CAN BRAND ATTENTION BE A DISADVANTAGE FOR AN INDUSTRY?

THE IMPACT OF CYBERCRIME ON TRUST IN THE CLOUD COMPUTING SERVICE INDUSTRY

by

Christian Chandra Kurniatedja

written under the supervision of Professor Marian Beise-Zee

July 2015

Thesis Presented to the Higher Degree Committee

of Ritsumeikan Asia Pacific University

in Partial Fulfillment of the Requirements for the Degree of

Master of Business Administration (MBA)

CERTIFICATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that neither any part of this thesis nor the whole of the thesis has been submitted for a degree to any other university or institution.

I certify that my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations or any other material from the work of other people included in my thesis that is published or otherwise, are fully acknowledged in accordance with the standard referencing practice.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis's supervisor.

Date: 15th of July, 2015

Place: Ritsumeikan Asia Pacific University Japan

Christian Chandra Kurniatedja

ACKNOWLEDGEMENT

On this fruitful occasion of the successful completion of this master thesis, I would like to give thanks to God almighty who always showering blessings upon me and without His divine blessing, I would not have been able to attain this stage in my life.

I would like to express my sincere appreciation towards my principal supervisor Prof. Dr. Marian Beise-Zee for his patience, constants guidance and encouragement. Without his valuable assistance and persistent help this work would not have been possible.

I express my gratitude to all the lectures and professors in the Graduate School of Management Ritsumeikan Asia Pacific University for their support towards the successful of my studies in Japan.

I dedicate this work to my beloved Mother Paula Enggarwati, Father Yoseph Salim, Brother Vincentius Chandra and Sister Natasha Sherly, who are the ultimate reasons for my success. I would like to heartedly thank them for their irrational and unbreakable belief in me.

I pay sincere regards to my fiancé Florentina Lanny for all supports and love that have been given to me which also considered as the main motivation for me to finish this dissertation.

I specially thank all my friends in Japan and Indonesia who always motivate me in many ways.

I would also like to thank all scholars, researchers and organizations who gave permission for copyright material to be quoted and used.

Lastly, I would like to pay my deepest respect to all respondents of my questionnaire, without their help, this study would not have been completed.

15th of July, 2015 Beppu, Japan

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Purpose – In brand management theory it is recommended to leverage brand awareness and brand trust for growth of the whole industry. However in certain industries, especially new industries in which product failures happen more often, brands might not have a positive impact. Brands might worsen negative publicity of an industry in cases of product failure and disrupt the whole industry. This study aims to empirically compare the response from customers regarding their trust level in the whole industry between a branded and non branded context when several distrust factors are emerging. The carryover effect from brands and non brands is measured by comparing responses to various product failure situations. The nascent cloud service industry serves as a study context in which brands are suggested to a negative effect due to the public attention they draw to product failure cases.

Design/methodology/approach – An experiment will be used to compare all collected data which will be retrieved by an online questionnaire.

Findings – Although the data confirms several hypotheses the main hypothesis that a brand is perceived worse than a non brand in case of a product failure cannot be significantly confirmed.

Originality/value – The paper introduces a proposed negative effect of brands in that has not yet been described in literature. The study conceptualizes the bad experiences as the main cause and tests the hypothesis with a company with a low brand and one with a popular brand. It then measures the effect of distrust and the carryover effect.

Keywords

Internet, Marketing, Software Industry, Cloud Computing Technology, Brand, Trust Building Mechanism, Customer Distrust, Carryover effect

CHAPTER 1 INTRODUCTION

1.1. Background

Technology has grown extremely fast over the past few decades. One of the key drivers of this change is the internet. Based on the International Telecommunication Union (ITU), we acknowledge that the growth of internet users has been enormous for the last decade from around nine hundred million users in 2004 to almost 3 billion in 2014 (ITU, 2014). This phenomenon opens a lot of opportunities which also impacts entrepreneurship as analyzed by (Cumming & Johan, 2010). It stimulates a lot of people to create new innovative business models especially in the service industry. Service industry can be described as an industry which covers all those firms and employers whose major final output is some intangible or ephemeral commodity or, alternatively, that residual set of productive institutions in the formal economy whose final output is not a material good (Kakaomerlioglu & Carlsson, 1999). Apart from the positive impacts of the internet, it also changes the way business was conducted in several industries.

The software industry is one example of service industry because the value of its final outcome is not in physical form. It can be an application inside a phone, tablet or a desktop application. Therefore in this industry the ownership model itself has changed, consumers do not own a physical product instead they utilize the value from it. By eliminating the ownership towards a product, there will be a big trade-off between economical value and risk. For example, by renting a car instead of purchasing a car, the sense of anxiety due to maintenance cost and tax

will be reduced, but both parties have the risk of customer misbehavior or product failure. Furthermore, removing the ownership will not always work for all products because of prestige of ownership. The attraction of owning a luxury vehicle is being able to own and drive a car with superior comfort and performance. As not many people are able to afford a luxury car, owning one would bring pride and joy to the owner (Chuah, 2010) and might increase the social status of the owner.

Yet, in the software industry the prestige factor does not play an important role. Hence, the effect of the internet has outstanding impacts in this particular industry. Moreover it does not require a huge investment in machinery and the operational cost is relatively low. The software industry becomes more of a total service industry over time as the concept of "software on demand" or "Software as a Service" (SaaS) becomes more common. Furthermore, with the introduction of cloud technology, where companies and consumers can store their electronic files in the internet, instead of a local flash drive or hard drive, and with the enormous growth of smart phone users, the service part of the IT industry grows and competition within this industry becomes tighter. According to National Standard Institute and Technology, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell, 2011). Due to the

benefits of the cloud computing technology, many industries try to adapt this technology.

One important element that should be taken into consideration in cloud computing service industry is the way the industry attracts its customers. But because the final output does not have a physical form, the marketing strategy and brand management for selling the product will be different. Without a physical product, the foundation between buyer and seller will be deeply based on one factor called trust which makes trust building mechanism play an important role. Many business models in this industry attract customers with subscription models and freemium. Freemium is a business model in which you give a core product away for free to a large group of users and sell premium products to a smaller fraction of this user base (Froberg, 2015). Brands are mostly seen as a decisive trust builder.

