A study on the damage costs for private information leakage using the contingent valuation method

S. Y. Lee, J. H. Chung & J. S. Lee
Safety Research Division,
National Disaster Management Institute, Korea

Abstract

This paper estimates the damage costs of data breaches. In January 2014, around 100 million records containing sensitive personal information were maliciously leaked in Korea. Since this leakage of personal information could lead to cybercrimes such as phishing, pharming and privacy invasion, it caused severe social confusion. Despite its seriousness, current studies rarely estimate the damage from the victims’ perspectives or evaluate the value of personal data. Therefore, this study aims to estimate the true social costs of this privacy invasion. In addition, we evaluate the non-market value of personal information by estimating willingness to pay (WTP). For the analysis, we use the contingent valuation method (CVM) with double-bounded dichotomous choice questions. The result of the CVM analysis shows that individual WTP for protecting personal information is KRW 2,940 which is KRW 35,280 in annual cost. According to the analysis, the estimated damage cost of personal information leakage occurred in 2014 in Korea was up to KRW 529 billion, considering the actual victims in the calculation.

Keywords: data breach, personal information leakage, social disaster, CVM, WTP.

1 Introduction

In January 2014, almost 100 million pieces of personal information were maliciously stolen in Korea. It was noted as the worst personal data theft case in Korea. It was ranked the 10th malicious case in the world, when considering a large amount of personal information stolen in a data breach case. Given that
thousands of individuals were negatively affected by this incident, a data breach was considered as a social disaster. 106 million pieces of personal data from 3 major card companies (KB, NH, Lotte Card) were stolen, and customers feared potential cybercrimes using their personal information, such as bank fraud or identity theft. The stolen personal data had the following personal identifiable information: names, resident registration numbers, mobile numbers, credit card numbers, credit card expiration dates and so on.

The Personal Information Protection Act, Article 2 states as follows: The term “personal information” means information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified, (including information by which the individual in question cannot be identified but can be identified through a simple combination with other information). According to the Personal Information Protection Commission, the private information is subdivided into 16 categories: general information, family, education and training, military service, real estate, income, other incomes, credit, employment, legal, medical, organization, telecommunication, location, physical information and hobby.

Recently, the number of cyber-attacks on major companies or government agencies for unauthorized access to personal information has massively increased, and these attackers target a wide range of individuals. As the cybercrimes induced by data breaches become more sophisticated and damage becomes more severe than ever before, it is very important to keep personal information safe and secure.

Even though there have been several data breach cases in Korea, many studies insufficiently discuss the damage from the victims’ perspectives or evaluate the value of personal information. And the damage costs in data breaches should comprehensively include the implicit costs of individual victims as well as the damage costs of enterprises.

If one can comprehend and estimate the exact size of the damage, it is not difficult to figure out the magnitude of social and economic effects caused by a data breach. This study also can help with government policy and government budget decision making on these data breach issues. In this study, we survey individuals living in 7 metropolitan cities in South Korea, whose ages are over 20, and ask how much they are willing to spend monthly for the prevention of possible data breaches if the payment were made for ten consecutive years. A double-bounded dichotomous question method is used for the survey.

We organize this study as follows. With a review of current literature, we will briefly explain about the CVM (contingent valuation method) in Section 3. Section 4 will be the explanation of the data we used in the study, and Section 5 will be focused on the result of the CVM analysis. Lastly, Section 6 provides conclusions and suggestions from implication of the analysis.

2 Literature review

Gordon and Loeb [1] classified types of damage from data breaches and defined factors for the damage. They specifically classified the types of the damage as
following: direct costs, indirect costs, explicit costs, and implicit costs. In
addition, the factors such as loss of confidentiality, loss of availability, and loss
of integrity are the criterion of defining the damage from data breaches.

Japan Network Security Association [2] estimated the damage of data
breaches by applying the ‘JO model’ (JNSA Damage Operation Model for
Individual Information Leak) for evaluation. With JO model, it analyzed
accumulated historical data breach cases. The JO model is a value evaluation
model developed by JNSA’s own criterion, which evaluates the value of
personal information and categorizes the damage types into three levels
of economic losses and three levels of mental damages. This JO model is
designed to estimate the damage costs by using the historical data as an input.

