Information Privacy Concerns of Real Estate Customers and Information Security in the Real Estate Industry: an Empirical Analysis

Deepa Mani, Alireza Heravi, Kim-Kwang Raymond Choo, Sameera Mubarak
School of Information Technology & Mathematical Sciences,
University of South Australia
Adelaide, South Australia

deepa.mani@mymail.unisa.edu.au,alireza.heravi@mymail.unisa.edu.au,
Raymond.choo@unisa.edu.au, Sameera.mubarak@unisa.edu.au

Abstract

An organisation in the real estate industry that uses information systems for its daily business operations for storing and transferring customers' data is a potential target of cyber-attacks. However, real estate is an understudied industry in terms of information security and customers' information security privacy concerns. In this paper, we surveyed 82 Australian real estate customers to explore their privacy concerns when providing personal information to real estate agencies and the conditions that they are willing to provide such information. We also interviewed 20 real estate businesses to understand their current information security practices. Our findings suggested that customers are naturally concerned when providing personal information to real estate agencies and that trust plays a key role. Our findings also highlight the need for real estate organisations to enhance their information security practices.

Keywords: *Information privacy, Information security, Real estate organisations, Social penetration theory.*

1 Introduction

Information privacy (e.g. ensuring the security and privacy of user data) is a topic of ongoing research and policy interest, particularly when our data are increasingly collected by a wide range of public and private sector organisations. In Australia, for example, customers provide or disclose personal and financial information (e.g. copies of their bank statement and passport) when submitting rental applications or when they are selling their properties to real estate firms. Customers are generally not aware how their information (electronic, scanned or physical documents) will be stored / secured, when and how their information will be disposed of and the security of the devices used to access, store and disseminate personal information. Similar to other service industries, real estate organisations use information systems for their daily business operations but information security is generally not their business priority. This is particularly true for small and medium-sized real estate businesses and many of the organisations outsource their information technology/security functions. To reduce the risk to customers' data, this paper aims to contribute to an in-depth understanding of information security practices in real estate organisations. As shown in Figure 1 this paper consists of two studies.

2 Study 1

To understand customers' concerns regarding information privacy when providing personal information and the conditions in which they are willing to do so, we use the five constructs outlined in Figure 2. In that the perceived risks/benefits and self-disclosure construct are based on social penetration theory. Note that the aim of this study is not to test the theory; rather it is used to guide the study.

2.1 Theoretical Background

The Social Penetration Theory suggests that relationships develop from lower levels of intimacy (superficial self-disclosure) to higher levels of intimacy (greater level of self-disclosure), and finally to disengagement (withdrawal of disclosure) (Altman & Taylor 1973). This theory links self-disclosure to interpersonal relationship development using a cost-reward approach. Individuals evaluate their relationship/interactions with others and if the associated costs are perceived to be less than the rewards, then the relationship/ interaction is considered satisfactory and vice versa (Giri 2009).

2.2 Hypotheses

This study focuses on the information privacy, which is defined as: "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves" (Clarke 2006). Information privacy concerns have attracted the attention of academics, and government agencies as rapid advances in information and communications technologies (ICT) have facilitated wide scale collection, aggregation and analysis of data (Malhotra, Kim & Agarwal 2004). *Cost-rewarding* and *self-disclosure* are two factors discussed in the theory described in Section 2.1. Cost-rewarding refers to the calculation of costs (risks) and rewards (benefits).

