ISSN 2278-5612

RISK MANAGEMENT OF MOBILE CHANNEL IN TRAVEL INDUSTRY

Huang-Wei Su

Associate Professor, Faculty of Department of Tourism and Leisure Management, Tung-Fang Design University, Kaohsiung, Taiwan, ROC.

hweisu@gmail.com

ABSTRACT

Mobile channel, like Uber or Airbnb, may lead to both cost-efficiency and flexibility, but it also inevitably triggers a certain degree of cost exposure. Unfortunately, there is little objective, scientific research focused on evaluating the risks that result from information exchange among mobile channels. In this study, the Grey Relational Analysis (GRA) were employed to identify and evaluate the risks of mobile channel business. This research finds “Jurisdiction”, “agreement and contract”, and “Social engineering” are the top three risk management factors. Especially in Taiwan, the law issue is the biggest rock on the road now. Collaborative consumption is a new inevitable business model, how to govern and constitute a legal environment is an unavoidable responsibility to our legislators.

Indexing terms/Keywords

mobile channel; risk management, the Grey Relational Analysis

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal Of Management & Information Technology

Vol . 10, No 10

editorsijmit@gmail.com

www.ijmit.com

ISSN 2278-5612

INTRODUCTION

In 2013 Airbnb launched new versions of its iOS and Android mobile channels, adding the ability for hosts to communicate with guests and respond directly to guest messages [1]. Mobile channel is a current trend that discloses the next-generation application in all different kind of business[2]. Not only personal use of cloud services such as webmail, facebook, YouTube for some years, but also the organizations have started to apply mobile channel as a tool for their IT needs. It is estimated that by 2013 the cloud market will have reached $8.1 billion[3]. According to Rizzi, technology has progressed so rapidly that Internet marketing has become more and more important in the "marketing mix [4]." In the past ten years especially, the economy and society have changed rigorously, and not only the incomes of consumers but also the dollar amounts of purchases have risen. Consumers' habits of purchasing travel products are more different than ever. In order to occupy this market, most travel industry have invested plenty of resources and man power in mobile channel in order to provide the new business opportunities and increased convenience the Internet can provide, through which customers can purchase their travel products.

As a result, this study has the following objectives:

- Identify the risk management factors attributable to mobile channel services using scientific and objective methods;
- Measure and analyze risk management factors from mobile channel;
- Provide administrators with the information necessary to make risk management decisions with regard to mobile channel;
- Provide support for management's authorization of mobile channel based on objective, scientific, risk-focused assessments.

Literature Review

The sensitive data of each enterprise resides within the enterprise itself and is subject to its physical, logistical, and personnel security control policies in a traditional model of on-premises application deployment[5] . However, in most mobile channel service models, enterprise data are stored externally. Because malicious users can exploit weaknesses in the data security model to gain unauthorized access to data, mobile channel vendors are urged to adopt additional security measures to prevent breaches. In other words, the use of mobile channel services implies system vulnerability associated with malicious employees[6] . Unfortunately, not all security breaches in mobile channel are caused by cloud service providers. Employees' mistakes may also result in security breaches [7] . One example is the use of weak security passwords or a standard company default password to log on to a network or e-mail platform[6] .Enterprises that use a mobile channel service may also have legal problems related to privacy, jurisdiction, and agreement or contract risks. The cloud infrastructure must address challenges beyond the traditional issues of remote access, data transfer, and intrusion detection and control through constant system monitoring[8] . Mobile channel's unique schema for physical data storage may sufficiently store the data of multiple clients on one physical device. This shared physical server model requires the vendor to ensure that each customer's data are kept separate, so that no data bleeding occurs across virtual servers[9] . Furthermore, enterprises and individuals interested in using mobile channel services must be aware of the privacy risks associated with their use and take these risks into account when deciding to use mobile channel services [10] . In many cases, vendor servers span multiple countries with different compliance and data privacy laws, making it unclear which legal entity has jurisdiction over the data[5, 8] . Mobile channel also raises potential legal issues between cloud users and cloud providers [11, 9] . The apportionment of liability in a cloud service contract may be unclear, or a user may get locked into a contractual arrangement that does not cater to the user's needs.

Cross-cloud compatibility is another risk that enterprises face when using a cloud computing service. An online storage service called "The Linkup" shut down on August 8, 2008, after losing access to as much as 45% of customer data. The Linkup's 20,000 users were told that the service was no longer available and were urged to use another storage site. Developing a new generalized usage model in which the same software infrastructure can be used across cloud service systems would mitigate these data lock-in concerns. Therefore, before developing interoperability technology an improving the portability of data and resources between different parts of the cloud, mobile channel services should first address the risk of cross-cloud compatibility because it creates significant uncertainty that will impact the efficiency of using a mobile channel service[8] .

