Master's Thesis
Information Science

Radboud University

Privacy-Trust-Behavior in Web-Based Insurance Services:

Identifying the Relationship between Privacy Concern with Customer's Trust and Behavioral Intention to Use Web-based Insurance Services in Indonesia

Author:
Rizka Eka Putri
s4336011

First supervisor/assessor:
Dr. Sjaak Smetsers
s.smetsers@science.ru.nl

Second supervisor/assessor:
Dr. Perry Groot
perry.groot@science.ru.nl

September 10, 2015

Abstract

Nowadays, the free movement of electronic information in social networks and public services are growing. However, hesitancy in providing personal information to web-based public services may interfere with the successful implementation of these public services. To study the relationship between privacy concern, trust and behavioral intention in using online services, a privacy-trust-behavioral intention model was presented in 2004 [34]. This research focuses on developing a new research model that also identifies the relationship between privacy concerns, trust, and behavioral intention in using web-based insurance services. The variables of the privacy concerns are taken from the previous study about concern for information privacy instruments [58]. By combining those two former studies, a new research model was developed with four variables of privacy concerns that influence the user's trust and behavioral intention to use the insurance web-services. This research was conducted using a quantitative approach. Data gathering was performed by distributing an online survey to 107 people with insurance schemes in Indonesia. The data was analyzed using Structural Equation Modeling and path analysis. The result of the study tells us that the model does not have a strong support from the use of structural equation modeling. However, it has strong support from the use of path analysis. Unauthorized access and errors in privacy concern has a strong positive relationship with the degree of trust while the degree of trust has a strong relationship with the behavioral intention and actual use of insurance web-services.

Acknowledgments

First, I would like to thank Allah SWT for His grace and blessing of health and strength during my study. Furthermore, I would like to express my earnest gratitude to my supervisor, Sjaak Smetsers, for the countless valuable knowledge, remarks, guidance and engagement through the learning process of this master thesis. I also would like to thank Perry Groot as my second supervisor and assessor to the topic as well for the support on the way. My sincere gratitude is also given to all the participants in my online survey, who have willingly shared their precious time during the process of data collection. This master thesis is also dedicated to my parents, sisters, and all of my best friends, who have supported me throughout the entire process, both by keeping me harmonious and helping me putting pieces together. I will be grateful forever for your love. Lastly, my special gratitude for Indonesian Endowment Fund for Education for giving me an opportunity to pursue my master degree and for Indonesian Student Association in Nijmegen for giving me a great motivation and help during my study.

Contents

Chapter 1

Introduction

1.1 Background

Most Internet users express concern about the privacy of their personal information, especially information related to finances and health [2]. One of users' main concerns is the likelihood of being a victim of Internet fraud. A possible threat is unauthorized access to personal information provided in web-based services [58]. In addition to fraud, other forms of cyber-criminality can attack the personal information of Internet users. Cyber-criminality is increasingly seen as a significant criminal activity by governments around the world, whether purely digital crimes or traditional crimes which are enhanced through the use of digital technology [23]. Many business activities have already moved their business transactions and processes into web-based applications (mobile or not) [60]. They force customers to place their personal information onto the website to obtain a better service [46]. The hesitancy to enter personal information in the website may affect the successful implementation of web-based application as one of the transaction channels.

One of the business sectors which has moved toward a web-based application for their business activities is insurance. Car insurance, property insurance, health insurance, and pension funds have developed and use web-based applications for their business functions, such as signing up or making claims. This tendency of web-based insurance is also reaching Indonesia, as one of the most rapidly growing countries in the use of Internet and social media [55]. The rapid growth of cyberspace in Indonesia means a vulnerability to cyber-security. Various forms of cyber-crime appear along the use of web-based applications in most business sectors, especially in e-commerce sectors (online shopping and electronic payment). The most notorious cyber-crime types in Indonesia are identity theft and data, piracy accounts, the spread of malware and malicious code, fraud, industrial espionage, hostage-critical information resources, and cyber warfare [55]. Those that get the most attention from the Indonesian government are data theft, release of private data, copyright violation, defacing, and patriotic hacking [55].

Theft of personal data and sensitive information has recurrently taken place in Indonesia[55]. The sources of vulnerability vary. It is related to the effort made by the data controller and the data processor. The data controller is a person who (either alone or with others) determines the purposes for which and the manner in which any personal data is, or is to be, processed [51]. Meanwhile, the data processor means any person (other than the data controller) who processes the data on behalf of the data controller [51]. Meanwhile, the data processor means any person (other than the data controller) who processes the data on behalf of the data controller [51].

Theft is often a result of neglecting to take adequate security measures in data storage [36]. In order to protect personal data, the data controller and the data processor must start taking precautionary measurements. In an attempt to ward off cyber-crime, standardization of privacy protection by both the data processor and the data controller is needed [36] and the data subject's privacy awareness must be increased in an attempt to safeguard personal data and sensitive information [30]. The one that should be aware of the privacy protection is none other than the data subject. The data subject is an individual who is the subject of personal data [51].

In addition to data subject displaying a lack of privacy awareness, we note that data-processors also lack critical security measurements. An example of this is the approximately 25

million entries of customer-data disclosed to an unauthorized third party in 2011 by a telecommunications provider [36].This was a big issue because there was no specific data protection regulation that could deal with it [36]. The impact of this leak was fraud, with fake SMSs to transfer some amount of money to a specific account number, with different techniques such as lying about needing money for certain damage that was caused or happened to family members of victims [36]. These techniques often succeeded since most data subjects believed that their phone number was only known to the acquaintances or family members [36]. The Indonesia Telecommunication Regulation Body could not rely on the UU Telekomunikasi (Telecommunication Act) to solve this issue. This kind of issue is still happening until now, however more and more data subjects are aware of this fraud technique [36]. This issue exposed the vulnerabilities of current privacy protection mechanisms, especially in Indonesia.

The issue of personal data theft that leads to fraud has come into the spotlight and makes citizens worry when providing their personal data in web-based application such as e-commerce services, and even mailing lists. The limitations of data protection, computer crime or even electronic payment protection laws and acts also lead to anxieties of Internet users in using web-based applications, even though such applications often offer more effective and efficient business transactions. The limitations of certain laws about data protection lead internet users to rely heavily on the companies concerned to safeguard their personal data. For example, a customer in the health sector relies heavily on hospital management and health care application management in processing and safeguarding their data [37]. Based on research by the Health Information Trust, executives believe that the health industry such as hospitals and health insurance providers need to standardize guidelines and provide uniform security frameworks to properly safeguard personal data and sensitive information of their customers [37].

Within this context, the main question is how the internet users can believe in a certain company when providing their personal data and sensitive information in web-based applications. Do concerns about personal data affect this decision? If yes, what are the aspects from the company that makes the customers believe that their personal data is safe with them? These questions can help us to identify whether privacy concerns really limit the implementation of web-based applications, especially for insurance company. In this research, we suggest and test a new model with structural equation modeling that takes into account Internet users' concerns about information privacy, their trust in a certain insurance company, and their behavior toward the use of web-based insurance applications. The model will suggest that concern for information privacy may affect the trust and behavioral intention of insurance participants to use web-based applications.

1.2 Research Objective and Questions

As explained above, this research aims to identify the relationship between privacy concerns with the trust, behavioral intention, and actual use of web-based insurance services by proposing a new research model. The proposed research model is developed to improve the privacy-trust-behavioral intention model [34] by separating the privacy itself into four main concerns, based on the previous study of concern for information privacy [58]. The new research model aims to describe the relationship between the most important privacy concerns with trust and behavioral intention, which is particularly relevant in insurance web services where the most sensitive personal information such as health information and financial information is needed. Furthermore, the proposed research model hopefully can be used in examining the relationships between the variables mentioned. This research also aims to enhance the success of web-based insurance services' usage and implementation generally and protect the privacy of the customer by enhancing security policies and measures in the services. In order to realize the objectives, the main research questions are as follows:

1. Does the new research model represent the relationship of privacy concern, trust, and behavioral intention for using web-based insurance services?
2. Do the privacy concerns impact the customer's trust to disclose their personal information in Indonesia's web-based insurance services?
3. Does the customer's trust impact the behavioral intention to use Indonesia's web-based insurance services?
4. What are the most influential variables in privacy concerns that impact the customer's trust and behavioral intention to use web-based insurance services?

1.3 Scope of the Study

This research is performed within the three limitations. First, this research is limited to the use and the implementation of web-based insurance services in Indonesia. The services within this scope are both private-owned insurance companies and public-owned insurance companies. As a consequence, the result of this research might not be applicable in other countries' situations. Second, this research is limited in how privacy concerns can impact the trust and behavioral intention in using web-based insurance services as presented in the research model. Other pre-existing factors will not be covered in this research. Thus, the research is carried out by analyzing the survey which is directed to address the insurance customers' perception and attitudes regarding privacy in disclosing their personal information and how the privacy concerns influence trust and actual participation in certain online activity [34].The perception of the customer toward the topic is addressed in the agreement of the statements in the survey. Third, this research aims to see whether the combination of two related research models can support the presented hypotheses and answer the research question in order to know how privacy concerns can impact the trust and behavioral intention of the users in using web-based insurance.

1.4 Chapter Outline

This research consists of six chapters.

- This chapter, chapter one, introduces the background of this research including the motivation in choosing this topic, the research questions, the objectives of the research, the research scope, and the research structure overview.
- Chapter two provides the theoretical background of the related research model which is used in this research. It also presents the theoretical background in web-based insurance services especially in Indonesia.
- Chapter three presents the research methodology in this research. It explains the research approach and methods for gathering and analyzing the data.
- Chapter four describes the findings from the data analysis in previous chapter. It addresses the answer of the hypotheses.
- Chapter five discusses the findings of this research. It includes discussion on the current state of web-based insurance services in Indonesia and its relationship to privacy concerns.
- Chapter six reiterates and answers the research question as the final remarks of this research. It also specifies the recommendations and suggestions for future studies and the limitations of this research.

Chapter 2

Theoretical Framework

2.1 Web-based Insurance Services Trend in Indonesia

The trend in using web-based services is growing quickly. Electronic commerce is proven to help organizations expand their business, understand the market's needs, and adapt to change in preferences and market trends [26]. Electronic commerce is not only used by organizations who sell products but also organizations who sell services such as banking, insurance, and even health consultations [5] [26]. In fact, the use of electronic commerce for the organizations that focus on service is growing in developing countries such as Indonesia, Malaysia, and other countries in Southeast Asia [28]. In the insurance sector, the trend shifts from paper-based insurance registration and paper-based claim submission to e-registration and online claim submission [27]. It helps the insurance companies in tracking and providing a better assistance for their customers as well as competing better with each other, especially in getting new customers and keeping existing customers with the more effective and efficient online transactions [4]. However, sometimes certain characteristics, cultural things, and technological factors related to the insurance sector limits the successful implementation of web-based services in the insurance sector [27].

In Indonesia, the insurance sector and pension funds are potentially important for economic growth due to low and medium levels of income and wealth accumulation [56]. One of the most prospective and promising insurance sectors in Indonesia is life insurance and pension funds [52] [56]. There are three most common types of insurance practice in Indonesia, bancassurance, unit link, and sharia-based insurance [52]. Bancassurance is a collaboration between an insurance company and a bank [45]. In Indonesia, the most known Bancassurance is AIG Life, which is supported by Lippo Bank [52]. Meanwhile, unit link is a combination of insurance service and investing service, which is popular among lower middle class customers due to low minimum deposit per month [52]. The market for this type of insurance is dominated by Prudential Indonesia, Allianz Life Indonesia, and AXA Mandiri Financial [52]. The last type of insurance and the most unique is sharia-based insurance. This insurance type is increasingly popular in countries with a large Muslim population such as Indonesia. Sharia-based insurance is known as takaful insurance [41]. Takaful insurance has a different financial provision based on the Islamic principles. The market for takaful insurance in Indonesia is dominated by PT Asuransi Jiwa Takaful Keluarga. In the beginning of 2007, there are only 2 takaful insurance companies, but now there are more of these than conventional insurance companies in Indonesia [52].

Most insurance companies in Indonesia have web-based services, especially for registering a claim and tracking a claim's status. For example, Lippo Insurance has e-Policy and e-Benefit as their primary web-based services for customers [15] [32]. E-Policy is also made to encourage customers to be environmentally friendly by reducing the use of paper for claims, accessing policies, and extending policies [32]. Meanwhile, e-Benefit is the overview of customer's benefits based on the current policy which is owned by the customers, and the customers can also track their claims in this web-based services [15]. Both of these web-based services require registration, but only e-Benefit's registration uses an online form, while e-Policy's registration is done by contacting the customer service of Lippo Insurance [15] [32]. This trend to web-based services is not only among private insurance companies, but also the government-owned

insurance company, BPJS Kesehatan. The citizens of Indonesia who are not working for a private company or government services are required to register themselves and their immediate family members to BPJS Kesehatan, paying a low-rate deposit or premium per month [43]. The registration can be done online, where they have to enter personal information related to themselves and their immediate family members [43] [48]. BPJS Kesehatan also offers two more online services to track the payment status of the premium and to communicate complaints directly online [49] [50]. The tendency of insurance companies in Indonesia to have web-based services as their complementary and supplementary service for their customers is considered high, based on these facts.

2.2 Concern of Information Privacy Instrument

Concern about privacy is not a new thing, considering how the free movement of data is handled nowadays. The concern for information privacy somehow appears to be much influenced by cyber-crime related to social media and e-commerce [34] [37]. Many organizations and businesses need to pay a lot of attention to the individual privacy concerns of their customers. Instruments or methods to measure the concern for individual privacy are then important. Instrument or methods to measure the concern for individual privacy is known as concern of information privacy instrument or CFIP [58]. Organizations needs to know the main variables of individual privacy concern to take the best security measures in order to protect their customers' personal data [58]. At the same time, organizations need to deliver an effective and efficient service for customers and make a profit for themselves [58].

Alongside the need for an information privacy instrument to measure the concern for individual privacy, many researchers have tried to identify the concerns regarding information privacy. The first known piece of research to identify the concern for information privacy was undertaken by Smith [57]. Using a systematic and iterative approach, he tried to specify the most important privacy variables, and found four main variables of concern for information privacy: collection, errors, secondary use, and unauthorized access [57]. These variables suggest that individuals are concerned if too much data is collected from them (collection), much of the data is inaccurate despite the care they took when they provided the data (errors), the use of their personal data is not notified to them or without their consent (secondary use), and there are poor security measures to safeguard their personal data (unauthorized access). These variables can be used in more extensive research especially in identifying the relationship and causality between the information privacy concern with organization practice in processing personal data, consumer perceptions of the organization, and consumers' behavioral intention and responses [58].