A lot of studies about marketing strategy and brand management have been done and most of them see the brand only from the positive side. Amongst the marketing strategies out there, brand is one of the common entities which is used to increase the awareness and trust toward the product and sometimes it can be used to create a strong brand identity such as Kleenex for facial tissue. According to Brent Banda, "A brand is a reputation. This reputation often is represented by a name, term, symbol or special design (or some combination of these elements) that is intended to identify a company or its product." (Banda, 2011). According to Jim Edmonds, having a strong brand identity is a must and in a certain case, re-branding the company is necessary (Edmonds, 2005). This paper tries to study a

brand entity from different perspective. The study will be focused on the effect of the customer towards the brand in cloud computing service industry by giving several distrust factors in a sequence with varying two independent variables, the level of brand and the level of risk.

1.2. Problem Statement

Brand is considered to be a trust agent and always has a positive impact in the industry. In case of a product failure, brand suffers negative publicity. However, we propose a case in which brands can have a negative effect on the whole industry even if the brand itself is not especially singled out as bad or directly affected by product failures. We suggest that in industries in which trust is important and brands are attracted by criminals, brands have a negative effect on customer trust towards the whole industry. This is known as a "carryover effect". As an example, the cloud server industry serves as the study context.

Based on computer literacy, any software and computer technology is merely a manipulation of electricity connection that is represented by a collection of bit, one or zero. Therefore there is an absolute weakness in cloud computing service industry. It has been mentioned that there is no 100% secure place inside the internet. According to John McBrayer, the prevalence of cybercriminal activities especially hacker and cracker has generated a large financial loss in the industry (McBrayer, 2014). Moreover the exponential expansion of computer technologies and the Internet have spawned a variety of new criminal behaviors and provided criminals with a new environment within which to operate (Maras,

2012). Therefore, understanding the motive and intention of cybercriminal is really crucial.

Because of the above reason, increasing brand awareness will also increase the vulnerability of the product because brands can attract good people and also bad people. According to Maras, the more users on a certain cloud service, the more valuable information can be retrieved and this becomes the biggest incentive for hackers to do their cybercrime action (Maras, 2012). In this situation, having a big brand might have more negative rather than positive effects. The distrust factors such as product failure, broken promises and expectancy disconfirmation can disrupt another company within the same industry. This is known as carryover effect (Darke, Ashworth, & Main, 2009). A study finds that such failures can also jeopardize other products from different companies within the same industry (Ahluwalia & Gurhan-Canli, 2000). To give more evidence about this technology vulnerability, several real case examples in 2014 can be used as reference. Dropbox a popular brand for cloud file storing service reported that there was a threat in their firewall system. Within the same year, Apple iCloud was also hacked by unknown people exposing private data through the internet. At the end of 2014, Sony corporation entertainment has been hacked, allegedly due of a movie called “The Interview” that was deemed offending to North Korea (Zetter, 2014). Early this year one of the UNIX gurus from Red Hat advisory stated that there is a high security threat inside the core system in UNIX system which is used by all servers in the world. He said this vulnerability can be exploited by

hackers to take full control of the main system without sending permission to the owner (Mimoso, 2015).

1.3. Research Objectives

According to the issue above, the cybercriminal will always have a way to hack or crack a software product. Hence, this study wants to see the reaction of customer trust levels when they are using a certain application and suddenly several distrust factors is applied. The study intends to measure the carryover effect to the whole industry of these distrust factors. This study will also test the moderating effect of different levels of risk. If the level of trust in a popular brand is reduced significantly more than trust in a low or non-brand company, it follows that brand equity has a more negative effect. Furthermore, the effect on trust in the whole industry is measured as well as test of the carryover effect.

1.4. Rational

For companies that have popular brands, branding budget is an important part of their financial planning process. Increasing the awareness of the product by promoting an innovative and attractive brand is one of the most common ways to build a strong brand. However, in certain cases, this study tries to prove that there is a condition where the company should keep the brand low and allocate the fund to other marketing tools which will result in a more positive impact to the company rather than focusing on building a strong brand that eventually may increase the vulnerability of the company itself. The result of this study can be

used by a software company that is engaged in cloud computing service as a reference to be more selective when choosing their marketing strategy and managing their brand.

1.5. Organization of the research

This study was conducted through several phases. The first phase was topic creation. Brainstorming methodology was used in order to find and choose recent hot topics and the topic that is related to the competence of the researcher. The topic should be sufficient to be researched and analyzed. The definition of sufficiency in here is not merely researchable but also must have significant impact or benefits for the readers especially in marketing and brand area. The first topic that was chosen was related to cloud computing.

After choosing the topic, the second phase was started. This phase is called generalization. This phase is about finding a foundation that can support the topic. Two main keywords that are closely related to the topic are service industry and ownership. Several literature studies about those keywords were also done within the same phase.

After good foundation was established to start the research, the next phase called conceptualization began. Within this phase, the topic was narrowed down. Conceptualization starts by defining real world and abstract world. Any real action from the real world should be conceptualized into the abstract world so that the action can be measured.

The next phase is called measurement. This phase basically is a time where finding a proper methodology to conduct an observation is decided. In order to decide the correct measurement, a questionnaire is used to gauge the response from the respondents after several distrust factors are given in a sequence. The preparation of the questionnaire was also done in this phase. The questionnaire is divided by four scenarios which is varied by the level of risk and brand.

Data collection is the next phase. The survey was conducted by using an online form. The respondent will be randomly redirected to one of the four scenarios. The sequence of the answer is also important and should be answered in order.

After getting all data, the final phase is analysis. The raw data was inputted into a statistical program so that the analysis can be done faster. Analysis of variance and mean is mainly used to measure the effect of each response.