The Ponemon Institute [3–5] in the United States has studied the damage
estimation of data breaches since 2005. By conducting surveys from 45
enterprises in 15 industries, the institute not only researched the direct costs and
indirect costs of data breaches, but also researched the overall costs. For example,
a credit problem or customer churn could also be considered as the overall costs.
The average amount of damage from data breaches was USD 201 in 2013, which
was increased by 6.9% compared to the USD 188 in 2012.

Changhee Han et al. [6] applied an idea from both the study of the Ponemon
Institute in the United States and the study of the Japan Network Security
Association (JNSA). While the Ponemon Institute suggested the damage
estimates of data breaches from the perspective of enterprises, and JNSA
suggested the damage estimates from the perspectives of individuals, Changhee
Han et al. [6] proposed that damage estimates in data breach cases
simultaneously cover the perspectives of both enterprises and individuals.
Specifically, the losses from enterprises included direct or indirect costs to
manage information leakage and recover business reputation: labor cost for the
workforce, investor relation cost, legal compensation cost, and possible profit
losses. The losses from individuals affected by data breaches could be evaluated
by estimating the lost value of personal information.

Complementing the previous studies, we focused more on dealing with the
estimation of the value of personal information from individuals’ perspectives,
than dealing with the profit loss or cost of the enterprises.

3 Contingent valuation method (CVM)

The contingent valuation method (CVM), a valuation method based on the
survey, is widely used to measure a willingness to pay (WTP) of the survey
respondents for non-market goods which are difficult to measure the exact value
from the market. In this study, we use the CVM in order to measure the value of
personal information and to see how much respondents are willing to pay for
protecting their personal information; the non-market good.

Depending on questionnaire formats, the types of elicitation methods are
various as follows: open-ended question, bidding game, payment card, single or
double-bounded dichotomous choice, etc. When using dichotomous questions, a
researcher randomly gives a sequence of bids to respondents, and asks for a yes or no vote on whether each bid exceeds the respondents’ WTP. Not only the method makes the respondents feel relatively comfortable to answer, it also minimizes potential biases such as starting point bias or the operational bias.

Bishop and Heberlein [7] confirmed that the method of dichotomous question was highly credible, and Hanemann et al. [8] proposed adding follow-up questions to obtain further information about the respondents’ WTP. By using the double bounded dichotomous question method which asks the follow-up questions, it is possible to complement the efficiency loss from the single-bounded dichotomous question. Therefore, in this study, we estimate respondents’ WTP for protecting personal information by adopting the double-bounded dichotomous question method.

A dichotomous question does not provide a direct level of WTP of the respondents. It only confirms a yes or no response, which reflects respondents’ reactions to the offered level of payment. Therefore, in order to estimate the economic value, the responses should be calculated by the probability function of WTP. Moreover, the fact that whether a response is a simple nonresponse of zero bid or a “protest” response, the zero bid should be checked since there may be a bias since a respondent with a protest response would not explicitly present their preference when answering the survey question (Cummings et al. [9]). Therefore, it is difficult to drive a statistically significant level of WTP from general CVM, and the adjustment on the zero bids is required. The protest responses should be excluded from the sample by assuming the responses as irrational payment decisions. In this study, in order to distinguish protest responses from true non-responses, we use a protest response identification method suggested in Hyungna Oh [10], and estimate respondents’ WTP for protecting personal information by adopting the double-bounded dichotomous question method.

4 Data

The survey was conducted by Embrain Online Research Company (Embrain Co., Ltd, Seoul, Korea) between November 11th and November 16th, 2014, and asked 1,000 individuals living in 7 metropolitan cities in South Korea, whose ages are in the range of over 20 and under 64. Among 1000 total respondents, we exclude 349 people who are protest respondents, in order to adjust a potential bias from the non-responses. We will explain further about the protest respondents in a later section of the paper. Table 1 shows the characteristics of the 651 respondents, excluding the 349 respondents who are considered as protest respondents. Among the 651 total respondents, 341 are male and 310 are female. The average age is 41.3, with the average education of 15.1 years. Additionally, the average salary is KRW 3.43 million.
Table 1: Characteristics of the respondents.