Those variables are developed to represent a standpoint or an attitude of consumers toward the personal data and sensitive information which are processed by the organizations [58]. However, using those four variables to identify the standpoint of business owners in defining privacy concern may not be totally suitable [58]. Based on multiple studies, those four variables are the greatest concerns for business customers [34][58]. The interrelationship between them suggests that those four variables have a strong correlation in affecting each other [58]. The definition of privacy itself also affects the adaption of those four variables as the biggest privacy concern. Privacy is defined as the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively [17]. Privacy is likely to be a concept that evolves as with changes in computer-based information collection, storage, and retrieval [13] [57]. The way the organization processes and obtains personal data from their customers makes data owners worry that their data can motivate cyber-crime activities, privacy infringement lawsuits, and government interference. Data owner is defined as the party having acquired, developed, or created information resources for which no other party has ownership

[47]. Consequently, the way personal data is collected can be separated into three forms [13]: (1) provided voluntarily by the customers, (2) collected implicitly through the websites, and (3) derived personal data where users are completely unaware that their personal data is collected aggregately from their previous activities on the particular website or their other personal information. The last form is known as the use of cookies.

It seems that Internet users desire to have full control of customization and configuration when providing their personal information based on their preferences. Despite the full control that they want in providing their personal information, they also rely on organizations to control the security of their personal information. This kind of situation is difficult to achieve in practice. That's why the four variables of CFIP are the best variables to illustrate what customers are really concerned about in terms of privacy in cyberspace. These variables have been tested for their validity and reliability in two previous studies, so can be applied as a standardized measure of customers' concerns for information privacy [34] [58].

2.3 Privacy-Trust-Behavioral Intention Model

A previous study by Liu has proposed and tested the first privacy-trust-behavioral intention model by conducting an experiment with 200 participants to measure their perceptions of privacy and the relation of this with their behavioral intention to make an online transaction [34]. They visualized the simple relationship between three variables in the figure below [34]:

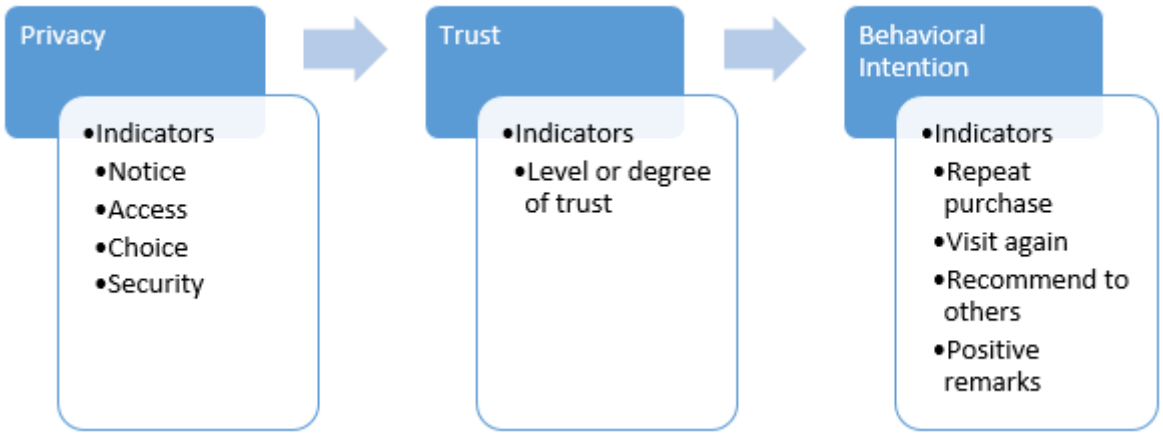

Figure 2.1: Privacy-Trust-Behavioral Intention Model

Based on the figure, the relationship between the three of them is described as influences. It can be inferred that privacy influences trust, and trust influences behavioral intention. We noted that they used four indicators of privacy from the US Federal Trade Commission (FTC). Based on the FTC's report, those four indicators are categorized as fair information practices in the e-commerce environment [34]. The further description of the four indicators of the privacy concern based on FTC is [34]:

- Notice means providing the user with notification that personal information is being collected prior to the collection of that information
- Access means providing the user with access to the data that is collected about them.
- Choice means providing the user with a choice to allow an organization to use or share information collected about them.

- Security means providing reasonable assurance to the user that personal information is kept secure.

Meanwhile, a trust variable has been studied and is quite popular especially in behavioral science and social science [8]. Trust is defined as behavior based on the beliefs that people own about the characteristic of another people [40]. In e-commerce the uncertainty in doing a transaction is higher than in a non-virtual environment, so trust will be a primary key to influence the behavioral intention of a user in doing a transaction online. One important fact is that the relationship between trust and information disclosure is quite strong. A previous study by Metzger said that trust is a precondition for self-disclosure since it reduces perceived risks in revealing private information [42]. The study also confirms that the user is willing to disclose the personal information online based on the different characteristics of the users themselves and the type of information requested from the web-services [42].

As for the behavioral intention variable, in the privacy-trust-behavioral intention model, this variable can be measured by some indicators such as repeat visits to the website, repeat purchases online on the same web site, positive comments and recommendations to the other users, and word-of-mouth recommendations of the website. These indicate the customer's satisfaction as well as their trust of the website [62]. However, in this study, since the online transaction will include a personal data disclosure to get a service from the insurance company, the indicators may be slightly different. If the users have experience in providing their personal information, they will be more willing to provide it than the first time. The users develop trust only if the website that they provided information to gives them the service that they want [42]. So it is important to know the first-timer users of online insurance service. If the users have concerns about the privacy, it will negatively influence the behavioral intention to disclose personal data [42]. In order to solve the problem, data controller and data processor need to give a detailed but brief overview of their privacy policy and how they handle the data given to them.

2.4 Structural Equation Modeling

Structural Equation Modeling (SEM) is a statistical method which enables researchers to answer research questions and prove hypotheses by modeling relationships among multiple independent and dependent variables simultaneously [20]. SEM can be undertaken using AMOS Tools, LISREL Tools, or Partial Least Squares [20]. The simultaneous analysis of SEM is better than linear regression using the ANOVA method or MANOVA method. It can analyze multiple layer of linkages between independent and dependent variables at the same time. SEM is currently being used in information system research [59]. The basic concept of SEM consists of three main components: variables, models, and errors [59]. These components are explained further below:

1. Latent Variable and Manifest Variable [59]

   A latent variable is a variable that cannot be measured directly, but only through its indicators [53]. Latent variables are usually used to represent motivation, satisfaction, and behavior in social research [53]. Latent variables have two properties: endogenous and exogenous variables. Endogenous variables are dependent variables. These are affected by the exogenous variables which are independent variable. A causal correlation between the variables can be represented using arrows. The arrows are also used to distinguish endogenous and exogenous variables. Endogenous variables must have at least one arrow that leads to it and can have arrows coming out of it, whereas exogenous variable only has arrows coming out from it. The two properties of variable can be seen in the next figure:

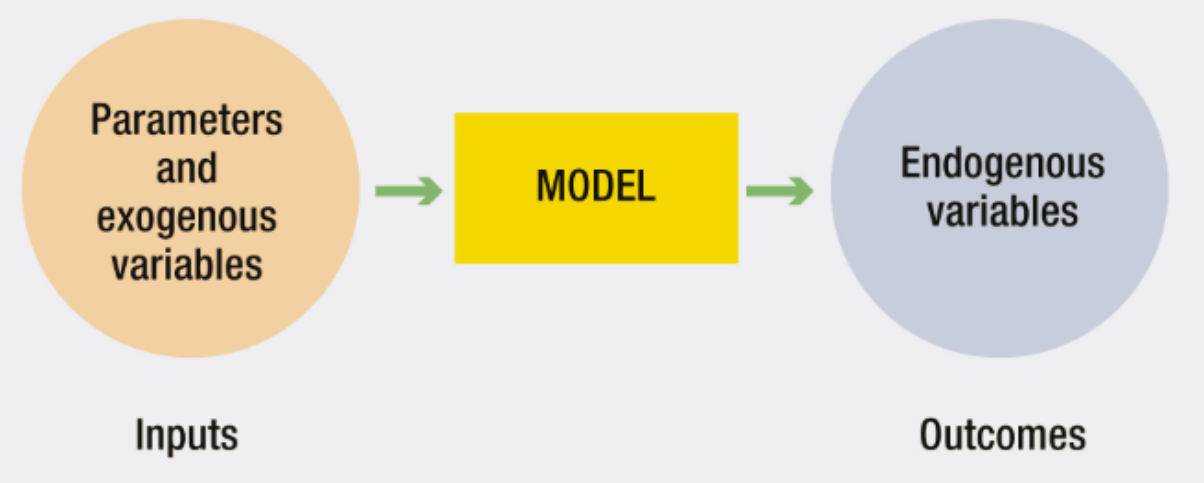

Figure 2.2: Endogenous and Exogenous Variable [24]

On the other hand, manifest variables are the indicators of latent variables, which can be measured directly from questionnaires or direct observation [59].

2. Structural Model and Measurement Model [59]

   A structural model describes the relationship between the latent variables in a linear manner in order to form a linear regression equation. Usually, a structural model is represented by path diagrams such as reciprocal causation and indescribable association. The path diagram will be analyzed using path analysis to examine the strength of the relationship between latent variables. On the other hand, measurement models describe the relationship between latent variables and manifest variables or the relationships between variables with indicators. The measurement model is used to analyze the factors that affect certain things.

3. Structural Error and Measurement Error [59]

   Structural errors in SEM can appear due to the inability of exogenous variables in explaining the things that will be analyzed by endogenous variables. Each endogenous variable is automatically provided with one error variable. The error variable acts as a possible factor that may not be measured or predicted perfectly. Meanwhile, measurement errors can appear due to inability of manifest variables or indicators to explain the things that will be analyzed by latent variables. Each manifest variable or indicator is automatically provided with one error variable.

2.4.1 Example in using SEM

The simplest example in using SEM is the trust-satisfaction-loyalty model. In this case, the owner of a store wants to know their customers' loyalty in buying their products. We can model this as the following:

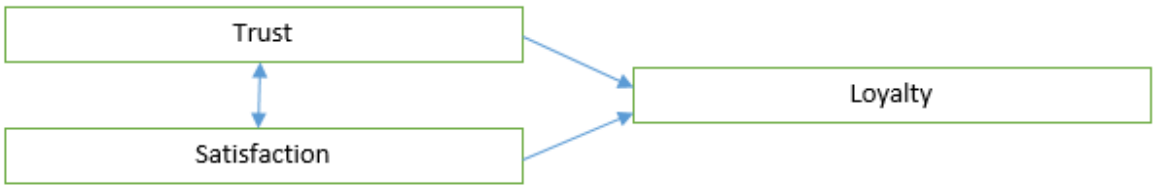

Figure 2.3: SEM Example

From the above model, there are three latent variables: loyalty, trust, and satisfaction. Loyalty is affected by satisfaction and trust, whereas there is a bidirectional relationship between satisfaction and trust. The satisfied customers are the customers who trust the store and will tend to stay loyal to the store. Loyalty has an endogenous variable property since it is dependent on the other two variables. Trust and satisfaction also have an endogenous variable property, since they are dependent on each other. However, the latent variables need more explanation. Loyalty, satisfaction, and trust are too abstract to be quantified without the indicators. In order to measure this relationship, we need manifest variables or indicators. We assume that we need three indicators per variable. Therefore the model can be drawn as the following:

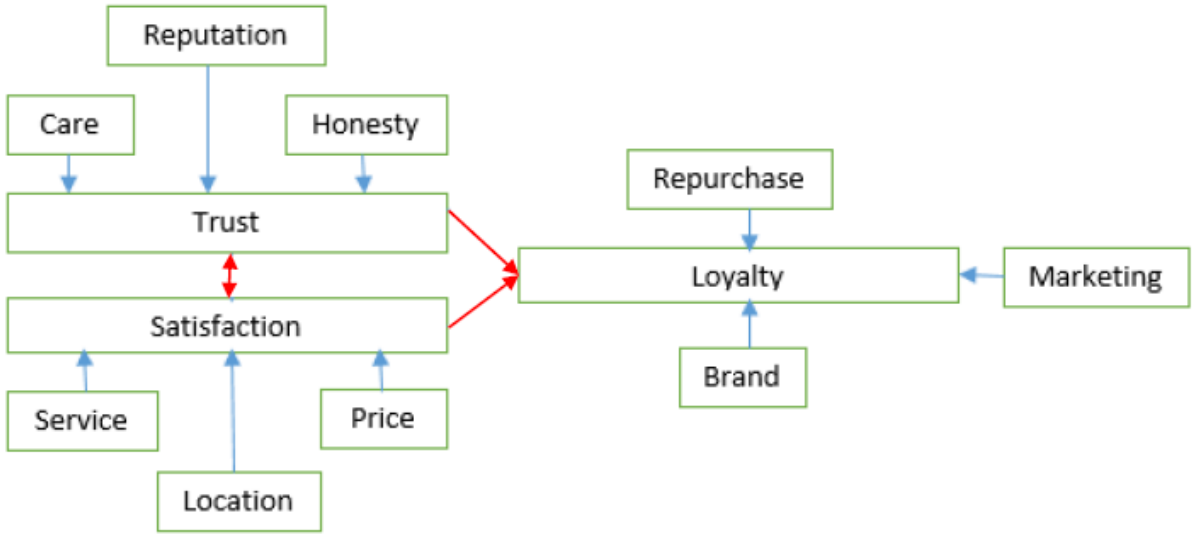

Figure 2.4: SEM Example with indicators

Now, there are three latent variables added with nine manifest variables as indicators: care, reputation, honesty, service, location, price, repurchase, brand, and marketing. The relationship between one latent variable with the three manifest variables is known as the measurement model (with blue arrows). Thus, in the example model there are three measurement models, which are the relationship between trust variables with its three indicators, the relationship between satisfaction variables with their three indicators, and the relationship between loyalty variables with their three indicators. The relationship between all the latent variables is known as the structural model (with red arrows). The visualization of the measurement model and structural model is known as the path diagram, which is analyzed using path analysis [53].