CHAPTER 2 LITERATURE REVIEW

2.1. The Service Industry

A number of researches have been done to investigate the importance of product ownership and its relationship to self-congruity (Barone, Shimp, & Sprott, 1999). Within their study, the measurement between ownership versus non-ownership has significantly proved that ownership acts as an important determinant towards the effect of self-congruence (Barone, Shimp, & Sprott, 1999). Another investigation from several studies confirmed that the brand or product preference of consumer will closely correspond to his or her own self-concept (Dolich, 1969; Barone, Shimp, & Sprott, 1999). However in service industry the element of ownership is absent. Because of the absence of ownership, the determinant factor towards the effect of self-congruence is also changed. In service industry especially in cloud computing service industry the possession of the physical product is not handled by the customer but handled by the vendor. This type of model changes the way customer perceives the product. The absence of the physical presence because of the adoption of cloud computing service in a certain industry has a difficulty to ensure the service quality due to the infancy of the technology (Coi & Jeong, 2014). Hence, the way vendor gain trust from its customer becomes a crucial factor.

2.2. Trust Building Mechanism

Trust is one of the crucial factors that influence customer's decision especially when the product has lack of physical presence. According to Lee and

Tuban, trust can be divided into three categories. Seen from personality theory, trust is defined as the faith that one has a certain thing, expect, or feeling and individual has already planted it among them deeply during the period developing in early personality. From sociology and economics view, trust is a situation that exists among team members. From social psychology view, trust is an expectancy to the trading partner to trust, and demonstrates that would like to believe the will of the trading partner, the trust degree that some factors will increase, maintain of affect both parties (Lee & Turban, 2001). In a service industry, the trust building model is different compared to retail industry which has physical product. According to Benedicktus et al. (2010), brick and mortal stores who have a physical presence tend to have more trust than non-physical stores (Benedicktus, Brandy, Darke, & Voorhees, 2010). Referring to Benecticktus et al. dissertation, cloud computing service industry might have similar situation as the non-physical stores. Another analogy to help explaining the difference of trust building methodology in service industry based on the researcher's own opinion is related to medical industry. The relationship between a doctor and a patient is not based only on the quality of the doctor. The interaction's experience is also one of the important determinations whether the doctor is trustworthy or not. The quality is important, however no matter how good the doctor is, if the privacy of the patient such as the illness or other privacy information cannot be confidentially kept, the trustworthiness of the doctor will be questioned. And this situation applies similarly to the cloud computing service industry. No matter how good the service and offer, if the privacy and security of the information cannot be securely

protected, the provider might face a severe problem gaining trust from the customer. Privacy and security problems are very critical issues which online customers care about (Huang & Liu, 2010). If the cloud providers relieve customer's fear of privacy and security, the company will win customer's trust (Huang & Liu, 2010). However as mentioned previously that there is an absolute weakness in cloud computing service industry regarding the safety of the data, the way cloud computing companies chose their trust building methodology should be more selective.

2.3. Online Brand Trust

According to Schurr and Ozanne, trust creates more favorable attitudes towards suppliers as well as customer loyalties. It also helps partners project their exchange relationships into the future (Doney & Cannon, 1997). With the growth of the technology and the advances in information technology, online trust becomes an important factor in both business-to-business and business-to-consumers transactions (Shah Alam & Mohd Yasin, 2010). Thus, online brand trust has been identified as a critical component in stimulating purchases over the internet (Shah Alam & Mohd Yasin, 2010). According to Shah Alam and Mohd Yasin (2010), there are six significant factors influencing online brand trust and those factors include perceived risk, security/privacy, word-of-mouth, online experience, quality of information and brand reputation (Shah Alam & Mohd Yasin, 2010).

However in cloud computing service industry, the online brand trust stimuli are slightly different. This study emphasizes two factors from the stimuli and tries to confirm that depending on the perceived risk, brand reputation may become a good or a bad stimulus for online brand trust due to the absolute weakness of the cloud computing service industry regarding the security and privacy.

2.4. Customer Loyalty

Many observations have been done to analyze the loyalty of a customer from the behavioral perspective, excluding attitudinal type data and concentrating on a deterministic perspective using stochastic models (Tellis, 1988; Ehrenberg & Goodhardt, 2000). Researcher acknowledged that there are numerous number of methods to analyze customer loyalty. Several recent studies also measured the relationship between customer satisfaction, quality and loyalty (Mittal & Lassar, 1998). Amongst those methodologies, one of the most suitable measurements for measuring the customer loyalty in this study is by measuring the likelihood of continuation using the same application after receiving several distrust factors in sequence. This study will measure the difference between customer loyalty from branded product and non-branded product.

2.5. Distrust Factors

Distrust factors can be defined by several meaning according to each case. According to Peter et al. (2010), there are four different factors which may lead to consumer distrust. It includes broken promises, misleading claims, product failure

and expectancy disconfirmation (Darke, Ashworth, & Main, 2009). In this study, the researcher picks two of those distrust factors, product failure and expectancy disconfirmation and use those distrust factors as dependent variable during the observation. Product failure will be analogized as a security failure from an application which leads to an expectancy disconfirmation. This product failure factor will be varied based on the locations and source which includes a product failure from similar product on different company towards own company and industry in total, a product failure from different product on the same company towards own company and industry in total and lastly, a product failure from own product towards own company and industry in total.

2.6. The Carryover Effect

A number of studies from Ahluwalia et al. confirm that a product failure within one industry will be carried over to more negative evaluations of highly similar attributes for the same product (Ahluwalia, Burnkrant, & Unnava, 2000). A study from Peter et al. confirms that the carryover effect happens only to the related industry for example a failure in Burger King may affect the consumer's attitude towards McDonald's (Darke, Ashworth, & Main, 2009). This study follows the same methodology to measure the carryover effect towards another similar product within the same industry.

2.7. Cloud Computing Service

As defined by The US National Institute of Standards and Technology (Mell, 2011) Cloud Computing is composed of five important characteristics, three types of delivery models and four types of deployment models (Mell, 2011).