<table>
<thead>
<tr>
<th>Personal factor</th>
<th>Composition</th>
<th>Freq.</th>
<th>Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Man</td>
<td>341</td>
<td>52.4</td>
</tr>
<tr>
<td></td>
<td>Woman</td>
<td>310</td>
<td>47.6</td>
</tr>
<tr>
<td>Age</td>
<td>20–29</td>
<td>146</td>
<td>22.4</td>
</tr>
<tr>
<td></td>
<td>30–39</td>
<td>146</td>
<td>22.4</td>
</tr>
<tr>
<td></td>
<td>40–49</td>
<td>155</td>
<td>23.8</td>
</tr>
<tr>
<td></td>
<td>50–59</td>
<td>156</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>~60</td>
<td>48</td>
<td>7.4</td>
</tr>
<tr>
<td>Education</td>
<td>High school</td>
<td>131</td>
<td>20.3</td>
</tr>
<tr>
<td></td>
<td>College</td>
<td>104</td>
<td>16.1</td>
</tr>
<tr>
<td></td>
<td>University</td>
<td>335</td>
<td>51.9</td>
</tr>
<tr>
<td></td>
<td>Graduate school</td>
<td>75</td>
<td>11.6</td>
</tr>
<tr>
<td>Salary</td>
<td>~1,000,000 KRW</td>
<td>53</td>
<td>8.1</td>
</tr>
<tr>
<td></td>
<td>1,010,000–2,000,000 KRW</td>
<td>118</td>
<td>18.1</td>
</tr>
<tr>
<td></td>
<td>2,010,000–2,500,000 KRW</td>
<td>88</td>
<td>13.5</td>
</tr>
<tr>
<td></td>
<td>2,510,000–3,000,000 KRW</td>
<td>65</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>3,010,000–3,500,000 KRW</td>
<td>61</td>
<td>9.4</td>
</tr>
<tr>
<td></td>
<td>3,510,000–4,000,000 KRW</td>
<td>48</td>
<td>7.4</td>
</tr>
<tr>
<td></td>
<td>4,010,000–5,000,000 KRW</td>
<td>85</td>
<td>13.1</td>
</tr>
<tr>
<td></td>
<td>5,010,000–7,000,000 KRW</td>
<td>86</td>
<td>13.2</td>
</tr>
<tr>
<td></td>
<td>~7,010,000 KRW</td>
<td>47</td>
<td>7.2</td>
</tr>
</tbody>
</table>

*Six respondents’ information on college attendance was excluded due to the difficulty in the clarification of the year of education.

5 Results of contingent valuation method (CVM)

In order to implement the survey with the double-bounded dichotomous question method, one should set the first offered amount. Therefore, we conducted a pretest open-ended survey of 100 employees working in National Disaster Management Institute in Korea. The respondents were asked to answer the amount of monthly payment they were willing to pay for prevention of possible personal information leakage with an explanation that the amount should be considered to be paid every month for 10 years. Excluding the amount of the lowest and highest 15%, the first offered amount was decided to KRW 2000, KRW 4000, KRW 6000, and KRW 8000. The first offered amount was arbitrarily assigned to the respondents with the certain ratio.

As explained above, it is important to distinguish whether a response is a true non-response or a protest response since protest respondents cause bias in an analysis, and it becomes difficult to draw a statistically significant WTP. Depending on the answers to the CVM questions, we identify a protest respondent with a criteria set as below in table 2. If one answers ‘economically
unaffordable’, the answer is not considered as a protest response since the answer is related to the personal affordability of the respondent. Moreover, if one answers ‘the damage from a private information leakage is not significant; it is not worth paying such an amount for protecting the personal information’, then the answer is not considered as a protest response either because the marginal utility of the respondent toward the personal information protection is practically close to zero. However, when one answers ‘a private information leakage is incurred mainly because of improper maintenance of an enterprise; the enterprise should take the full responsibility’, then the respondent becomes a protest respondent since he/she protests to explicit the WTP by pointing out the validity and the fairness of paying for the information protection (McFadden [11]). Likewise, the answer such as ‘protection against private information leakages is each individual’s responsibility’ is classified as a protest response, as the respondent of the answer is shown to believe that government and enterprises are unqualified to protect personal information in substance. Finally, the answer ‘a private information leakage is not a simple matter which can be prevented by paying money for the protection’ is also considered as a protest response due to its discredit upon government’s capability of implementing the task. Therefore, among 395 non-respondents of 1000 total respondents, we exclude 349 people who are protest respondents but include 46 people who are true non-respondents.