As stated before, there are measurement errors and structural errors in the SEM model. As not every questionnaire can exactly measure the latent variables, there will always be one measurement error for one indicator. The error variables cannot be observed directly. This is different to latent variables and manifest variables. The error can also happen in the relationship

between exogenous variables and endogenous variables. Structural errors are also known as residual errors or disturbance terms [53], which reflects the unexplained variance in endogenous variables. In the example, structural error happens due to the assumption that there may be an error when we predict the relationship between trust and satisfaction with loyalty. Below is the complete visualization of the example model in path diagram, assuming that the error variables are independent:

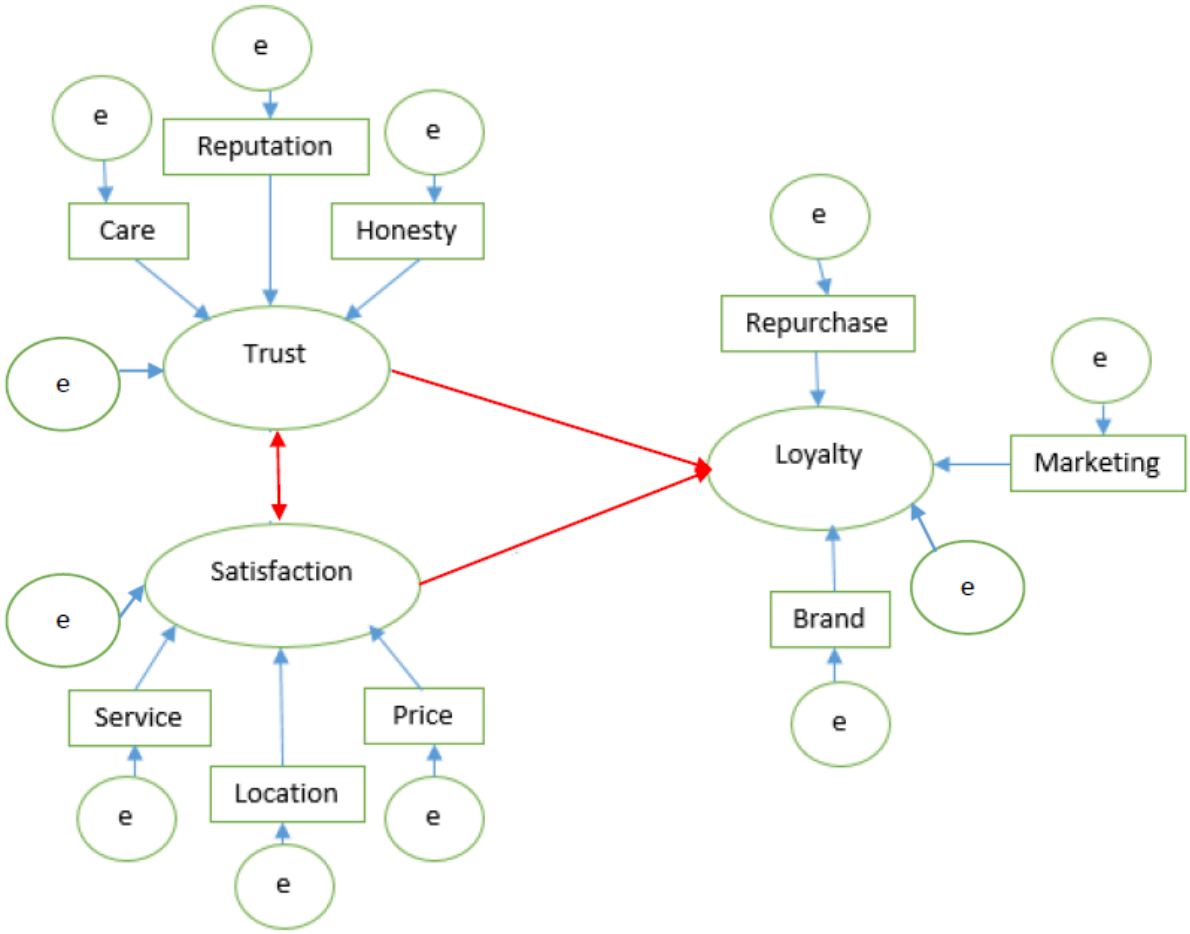

Figure 2.5: Complete SEM Model with error variables

2.4.2 Examination of whether the model can be estimated

Before examining whether the research model can be estimated or not, the degree of freedom of a research model should be calculated. The degree of freedom calculation is undertaken to determine whether there is a solution for the structural equation model [53]. The degree of freedom score identifies whether the data analysis for the research model can be continued. There are three conditions whether the data analysis can be continued based on the degree of freedom identification that may occur in the analysis using SEM, namely:

1. Just identified

   The degree of freedom of the model equals to zero. This type of model does not need to be estimated further or even modified. Thus the interpretation of the computer output can be done directly.

2. Under identified

The degree of freedom of the model has a negative value. This type of model can never be solved.

3. Over identified

   The degree of freedom of the model is more than zero, and thus the model can be estimated and modified further.

The formula to calculate the degree of freedom in the SEM model is the total of sample moments subtracted by the free parameters. Total of sample moments is all the correlations derived from the data [53]. Free parameters are the error variables, manifest variables, and all the independent variables [53].

2.4.3 Estimation of the Model based on the Data Collection

If the model is over-identified, the estimation of the model can be undertaken as the next step. This step is done in order to know the strength of the relationship between the variables in the model. Before the estimation process is undertaken, the raw data from the data collection process will be converted into covariance matrices. AMOS tools automatically do this when the data is inputted. The estimation of the model is based on three statistical procedures, namely:

1. Total sample

   Ideally, the total sample for structural equation modeling method should be in the range of 150-400 samples. However, in practice, the data collection and the time used to collect the data will be a challenge, thus 100-200 samples are approved as representative total samples for the structural equation modeling method [53].

2. Data Normality

   The data that will be analyzed further should have a normal distribution to reduce the bias from analysis results. The first step to test the normality of the data is to test the normality of the variables separately. At the end, the normality of the variables is tested together.

3. Outliers

   Outliers are data which have a value far above or below the average range of the whole data. Outliers can be detected with a data normality test.

For research that will measure the behavior intention and actual use of system based on facts in the field, normality test results can be ignored, and outliers do not need to be deleted [53]. Maximum Likelihood Estimation in SEM can still be used although the normality requirement is not fulfilled.

2.4.4 Examination of The Model based on the AMOS Calculation

If the total sample, data normality, and outliers of the data fit with the SEM-specific criterion, an examination of the model based on the AMOS calculation can be undertaken. The examination of the model based on the AMOS calculation aims to find out whether the indicators can explain the dimensions in the proposed model. The examination of the model based on the AMOS calculation is undertaken in two steps: firstly, the validity of the measurement model is tested, and secondly, the validity of the structural model is tested. The validity test for the measurement model can be done using a goodness of fit test. There are two standards of goodness of fit test which should be fulfilled by the research model, namely:

1. Absolute Fit Indexes

   This standard compares covariance matrices of the sample with the estimated covariance matrices. This standard uses a chi-square score to measure the differences between covariance matrices of the sample and the estimated covariance matrices. The chi-square of the model will be calculated by AMOS tools, whereas the standard chi-square score can be obtained from the chi-square table based on the degree of freedom score of the model. There are four conditions that can be examined:

   - If the chi-square of the model is less than the standard chi-square score, the covariance matrices of the sample do not differ from the estimated covariance samples. However, if it is greater than the standard chi-square score, the covariance matrices of the sample differs significantly from the estimated covariance samples.
   - If the probability score from AMOS's output is greater than five percent, the covariance matrices of the sample do not differ from the estimated covariance matrices. However, if it is less than five percent, the covariance matrices of the sample differs significantly from the estimated covariance matrices.

   The model does not need to be modified if the covariance matrices of the sample do not differ from the estimated covariance matrices. It must be supported by other standards, namely:

   (a) GFI (Goodness of Fit Index), AGFI (Adjusted Goodness of Fit Index), and RMR (Root Mean Residual)

   GFI, AGFI, and RMR are the alternative standards to support the use of chi-square in calculating the difference between the covariance matrices of the sample and the estimated covariance matrices. There are two conditions which can be examined based on those three standards:

   - If the GFI score and AGFI score of the model is closer to 1, the research model doesn't need to be modified.
   - If the RMR score is closer to zero, the research model doesn't need to be modified

2. Incremental Fit Indexes

   This standard compares the research model with the null model. The null model is the research model where all of the indicators in the model do not have any correlation with each other. This standard also uses chi-square scores. However, the chi-square of the research model will be compared to the chi-square of null model (baseline model). There are four conditions that can be examined:

   - If the NFI (Normed Fit Index) and RFI (the derivative of NFI index) is greater than 0.9 then the research model doesn't need to be modified.
   - If the CFI (Comparative Fit Index) score is greater than 0.9 then the research model doesn't need to be modified.
   - If the IFI (Incremental Fit Index) is greater than 0.9 then the research model doesn't need to be modified.
   - If the TLI (Tucker Lewis Index) is greater than 0.9 then the research model doesn't need to be modified

Below are the standards often used by researchers to determine whether the model is acceptable:

1. The NFI exceeds 0.9 or 0.95 [54]
2. The GFI exceeds 0.9 [7]
3. The CFI exceeds 0.93 [7]
4. The RMR is less than 0.09 [6]

However, these standards are merely guidelines, and do not have to be strictly adhered to [3]. If the model is acceptable, the next steps are the convergent validity test and discriminant validity test. AMOS will calculate the indicator's factor loading score. If the indicator's factor loading score is greater than 0.5 then the indicators can be used to measure the variables. For the discriminant validity test, AMOS will calculate the correlation score between the variables. If the correlation square is greater than 0.5, there is a relationship between the variables. The final step is to test the validity of the structural model. The validity test for structural model is conceptually the same as the validity test for measurement model. The standards and the methods used are also the same.

2.4.5 Modification of the Model

If the model is considered fit, the proposed model can be considered as valid. However, sometimes a valid research model needs modifications to make it fit with the available data for future research. The modification step is done to minimize the chi-square score to fit with the defined standards [53]. The modification can be done by eliminating some of indicators or even variables to reach the best score in the goodness of fit test. If, following modification, the model is still not acceptable or does not fit with the available data, path analysis can be undertaken. Path analysis is a path diagram analysis where the indicators are combined into one indicator based on factor loading [53].

2.4.6 Acceptance or rejection of the model

To accept or reject the relationship between variables and also to prove the hypotheses made to answer the research question, critical ratio score analysis is undertaken. Critical ratio score for every relationship between variables is compared to the critical score cut-off point which is 1.65, with a probability under 0.05. The relationship between the variables is positive if the critical ratio score is greater than cut-off point, with a probability under 0.05. It means the relationship in the model is accepted. Conversely, the relationship between the variables is negative if the critical ratio score is less than the cut-off point, with a probability above 0.05. In this case, the relationship in the model is rejected [53]

Chapter 3

Research

3.1 Research Design

3.1.1 Research Model

In a previous study, the privacy-trust-behavioral intention model only has three main variables, and the privacy variable is measured with only four indicators [34]. Meanwhile, privacy concerns may differ between individuals and have more than one aspect [57]. In previous studies, there are four most important aspects in privacy, which later become the most important privacy concerns [57] [58]. The privacy variable in the privacy-trust-behavioral intention model can be separated into those four main information privacy concerns. The proposed research model can identify the relationship between each of the four privacy concerns toward the trust and behavioral intention, which was done in either of the previous studies. The upgraded research model in particular will describe those relationships in the use of insurance web-services.

In this research, the privacy-trust-behavioral intention model [34] and concern for information privacy model [58] are adopted to assess Indonesians' concerns about privacy and how it relates to their behavioral intention to use web-based insurance services. The proposed model combines two models that were tested using structural equation modeling. Thus, the proposed model will also be tested using structural equation modeling. The proposed model selects four components of privacy concern from the concern for information privacy model since they represent an attitude or cognitive state of consumers (in this research, insurance participants or insurance information system users) towards the use of personal information [58]. As for the degree of trust and behavioral intention, these components are selected from the privacy-trust-behavioral intention model. The proposed model suggests that privacy concerns may have positive relationships with developing trust since users must first believe that an online transaction will consistently fit with their expectations. The proposed model then suggests that the development of trust will affect users' behavioral intention to use the information system. The proposed model can be seen in Figure 3.1:

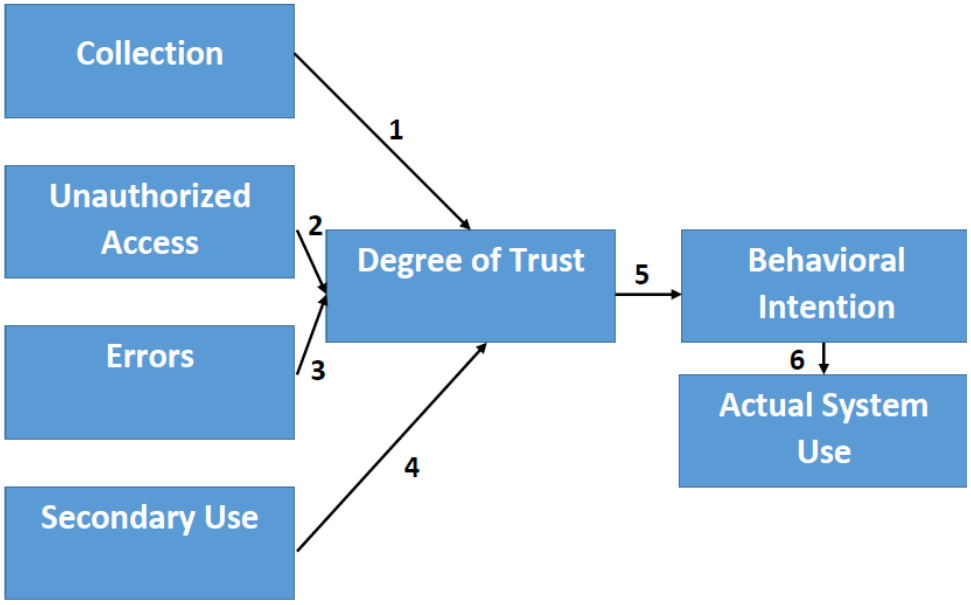

Figure 3.1: Research Model.

3.1.2 Explanation of the Model

Based on the research model, the definitions of the variables are summarized in Table 3.1.