The five important characteristic in cloud computing technology consist of on-demand self service, ubiquitous network access, location-independent, resource pooling, rapid elasticity and measured service (Coi & Jeong, 2014). By using rapid elasticity, the company can optimize the resource by easily scaling up and down the required resource. Three types of delivery models of cloud computing technology are software as a service (SaaS), platform as a service (PaaS) ad infrastructure as a service (IaaS) (Coi & Jeong, 2014).

In IaaS, the provider offers a set of infrastructure components for enabling the cloud computing technology. This type of business usually uses business-to-business model since the main target customer is not mass market. Several critical areas in this business are the trust towards virtual machines, hosts and inter-host communication safety.

In PaaS, the provider provides a platform which will become a medium between IaaS and SaaS. This business area does not target mass market as well, hence the business model mostly adapts business-to-business model.

Finally, In SaaS, the provider provides a cloud application as on-demand services. The main critical issue in this area is ensuring that the information handled is securely protected (Coi & Jeong, 2014).

This study will only include software as a service (SaaS) as the research object, therefore addressing the critical issue of SaaS becomes the fundamental base for this study. In order to ensure that the information is well protected, the cloud provider should gain customer's trust which is not easy due to the absence of physical presence. Therefore, a trust building mechanism inside a product which lacks physical presence should be taken into consideration.

Apart from academia literature review, Researcher wants to put some facts regarding the monetization in cloud computing service industry. According to Dropbox's CEO Drew Houston, in 2011, there were 50 million users, about 4% of whom were paying, with subscriptions starting at $100 annually (Rogowsky, 2013). And after the introduction of a new business model so called "Dropbox for Business", it is written that out of 175 million customers, 2 million are paying customers or barely over 1% of the total customer base on recent years (Rogowsky, 2013). Based on this fact, within two years, the number of customer was tripled however the percentage of paying customers was reduced by more than 2 percent. The problem in this business model is the infrastructure resource. Even though the non-paid customers have a limited space on a free package, it consumes several resources from the company, on the other word, increasing the cost of goods sold within a company without increasing the revenue.

In this particular case, there might be a better alternative way of conducting the business by not increasing the awareness of the brand so that it minimizes the attraction towards non-paid customers and focusing more on paid customers by approaching different marketing strategy. The optimal solutions for this kind of

business is to reduce the non-paid customers as minimum as possible and increase the paid customers as much as possible. Therefore, brand as one of the marketing strategies might not be a good choice to gain paid customers. Moreover even though brand is perceived as a trust agent, however in this particular case, brand might give more negative feedbacks to the company rather than positive ones. Brand can indeed attract people, however brand cannot differentiate between good and bad people. By increasing the number of users, it will give more incentive to hackers to do their cybercrime actions, thus increasing the vulnerability of the company.

CHAPTER 3 CONCEPTUALIZATION

3.1. Conceptual Relationships

The conceptualization in this study has several relationships between three different sources of distrust factor and two target areas that will be observed. These relationships form six combinations concepts that will be measured in this study as shown in table below.

		Impact towards	
		Own Company	**Industry**
Sources of distrust factor	**Own product**	Customer Loyalty	Industry Carryover Effect
	Different product within the same company	Customer Loyalty	Industry Carryover Effect
	Similar product from different company	Loyalty Carryover Effect	Industry Carryover Effect

Table 1 *Relationship between sources of distrust factor and target areas that will be observed*

3.1.1. Customer loyalty and distrust factor

Relationships that affect direct customer loyalty are represented by two conditions. When the distrust factors come from own product or from different product within the same company, the impact towards the company will affect the customer loyalty for the company as explained in the below figure.

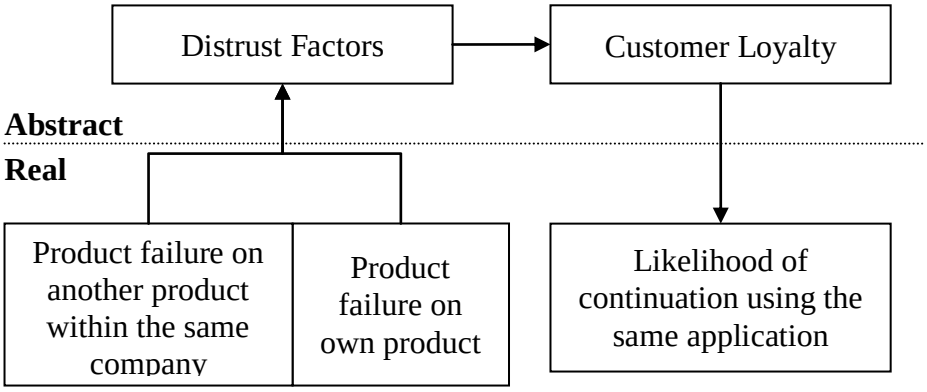

Figure 1 *Conceptual relationship between distrust factor and customer loyalty*

From the conceptual relationship above, the relationship between distrust factors and customer loyalty is represented by a real context or action. The distrust factor that is being used in this study is represented by a product failure which is analogized as a product that is successfully hacked. This conceptualization assumes that this distrust factor both from own product failure and another product within the same company may affect the customer loyalty towards own product. The real context of customer loyalty can be measured by observing the transformation of the likelihood of continuing the same application rather than switching to another substitutable product which will be explained in detail on the next chapter.

3.1.2. Loyalty carryover effect and distrust factor

Relationship that affects customer loyalty carryover is represented from one condition. When the distrust factors come from similar product in different company, the impact towards customer loyalty on own company will be affected as explained in the below figure.