Table 2: Identification of protest respondents.

<table>
<thead>
<tr>
<th>Description of the responses</th>
<th>Number of people</th>
</tr>
</thead>
<tbody>
<tr>
<td>True non-response</td>
<td></td>
</tr>
<tr>
<td>Economically unaffordable</td>
<td>26</td>
</tr>
<tr>
<td>it is not worth paying such an amount for protecting personal information</td>
<td>20</td>
</tr>
<tr>
<td>Protest response</td>
<td></td>
</tr>
<tr>
<td>A corporation should take the full responsibility</td>
<td>237</td>
</tr>
<tr>
<td>Protection against private information leakages is each individual’s full responsibility</td>
<td>8</td>
</tr>
<tr>
<td>A private information leakage is not a simple matter which can be prevented by paying money for the protection</td>
<td>84</td>
</tr>
</tbody>
</table>

The double bounded dichotomous question method is implemented as follows: If a respondent indicates a willingness to pay the first offered amount and says yes, the new threshold is about double the first one. However, if the respondent says no to the first offered amount, the new threshold is about half of the first one. Let the first offered threshold, assigned to the respondents, be denoted \((t_1, t_2)\). The double bounded dichotomous method can simply be expressed as form (1) below.
(Yes/Yes) : $WTP \geq t^2$
(Yes/No) : $t^1 \leq WTP < t^2$
(No/Yes) : $t^2 \leq WTP < t^1$
(No/No) : $WTP < t^2$

(1)

Table 3 shows the distribution of CVM responses excluding the answers of protest respondents. It is confirmed from the table that the first offered amount is relatively evenly distributed among the respondents, even if the protest respondents are excluded from the sample. In addition, the ratio of answering ‘No/No’ increases as the first offered amount becomes higher.

Table 3: Distribution of respondents by first offered amount.

<table>
<thead>
<tr>
<th>First offered amount (KRW/month)</th>
<th>N (= 651)</th>
<th>Response regarding WTP</th>
<th>Yes/Yes</th>
<th>Yes/No</th>
<th>No/Yes</th>
<th>No/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>173</td>
<td>21</td>
<td>12.1%</td>
<td>64</td>
<td>37%</td>
<td>53</td>
</tr>
<tr>
<td>4000</td>
<td>158</td>
<td>8</td>
<td>5.1%</td>
<td>33</td>
<td>20.9%</td>
<td>51</td>
</tr>
<tr>
<td>6000</td>
<td>161</td>
<td>8</td>
<td>5%</td>
<td>29</td>
<td>18%</td>
<td>49</td>
</tr>
<tr>
<td>8000</td>
<td>159</td>
<td>13</td>
<td>8.2%</td>
<td>31</td>
<td>19.5%</td>
<td>32</td>
</tr>
</tbody>
</table>

The case of $t^1 \leq WTP < t^2$ can be considered as a situation when a respondent answers ‘yes’ to the first offered amount and ‘no’ to the second offered amount. This probability takes the explicit form:

$$Pr(1,0) = Pr(t^1 \leq WTP < t^2) = Pr(t^1 \leq z_i \beta + u_i < t^2)$$

$$= Pr \left( \frac{t^1 - z_i \beta}{\sigma} \leq \frac{t^2 - z_i \beta}{\sigma} \right)$$

$$= \Phi \left( \frac{t^2 - z_i \beta}{\sigma} \right) - \Phi \left( \frac{t^1 - z_i \beta}{\sigma} \right)$$