Variable	Definition	Source
Collection	Privacy concern that extensive amounts of personally identifiable data are being collected and stored in databases	[58]
Unauthorized Access	Privacy concern that personal data is readily available to people who are not authorized to view or retrieve the data	[58]
Errors	Privacy concern that protections against deliberate and accidental errors in personal data are inadequate	[58]
Secondary Use	Privacy concern that information is collected for one purpose but is used for another without authorization from the data owner	[58]

Variable	Definition	Source
Degree of Trust	Insurance participant's confidence in using insurance information system based on their belief in the provider which depends on the organization's norms, regulations, policies, and procedures	[34]
Behavioral Intention	Insurance participant's intention in providing their personal data into the insurance information system	[34]
Actual System Use	Insurance participant is actually using the information system	[34]

Table 3.1: Definition of Dimension.

The relationship between variables which will be the foundation for constructing the hypotheses are summarized in Table 3.2:

Arrow	Definition	Hypotheses
1	Does collection as a privacy concern impact a customer's degree of trust in web-based insurance services?	H1
2	Does unauthorized access as a privacy concern impact a customer's degree of trust in web-based insurance services?	H2
3	Does errors as a privacy concern impact a customer's degree of trust in web-based insurance services?	H3
4	Does secondary use as a privacy concern impact a customer's degree of trust in web-based insurance services?	H4

Arrow	Definition	Hypotheses
5	Does customer's trust impact a customer's behavioral intention to use web-based insurance services?	H5
6	Does behavioral intention impact the actual use of web-based insurance services?	H6

Table 3.2: Relationship between Variables.

3.1.3 Hypotheses

Based on the research model, the following hypotheses are made:

- H1: The way an insurance provider collects and stores personal data has a positive relationship with an insurance participant's degree of trust.
- H2: The way an insurance provider ensures there is no unauthorized access to personal data has a positive relationship with an insurance participant's degree of trust.
- H3: The way an insurance provider ensures the accuracy and integrity of personal data has positive relationship with an insurance participant's degree of trust.
- H4: The way an insurance provider ensures there is no secondary use of the personal data has positive relationship with insurance participant's degree of trust.
- H5: There is a positive relationship between an insurance participant's degree of trust and the insurance participant's intention to use the insurance information system by providing their personal data.
- H6: There is a positive relationship between an insurance participant's intention to use the insurance information system and the actual use of information system by the insurance participant.

3.2 Research Guiding Framework

This research was performed with a quantitative approach to test all the hypotheses stated. A quantitative approach turns the data gathered into numbers by using measurements or quantification. Analysis and interpretation of the data will use a statistical approach [11]. The guiding framework can be seen in Figure 3.2.

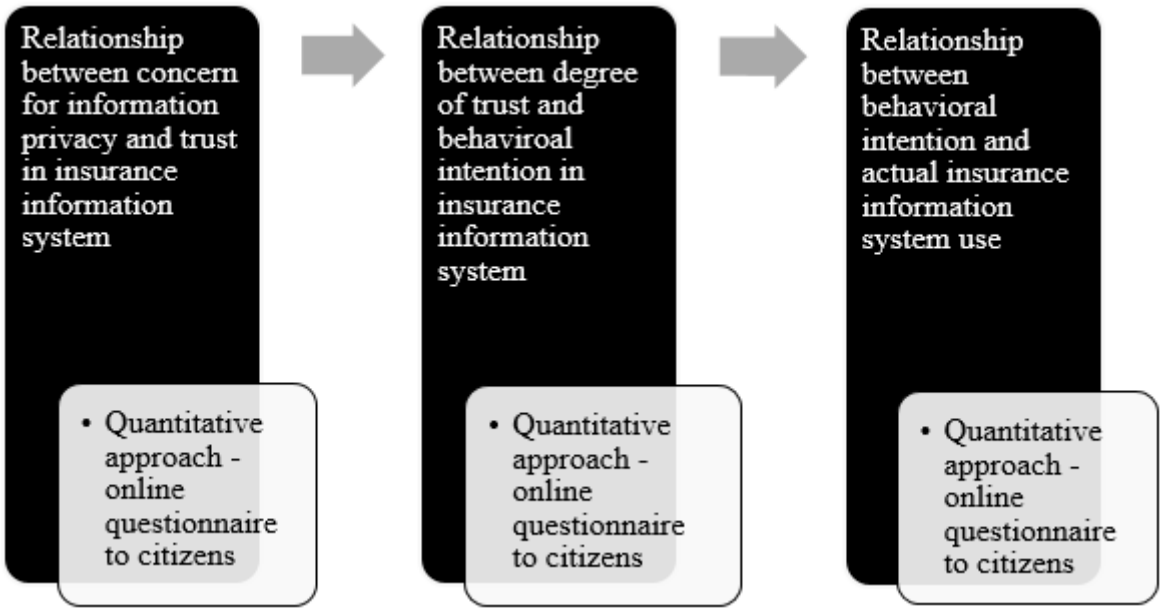

Figure 3.2: Guiding Framework.

3.3 Data Collection

3.3.1 Online Questionnaire

An online questionnaire is constructed from the research model. Since a large sample is needed, an online questionnaire is used to attract a large audience and to collect more data than with face-to-face interviews or focus groups. It also saves time and costs in doing data collection [61]. An online questionnaire also allows the researcher to control the question order, ensure the completeness of the respondent's answer, and filter the results more easily.

3.3.2 Questionnaire Development

The online survey was developed in Qualtrics. The questions about privacy concern and behavioral intention were grounded on the surveys that were done by Stewart and Segars to examine the concern for information privacy instruments [58]. The questions about trust and actual system use are based on Liu's research about privacy-trust-behavioral intention model of e-commerce [34]. The questions are modified to fit with this research purpose.

The questionnaire contains 26 questions consisting of Likert-style scale, dichotomous questions, and open and closed questions. The Likert scale is a technique to measure a respondent's agreement or disagreement with each statement in the questionnaire [44]. The scale is able to quantify the data that the researcher needs. The questionnaire is divided into five sections: demographics, privacy concerns, degree of trust, behavioral intention, and actual use of insurance information system. The questions are designed and ordered based on the research model. The table below shows how the questions in the survey answer the hypotheses (see Appendix A for full questionnaire).

Item Code		Hypothesis	Number in Questionnaire	Source
Collection	COL1	H1	4	[34], [58]
	COL2		5	
	COL3		6	
Unauthorized Access	UA1	H2	7	[34]
	UA2		8	
Errors	E1	H3	9	[34]
	E2		10	
	E3		11	
Secondary Use	SU1	H4	12	[58]
	SU2		13	
	SU3		14	
Degree of Trust	DT1	H5	15	[34]
	DT2		16	
	DT3		17	
	DT4		18	
	DT5		19	
Behavioral Intention	BI1	H6	20	[34]
	BI2		21	
	BI3		22	
	BI4		23	
Actual System Use	AS1		24	-
	AS2		25	
	AS3		26	

Table 3.3: Questionnaire Development.

3.3.3 Procedure and Sampling

Participants for the survey were recruited through advertisement on mailing lists and social media. In the advertisement, the researcher asked for mailing list and social media users who met two conditions: 1) participants interested in using web-based insurance services; 2) participants who are using web-based insurance services. These users are the population of research. To increase the number of participants and to appreciate the participants' willingness for contribution, the researcher entered all participants into a free prize draw to win one online shopping voucher. In the introduction of the questionnaire, the participants were provided with brief information regarding the survey.

Based on the procedure definition, the sampling technique used in this research was conve-

nience sampling. Convenience sampling is a type of non-probability sampling in which people are sampled simply because they are convenient sources of data for researchers [31]. Convenience sampling differs from purposive sampling in that expert judgment is not used to select a representative sample of elements. Rather, the primary selection criterion relates to the ease of obtaining a sample. Ease of obtaining the sample relates to the cost of locating elements of the population, the geographic distribution of the sample, and obtaining the interview data from the selected elements [31]. There is a disadvantage in using convenience sampling. Since the participants are basically volunteers, there will be bias in their answers [38]. This bias can be seen from the similarity of opinion on the same question. The results from convenience sampling have to be considered carefully, especially when generalizing the result [38]. In order to have results which can represent the population correctly, validity and reliability test must be undertaken [38].

In this research, convenience sampling was done by recruiting participants for an online questionnaire through mailing lists and social media. This method helped the researcher to collect many samples, which is necessary for structural equation modeling.

3.4 Pilot Study

Before distributing the real survey, the researcher conducted a pilot study using the questionnaire and got a feedback about the readability, understand-ability, and time to complete the questionnaire from the pilot study participants. These participants were Indonesian master's and PhD students at Radboud University Nijmegen. The questions were written in Bahasa Indonesia instead of English, since this made it easier for participants to answer the questions. The full questionnaire, translated into English, can be seen in Appendix A.

3.4.1 Validity and Reliability

Prior to data collection using the survey, reliability and validity tests were undertaken in the pilot study to ensure the survey's components are accurate [33]. The accuracy of a survey's components affects the data obtained from the data collection process. Reliability is a statistical measure of how reproducible the survey's components' data are [33], while validity is a procedure to assess how well a survey's components measures what the survey sets out to measure.

In this research, the type of validity test used is a content validity test, which measures how well the items in a questionnaire can really measure the behavior of participants by reviewing either the selection of words in questions or the structure of the questionnaire [39]. A content validity test was performed by an IT security and privacy expert from XL Axiata Indonesia. XL Axiata is one of the biggest telecommunication providers in Indonesia and its service has been used by the most of the country's insurance companies. The expert was selected since it is necessary that he is knowledgeable about the variables, especially privacy concern variables, to make sure they are adequate and consistent with the purpose of the research [39]. A content validity test was done by showing the expert the questions contained in the questionnaire, and asking about the content of the questionnaire as a whole. The expert was experienced in testing the validity of privacy-related surveys since most of his clients consult him about the IT security and privacy regulation compliance. The reliability test was undertaken by comparing Cronbach's alpha for each component. The calculation of Cronbach's alpha score uses SPSS. Cronbach's alpha score represents the inter-correlation between all the survey items, if the Cronbach's alpha score is high then it can be concluded that the item has a high correlation with other items, and thus can produce consistent results [12]. The component is considered reliable if the Cronbach's alpha score is greater than 0.7 [22].

Validity and reliability tests were conducted using data collected from 10 pilot study participants. The number of pilot study participants was based on ten percent of the sample that

will be projected in the real survey [9]. Since the sample of this study will be around 100-150 participant, minimum pilot study participant are 10-15 people. Since the sample of this study was around 100-150 participants, the minimum number of pilot study participants was 10-15. This pilot study was also done to examine the readability of questionnaire questions, to avoid ambiguity and confusion in answering those questions.

Based on the review of the questionnaire's items by the IT security and privacy expert, the questions related to the privacy concern variables had to be redefined by adding the main purpose of the insurance company in collecting the customer's personal information, for example to support claim processes or new user registration. Thus, in the introduction of the questionnaire, a detailed introduction and instruction was provided for the survey's participants. Another remark by the expert is that items COL1 and COL2 needed to be explained more clearly. The other items in the questionnaire were adequate to measure the privacy concern of insurance web service users, according to the expert.

For the reliability test, we used an SPSS tool to calculate the Cronbach's alpha after collecting 10 samples from the pilot study. This is summarized in the following table:

Variable	**Cronbach's Alpha Score**	**Minimum Cronbach's Alpha**	**Summary**
Collection	0.136	0.7	Reliable with condition
Unauthorized Access	0.926	0.7	Reliable
Errors	0.895	0.7	Reliable
Secondary Use	1.00	0.7	Reliable
Degree of Trust	0.959	0.7	Reliable
Behavioral Intention	0.729	0.7	Reliable
Actual System of Use	0.905	0.7	Reliable

Table 3.4: Summary of Reliability Test

The closer Cronbach's alpha coefficient of the variable is to 1, the more consistent the variable is [21]. We noted that for the Collection variable, Cronbach's alpha is less than 0.7. Therefore it could produce inconsistent result from the real data collection. However, we still had to use this variable since it was one of the main privacy concerns according to previous research [34][58]. In order to know whether the collection variable really has an impact on the research model with the real data, not only from the pilot study, the collection variable is analyzed further using structural equation modeling. If, in this analysis, the collection variable is unacceptable in the research model, the model will be modified by removing the collection variable.

Chapter 4

Analysis

4.1 Data Overview

4.1.1 Data Availability

The response rate of the questionnaire was 153. However, the full questionnaire was only completed by 112, as the preliminary question in the first section of the questionnaire selected the participants who actually use the insurance web services. The legitimate questionnaire reached only 107 in total. The questionnaire is available and can be accessed using the short link `http://bit.ly/qualtricsthesisrizka`. The raw responses of the participants are available using the short link `http://bit.ly/1UEpSwG`.

4.1.2 Data Demographic

The participants of the survey were recruited through advertisements on Indonesian Endowment Fund for Education scholarship's mailing list, since this list has more than one thousand members from very diverse backgrounds and from every region in Indonesia. For three weeks, from 20th May 2015 until 9th June 2015, we also used Facebook and Twitter to advertise the questionnaire. The summary of the general overview of the participants can be seen in the following table:

The Range of Age	**Total**
20-35 years old	131 participants
More than 35 years old	22 participants

Table 4.1: The summary of range of age.

Profession and Background	**Total**
Student	32 participants
IT-related	20 participants
Civil servants	14 participants
Researcher and Lecturer	14 participants
Auditors	8 participants
Entrepreneur	4 participants

Profession and Background	Total
Others	61 participants

Table 4.2: The summary of profession and background.

The use of insurance service	Total
Yes	134 participants
No	19 participants

Table 4.3: The summary of insurance services usage.

The insurance services provide web services	Total
Yes	123 participants
No	11 participants

Table 4.4: The summary of insurance web-services.

Based on the summary, the use of insurance web-services is quite popular, especially for participants aged 20-35 years old. Most students and IT-related people such as engineers and programmers are likely to use insurance web-services. However, from the 123 questionnaires, only 107 questionnaires are used for the data analysis.

