To address this gap, the objective of this paper is to investigate the information privacy concerns at the organizational level in the bank sector, answering the question: what are the dimensions that influence information privacy concerns at the organizational level? We performed the literature review and semi-structured interviews with experienced bank executives to identify the antecedents of organization information privacy concern. Three antecedents were identified on the literature (regulations, customer information, organization information), while other three emerged from the empirical data (cultural aspects, protection culture, and financial impact).

Keywords

Information privacy, privacy concern, organizational level, organization information privacy concern.

Introduction

The leakage of private information in corporations continue to occur on a large scale, with loss of thousands of records like credit card number, password, email, documents, and financial data, representing a risk of privacy (Bloomberg, 2015). The financial sector maintains large databases with confidential information, which are constant targets of attacks for theft and disclosure of corporate information. Since 2005, over 335 million records leaked from financial companies in 590 cases of information breach that became public (Private Rights Report, 2015). The JP Morgan leaked 83 million records in August 2014, a case that simple measures could have avoided the information breach (The New York Times, 2014).

The disclosure behavior is a multidimensional construct, where “different people have different tendencies to disclose different types of information” (Knijnenburg et al., 2013, p. 1145). A large number of academic researches maintain their focus on individual level of analysis, while a low number of studies investigate dimensions that influence organizational information privacy concerns (Pavlou, 2011; Smith et al., 2011). Researches about privacy concerns on organization are important as it affects success of e-business initiatives, can influence collaboration and success of intercompany systems, and defines organization's attitudes about privacy (Belanger and Crossler, 2011).
Our objective in this research is to investigate the information privacy concerns at the organizational level, specifically in the bank sector. Our research aim to answer the question: what are the dimensions that influence information privacy concerns at the organizational level? We started our investigation on previous literature. We performed two semi-structured interviews with bank executives in Brazil. Data analyses employed qualitative tools to identify the influential elements discussed by the executives during the interviews. Finally, we present the results and discuss the main findings.

**Theoretical Approach**

Previous researches investigated information privacy concern at the individual level, with many definitions. The literature does not offer the same broad base of definition for the organization information privacy concern. For this reason, we adopted Belanger and Crossler’s definition for the organizational level of analysis, which guides the current research: “organizational information privacy concerns reflect the overall concern that organizational leaders have regarding the privacy of the information the organization possesses and has access to” (Belanger and Crossler, 2011, p. 1033).

The theoretical approach started by the analysis of the articles of Smith et al. (2011) and Belanger and Crossler (2011) about information privacy. These articles offered a detailed review of previous researches and suggested future directions. We performed backward and forward search (Webster and Watson, 2002) based on these articles to propose the research model on figure 1 following two premises. First, the macro model of Smith et al. (2011), which establishes the relationship between privacy concerns with antecedents and outcomes (APCO model). Second, the multilevel model of Belanger and Crossler (2011), selecting only the organizational aspects. Previous research (e.g., Earp et al., 2005) pointed out there is no link between individual privacy concerns and privacy policies set by organizations, because organizations use privacy policies for their own purpose (Belanger and Crossler, 2011). Two types of organizational privacy concerns emerge: concerns for privacy of the organization’s information, and concerns for privacy of the customer information collected by the organization. The figure 1 presents the preliminary model and next subsections explain the model dimensions.

![Figure 1. Preliminary Research Model](image)

**Regulation**

The regulation dimension represents laws, guidelines, and regulations that govern information privacy practices at the organizations, while provide a level of security about privacy of organizational information. It encompass government laws, (Li, 2012), industry’s self-regulation (Xu et al., 2009), and organizational privacy policy (Faja and Trimi, 2006; Xu et al., 2011). In bank sector, several entities provide such regulation, as government, central banks, and global councils.
Agency theory supports the discussion about regulation on privacy (Li, 2012). The agency theory approach establishes that the private information has an economic value, and the organization collects and uses private information during and after transactions. In this situation, uncertain about privacy risks emerges, and regulations help to mitigate privacy concerns, but resulting in agency cost for doing business (Kim et al., 2008; Li, 2012; Culnan and Armstrong, 1999). Regulations imposed to banks, like federal laws, represents an example of the influence of agency theory, leading to the following proposition:

**Proposition 1:** Regulation influences the organization information privacy concern.

**Customer Information**

The customer information is the personal information that organizations collect and store about the customers and need to secure privacy. Organizations have the interest to collect private information for transactions, data mining, business analytics and reports, and develop governance mechanism (e.g., corporate privacy policies, data classification) for organizational information privacy purposes (Belanger and Crossler, 2011; Earp et al., 2005).