(2)

The log-likelihood function for the double bounded dichotomous question model then takes the following from (Cameron and Quiggin [12]):

$$\ln L = \sum_{i=1}^{N} [I_i^{yy} \ln(\Phi \left( \frac{t^2 - z_i \beta}{\sigma} \right) - \Phi \left( \frac{t^1 - z_i \beta}{\sigma} \right)) + I_i^{yy} \ln(\Phi \left( \frac{z_i \beta - t^2}{\sigma} \right))]$$

$$+ I_i^{yy} \ln(\Phi \left( \frac{t^2 - z_i \beta}{\sigma} \right) - \Phi \left( \frac{t^1 - z_i \beta}{\sigma} \right)) + I_i^{nn} \ln(1 - \Phi \left( \frac{z_i \beta - t^2}{\sigma} \right))]$$

(3)
The superscript of the indicator function ‘I’ corresponds to the respondent’s answer to the question, and becomes 1 if one of the case(s) ‘yn, yy, ny, nn’ fits to the respondent’s answer and becomes 0 if does not fit to the answer. The parameter of eqn. (3) is estimated by maximum likelihood estimator, and the result is shown in the table 4 below. When the 651 respondents’ willingness pay amount is estimated after excluding the protest respondents, the WTP is KRW 2940. With the inclusion of protest respondents in the analysis, the WTP is KRW 580. The two results are statistically significant, but not significant regarding the respondents’ gender, age, education, and salary.

Table 4: WTP.

<table>
<thead>
<tr>
<th>Protest respondents</th>
<th>WTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excluding pretest respondents (N=651)</td>
<td>2939.7</td>
</tr>
<tr>
<td>Including protest respondents (N=1,000)</td>
<td>575.1</td>
</tr>
</tbody>
</table>

*Statistically significant in the confidence level of 1%.

When calculating the amount into the annual payment, it is KRW 35,277 and KRW 6,902. The damage from the loss of personal information in data breach cases in 2014 can be estimated to KRW 529 billion. In the case, the number of personal data which were leaked was over 100 million, and the actual victims of these data breaches were 15 million.

The estimated annual WTP in this study is slightly lower than the results from previous studies, KRW 46,800 in the study of Yeora Kim et al. [13] and KRW 88,128 in the study of Korea Online Privacy Association [14]. The difference in these results can be interpreted as the consequence of majority’s insensitivity to the protection of personal information because of their frequent exposure to the breach cases. Because people have been repeatedly exposed to data breach cases, they have doubts about usefulness of protection methods provided by government or enterprises.

6 Conclusions

In this study, we evaluated non-market value of personal information by estimating the willingness to pay (WTP) of each individual using the survey data. Recently, the number of the stolen personal data becomes massive and the range of the victims becomes wider than ever before. Moreover, the cyber-crimes induced by these private information leakages become more serious. It is not difficult to see that victims of frauds or identity thefts have been recently increased, and the crimes become very complicated. As financial frauds become more sophisticated, the policy regarding personal information protection should be enhanced to effectively deal with the potential crimes.

The following is the result of the study, which is based on the survey conducted of the 1000 individuals living in 7 metropolitan cities in South Korea,
whose age is over 20. When estimating the amount of willingness to pay of 651 respondents excluding the protest respondents, the WTP is KRW 2940. When calculating the amount into the annual payment, it is KRW 35,277. In addition, the damage costs of the loss of personal records caused by the private information leakages in 2014 in Korea can be estimated to KRW 529 billion.

The study estimates the value of personal information using the CVM analysis. We recognized that it is preferred to conduct interview surveys in order to gather further information from the respondents. However, because of technical limitations, we conducted online surveys, and there may be biases from the respondents’ characteristics or levels of understanding. However, in the analysis, we applied several methods to adjust the biases, and therefore this study can contribute to the estimation of the exact size of the damage. This study helps the majority to figure out the magnitude of the social and economic effects caused by a private information leakage. Moreover, the study can also help with the government’s policy and budgeting decisions with regard to private information leakage issues.

References