4.2 Structural Equation Modeling

4.2.1 Formulation of SEM Model

We represent the research questions by developing a research model that contains independent variables and dependent variables. The research model is represented in a path diagram form. The path diagram is developed using AMOS version 21 tool. The research model formed using AMOS tool is shown below:

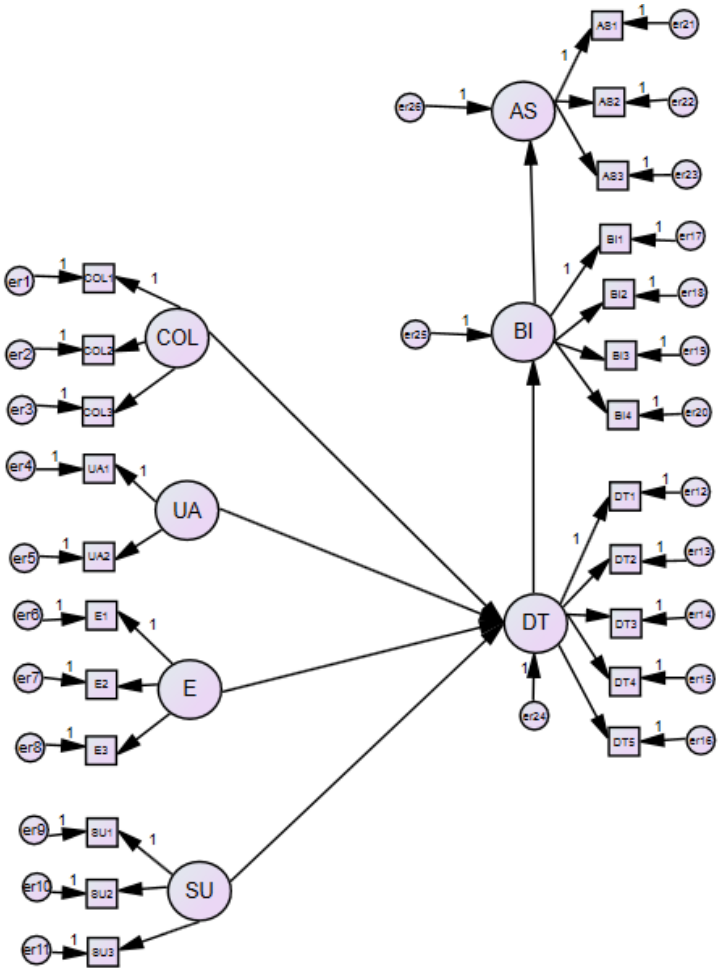

Figure 4.1: Path Diagram Representation of the Research Model based on Table 3.3.

4.2.2 Examination of the Model using Degree of Freedom

We can examine whether or not the model can be estimated. The model can be estimated if it is over identified. AMOS is able to calculate the degree of freedom from the proposed model. The model is considered over-identified if the degree of freedom has a positive value. The degree of freedom is calculated by subtracting the free parameters (the total of relationship between constructs) from the total sample. The following is the output note from AMOS tool related to the degree of freedom of the proposed model. The model is over- identified and thus can be estimated further.

Computation of degrees of freedom (Default model)

Number of distinct sample moments:	276
Number of distinct parameters to be estimated:	52
Degrees of freedom (276 - 52):	224

Figure 4.2: The Result of Degree of Freedom Calculation.

4.2.3 Estimation of the Model based on the Total Sample, Data Normality, and Outliers

The estimation of the model will rely on statistical procedures such as total sample, data normality, and outliers.

1. Total Sample

   The total sample for this research is 107. It is considered sufficient and representative since the total of representative samples for SEM is between 100-200 samples [53]

2. Data Normality and Outliers

   Since this study is conducted in order to measure behavioral intention and actual use of system, the data normality and outliers will not really have an effect in this step [53], so this step will be skipped.

4.2.4 Examination of The Model based on the AMOS Calculation

The examination of the model based on the AMOS calculation is measured based on a goodness of fit test. The goodness of fit test has some standards often used by researchers to determine whether the model is acceptable or not. In the previous section, we described that the standards that are followed are the NFI, GFI, CFI, and RMR. What follows is a summary of the goodness of fit test for the research model using AMOS.

Index Goodness of Fit	**Cut-off point**	**Model's Score**	**Conclusion**
Chi-Square	Chi-square for saturated model<Chi-quare score for default model<Chi-square for independent model	0<424.102<1426.487	Model doesn't need to be modified
NFI	NFI should exceed 0.9 or 0.95 [54]	0.703	Model needs to be modified
GFI	GFI should exceed 0.9 [7]	0.753	Model needs to be modified
CFI	CFI should exceed 0.93 [7]	0.829	Model needs to be modified
RMR	RMR should be less than 0.09 [6]	0.109	Model needs to be modified

Table 4.5: Summary of Goodness of Fit Test.

The complete results of the goodness of fit test from AMOS tools can be seen in appendix B. Based on these results, the model should be modified since only the Chi-square standard is fulfilled. Modification of the model will be explained further in the following sub-section.

4.2.5 Modification of Model

The model can be modified by eliminating some indicators or even variables to reach the best score in the goodness of fit test. The next steps to decide what should be modified in the model are the convergent validity test and discriminant validity test. Convergent validity test results determine whether the indicators within all variables can be used to measure the variables and the discriminant validity test determines the correlation between all the variables. If the factor loading score for the indicator exceeds 0.5 then the indicator describes the variable well. For the discriminant validity test, if the correlation score exceeds 0.5 between two variables in one model then the correlation between them is strong. The discriminant validity test result will not affect the modification of the model, but just shows the relationship between all variables. Below is the result of the convergent validity test and discriminant validity test for the model.

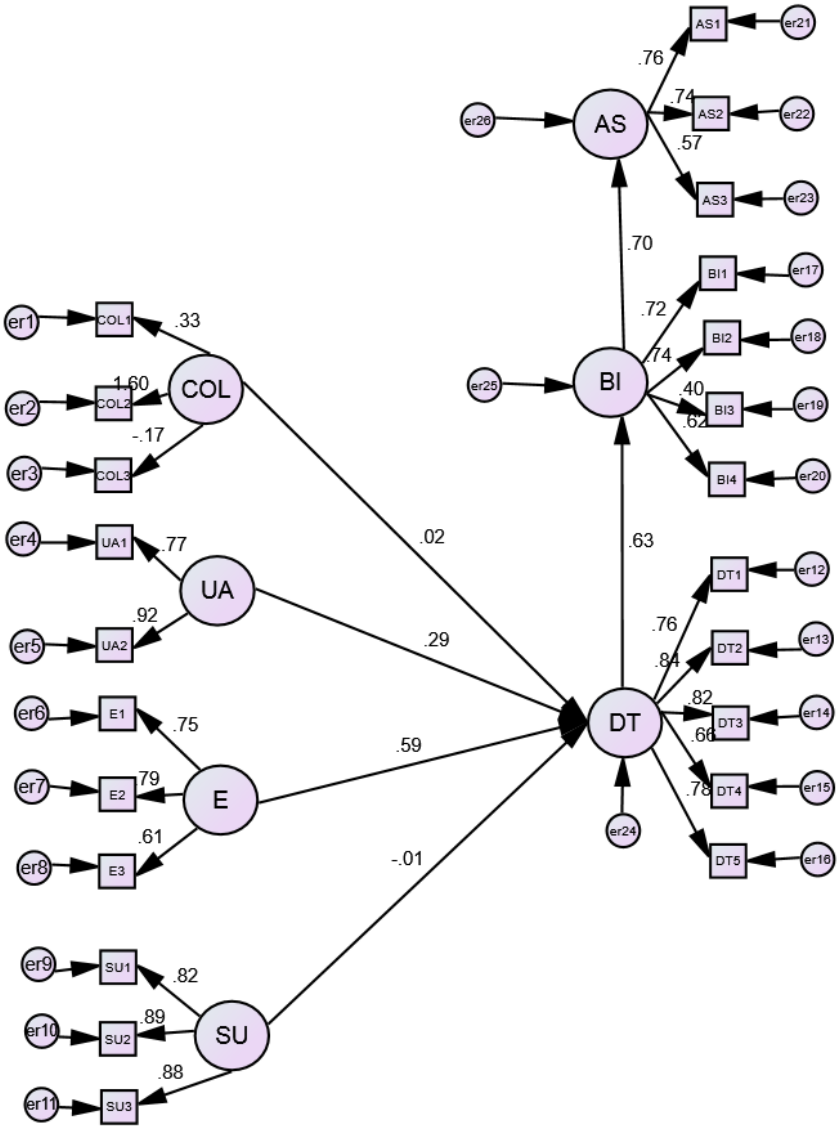

Figure 4.3: Convergent Validity Test and Discriminant Validity Test Result.

From the convergent validity test and discriminant validity test result, it can be seen that the factor's loading score of COL1 (0.33), COL3 (-0.17), and BI3 (0.40) are not sufficient. Those three indicators may be removed for further modification to see whether the model reached the goodness of fit test. Since the collection variable only has one indicator, this variable may be removed as well, as for SEM one variable needs to have two or more indicators to explain it [53]. This is related to the pilot study result, showing that the collection variable does not fit with the research model. Below is the model after the removal of the collection variable and BI3 indicator and the summary of the goodness of fit test, after removal of collection variable and BI3 indicator from Behavioral Intention variable.

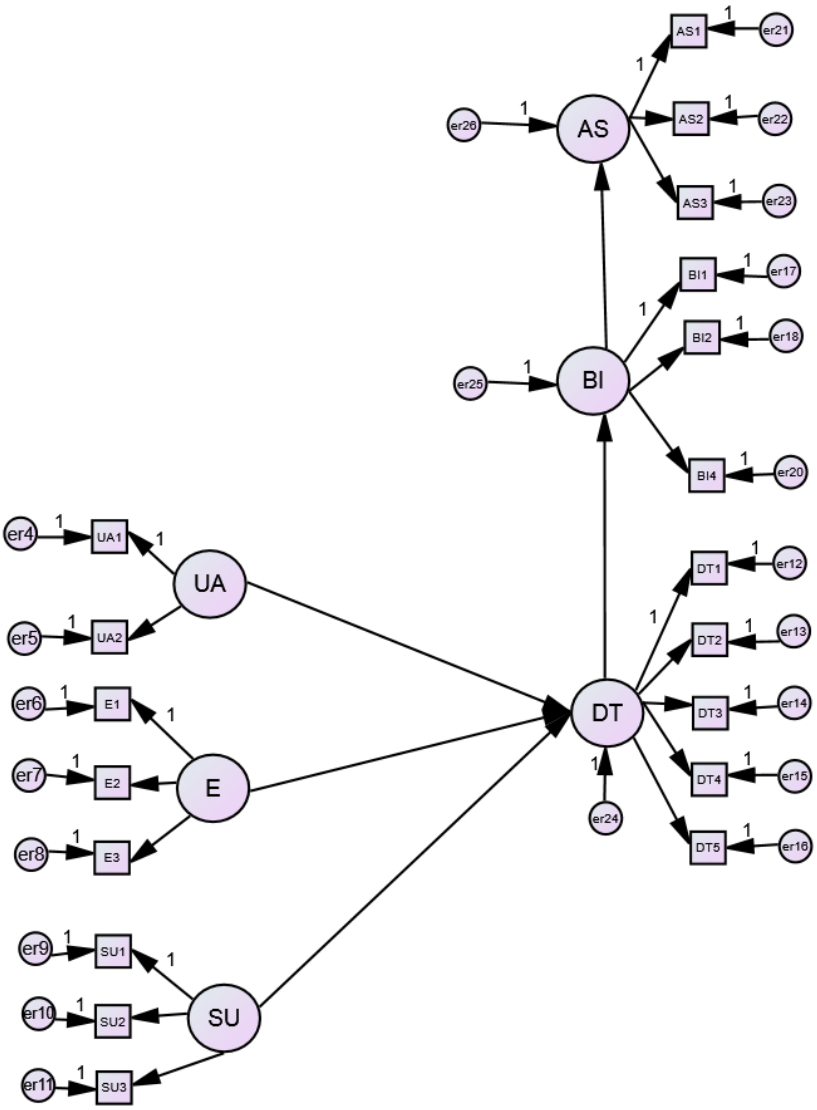

Figure 4.4: The Model After the Removal of Collection Variable and BI3 Indicator.

Index Goodness of Fit	**Cut-off point**	**Model's Score**	**Conclusion**
Chi-Square	Chi-square for saturated model<Chi-quare score for default model<Chi-square for independent model	0<313.899<1255.926	Model doesn't need to be modified
NFI	NFI should exceed 0.9 or 0.95 [54]	0.750	Model needs to be modified
GFI	GFI should exceed 0.9 [7]	0.779	Model needs to be modified
CFI	CFI should exceed 0.93 [7]	0.846	Model needs to be modified
RMR	RMR should be less than 0.09 [6]	0.111	Model needs to be modified

Table 4.6: Summary of Goodness of Fit Test After the Removal of Collection Variable and BI3 Indicator.

The complete result of the goodness of fit test from AMOS tools for modification model can be seen in appendix C. Based on the summary of goodness of fit test, after the removal of collection variable and BI3 indicator, the model should be modified further, since only the Chi-square standard is met. Further modification can be undertaken based on the modification indices in Appendix D. Modification indices shows how much the Chi-Square score can be reduced until the model is said to fit [53]. Based on the modification indices, the model needs to add correlation between the UA (Unauthorized Access) and E (Errors) variables. The correlation between those two variables may happen due to the strong correlation of the participant's answers for the UA variable with the participant's answers for the E variable. Below is the model after the addition of correlation between the Unauthorized Access variable and Errors variable and the summary of the goodness of fit test after the addition of correlation between the Unauthorized Access variable and Errors variable.