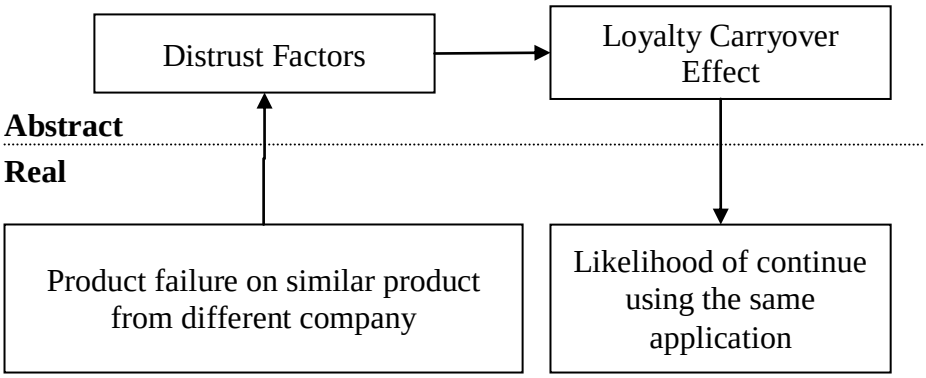

Figure 2 *Conceptual relationship between distrust factor and loyalty carryover effect*

From the conceptual relationship above, the relationship between distrust factors and customer loyalty is represented by a real context or action. The distrust factor that is being used in this study is represented by a product failure which is analogized as a product that is successfully hacked. This conceptualization assumes that the distrust factor from similar product on different company may affect the customer loyalty towards own product. The real context of customer loyalty can be measured by observing the transformation of the likelihood of continuing the same application rather than switching to another substitutable product which will be explained in detail on the next chapter.

3.1.3. Industry carryover effect and distrust factor

Relationships that affect industry carryover are represented from three different conditions. When the distrust factors come from own product, different product within the same company or similar product in different company, the impact towards customer's trust for industry in total will be affected as explained in the below figure.

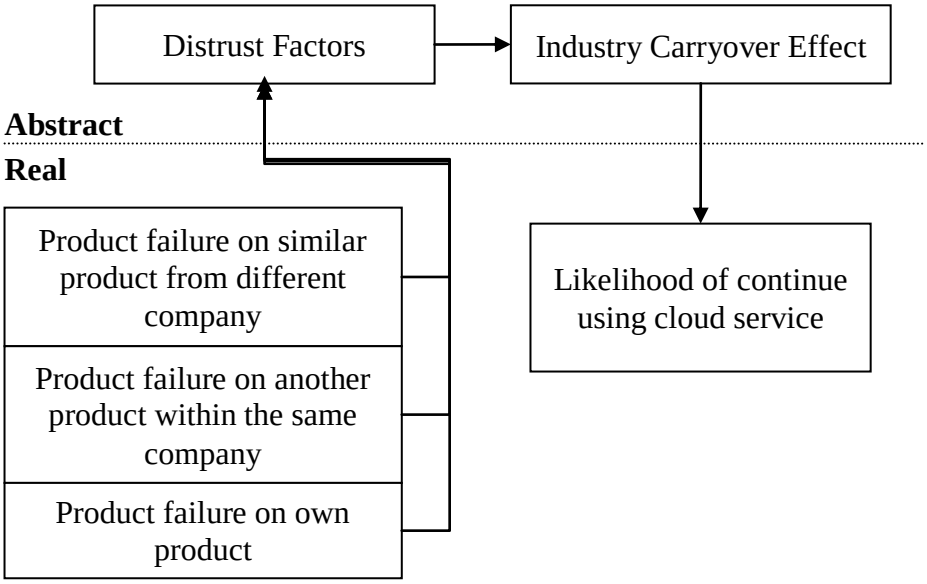

Figure 3 *Conceptual relationship between distrust factor and industry carryover effect*

From the conceptual relationship above, the relationship between distrust factors and customer's trust for industry in total is represented by a real context or action. The distrust factor that is being used in this study is represented by a product failure which is analogized as a product that is successfully hacked. This conceptualization assumes that distrust factors either come from own product, different product on the same company or similar product on different company may affect the customer's trust for industry in total. The real context of customer's trust can be measured by observing the transformation of the confidence level which represented by the likelihood of continuing the cloud service which will be explained in detail on the next chapter.

3.2. Hypotheses

Proposed model in this study will be used to explain all hypotheses that want to be observed. There are two models that will be used for maximizing the observation reliability. This study will apply two independent variables towards six dependent variables. The independent variables are the level of brand and the level of risk which also act as the amplifier, while the dependent variables will be the distrust factors. The first model shows the effect on customer loyalty when distrust factor from three different sources is given as explained in this figure below.

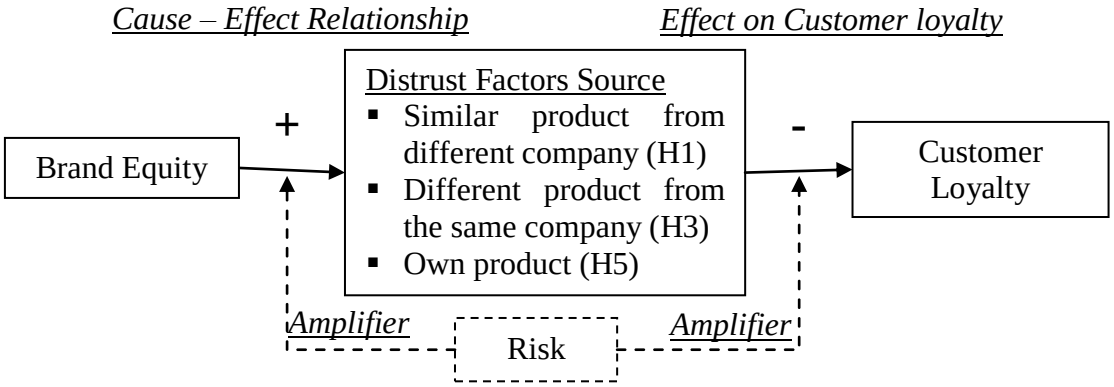

Figure 4 *Model for observing the transformation of customer loyalty*

The second model shows the carryover effect on trust for industry in total when distrust factor from three different sources is given as explained in this following figure.