To draw a conclusion from the prior literature review (a) Agreement or contract, (b) Privacy, (c) Jurisdiction, (d) Damaged or spoiled by employees, (e) Burglary, (f) Normal wear and tear or malfunction, (g) Natural disaster, (h) System vulnerability, (i) Social engineering, (j) Jurisdiction are ten risks of mobile channels. This study also conducted a Delphi study and the Grey Relational Analysis (GRA) to identify the risks of using cloud services and the relative weights of each risk management factor.

Methodology

The participants (N = 10) were selected by purposive sampling of people who were managers or related experts in travel agencies. Purposive sampling is mainly used for opinion surveys. For this study, participants were required have been in the travel agent business for at least 5 years. Interviews were conducted via phone with ten participants, five from travel agents in Taiwan, and five from the college teachers in tourism department.

The questionnaire is composed of two parts. First the questionnaire addresses demographics, including gender, age, professional position, marriage, number of kids, part-time job, and education. Second, the questionnaire addresses the characteristics of travel agency salespeople, using 10 items of responds to the rising application of mobile channel. The answers are constructed with the Likert scale. The interviews protocol was developed in English and based on the literature review. The interviews explored more fully the perceptions of the people of experience about the travel agent and mobile channel. Interviews were conducted in Chinese. The codes and supporting words emerging from the transcripts of interviews were translated into English for analyzing.

Grey Relational Analysis Methodology.

The grey system method, as developed by Deng [12], has been extensively applied in various fields, including decision science. In this study, the GRA is applied to construct an evaluation method for selecting the risk management factors of travel business with mobile channels in Taiwan. The GRA is calculated as follows:

Let X_0 be the referential series with *k* entities (or criteria) of X_1, X_2, …,X_i, …, X_N (or *N* measurement criteria). Then

$$X_0 = \{x_0(1),\ x_0(2),\ ...,\ x_0(j),\ ...,\ x_0(k)\},$$

$$X_1 = \{x_1(1),\ x_1(2),\ ...,\ x_1(j),\ ...,\ x_1(k)\},$$

$$\vdots$$

$$X_i = \{x_i(1),\ x_i(2),\ ...,\ x_i(j),\ ...,\ x_i(k)\},$$

$$\vdots$$

$$X_N = \{x_N(1),\ x_N(2),\ ...,\ x_N(j),\ ...,\ x_N(k)\}.$$

The grey relational coefficient between the compared series X_i and the referential series of X_0 at the *j*-th entity is defined as

$$\gamma_{0i}(j) = \frac{\Delta\min + \Delta\max}{\Delta_{0j}(j) + \Delta\max}, \qquad (1)$$

where $\Delta_{0j}(j)$ denotes the absolute value of difference between X_0 and X_i at the *j*-th entity,that is

$\Delta_{0j}(j) = |x_0(j) - x_i(j)|$, and $\Delta\max = \max_i \max_j \Delta_{0j}(j)$, $\Delta\min = \min_i \min_j \Delta_{0j}(j)$.

The grey relational grade (GRG) for a series of X_i can be expressed as

$$\Gamma_{0i} = \sum_{j=1}^{K} w_j \gamma_{0i}(j), \qquad (2)$$

Where w_j represents the weight of *j*-th entity. If the weight does not need to be applied, take $\omega_j = \frac{1}{K}$ for averaging.

Before calculating the grey relation coefficients, the data series can be treated based on the following three kinds of situation and the linearity of data normalization to avoid distorting the normalized data [13]. They are:

1. Upper-bound effectiveness measuring (i.e., larger-the-better)

$$x_i^*(j) = \frac{x_i(j) - \min_j x_i(j)}{\max_j x_i(j) - \min_j x_i(j)}, \qquad (3)$$

where $\max_j x_i(j)$ is the maximum value of entity *j* and $\min_j x_j(j)$ is the minimum value of entity *j*.

2. Lower-bound effectiveness measuring (i.e., smaller-the-better)

$$x_i^*(j) = \frac{\max_j x_i(j) - x_i(j)}{\max_j x_i(j) - \min_j x_i(j)}, \qquad (4)$$

ISSN 2278-5612

If $\min_j x_i(j) \le x_{ob}(j) \le \max_j x_i(j)$, then $x_i^*(j) = \dfrac{|x_i(j) - x_{ob}(j)|}{\max_j x_i(j) - \min_j x_i(j)}$, (5)

If $\max_j x_i(j) \le x_{ob}(j)$, then $x_i^*(j) = \dfrac{x_i(j) - \min_j x_i(j)}{x_{ob}(j) - \min_j x_i(j)}$, or (6)

If $x_{ob}(j) \le \min_j x_i(j)$, then $x_i^*(j) = \dfrac{\max_j x_i(j) - x_i(j)}{\max_j x_i(j) - x_{ob}(j)}$. (7)

where $x_{ob}(j)$ is the objective value of entity *j*.