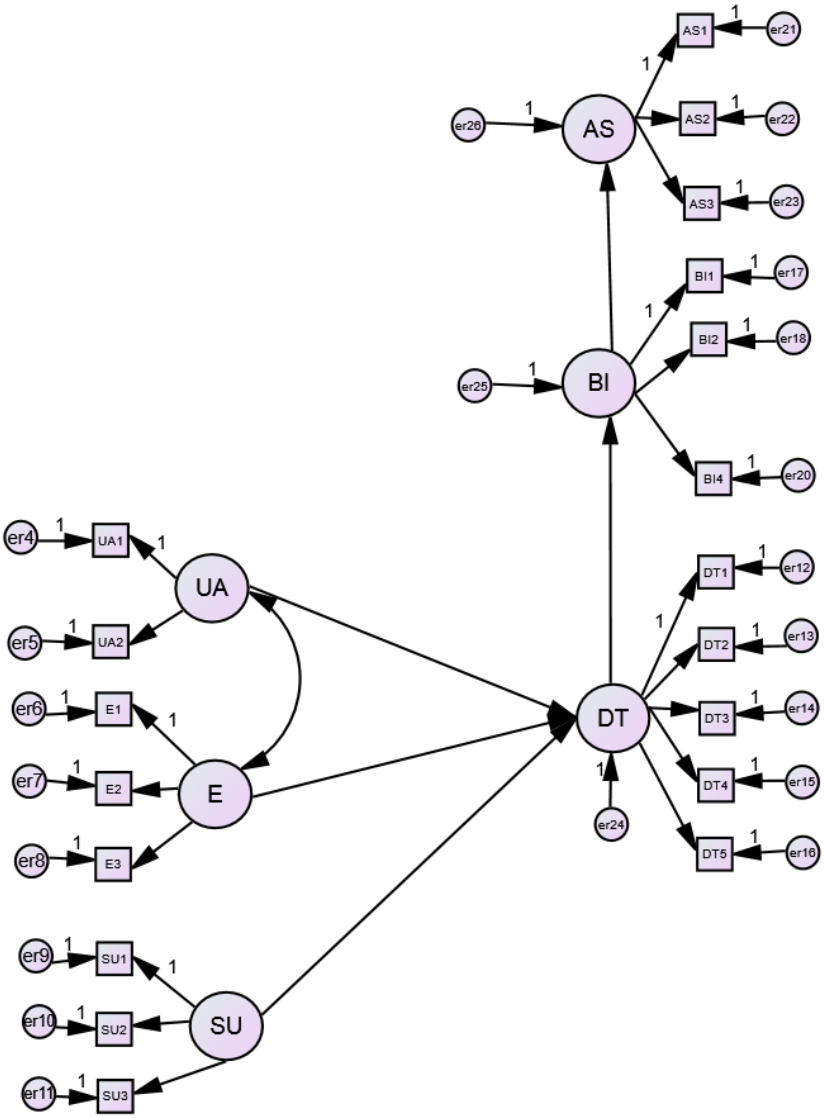

Figure 4.5: The Model After the Addition of Correlation between the Unauthorized Access Variable and Errors Variable.

Index Goodness of Fit	Cut-off point	Model's Score	Conclusion
Chi-Square	Chi-square for saturated model<Chi-quare score for default model<Chi-square for independent model	0<248.498<1255.926	Model doesn't need to be modified
NFI	NFI should exceed 0.9 or 0.95 [54]	0.802	Model needs to be modified
GFI	GFI should exceed 0.9 [7]	0.806	Model needs to be modified
CFI	CFI should exceed 0.93 [7]	0.906	Model needs to be modified
RMR	RMR should be less than 0.09 [6]	0.051	Model doesn't need to be modified

Table 4.7: Summary of the Goodness of Fit Test After the Addition of Correlation between the Unauthorized Access Variable and Errors Variable.

The complete result of the goodness of fit test from AMOS tools for the second modification of the model can be seen in appendix E. Based on the summary of the goodness of fit test after the addition of correlation between the Unauthorized Access variable and Errors variable, the research model does not really represent the data which has been collected. All the fit indices get closer to the cut-off point, but only Chi-square score and RMR pass the cut-off point. If after certain modification the model still does not fit with the available data, an alternative method to find the causal relationship in the research model is path analysis.

4.2.6 Path Analysis

Path analysis is the alternative method to find the causal relationship in the research model where all of the manifest variables in one latent variable combine into one manifest variable [53]. Basically, the path analysis is the special case of SEM, where there is only a structural model without a measurement model [19]. The path analysis will analyze the factor score weights from all the indicators in one variable [53]. The factor score weight is the inter-correlation score between the manifest variables and the latent variables [35]. The factor score weight can be found using AMOS tools. Below is the factor score weight of all the indicators toward their variable.

Item Code					
Unauthorized Access	**UA2**	**UA1**			
	0.503	0.179			
Collection	**COL3**	**COL2**	**COL1**		
	0.105	0.621	-0.198		
Errors	**E3**	**E2**	**E1**		
	0.168	0.303	0.298		
Secondary Use	**SU3**	**SU2**	**SU1**		
	0.279	0.415	0.197		
Actual System Use	**AS3**	**AS2**	**AS1**		
	0.107	0.504	0.164		
Behavioral Intention	**BI4**	**BI3**	**BI2**	**BI1**	
	0.162	0.097	0.291	0.321	
Degree of Trust	**DT5**	**DT4**	**DT3**	**DT2**	**DT1**
	0.161	0.1	0.169	0.294	0.173

Table 4.8: Factor Score Weights for All Variables

After the discovery of factor weights, we can draw the path diagram for path analysis. It is slightly different to the path diagram in SEM as explained before. Below is the path diagram for the path analysis:

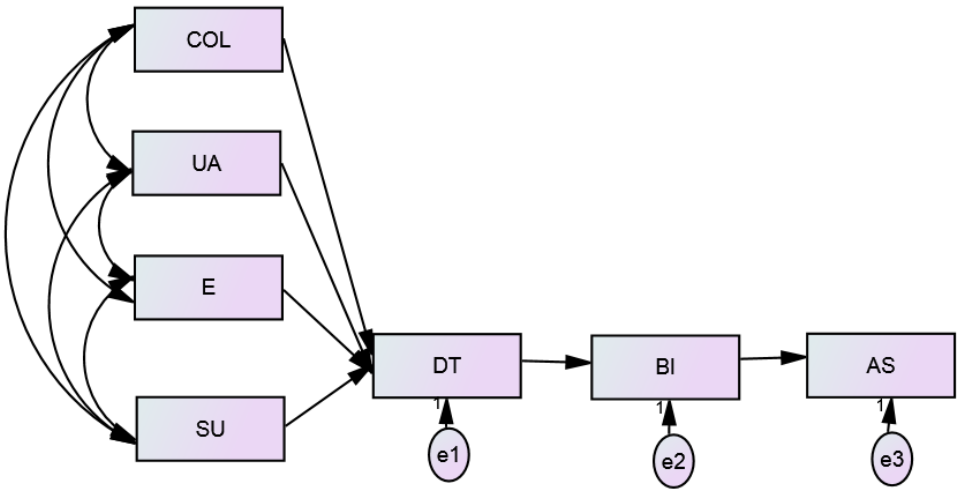

Figure 4.6: Path Diagram for Path Analysis.

The next step is to analyze the goodness of fit of the path diagram. This follows the same procedure as in the structural equation modeling. The complete result of the goodness of fit test from AMOS can be seen in appendix F. Below is the summary of the goodness of fit test for path analysis:

Index Goodness of Fit	Cut-off point	Model's Score	Conclusion
Chi-Square	Chi-square for saturated model<Chi-quare score for default model<Chi-square for independent model	0<13.412<212.598	Model is fit
NFI	NFI should exceed 0.9 or 0.95 [54]	0.937	Model is fit
GFI	GFI should exceed 0.9 [7]	0.966	Model is fit
CFI	CFI should exceed 0.93 [7]	0.977	Model is fit
RMR	RMR should be less than 0.09 [6]	0.017	Model is fit

Table 4.9: Summary of the Goodness of Fit for Path Analysis.

Since all the cut-off points for the goodness of fit are accepted, the model fits with the data available and can be used to test the hypotheses of causal relationship between all the variables.

4.2.7 Acceptance or Rejection of the Model

To find the causal relationship based on the hypotheses made before, the relationship between all the variables have to be accepted or rejected. To accept or reject the relationship between variables and also to test the hypotheses for the research question, a critical ratio score analysis is undertaken [53]. A critical ratio score for every relationship between variables is compared to the critical score cut-off point which is 1.65, with probability under 0.05 [53]. The relationship between the variables is positive if the critical ratio score is greater than the cut-off point, with probability under 0.05 [53], meaning the relationship in the model is accepted. Conversely, the relationship between the variables is negative if the critical ratio score is less than the cut-off point, with probability above 0.05, meaning the relationship in the model is rejected [53]. The critical ratio (C.R.) score result from AMOS can be seen in the following table:

Hypotheses				Estimate	S.E.	C.R.	P	Notes
H1	**DT**	$<-$	**COL**	0.036	0.079	0.459	0.646	Rejected
H2	**DT**	$<-$	**UA**	0.281	0.109	2.591	0.01	Accepted
H3	**DT**	$<-$	**E**	0.464	0.113	4.118	***	Accepted
H4	**DT**	$<-$	**SU**	0.009	0.13	0.067	0.946	Rejected

Hypotheses				Estimate	S.E.	C.R.	P	Notes
H5	**BI**	< –	**DT**	0.5	0.076	6.568	***	Accepted
H6	**AS**	< –	**BI**	0.423	0.076	5.567	***	Accepted

Table 4.10: The Result of C.R. Score.

4.3 Analysis of the Former Privacy-Trust-Behavioral Intention Research Model

In order to know whether the available data fits with the previous privacy-trust-behavioral intention model [34], an analysis using SEM with AMOS tools is undertaken. In order to be relevant to the previous research model, the four privacy concern variables are transformed into the indicators of privacy variables in the privacy-trust-behavioral intention model. The score of the indicator will use the factor weights score, which is already known in the path analysis section. The research model is represented in a path diagram form as the following:

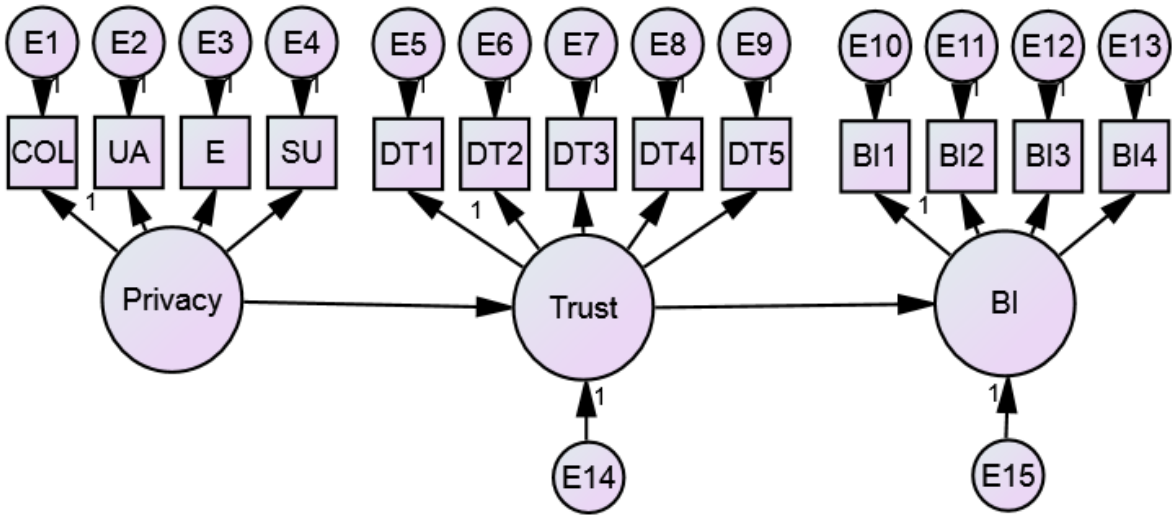

Figure 4.7: Path Diagram for Privacy-Trust-Behavioral Intention Model.

4.3.1 Examination of Model based on Degree of Freedom

Below is the output note from the AMOS tool related to the degree of freedom of the proposed model:

Notes for Model (Default model)

Computation of degrees of freedom (Default model)

Number of distinct sample moments:	91
Number of distinct parameters to be estimated:	28
Degrees of freedom (91 - 28):	63

Result (Default model)

Minimum was achieved
Chi-square = 96.907
Degrees of freedom = 63
Probability level = .004

Figure 4.8: The Result of Degree of Freedom Calculation.

The model is over identified, so can be estimated further.

4.3.2 Examination of The Model based on the AMOS Calculation

The standards that determine the fitness of the model are the NFI, GFI, CFI, and RMR, as discussed above. Below is the summary of goodness of fit test for the research model using AMOS.

Index Goodness of Fit	Cut-off point	Model's Score	Conclusion
Chi-Square	Chi-square for saturated model<Chi-quare score for default model<Chi-square for independent model	0<96.907<673.175	Model is fit
NFI	NFI should exceed 0.9 or 0.95 [54]	0.856	Model needs to be modified
GFI	GFI should exceed 0.9 [7]	0.883	Model needs to be modified
CFI	CFI should exceed 0.93 [7]	0.943	Model is fit
RMR	RMR should be less than 0.09 [6]	0.028	Model is fit

Table 4.11: Summary of Goodness of Fit Test.

Based on the goodness of fit test, the previous model does not fit with the data available, as the NFI and GFI score don't reach the cut-off point. However, based on modification indices (see appendix G), the model can be modified by adding a correlation between certain error variables to make it fit perfectly with the data. Correlation between certain error variables can happen if the data collection is performed using a one-time interview or questionnaire, since all of the questions are related to each other [25]. Below is the model after an addition of correlation between error variables based on the modification indices and the goodness of fit result after the modification.

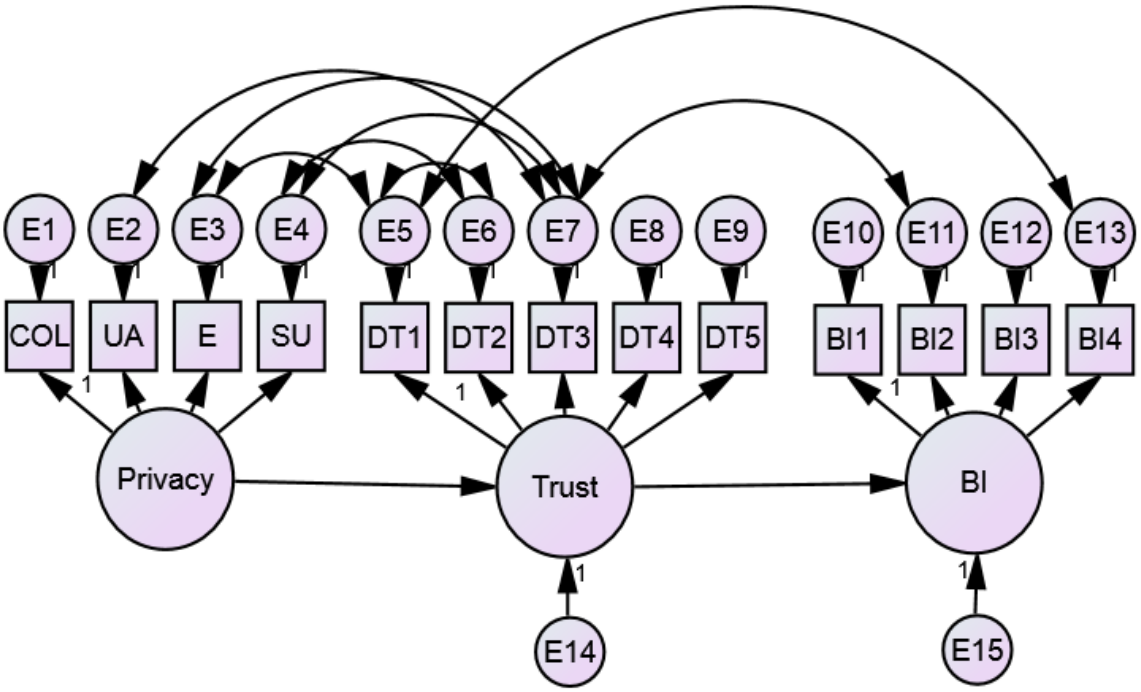

Figure 4.9: Path Diagram for Privacy-Trust-Behavioral Intention Model After the Addition of Error Variables' Correlation.