Privacy calculus theory postulates that privacy disclosure behavior is based on risk-benefit assessment, and the perception of the benefit compared to risks determines the course of action (Li, 2012). Organizations need to develop policies and mechanisms, and inform their customers about the information privacy policies and procedures, reinforcing the benefit perception of doing business with the organization, and resulting in a possible competitive advantage (Smith et al., 2011). This is especially important in an information sensitive segment as banking. Organizational leaders are responsible for develop and communicate privacy policies and mechanisms to reinforce the benefit perception, suggesting the following proposition:

**Proposition 2:** Customer information influences organization information privacy concern.

**Organization Information**

Organization information is the data generated inside the organization. The information lifecycle management is composed of creation and collection, storage, distribution and transmittal, access and use, maintenance, disposition and destruction (Bernard, 2007). The organization generates information using its own information and information collected during transactions. There is a management concern about the privacy of the organization’s information, resulting in effective actions to protect such information (Belanger and Crossler, 2011). In this sense, we postulate the organization has high concern about the privacy of their information, what lead to the following proposition:

**Proposition 3:** Organization Information influences organization information privacy concern.

**Organization Information Privacy Concern**

Information privacy concern is the central dimension consolidated on privacy literature. The perception of information privacy concerns are influenced by external conditions, as industry sector, culture, and regulatory laws (Malhotra et al., 2004), and it is considered a multilevel construct (Li, 2012; Belanger and Crossler, 2011, Smith et al., 2011).

Previous empirical research found that privacy concerns construct impacts behavioral reactions (Dinev and Hart, 2006; Smith et al., 1996; Malhotra et al., 2004; Keith et al., 2013). Consistent with organization information privacy concern definition used in this research, we postulate that behavioral reactions of management leaders will be determined by privacy concerns that emerge in the organization. In banking sector, includes the need to build trustworthy image. Hence, we propose that:

**Proposition 4:** Organization information privacy concern influences behavioral reactions.

**Behavioral Reactions**

Behavioral reactions on the organizational level represent the activities performed in the organizations to build trust by exhibiting procedural justice handling private information (Smith et al., 2011). Management leaders are responsible to implement policies and procedures that address organization privacy concern
to safeguard information kept on the information systems. Behavioral reactions of the management leaders include implementation of fair information practices (Culnan and Armstrong 1999), explicit communication of a privacy policy (Eastlick et al. 2006), privacy policy development (Xu et al. 2005), and display of privacy notices (Smith et al. 2011).

Methodology

The article made use of a qualitative research strategy, which proved to be the most appropriate as it allows the phenomenon understanding and supports the objective of the article. Positivist and interpretive approaches were considered. At this research stage, the interpretive approach was chosen in order to identify new dimensions that could emerge from the analysis aiming to enrich the model presented.

Semi structured interviews joint with literature review were used to collect the data. A subset of questions was selected to incentive the interviewee to present its experience about the subject in study. Two senior executives, from the top 5 financial institution in Brazil, within 17 and 24 year experience in information security were interviewed. The interviews were carried out with both researchers through skype session and took around one hour each. The data collected was recorded and later transcribed.

We analyze the collected data using the content analysis technique supported of Atlas.ti. No pre-defined categorization was used, as the study aimed to identify the most relevant categories that would emerge from the data collected and to avoid bias in the analysis.

Data Analysis and Discussion

To start with the analysis from organizational perspective, it is necessary to first understand the dimensions that emerged during the data analysis that may influence organizations’ perspectives in regard to personal information.

There is neither a single nor a clear concept of information privacy. The ones revealed by the interviews are:

- “Information is dynamic so privacy is relative” (Interviewed P1).
- “Concerns about data privacy vary among the generations” (Interviewed P1). Current generation makes use of social media, relationship sites and mobile solution to publish information. This behavior shows a lower concerns about information privacy;
- “Privacy is everything that you want to keep under information restrict rules” (Interviewed P2).

The globalization is forcing organizations to adopt higher security standards to protect information. This is happening within different sectors and countries. Most of the financial organizations have already created an area responsible only for the information security (Interviewed P1).

Cloud solutions are also emerging as a logical security solution to provide data protection. At the same time, it is possible to observe that customers, increasingly self-sufficiency, look for solutions user-friendly and fully integrated with mobility. This behavior strengthens the perception of information privacy by means of access control solutions (Interviewed P1 and P2).

The leakage of transparency of which information is being gathered, for what purpose and how it will be stored, together with the lack of responsibilities clarity are being argued by the specialized professionals aiming to approve regulations and federal laws that force the organizations to improve their controls and establish minimum security standards for an adequate governance.