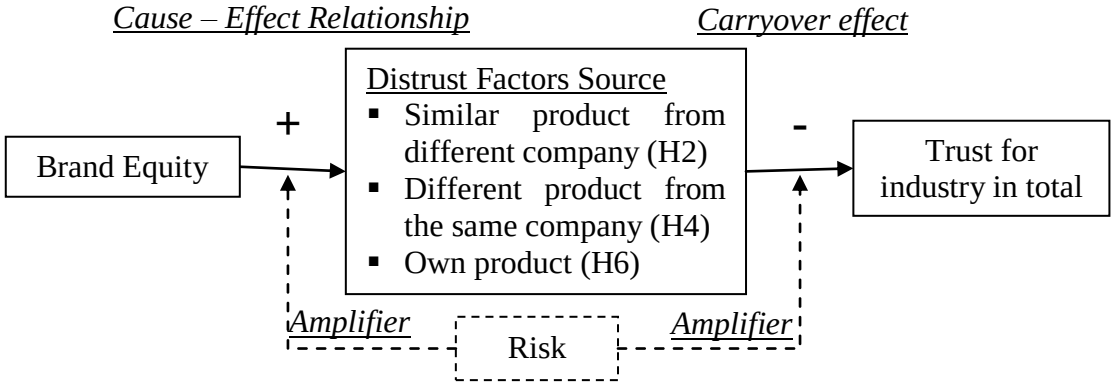

Figure 5 *Model for observing carryover effect*

From the above models, there are three hypotheses will be measured on the first model and three other hypothesis that will be measured on the second model. The researcher assumes that the first distrust factor is a product failure from similar product on different company may have smaller impact towards the customer loyalty and the carryover effect, hence, these first and second hypothesis are based on the first distrust factor and explained as below:

H1. Product failure from a popular brand has bigger negative impact towards customer loyalty in another similar product.

H2. Product failure from a popular brand has bigger negative impact towards trust for the industry in total.

The second distrust factor that will be used is the effect after a product failure happens to another product within the same company. The researcher assumes that this distrust factor may have bigger effect towards the first and second hypothesis. The third and fourth hypothesis will be based on this second distrust factor and explained as below:

H3. Product failure from different product within a company has bigger negative impact towards customer loyalty of another product from the same company if the company has bigger brand popularity.

H4. Product failure from different product within a company has bigger negative impact towards trust for the industry in total if the company has bigger brand popularity.

The third distrust factor is a product failure on own product. The researcher assumes that this distrust factor has the most severe impact towards customer

loyalty and might give bigger carryover effect compare to previous hypotheses. Thus, this hypothesis should be measured last. These fifth and sixth hypotheses are explained as below:

H5. Tolerance level for a product failure from a popular brand is lower if the company has bigger brand popularity

H6. Trust level for industry in total towards product failure will reduce more if the popularity is higher

Referring on those six hypotheses above, the measurement of the brand and risk will be as follows:

		Company that is given distrust factors	
		Popular Brand	**Unpopular Brand**
Target Company	**Popular Brand**	(B1) Effect from popular brand towards popular brand	(B2) Effect from unpopular brand towards popular brand
	Unpopular Brand	(B3) Effect from popular brand towards unpopular brand	(B4) Effect from unpopular brand towards unpopular brand

Table 2 *Model for measuring the effect from the level of brand*

		Company that is given distrust factors	
		High Risk	**Low Risk**
Target Company	**High Risk**	(R1) Effect from high risk towards high risk	(R2) Effect from low risk towards high risk
	Low Risk	(R3) Effect from high risk towards low risk	(R4) Effect from low risk towards low risk

Table 3 *Model for measuring the effect from the level of risk*

This study considers only number (B2) and (B3) which is the effect from unpopular brand towards popular brand and from popular brand towards unpopular brand as the combination for measuring the loyalty carryover effect while (B1) and (B3) are used to measure the carryover effect within the same company. For the level of risk, only number (R1) and (R4) are used for all measurement.

CHAPTER 4 METHOD

4.1. Research Design

In order to evaluate the impact of the distrust factors on customer's loyalty, an experimental method is applied. Fictive cloud application software will be used as an example of hypothetical product in this study. Scenarios of a hypothetical product are manipulated by varying the level of brand and risk. A 2 (level of risk) X 2 (level of brand) model is designed, composed of two levels for the level of the risk and two level for the level of the brand. The level of risk is categorized into high risk and low risk which will be represented by the level of importance of the data stored inside the application. Meanwhile the level of brand is categorized into popular brand and unpopular brand which will be represented by a well known company brand and an unknown company brand respectively. In order to get an optimal result, all four combinations were used as stimuli. These stimuli will cover the high risk with popular brand scenario, high risk with unpopular brand scenario, low risk with popular brand scenario and low risk with unpopular brand scenario as shown in Table I. More detailed information about the table is provided in the appendix.

	High Risk	**Low Risk**
Popular Brand	Scenario 1	Scenario 3
Unpopular Brand	Scenario 2	Scenario 4

Table 4 Scenarios used in study

In order to make the scenario unambiguous to the respondent, a detail explanation about the scenario and the basic functionality of the application are explained in the beginning of each questionnaire. This explanation is used to minimize the ambiguity of the scenario. The first scenario asked respondents to imagine if they are using an application for saving their credential data in the cloud service or internet, the company who creates this application is Sony Corporation and the product name is called Sony Password Manager. The second scenario asked respondents to imagine if they are using an application for saving their credential data in the cloud service or internet, but the company who creates this application is an unpopular company called DataSecure Incorporation. The third scenario asked respondents to imagine if they are using an application for saving their favorite movie list and this application can remind them about the release date of the movie. In this third scenario, the company who creates the application is Sony Corporation and the product name is called Sony My Movie List. The last scenario asked respondents to imagine if they are using an application for saving their favorite movie list as well as the reminder for the release date of the movie, however the company who creates this application is an unpopular company called Movie Media Incorporation. The first three questions in the questionnaire are used as a manipulation check. This manipulation check makes sure that only the respondents who acknowledge the level of brand and risk which are correspond to the scenario will be counted and used.