Index Goodness of Fit	**Cut-off point**	**Model's Score**	**Conclusion**
Chi-Square	Chi-square for saturated model<Chi-quare score for default model<Chi-square for independent model	0<56.215<673.175	Model is fit
NFI	NFI should exceed 0.9 or 0.95 [54]	0.916	Model is fit

Index Goodness of Fit	**Cut-off point**	**Model's Score**	**Conclusion**
GFI	GFI should exceed 0.9 [7]	0.928	Model is fit
CFI	CFI should exceed 0.93 [7]	0.998	Model is fit
RMR	RMR should be less than 0.09 [6]	0.024	Model is fit

Table 4.12: Summary of Goodness of Fit Test After the Addition of Error Variables' Correlation.

We can conclude that the former privacy-trust-behavioral intention model fits with the available data only with the addition of error variables' correlation.

Chapter 5

Discussions

5.1 Research Model and Methodology

The new research model with the use of structural equation modeling method doesn't really represent the available data. There are some discrepancies, which mean that the model is unfit even after two modifications. The first modification completely removed collection from the privacy concerns, and for the second modification there is a strong correlation between unauthorized access and errors variables. Since the unauthorized access only has two indicators, it depends on the other variable to fit with the model [1]. However, the goodness of fit test result is still not satisfactory for the model to be considered as fit, so we cannot take any further action to prove the causal relationship between all the variables.

Therefore, path analysis method was undertaken. As mentioned before, the path analysis is a special case of SEM, where there is only a structural model but no measurement model [19]. Path analysis is used to test the predictive relationship between variables in mathematical problem-solving [14]. The path analysis procedures is the same as structural equation modeling, only there are no convergent validity and discriminant validity tests involved, since all the indicators or manifest variables are combined into each other. So all the latent variables are simply formed into manifest variables [53]. From the path analysis procedure, the model proved to be fit, and the causal relationship between all the variables can be inferred based on the following hypotheses:

- H1: The way an insurance provider collects and stores the personal data has a positive relationship with an insurance participant's degree of trust.
  - This hypothesis is rejected based on the critical ratio score from the results of path analysis. There is no positive relationship between the collection variable and the degree of trust variable
- H2: The way an insurance provider ensures there is no unauthorized access to the personal data has a positive relationship with an insurance participant's degree of trust.
  - This hypothesis is accepted based on the critical ratio score from the results of path analysis. There is a positive relationship between the unauthorized access variable and the degree of trust variable.
- H3: The way an insurance provider ensures the accuracy and integrity of the personal data has a positive relationship with an insurance participant's degree of trust.
  - This hypothesis is accepted based on the critical ratio score from the results of path analysis. There is a positive relationship between the error variable and the degree of trust variable.
- H4: The way an insurance provider ensures there is no secondary use of personal data has a positive relationship with an insurance participant's degree of trust.

  - This hypothesis is rejected based on the critical ratio score from the results of path analysis. There is no positive relationship between the secondary use variable and the degree of trust variable.

- H5: There is a positive relationship between an insurance participant's degree of trust and an insurance participant's intention to use the insurance information system by providing their personal data
  - This hypothesis is accepted based on the critical ratio score from the results of path analysis. There is a positive relationship between the degree of trust variable and the behavioral intention variable.

- H6: There is a positive relationship between an insurance participant's intention to use the insurance information system and the actual use of information system by the insurance participant.
  - This hypothesis is accepted based on the critical ratio score from the results of path analysis. There is a positive relationship between the behavioral intention variable and the actual system use variable.

To conclude, the research model that represents the available data is the structural model, which turns all latent variables into manifest variables, and the suitable method is a path analysis.

The concern of information privacy from a previous study by Stewart and Segars [58] does not fit with the privacy-trust-behavioral model from the previous study by Liu [34]. From Liu's study, the privacy concern is one single variable [34], while in this study, the privacy concern is divided into four bigger variables, taken from the study of Stewart and Segars [58]. Although not all the privacy concerns have a positive relationship with the degree of trust, the degree of trust really influences the behavioral intention and the actual system use.

The new research model, which is based on the case study of insurance web-services usage in Indonesia with a combination of previous studies [34][58], has both strengths and weaknesses. The first strength is that the new research model with evidence-based results from the case study may have less bias than the new research model developed from theoretical studies [16]. The new research model may offer a novel theory that has not been found in the previous studies. The second strength is that the new research model is from a case study, which is most likely to prove similar hypotheses that may be different from previous studies [16]. The new research model also offers the theory that is most likely to be relevant in reality [16]. In this study, we can infer that collection and secondary use are not really privacy concerns in using insurance web-services.

Despite all the strengths and benefits of the new research model, there are some weaknesses that should be noted. The first one is the narrow result [16]. The applicability of this new research model may only conform to other countries that are relatively new in insurance web-services and privacy awareness. Since this is also a behavioral study that aims to find the causal relationship variable, the use of SEM and path analysis may also have strengths and weaknesses. One of the most notable advantages of SEM is that the method is effective when there are previous studies and a theoretical framework related to each other [18]. In terms of disadvantages, both SEM and path analysis should be interpreted cautiously because the goodness of fit tests are relative and not absolute [58].

5.2 The Impact of Privacy Concerns to The Customer's Trust and The Most Influential Privacy Concern

Based on the previous section, we can see that only two of four privacy concerns have a positive relationship with a customer's trust of an insurance company, particularly in terms of providing their personal information on a website in return for a service from the company. Based on the data analysis, the insurance participants are concerned on how the insurance company keeps their personal information, especially the ones related to unauthorized access to medical data and financial data while they are using insurance web-services. Insurance participants are also concerned that the insurance company should not release their personal information or let that happen without their consent. If they feel that their insurance company has a strong security mechanism and has a good reputation for preventing data leakage, they tend to trust the insurance company.

The other thing is the insurance participants' concern about how the insurance company will try to ensure that their personal information is accurate and free from incorrect information. Managing personal information in insurance service is really important, as the information is used by several parties such as health services, pension fund services, and the insurance companies themselves [29].The correctness of the data will affect the efficiency and quality of the services provided by all the parties related to the insurance companies [29].

The two other privacy concerns, namely collection and secondary use, have a negative relationship to the degree of trust toward the insurance company. They are still part of the privacy concerns, but it doesn't really impact the degree of trust of the insurance participants. In other words, how the insurance company collects personal information and gives reasons for personal information collection to the insurance participant doesn't affect the degree of trust toward the insurance company. The secondary use of personal information stored in the insurance database also does not affect the degree of trust in the insurance company. It is described in the unauthorized access concern. Secondary use means the use of personal data by other parties beside the insurance services themselves, without consent from the insurance participants. If neither the company nor the participants themselves give consent and proper authorization it is considered as unauthorized secondary use [57].

Based on the results of path analysis, the most influential privacy concern can be determined by assessing the biggest critical score between all the variables [19] or the biggest estimate correlation score [18]. Based on Table 4.16, the correlation between the errors variable and the degree of trust variable (the estimate score) is the highest among all the privacy concerns, and its critical ratio score is also the highest among all the privacy concerns. The errors variable indicates that the insurance participant tend to be more concerned about how the insurance company protects their personal information against deliberate and accidental errors [57]. It is also to guarantee that they get a high-quality service based on the correct personal information stored in the database.

5.3 The Impact of The Customer's Trust to The Behavioral Intention and Actual System Use

As described before, the degree of trust indicates the insurance participant's confidence in using insurance web-services, based on their belief in the insurance company given the insurance company's norms, regulations, policies, and procedures [34]. After experiencing the use of insurance web-services, the users tend to trust more and therefore provide their personal data and actually use the information system. In contrast to the correlation between the privacy concern and the degree of trust, the degree of trust as a whole really influences the behavioral intention of the insurance participants. The behavioral intention of the insurance participants can be shown

by the willingness of the insurance participant to provide the necessary personal information into the insurance website, the willingness of the insurance participant to recommend the use of the insurance website to the others, and the willingness to give a positive remark about the insurance web-services that they use.

The actual system use indicates that the insurance participants actually use the system to get a service from the insurance company. They are using it because they believe the company's policy and procedure as well as the security measures comply with their privacy concerns. Furthermore, they are using the insurance web-services due to a decent reputation of the insurance company they are registered with. Additionally, they use the insurance web-services due to their ease of use, despite all the privacy concern they have about the use of insurance web-services. They believe the use of web-services in insurance is more effective and efficient than paper-based services [5]

Chapter 6

Conclusions

6.1 Concluding Remarks

The aim of this study was to investigate whether the privacy concerns influence the degree of trust and behavioral intention that lead to actual use of insurance web-services. For this purpose, a new research model was developed by combining the existing privacy-trust-behavioral intention model [34] with the concern for information privacy research [58], which identified the most important aspects in privacy. The new research model was tested using a structural equation modeling and path analysis method. The model was a combination of previous studies related to privacy concerns and degree of trust [34] [58]. With the whole structural equation model method, the new research model had to be modified twice, but it still does not represent the data collected from the questionnaire. Path analysis was undertaken as an alternative method to test the new research model. With the modified model using path analysis, the model was proven to fit with the data collected from the questionnaire, and thus the causal relationship and all the hypotheses can either be accepted or rejected.

From the results of the path analysis, it can be concluded that the way an insurance provider collects and stores personal data does not really influence the degree of trust toward the insurance provider. Similarly, it is proven that the way an insurance provider ensures there is no secondary use of personal data does not really influence the degree of trust toward the insurance provider. Conversely, the way an insurance provider ensures there is no unauthorized access to personal data, and the way they ensure the accuracy and integrity of the personal data have positive relationships with the insurance participant's trust in the company. The most influential factor in terms of the privacy concerns of the insurance participant is errors. Insurance participants are more concerned about errors in their personal data than the other privacy concerns described in the research model.

The degree of trust in the insurance company influences the behavioral intention and the actual use of the web service provided by the company. Simply put, if the insurance participants trust their insurance company, they are willing to input their important personal data into web-services, despite their privacy concerns. They are also willing to use these web-services repeatedly and recommend the use of such services from the insurance company to others. Most of the participants who trust and have a good behavioral intention toward their insurance company have used the company's web-services and feel satisfied with it.

The findings of this study should be of interest to both academics and practitioners, especially for raising awareness of privacy protection both from the insurance participants' point of view and the insurance company's point of view. The whole study demonstrates that privacy concerns within the insurance web-services impacts the degree of trust in the company as a whole and further impacts the actual use of the web-services.

6.2 Limitation

There are some limitations to this study that should be discussed. First, the samples only focused on Indonesian, where insurance web-services are still growing and may still be a bit new to some people. Thus to gather more than 100 participants was a bit more difficult. Second,

the survey was conducted online, so there were participants who stopped doing the survey in the middle (for unknown reasons) and did not complete it, so we could not observe directly how they behave towards the insurance web-services. Third, since only 107 participants completed the questionnaire, it is a relatively small sample for SEM. Thus, it might affect the SEM results since the model is proven not to fit with the available data.

Finally, this study is only focused on four privacy concerns while there may in fact be more, especially for the use of insurance web-services. In the future, those four privacy concerns may not even be there as concerns. There may be some different perspectives from all the insurance participants about what most concerns them when using the insurance web-services. There may also be additional privacy protection features within the insurance web services, so the results in future research can differ from current results.

6.3 Future Work

For future work, the research model can be modified by adding more indicators to all variables. Therefore, if there are indicators that do not pass the validity and reliability test both in the pilot study and in the real analysis, there will still be at least two variables. The research model analysis should be done not only with SEM or path analysis but also with the other multivariate statistical methods such as partial least squares, in order to compare the results and to ensure that the results from the model testing are reliable. The research model can also be extended in the future by adding more privacy concerns and other external factors such as age, experience in using web-services technology, or even the education of the participants.

Related to the addition of privacy concerns, it may be wise to hold some focus group discussions with people from insurance companies, insurance participants, and some privacy experts. The discussion can conclude what are the most important privacy concerns that can really affect the degree of trust in using web-services, particularly insurance web-services. The discussion can also contribute to the additional of external variables. Furthermore, in order to have a precise determination in choosing the indicators for the variables, direct observation techniques using a dummy insurance web-service platform for the participant may be a good idea. The use of a dummy platform can guarantee a validity of all the indicators in the variables [10]. The dummy insurance web-service can be given all the features related to privacy concerns. The use of the features can contribute to the determination of the indicators. As a conclusion, most of the future work involves designing the research model more carefully.

Bibliography

[1] JL Arbuckle. Wothke w. *Amos 4.0 user's guide*, pages 1995–1999, 1999.

[2] Gaurav Bansal, David Gefen, et al. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2):138–150, 2010.

[3] Kenneth A Bollen. *Structural equations with latent variables*. John Wiley & Sons, 2014.

[4] Jeffrey R Brown and Austan Goolsbee. Does the internet make markets more competitive? Technical report, National Bureau of Economic Research, 2000.

[5] Jeffrey R.. Brown and Austan Goolsbee. *Does the Internet make markets more competitive?: evidence from the life insurance industry*. National Bureau of Economic Research, 2000.

[6] Michael W Browne, Robert Cudeck, Kenneth A Bollen, and J Scott Long. Alternative ways of assessing model fit. *Sage Focus Editions*, 154:136–136, 1993.

[7] Barbara M Byrne. *Structural equation modeling with EQS: Basic concepts, applications, and programming*. Routledge, 2013.