Listed below are the factors identified in the analysis:

Regulations

This is a factor with different levels of regulation. There are internal movements in the organizations to protect their data, which are already considered an asset. This includes the implementation of policies to protect the data. The next regulation step can be seen at the segment level. The Brazilian Central Bank (BACEN) clearly attribute to the banks the responsibility to the information aggregated to the customer
data. Moreover, professionals of information security segment are working on a federal law project to regulate a disadvantaged area of specific legislation in the country. It aims to ensure citizens the control and ownership over their own personal information, in order to guarantee the constitutional right to privacy. It is increasingly common that private information is obtained and used without the knowledge of its owner and often even against their will.

Customer Information

The interviews revealed a new people generation not so worried about their private information. These people are strongly connected with technology and easily navigate in technological solutions used by the organizations they have access to. They are auto-sufficient and like to do things by themselves. Notwithstanding the increase of customers coming from mature markets, information privacy is relied to a strong authentication process, which they believe is enough to protect their personal data. The personal information is not necessarily private information, but this concern emerges when organizations aggregate value to personal information. “Public personal information can be obtained through the internet of things, but when organizations aggregate value to this information, it moves from public to private classification” (Interviewed P1). They also act reactively: unless they are directly impacted, information privacy is not a concern. Sometimes they not even know the risk they are exposed to until their information become public. As a result, individual level privacy concerns have no bearing on their organizational level privacy concerns.

Organization Information

Organizations are being focus of attacks. According to P1, “information has a significant value for the organizations”. The organizational information leakage can risk a competitive advantage reached by the organization. There is a movement into organizational privacy, mainly related to strategic information. Financial organizations monitor email flows to/from external address (Interviewed P2).

Cultural Aspects

From organization perspective, “[...] notwithstanding the executive has conscience of the information privacy importance, they are much more reactive” (interviewed P1) “[...] waiting until the organization is sue for then address the issue” (interviewed P2). This is a cultural behavior. In addition to it, the organizational image is very important in Brazilian culture. Public communication of leakage incident of private information in corporations is understood as a weakness rather than a commitment to a transparent behavior. As stated by interview P1: “[...] if I tell customers that data has been lost, or that privacy has been violated, it will generate a stronger negative image for the organization”.

Protection Culture

Information is stored in organizations that may be target of attacks. They are responsible to preserve the data and protect the access to them. The existence or lack of a protection culture from customers may also expose the organizations. Via social engineering frauds the customers can facilitate the leakage of privacy information under organization responsibility. According to interviewed P1, “this is not an attack to a security component breach. It’s social engineering”.

Financial Impact

Brazilian executives are concerned about financial losses they may have that could impact the organization profits. Events related to information privacy are still considered more qualitative than quantitative by them, in other words, they impact more the organization image than the organization profits. The cost involved to keep a preventive information privacy solution is much higher if compared with the costs generated in a reactive process. Interviewed P2 argued that “[...] even if I have to pay for a fine, I am saving money, as I did not have to invest on preventive controls. Reactive organizational behavior has a low operational cost”, and complemented saying that “the investment on information privacy is high, so I keep the controls at a minimum level to avoid most of common events”.

Due the exploratory character of this research, three additional dimensions emerged with the empirical data: cultural aspects, protection culture and financial impact, illustrated in figure 2.

![Figure 2. New model emerged from empirical data](image)

### Conclusion

The objective of this research in progress is to investigate the information privacy concerns at the organizational level in the bank sector. The preliminary research model was developed based on the literature review with three antecedents (regulation, customer information, and organizational information), and a new model emerged based on the analysis of the empirical data with three additional dimensions (cultural aspects, financial impact, and protection culture). References on these later antecedents are present on the literature at the individual level of analysis. Wu et al. (2012) found the influence of cross-cultural factor on privacy concerns and perceived risks. The data collected during this research suggest the same cultural effect influences the organizations, but in different ways. First, the cultural aspects determine the reactive behavior of executives on privacy protection decisions and communication of privacy incidents. Second, the protection culture varies on customers that can facilitate the leakage of privacy information under organization's responsibility, and require actions to protect the
privacy of the corporate information. Finally, the financial impact dimension represents monetary losses and is related to cost/risk evaluation performed by executives, finding literature reference in Li (2012).

The investigation of information privacy concerns at the organization level is important to identify the dimensions that influence organization and management leaders, helping to formulate information privacy policies, mechanisms and decisions. While our study is on its initial stage, next steps of this research are continue data collection with banking executives to reinforce the exploratory model, share findings with academics and executives, and advance to an additional quantitative stage for the confirmation of the emergent model. Ultimately, we expect to contribute with new concepts and dimensions to benefit the academic research and practitioners with future publications.

REFERENCES


Pavlou, P. A. 2011. “State of the information privacy literature: where are we now and where should we go?”, MIS quarterly (35:4), December, pp. 977-988.