4.2. Measurement

4.2.1. Manipulation Checks

The first two questions inside the questionnaire are used to check whether the respondent understand the level of risk for the given scenario or not. Those two questions are measured by five point likert scale. The first question asks about the uneasiness feeling of using the application (1 = “very uneasy” to 5 = “very safe”), while the second question asked respondents about the riskiness level of putting data into cloud service. Referring back to the previous four scenarios, the first and second scenario should be considered as high risk scenario and the other two should be considered as low risk scenario. (1 = “Very Risky” to 5 = “Not Risky”).

The second question in questionnaire is used to check whether the respondent acknowledge the popularity of the brand. In this context, the brand is represented by the company who creates the application. The interpretation will be measured by a three point likert scale which consists of 1 = “Do not know the company at all”, 2 = “Heard the company, but do not know” and 3 = “Know the company”. According to four scenarios in this study, the scenario 1 and scenario 3 should be considered as popular brand and the other two should be considered as unpopular brand. Any response which is not corresponding to the expected group will be excluded for the analysis. This manipulation check will be considered as the first measurement (M1).

4.2.2. The effect of another company's product failure on a company's customer loyalty

This measurement is represented by question number four in the questionnaire and it plays an important role for the analysis and the findings. In this question the interviewer measures the likelihood of switching to a substitute product because of the given distrust factor that happens in similar product from another company within the same industry. The question that is used for the questionnaire asked respondents to imagine if they have been using a certain application for a while and suddenly news rises. The news says that another company within the same industry which has different brand level has been hacked for the first time and their similar application data is leaked and spread through the internet. However the application that is being used is safe. This measurement will be considered as the second measurement (M2) and it will be used to answer the first hypothesis which says that a product failure from a popular brand may have bigger negative impact towards customer loyalty in another similar product (H1). Five point likert scale is used to measure the likelihood responses. 1 = "will switch to another application for sure", 2 = "will likely switch to another application", 3 = "might continue or might switch", 4 = "will likely continue using the same application" and 5 = "will continue using the same application for sure". The variation of the scenarios for this question will be divided into two variations. Scenario 1 and scenario 3 will measure the product failure effect from another unpopular brand towards a popular brand's product. Whereas the other two

scenarios will measure the product failure effect from another popular brand towards an unpopular brand's product.

4.2.3. Industry carry over effect of another company's product failure

This measurement is related to the carryover effect towards trust of cloud service industry in total. The measurement is represented as the additional question to the fourth question providing the second likert scale as the measurement tool. In this question the interviewer measures the likelihood of discontinuation using a cloud service because of the given distrust factor that happens in similar product from another company who has different brand level within the same industry. The question sentence that is used for the questionnaire asked the respondent about the safety of cloud service industry after being given a distrust case. This measurement will be considered as the third measurement (M3) and it will be used to answer the second hypothesis which says that a product failure from a popular brand may have bigger negative impact towards trust for the industry in total (H2). Five point likert scale is used to measure the likelihood responses. 1 = "will stop using cloud service for sure", 2 = "will likely stop using cloud service", 3 = "might continue or might stop", 4 = "will likely continue using cloud service" and 5 = "will continue using cloud service for sure". The variation of the scenarios for this question will be divided into two variations. Scenario 1 and scenario 3 will measure the product failure effect from another unpopular brand towards a popular brand's product. Whereas the other two scenarios

will measure the product failure effect from another popular brand towards an unpopular brand's product.

4.2.4. The effect of a different product failure on customer loyalty

This measurement is represented by question number five and it is used for the main analysis. In this question the interviewer measures the likelihood of switching to a substitute product because of the given distrust factor that happens inside the company but from different product. The question that is used for the questionnaire asked the respondents to imagine if they have been using a certain application for a while. Suddenly an apology message from the company appears informing that theirs payment system was hacked. However the application and its data are safe. This measurement will be considered as the fourth measurement (M4) and it will be used to answer the third hypothesis which says that a product failure from different product within a company has bigger negative impact towards customer loyalty of another product from the same company if the company has bigger brand popularity (H3). Five point likert scale is used to measure the likelihood responses. 1 = "will switch to another application for sure", 2 = "will likely switch to another application", 3 = "might continue or might switch", 4 = "will likely continue using the same application" and 5 = "will continue using the same application for sure". The variation of the scenarios for this question will be divided into four variations. Scenario 1 until scenario 4 will measure the product failure effect from different product within the same company, however the first

scenario will be based on the high risk product in a popular brand, the second scenario will be based on the high risk product in an unpopular brand, the third scenario will be based on the low risk product in a popular brand and the last scenario will be based on the low risk product inside an unpopular brand.

4.2.5. Industry carry over effect of a different product failure

This measurement is used to analyze the carryover effect towards trust of cloud service industry in total. The measurement is represented as the additional question to the fifth question providing the second likert scale as the measurement tool. In this question the interviewer measures the likelihood of stop using a cloud service because of the given distrust factor that happens inside the company but from different product. The question sentence that is used for the questionnaire asked the respondent about the safety of cloud service industry after being given the distrust case. This measurement will be considered as the fifth measurement (M5) and it will be used to answer the fourth hypothesis which says that a product failure from different product within a company may have bigger negative impact towards trust for the industry in total if the company has bigger brand popularity (H4). Five point likert scale is used to measure the likelihood responses. 1 = “will stop using cloud service for sure”, 2 = “will likely stop using cloud service”, 3 = “might continue or might stop”, 4 = “will likely continue using cloud service” and 5 = “will continue using cloud service for sure”. The variation of the scenarios for this question will be divided into four variations. Scenario 1 until scenario

4 will measure the product failure effect from different product within the same company, however the first scenario will be based on the high risk product in a popular brand, the second scenario will be based on the high risk product in an unpopular brand, the third scenario will be based on the low risk product in a popular brand and the last scenario will be based on the low risk product inside an unpopular brand.