Data Analysis

Table 1. Questionair data of the risk management factors

Factors \ Expert	1	2	3	4	5	6	7	8	9	10
Agreement or contract	5	5	3	4	5	4	3	5	5	5
Jurisdiction	4	5	5	4	5	5	4	4	5	5
Damaged or spoiled by employees	4	5	4	4	3	4	3	4	4	4
Burglary	3	4	3	4	2	3	4	2	3	4
Normal wear and tear or malfunction	3	4	3	2	3	2	2	3	2	3
Natural disaster	2	3	3	2	2	3	2	3	3	2
System vulnerability	3	4	4	4	3	4	4	4	4	4
Mistakes made by employees	4	3	4	3	4	4	5	4	5	5
Social engineering	4	5	4	5	4	4	5	4	4	4
Privacy	5	3	3	4	2	3	4	3	3	3

Calculation of $\Delta_{0j}(j)$ equals the difference between X_0 and X_i .The result is in table 2。

Table 2.the calculation result of $\Delta_{0i}(j)$ of the risk management factors

	1	2	3	4	5	6	7	8	9	10
Δ_{01}=	0.0000	0.0000	2.0000	1.0000	0.0000	1.0000	2.0000	0.0000	0.0000	0.0000
Δ_{02}=	1.0000	0.0000	0.0000	1.0000	0.0000	0.0000	1.0000	1.0000	0.0000	0.0000
Δ_{03}=	1.0000	0.0000	1.0000	1.0000	2.0000	1.0000	2.0000	1.0000	1.0000	1.0000
Δ_{04}=	2.0000	1.0000	2.0000	1.0000	3.0000	2.0000	1.0000	3.0000	2.0000	1.0000
Δ_{05}=	2.0000	1.0000	2.0000	3.0000	2.0000	3.0000	3.0000	2.0000	3.0000	2.0000
Δ_{06}=	3.0000	2.0000	2.0000	3.0000	3.0000	2.0000	3.0000	2.0000	2.0000	3.0000
Δ_{07}=	2.0000	1.0000	1.0000	1.0000	2.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Δ_{08}=	1.0000	2.0000	1.0000	2.0000	1.0000	1.0000	0.0000	1.0000	0.0000	0.0000
Δ_{09}=	1.0000	0.0000	1.0000	0.0000	1.0000	1.0000	0.0000	1.0000	1.0000	1.0000
Δ_{010}=	0.0000	2.0000	2.0000	1.0000	3.0000	2.0000	1.0000	2.0000	2.0000	2.0000

Employ an application with the linearity of data normalization to avoid distorting the normalized data。The calculation result is in Table 3.

ISSN 2278-5612

Table 3. The result of the linearity of data normalization

	1	2	3	4	5	6	7	8	9	10
γ_{01}=	1.0000	1.0000	0.4286	0.6000	1.0000	0.6000	0.4286	1.0000	1.0000	1.0000
γ_{02}=	0.6000	1.0000	1.0000	0.6000	1.0000	1.0000	0.6000	0.6000	1.0000	1.0000
γ_{03}=	0.6000	1.0000	0.6000	0.6000	0.4286	0.6000	0.4286	0.6000	0.6000	0.6000
γ_{04}=	0.4286	0.6000	0.4286	0.6000	0.3333	0.4286	0.6000	0.3333	0.4286	0.6000
γ_{05}=	0.4286	0.6000	0.4286	0.3333	0.4286	0.3333	0.3333	0.4286	0.3333	0.4286
γ_{06}=	0.3333	0.4286	0.4286	0.3333	0.3333	0.4286	0.3333	0.4286	0.4286	0.3333
γ_{07}=	0.4286	0.6000	0.6000	0.6000	0.4286	0.6000	0.6000	0.6000	0.6000	0.6000
γ_{08}=	0.6000	0.4286	0.6000	0.4286	0.6000	0.6000	1.0000	0.6000	1.0000	1.0000
γ_{09}=	0.6000	1.0000	0.6000	1.0000	0.6000	0.6000	1.0000	0.6000	0.6000	0.6000
γ_{010}=	1.0000	0.4286	0.4286	0.6000	0.3333	0.4286	0.6000	0.4286	0.4286	0.4286

After calculation, the main impact factors of the risk management factors were decided. The result is in Table 4.