[8] Juan Carlos Roca, Juan José García, and Juan José de la Vega. The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 17(2):96–113, 2009.

[9] LM Connelly. Pilot studies. *Medsurg nursing: official journal of the Academy of Medical-Surgical Nurses*, 17(6):411, 2008.

[10] Donald R Cooper and C William Emory. Business research methods, chicago: Richard d. irwin, 1995.

[11] John W Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2013.

[12] LeeJ. Cronbach. Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3):297–334, 1951.

[13] Mary J Culnan. " how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, pages 341–363, 1993.

[14] Otis Dudley Duncan. Path analysis: Sociological examples. *American journal of Sociology*, pages 1–16, 1966.

[15] E-benefit.lippoinsurance.com. E-benefit lippo insurance, 2015.

[16] Kathleen M Eisenhardt. Building theories from case study research. *Academy of management review*, 14(4):532–550, 1989.

[17] Kanna Al Falahi, Yacine Atif, and Said Elnaffar. Social networks: Challenges and new opportunities. In *Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, pages 804–808. IEEE Computer Society, 2010.

[18] DM Fergusson. A brief introduction to structural equation models. *P. Verhulst & H. Koot (Eds.), Handbook of Childhood Psychiatric Epidemiology*, pages 122–145, 1995.

[19] G David Garson. Path analysis. *from Statnotes: Topics in multivariate analysis. Retrieved*, 9(05):2009, 2008.

[20] David Gefen, Detmar Straub, and Marie-Claude Boudreau. Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, 4(1):7, 2000.

[21] Joseph A Gliem and Rosemary R Gliem. Calculating, interpreting, and reporting cronbach's alpha reliability coefficient for likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, 2003.

[22] Joseph F Hair, R.L. Tatham, and R.E. Anderson. *Multivariate Data Analysis*. Prentice Hall, 2006.

[23] Claire Hargreaves and Daniel Prince. Understanding cyber criminals and measuring their future activity. 2013.

[24] Charles I Jones. Intermediate goods and weak links in the theory of economic development. *American Economic Journal: Macroeconomics*, pages 1–28, 2011.

[25] Yutaka Kano and Yukari Azuma. Use of sem programs to precisely measure scale reliability. In *New developments in psychometrics*, pages 141–148. Springer, 2003.

[26] Melody Y Kiang, TS Raghu, and Kevin Huei-Min Shang. Marketing on the internet—who can benefit from an online marketing approach? *Decision Support Systems*, 27(4):383–393, 2000.

[27] Adam Klauber. Insurance on the internet. *Risk Management and Insurance Review*, 3(1):45–62, 2000.

[28] Sherah Kurnia. E-commerce adoption in developing countries: an indonesian study. In *San Diego International Systems Conference*, pages 14–16, 2006.

[29] C Lambrinoudakis and S Gritzalis. Managing medical and insurance information through a smart-card-based information system. *Journal of Medical Systems*, 24(4):213–234, 2000.

[30] Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *UbiComp 2002: Ubiquitous Computing*, pages 237–245. Springer, 2002.

[31] Paul J Lavrakas. *Encyclopedia of survey research methods*. Sage Publications, 2008.

[32] Lippoinsurance.com. Lippoinsurance epolicy, 2015.

[33] Mark S Litwin. *How to measure survey reliability and validity*, volume 7. Sage Publications, 1995.

[34] Chang Liu, Jack T Marchewka, June Lu, and Chun-Sheng Yu. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, 42(2):289–304, 2005.

[35] John C Loehlin. *Latent variable models: An introduction to factor, path, and structural equation analysis*. Psychology Press, 2004.

[36] Muharman Lubis, Mira Kartiwi, and Sonny Zulhuda. A guideline to enforce privacy and data protection regulation in indonesia. *South East Asia Journal of Contemporary Business, Economics and Law*, 2(3):56–63, 2013.

[37] Muharman Lubis, Mira Kartiwi, and Sonny Zulhuda. An overview of legal framework for personal data protection on electronic voting in indonesia. Kuala Lumpur International Business, Economics and Law Conference, 2013.

[38] Thomas R Lunsford and Brenda Rae Lunsford. The research sample, part i: Sampling. *JPO: Journal of Prosthetics and Orthotics*, 7(3):17A, 1995.

[39] Mary R Lynn. Determination and quantification of content validity. *Nursing research*, 35(6):382–386, 1986.

[40] Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of management review*, 20(3):709–734, 1995.

[41] Ramin Cooper Maysami and W Jean Kwon. An analysis of islamic takaful insurance: A cooperative insurance mechanism. *Journal of Insurance Regulation*, 18(1):109, 1999.

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

[43] Peraturan Presiden Republik Indonesia Nomor. Peraturan presiden nomor 111 tahun 2013 tentang jaminan kesehatan. *Jasa Pemerintah*, 2013.

[44] J. Noor. *Metodologi Penelitian*. Kencana Prenada Media Group, 2013.

[45] L Paige Fields, Donald R Fraser, and James W Kolari. Is bancassurance a viable model for financial firms? *Journal of Risk and Insurance*, 74(4):777–794, 2007.

[46] Dino Pedreschi, Francesco Bonchi, Franco Turini, Vassilios S Verykios, Maurizio Atzori, Bradley Malin, Bart Moelans, and Yücel Saygin. Privacy protection: regulations and technologies, opportunities and threats. In *Mobility, Data Mining and Privacy*, pages 101–119. Springer, 2008.

[47] Constantine Photopoulos. *Managing catastrophic loss of sensitive data: a guide for IT and security professionals*. Syngress, 2011.

[48] Harry Ramadan. Bpjs kesehatan, 2015.

[49] Harry Ramadan. Bpjs kesehatan, 2015.

[50] Harry Ramadan. Bpjs kesehatan, 2015.

[51] Reading.ac.uk. Data protection glossary - university of reading, 2015.

[52] Malia Rochma. Prospek industri asuransi jiwa di indonesia. *Economic Review*, (210):1–7, 2007.

[53] Singgih Santoso. *Analisis SEM Menggunakan AMOS*. Elex Media Komputindo, 2012.

[54] Randall E Schumacker and Richard G Lomax. *A beginner's guide to structural equation modeling*. Psychology Press, 2004.

[55] Farisya Setiadi et al. An overview of the development indonesia national cyber security. *International Journal of Information & Computer Science*, 6:108, 2012.

[56] Sayuri Shirai. Overview of financial market structures in asia—cases of the republic of korea, malaysia, thailand and indonesia—. 2001.

[57] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, pages 167–196, 1996.

[58] Kathy A Stewart and Albert H Segars. An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1):36–49, 2002.

[59] Setyo Hari Wijanto. Structural equation modeling with lisrel 8.8. *Yogyakarta: Graha Ilmu*, 2008.

[60] Susan G Wilson and Ivan Abel. So you want to get involved in e-commerce. *Industrial Marketing Management*, 31(2):85–94, 2002.

[61] Kevin B Wright. Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication*, 10(3):00–00, 2005.

[62] Valarie A Zeithaml, Leonard L Berry, and Ananthanarayanan Parasuraman. The behavioral consequences of service quality. *the Journal of Marketing*, pages 31–46, 1996.

Appendix A

Full Questionnaire

1. What age group do you belong to?
    - <20
    - 20-25
    - 25-30
    - 30-35
    - >35
2. What is your profession?
3. Do you use insurance? Does your insurance companies provide web services? If yes please answer the following questions.
4. I was informed about what information the insurance company would collect about me
    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree
5. The insurance company explained why they were collecting my personal information
    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree
6. I am concerned that insurance company are collecting too much personal information about me
    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree
7. I feel that the insurance company is using a good security mechanism to keep my personal information related to medical data and financial data out of the hands of unauthorized individuals

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

8. I feel that the insurance company will not release personal information about me without my consent

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

9. I feel that the insurance company has made a reasonable effort to ensure that the information collected about me is accurate

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

10. The insurance company gave me a clear choice before disclosing personal information about me to third parties

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

11. The insurance company has a mechanism to review and change incorrect personal information

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

12. An insurance company should not use personal information for any purposes rather than the main purposes unless it has been authorized by the individuals who provided the information

(a) Strongly disagree
(b) Disagree

(c) Neutral

(d) Agree

(e) Strongly Agree

13. An insurance company should never sell the personal information from their computer databases to other companies

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly Agree

14. An insurance company should never share personal information with other companies unless it has been authorized by the individuals who provided the information

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly Agree

15. An insurance company's privacy policy concerning the notice of personal information collection makes me feel the company is trustworthy

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly Agree

16. An insurance company's policy on how it would use my personal information makes me feel the company is trustworthy

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly Agree

17. The insurance company's policy on how it will share my personal information with third party (in this case hospital) makes me feel the company is trustworthy

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly Agree

18. An insurance company's level of encryption for its information systems and other security measures makes me feel that the company is trustworthy

    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree

19. An insurance company's information system's policy to ensure that all the data is accurate and complete makes me feel that the company is trustworthy

    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree

20. After visiting the insurance website where I am registered / will be registered, I would be willing to provide my personal information to this site

    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree

21. I would be willing to recommend the use of the insurance website where I am registered or will be registered to others

    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree

22. I would choose the insurance website where I am registered or will be registered rather than another insurance company if I had to apply insurance again

    (a) Strongly disagree
    (b) Disagree
    (c) Neutral
    (d) Agree
    (e) Strongly Agree

23. I have positive things to say about the insurance website where I am registered or will be registered

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

24. I decided to use the insurance website where I am registered or will be registered to apply for my insurance because the company's policy and procedure and the security measures address my privacy concerns

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

25. I decided to use the insurance website where I am registered or will be registered in applying my insurance rather than the other company because of the company's decent reputation

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

26. I decided to use the insurance website where I am registered or will be registered to apply for my insurance because of the ease of use

(a) Strongly disagree
(b) Disagree
(c) Neutral
(d) Agree
(e) Strongly Agree

Appendix B

Model Fitness Result from AMOS

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	52	424.102	224	0	1.893
Saturated model	276	0	0	–	–
Independence model	23	1426.487	253	0	5.638

Model	RMR	GFI	AGFI	PGFI
Default model	0.109	0.753	0.695	0.611
Saturated model	0	1	–	–
Independence model	0.213	0.324	0.263	0.297

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	0.703	0.664	0.834	0.807	0.829
Saturated model	1	–	1	–	1
Independence model	0	0	0	0	0

Appendix C

Model Fitness Result (First Modification) from AMOS

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	43	313.899	147	0	2.135
Saturated model	190	0	0	–	–
Independence model	19	1255.926	171	0	7.345

Model	RMR	GFI	AGFI	PGFI
Default model	0.111	0.779	0.715	0.603
Saturated model	0	1	–	–
Independence model	0.237	0.303	0.226	0.273

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	0.750	0.709	0.849	0.821	0.846
Saturated model	1	–	1	–	1
Independence model	0	0	0	0	0

Appendix D

Modification Indices Table

			Modification Indices	Par Change
UA	$<--->$	**E**	47.024	0.351
er26	$<--->$	**SU**	5.474	0.06
er23	$<--->$	**SU**	6.402	0.07
er23	$<--->$	**er25**	6.357	0.10
er21	$<--->$	**E**	9.567	0.14
er21	$<--->$	**UA**	10.942	0.15
er21	$<--->$	**er25**	4.953	-0.08
er15	$<--->$	**er23**	10.999	0.129
er15	$<--->$	**er21**	6.267	-0.09
er14	$<--->$	**SU**	4.822	-0.05
er14	$<--->$	**er23**	11.733	-0.123
er13	$<--->$	**SU**	6.28	0.05
er13	$<--->$	**er21**	4.867	0.06
er12	$<--->$	**er13**	8.295	0.07
er20	$<--->$	**er12**	4.415	0.07
er17	$<--->$	**er23**	4.33	0.09
er17	$<--->$	**er21**	5.173	-0.09
er17	$<--->$	**er13**	4.224	-0.06
er11	$<--->$	**er23**	6.351	0.05
er11	$<--->$	**er21**	9.118	-0.06
er11	$<--->$	**er15**	14.292	0.06
er11	$<--->$	**er14**	4.09	-0.03
er10	$<--->$	**er21**	5.472	0.03
er9	$<--->$	**er15**	10.182	-0.05
er8	$<--->$	**er21**	4.073	0.10
er7	$<--->$	**UA**	8.288	0.13
er7	$<--->$	**er14**	6.22	0.08
er7	$<--->$	**er17**	6.222	0.10
er6	$<--->$	**SU**	5.118	0.06

			Modification Indices	Par Change
er6	$<--->$	**UA**	6.963	0.13
er5	$<--->$	**E**	12.776	0.18
er5	$<--->$	**er21**	6.181	0.11
er5	$<--->$	**er11**	4.714	-0.05
er5	$<--->$	**er7**	6.357	0.115
er4	$<--->$	**er6**	6.22	0.10

Appendix E

Model Fitness Result (Second Modification) from AMOS

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	44	248.498	146	0	1.702
Saturated model	190	0	0	–	–
Independence model	19	1255.926	171	0	7.345

Model	RMR	GFI	AGFI	PGFI
Default model	0.05	0.806	0.747	0.619
Saturated model	0	1	–	–
Independence model	0.237	0.303	0.226	0.273

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	0.802	0.768	0.908	0.889	0.906
Saturated model	1	–	1	–	1
Independence model	0	0	0	0	0

Appendix F

Model Fitness Result (Path Analysis) from AMOS

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	19	13.142	9	0	1.749
Saturated model	28	0	0	–	–
Independence model	7	21.598	21	0	10.124

Model	RMR	GFI	AGFI	PGFI
Default model	0.017	0.966	0.894	0.31
Saturated model	0	1	–	–
Independence model	0.102	0.582	0.443	0.437

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	0.937	0.853	0.978	0.946	0.977
Saturated model	1	–	1	–	1
Independence model	0	0	0	0	0

Appendix G

Modification Indices Table for Privacy-Trust-Behavioral Intention Model

			Modification Indices	Par Change
E7	$<--->$	**E11**	4.216	0.069
E5	$<--->$	**E13**	5.094	0.08
E5	$<--->$	**E6**	8.273	0.067
E4	$<--->$	**E7**	4.569	-0.039
E4	$<--->$	**E6**	6.453	0.041
E3	$<--->$	**E7**	8.305	0.056
E3	$<--->$	**E5**	6.353	-0.05
E2	$<--->$	**E7**	15.652	-0.05