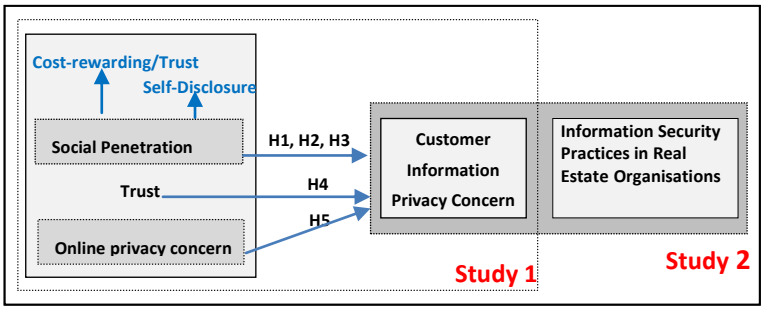

Figure 1. Research Model used in this paper

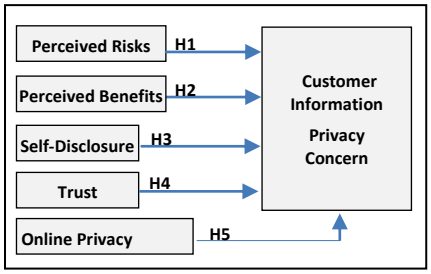

Figure 2. Study 1 Research Model

In this study, we adopted the term "risk-benefit" as this is more reflective of the customer-real estate organisation relationship. We will investigate the risk's effect on customers' information privacy concerns when providing personal information to the real-estate agency in this study. Therefore, we posit the following hypothesis:

H1: Risks perceived by customer will have a positive effect on his/her information privacy concerns on providing personal information to the real estate organisation.

H2: Benefits perceived by customer will have a positive effect on his/her information privacy concerns on providing personal information to the real estate organisation.

Self-*disclosure* is defined as "any message about the self that a person communicates to another" (Wheeless & Grotz 1976). In this study, we investigate whether being open or closed (high/low level of self-disclosure) affects one's information privacy concern when providing personal information to the real estate organisation. Therefore, we posit the following hypothesis:

H3: The degree of self-disclosure by the customer will have a positive effect on his/her information privacy concerns on providing personal information to the real estate organisation.

In the cost-rewarding calculation, it is believed that *trust* is used, and high trust correlates with low cost and vice versa (Dwyer, Hiltz & Passerini 2007). According to Metzger (2004), high trust reduces the perceived risks of self-disclosure. In this study, we investigate whether customers' trust in the real estate organisation affects their information privacy concerns when they provide personal information. For this reason we posit the following hypothesis:

H4: Customer's trust in the real estate organisation will have a negative effect on his/her information privacy concerns on providing personal information.

In the current ICT-enabled society, most of our communications take place over the Internet, and real estate companies are no exception. Customers are likely to email these organisations regarding property inquiries, provide electronic or scanned copies of documents, etc. (Mani, Choo & Mubarak 2014), and such information will be stored on the organisation's systems. Therefore, customer's general online privacy concerns may have an impact on his/her information privacy concerns when the customer provides personal information. Therefore, we posit the following hypothesis:

H5: The degree of online privacy concerns of customer will have a positive effect on his/her provision of personal information to the real estate organisation.

2.3 Data Collection

An online questionnaire was sent to students and staff of the University of South Australia. A total of 82 respondents who had rented/bought/sold a property through a real estate company in South Australia in the last 12 months participated in the survey. The scales were refined based on the pilot study results. The final questionnaire consists of eight sections. Section one collects the demographic information about the participants – see Table 1. The second section is designed to determine the level of trust in the real estate organisation(s) that the respondents had dealt with. The third and fourth sections are designed to understand the perceived risks, and the respondents' information privacy concerns. The last four sections focused on information sensitivity, perceived benefits, disclosing personal information, and online privacy concerns of the respondents.

Category	Subcategory	Frequency	Percentage
Gender	Male	50	61%
	Female	32	39%
Age	18-24	15	18%
	25-34	40	49%
	35-44	18	22%
	45 or older	9	11%
Country of origin	Australia	25	31%
	Malaysia	9	11%
	India	10	12%
	Other	38	46%
Education	High School	12	14%
	Bachelor Degree	16	20%
	Honours Degree	6	07%
	Masters Degree	31	38%
	Doctorate Degree	16	20%
	Other	1	01%

Table 1: Respondents' demographic details

2.4 Findings

The individual constructs of the data were tested for reliability, convergent and discriminant validity. The

calculations were performed using the SmartPLS software package. For reliability analysis, Cronbach's alpha was tested to analyse the constructs' internal consistency measure for each construct. The constructs ranged from 0.75 to 0.95. Since all the constructs exceeded the 0.70 cut-off values, the recommended threshold for construct reliability is exceeded.