Table 4.Grey relational grade (GRG) of the risk management factors

Risk Management Factors	γ_{0i}
Agreement or contract	0.8057
Jurisdiction	0.8400
Damaged or spoiled by employees	0.6057
Burglary	0.4781
Normal wear and tear or malfunction	0.4076
Natural disaster	0.3810
System vulnerability	0.5657
Mistakes made by employees	0.6857
Social engineering	0.7200
Privacy	0.5105

According to γ_{0i}, the priority of the main impact factors of the risk management factors is listed as the follows:

FACTOR2> FACTOR1 > FACTOR9 > FACTOR8 > FACTOR3 > FACTOR7 > FACTOR10 > FACTOR4 > FACTOR5 > FACTOR6

Conclusion

With the process of Grey relational grade, the top three appropriate risk management factor selected by the interviewers were “Jurisdiction”, “agreement and contract”, and “Social engineering”. Since the development of mobile channel for travel industry is inevitable, a positive risk management consideration is even more important.

The first risk management consideration is jurisdiction. Jurisdiction is the practical authority to interpret and apply the law that the legislators still too busy with their elections to deal with the law issue of sharing economy. Since collaborative consumption is a new inevitable business model, how to govern and constitute a legal environment is an irresistible responsibility to our legislators. Or there will be potential cost while there is conflict between the customer and the service provider. Therefore, how to lobby the legislators to constitute a fair trade environment of related law is an urgent assignment right now.

The second risk management consideration is agreement and contract. Since the law issue is still not settled, the base of the agreement and contract is remain ambiguous, so whenever there is a law suit, the representative will have to argue based on the ambiguity. Such circumstance will cost expensive human resource spends on much more court employees. After the basic law of mobile channels is done, a feasible standard contract should be developed that the whole business deal will be processed on the right track.

Sharing economy refers to online peer-to-peer-based sharing of access to services. The third risk management consideration, social engineering, is inescapable that it is an information security issue on Internet (Anderson, 2008). The

hackers are attacking mobile channels all the time with all different kind of tricks to manipulate people psychologically into divulging confidential information. To obtain private information, the hackers may send emails that appear to come from legitimate business requesting "verification" of private information and warning of some awful consequence if it is not provided. Such phishing technique of social engineering damages the creditability of mobile channels.

As one of the members of information society, it is a collaborative responsibility to face the sharing economy for customers, entrepreneur, and government. Sharing economy with mobile channels makes it easy for people and organizations in the community to transact directly, and reduce the friction of share-based travel business and organizational models. As long as the risk management factors were properly regulated, those social lending, peer-to-peer travel experiences or peer-to-peer accommodation will be a great contribution to our community in Taiwan.

References

[1] S.Shankman. *Airbnb Gives Hosts the Tools to Become Hoteliers in App Redesign*, http://skift.com/2013/11/13/airbnb-gives-hosts-the-tools-to-become-hoteliers-in-app-redesign/, Retrieved26 Nov., (2015).

[2] C. Hutchinson, J. Ward and K. Castilon, Navigating the next-generation application architecture. *IT Professional*.**1** (2), 18-22, (2009).

[3] BBC News,*Cloud computing for business goes mainstream, 06 May 2010* [Online].http://www.bbc.co.uk/news/10097450Accessed 10.12.12, (2010).

[4] J. Rizzi, In the Mix, *Target Marketing*, **24**, 13, (2001).

[5] S. Subashini, V. Kavitha, A Survey on Security Issues in Service Delivery Models of CloudComputing, Journal of Network and Computer Applications. 341-11,(2011).

[6] J. Casale, Social Networking, Cloud Computing Bring New Risk Exposures, BusinessInsurance. 44(38), 17,(2010).

[7] E. Bublitz, Catching The Cloud: Managing Risk When Utilizing Cloud Computing, NationalUnderwriter P & C. 114(39), 12-16,(2010)

[8] S. Paquette, P.T. Jaeger,S.C. Wilson, Identifying the Security Risks Associated withGovernmental Use of Cloud Computing', Government Information Quarterly. 27, 245-53,(2010)

[9] P.T. Jaeger, J.M. Grimes, J. Lin, S.N. Simmons, Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing. 14(5), 4-15, (2009).

[10] D. Svantesson, R. Clarke, Privacy and Consumer Risks in Cloud Computing, Computer Law& Security Review. 26, 391-397,(2010).

[11] M. Armburst, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, Above the Clouds: A Berkley View of Cloud Computing'. Accessed on from Dec 5, 2011, http://radlab.cs.berkekey.edu/, (2009).

[12] J.L. Deng, Introduction to Grey System, Journal of Grey System, 1(1), 1-24, (1989).

[13] J. Deng, Grey System Theory and Applications, Lao-Li, Taiwan, (1999).

[14] Ross J. Anderson, Security engineering: a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley, (2008).