Construct	CR	AVE	PR	PB	SD	TR	OPC	IPC
PR	0.97	0.95	**0.97**					
PB	0.87	0.77	0.25	**0.88**				
SD	0.86	0.62	0.24	0.39	**0.79**			
TR	0.88	0.66	-.13	0.22	0.15	**0.81**		
OPC	0.87	0.70	0.34	0.15	0.20	-.05	**0.84**	
IPC	0.91	0.66	0.56	0.09	0.14	-.38	0.47	**0.81**

Table 2: CR, AVE, and Inter item correlations

The convergent validity was also assessed using the Average Variance Extracted (AVE). The AVE and the Composite Reliability (CR) of all the constructs were above 0.5 and 0.6 respectively, indicating sufficient convergent validity as shown in Table 2. Likewise, the square root of the AVE reveals that the value of each construct is larger than its correlation with other constructs and, thus, satisfies the discriminant validity of the constructs. Since all the items had adequate reliability and validity, all the measurement items were used to test the structural model. The Partial Least Squares (PLS) and bootstrapping test were respectively used to determine the hypothesised path (and the path coefficient, β) and to estimate the path significance using t-values. The computed results are shown in Figure 3.

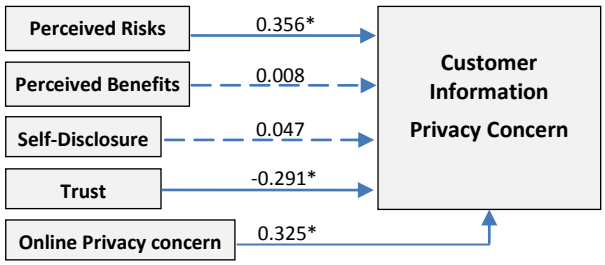

Figure 3: Results of the Structural Model Testing

Note: The dotted line indicates that the item is not significant. * indicates that the item is significant at p<0.01

2.5 Discussion

In study 1, we examined perceive risk/benefit, self-disclosure, trust and online privacy concerns regarding customers' information privacy concerns. The analysis results suggest that three out of five hypotheses are supported. H1 and H2 propose there is a positive relationship between perceived risk/perceive benefit and real estate customers' information privacy concerns. H1 (β= 0.356, P <0.01, t=6.967) was supported but H2 (β= 0.008, P=NS, t=0.183) was not. This indicates that while customers' perceived risk influences their concerns about information privacy, the perceived benefits do not. Therefore, it can be concluded that customers are more concerned about the potential risks of providing personal information rather than the benefits that they might gain when dealing with a real estate organisation. To our surprise, H3 (β= 0.047, P=NS, t=1.259) was not supported. This suggests that self-disclosure does not have a significant impact on information privacy concerns. In other words, being open or closed (high/low level of self-disclosure) does not affect one's information privacy concerns when providing personal information to a real estate firm. H4 (β= -0.291, P= <0.01, t=6.700) was supported; as expected when individuals trust the company they are dealing with, they will be less concerned about their information privacy. Finally, H5 (β= 0.325, P= <0.01, t=8.162) was supported; indicating that online privacy concerns have a significant effect on information privacy concerns. Therefore, people who do have concerns about privacy when they are online are more likely to be concerned about information privacy when dealing with a real estate agency.

3 Study 2

In study 2, we analysed real estate organisations' information security practices in terms of people, process, and technology. For data collection, 50 South Australian real estate organisations, members of Real Estate Institute of South Australia (REISA), were contacted by email. Of these 50 organisations, 20 participated in the semi-structured face-to-face interviews. Each interview took approximately 30 minutes to do and they were audio-recorded and transcribed verbatim for analysis using comparison and contrast methods.

3.1 Current Information Security Practices in Real Estate Organisations

To protect a real estate company's business it is necessary to address the three important aspects of business operations, namely people, process and technology. These aspects play a major role in protecting the confidentiality and integrity of customer information.

3.1.1 People

People are the real estate organisations' employees who use the technology and access customer information. To protect customer information, it is important that employees have adequate training/qualification in information security. All 20 participants reported that their organisations provide induction training for all new employees. However, only six participants indicated that their organisations include a basic information security module in the induction training. It is important for real estate organisations to conduct regular information security training for all employees and create a culture of security to ensure that employees are kept abreast of recent cybercrime threats and is equipped to respond to such threats (Imgraben, Engelbrecht & Choo 2014).

3.1.2 Process

An effective process needs to have policies that are specified as well-defined documents. Since the core business of real estate organisation is not in information technology, it is unsurprising that these organisations do not have any information security policies. Half of the participants were either not aware whether there is an acceptable IT technology use policy or reported that their

organisation does not have such a policy or bring their own devices (BYOD) policy. This is despite BYOD being a norm in all the 20 organisations. The real estate organisations collect significant amount of personal information about their customers; therefore, it is essential to have policies for document retention and disposal. Of the 20 interviewed participants, six mentioned that their organisation never deletes customer information. Twelve participants reported that their organisations kept customer information for five to seven years, and the remaining two organisations reported that customer information is kept for only a year. However, when asked about deleting electronic or scanned files, only two organisations reportedly used wiping software to delete such files. It is necessary for real estate organisations to have an appropriate media disposal best practice, particularly for electronic media, as data can be forensically recovered from unwiped media (Quick, Martini & Choo 2013).

3.1.3 Technology

Smart mobile and portable devices are commonly used in the real estate industry. Several organisations allowed BYOD. However, only half of the interview participants indicated that their organisations have an acceptable BYOD policy in place. When asked about security protections on the mobile devices used for work purpose, 85% indicated that their devices are protected with a password, 55% reported having antivirus software installed on their mobile devices, and only 20% mentioned they have remote wiping apps installed. Over 85% of participants reported incidents involving malware attacks on their work computers and other hardware and/or had their hardware such as laptops, CCTV cameras, and mobile and other portable devices lost or stolen.

3.2 Discussion

Our findings suggest that the level of employee security awareness is generally inadequate. For example, using mobile and portable devices for both work and personal purposes is a norm in these organisations, but they did not have any security measures in place to ensure the security and privacy of data that such devices could be used to access once lost, stolen or compromised. Only half of the interview participants reported that their organisations have acceptable mobile device use policies. Anti-virus software is common in personal computers but not on their mobile devices. In our study, 13 (65%) participants reported incidents of malware infection on their hardware which did have antivirus installed. This highlighted the fact that installing antivirus software is not sufficient on its own. It is necessary to ensure that the software is updated regularly with the latest signature, as well as the need to introduce security hygiene. It is also necessary for organisations to educate the importance of incident reporting as well as how to report such incidents, so that future events may be prevented.

4 Conclusion

In this paper we found that: (1) individuals are more concerned about the potential risks than the benefits that they may gain when providing personal information to a real estate organisation; (2) there is no difference between an open and a closed (high/low level of self-disclosure) individual regarding information privacy concerns when dealing with a real estate organisation; (3) the more a customer trusts a real estate organisation, the less concerned he/she will be about information privacy; and finally real estate customers who were more concerned about their privacy when they were online would be more likely to worry about their information privacy. In study 2, our findings highlighted the need for such organisations to invest more in information security, and understand that information security is not a cost because it can deliver business benefits. It is clear from study 1 that the customers are generally concerned about how their information is protected. However, findings of study 2 indicate that real estate organisations are not taking the necessary precautionary steps to protect customer private information.

5 References

Altman, I. and. Taylor, D. A. (1973): *Social penetration: The development of interpersonal relationships*, Holt, Rinehart & Winston.

Clarke, R. (2006): Introduction to Dataveillance and Information Privacy, and Definitions of Terms, www.anu.edu.au/people/Roger.Clarke/DV/Intro.html. Accessed 29 June 2014.

Dwyer, C., Hiltz, S. and Passerini, K. (2007): Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. AMCIS 2007 Proceedings: 339.

Giri, V.N. (2009): *Social Penetration Theory. Encyclopedia of Communication Theory. SAGE Publications, Inc*, SAGE Publications, Inc., Thousand Oaks, CA.

Imgraben, J., Engelbrecht, A. and Choo, K. K. R. (2014): Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology* **33**(12): 1347-1360.

Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004): Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research **15**(4): 336-355.

Mani, D., Choo, K. K. R. and Mubarak, S. (2014): Information security in the South Australian real estate industry: A study of 40 real estate organisations. *Information Management & Computer Security* **22**(1): 24-41.

Metzger, M. J. (2004): Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* **9**(4): 00-00.

Quick, D., Martini, B. and Choo, K.K.R. (2014): *Cloud Storage Forensics*, Syngress.

Wheeless, L. R. and Grotz, J. (1976): Conceptualization and measurement of reported self-disclosure. *Human Communication Research* **2**(4): 338-346.