4.2.6. Tolerance level of the customer towards product failure

This measurement is represented by question number six and it is used for the main analysis. In this question the interviewer measures the likelihood of switching to a substitute product because of the given distrust factor that happens to the product that is being used. The severity level of the distrust factor in this question is really high, because the user losses their data due to a security failure. Cybercriminal or hacker has successfully penetrated the database and spread the data through the internet. Several customers who put their credit card data inside the application face a huge loss due to a credit card fraud. The company apologizes, refunds the money and takes full responsibility but they cannot recover the data. The question that is used for the questionnaire asked the respondents to imagine if they have been using a certain application for a while. Suddenly all data is gone because it has been hacked. This measurement will be considered as the sixth measurement (M6) and it will be used to answer the fifth hypothesis which says that tolerance level for a product failure from a popular brand is lower if the company has

bigger brand popularity (H5). Five point likert scale is used to measure the likelihood responses. 1 = “will switch to another application for sure”, 2 = “will likely switch to another application”, 3 = “might continue or might switch”, 4 = “will likely continue using the same application” and 5 = “will continue using the same application for sure”. The variation of the scenarios for this question will be divided into four variations. Scenario 1 until scenario 4 will measure the product failure effect from the product that are being used, however the first scenario will be based on the high risk product in a popular brand, the second scenario will be based on the high risk product in an unpopular brand, the third scenario will be based on the low risk product in a popular brand and the last scenario will be based on the low risk product inside an unpopular brand.

4.2.7. The effect of product failure on industry trust level

This measurement is used to analyze the carryover effect towards trust of cloud service industry in total. The measurement is represented as the additional question to the sixth question providing the second likert scale as the measurement tool. In this question the interviewer measures the likelihood of stop using a cloud service because of the given distrust factor that happens to the product that is being used. The severity level of the distrust factor in this question is really high, because the user losses their data due to a security failure. Cybercriminal or hacker has successfully penetrated the database and spread the data through the internet. Several customers who put their credit

card data inside the application face a huge loss due to a credit card fraud. The company apologizes, refunds the money and takes full responsibility but they cannot recover the data. The question sentence that is used for the questionnaire asked the respondent about the safety of cloud service industry after being given the distrust case. This measurement will be considered as the seventh measurement (M7) and it will be used to answer the sixth hypothesis which says that trust level for industry in total towards product failure will reduce more if the popularity is higher (H6). Five point likert scale is used to measure the likelihood responses. 1 = “will stop using cloud service for sure”, 2 = “will likely stop using cloud service”, 3 = “might continue or might stop”, 4 = “will likely continue using cloud service” and 5 = “will continue using cloud service for sure”. The variation of the scenarios for this question will be divided into four variations. Scenario 1 until scenario 4 will measure the product failure effect from different product within the same company, however the first scenario will be based on the high risk product in a popular brand, the second scenario will be based on the high risk product in an unpopular brand, the third scenario will be based on the low risk product in a popular brand and the last scenario will be based on the low risk product inside an unpopular brand.

4.3. Sampling

The sampling is related to the objective of the study: to measure the effect of the product failure due to a given distrust factor by varying the level of risk and brand into four different combination scenarios. The appropriate group for the test is people around 18 until 35 years old both male and female who have already experienced the internet and are using the smart phone or computer. The sample group varies from the nationality, occupation, age and gender. The survey was conducted online through a combination between the interviewer's website and 3rd party form builder service that has already been modified. The link for the survey was masked by a short uniform resource locator as known as url. The respondent who triggers the link will be randomly redirected into one of the scenarios. A simple program has been applied to remember the scenario and IP address of the respondent in order to prevent multiple inputs from the same respondent. This simple program also has the ability to balance the number of respondents from each scenario.

Translations of the scenarios and questions into two languages English and Indonesian were done by the language expert and under the supervision of interviewer's supervisor. A pre-test of the questionnaire were used to check the relevancy of the questions and the accuracy of the scenarios and it was done in advance by asking 5 random people. Data collection was done through the internet for around three weeks. Total data collected for each scenario was around 35 data. It makes the overall number of the observation around 140 data. There were 7 data did not pass the manipulation check, in order to balance the number of

respondent, the interviewer limits the number of respondents of each scenario to 30 data.

CHAPTER 5 RESULTS

5.1. Product Failure and Customer Loyalty

In order to reject the null hypothesis, several analyses should be taken. The first three questions are considered as the first measurement which is used as a manipulation check, this manipulation check is used to filter the data, therefore the significant level of risk for the first two questions is below 5% and the significant level of brand in the third question is below 5%. By doing the manipulation check filter, it was proven that the data used for the analysis are relevant. The analysis itself starts from the fourth question which is explained as the second measurement (M2). This second measurement measures the transformation of customer loyalty towards the product being used when another product which has similar functionality from another company is hacked. The result turns out as expected, the likelihood level of continuing with the same product after being given a distrust factor for scenario 1 (high risk popular brand) is lower than scenario 2 (high risk unpopular brand) with the average mean 3.17 and 3.50 respectively. Whereas scenario 3 (low risk popular brand) is lower than scenario 4 (low risk unpopular brand) represented by the average mean of 3.83 and 3.93 respectively.

Second Measurement (M2)	Simple main effect test comparison of means			
	High Risk		Low Risk	
	Popular Brand (Scenario 1)	Unpopular Brand (Scenario 2)	Popular Brand (Scenario 3)	Unpopular Brand (Scenario 4)
Customer Loyalty *Likelihood of continue using same application*	3.13	3.50	3.83	3.93
Std. Deviation	1.224	.900	.699	.828

Table 5 *Descriptive Statistics for customer loyalty after another company is given a distrust factor*

From the above table, we can see the likelihood of continuing the same application if another similar product from another company is given a distrust factor. The result from the four scenarios can be classified into two categories. The first one is high risk application and the other is low risk application. From both high risk and low risk applications, the possibility to stay and continue with the same application is higher when the brand is not popular. However the effect is bigger when the product has higher risk. Although the result answers the first hypothesis which mentions that a product failure from a popular brand may have bigger negative impact towards customer loyalty in another similar product (H1), the difference between unpopular brand and popular brand in a low risk application is very small and insignificant as shown in Figure 6 below.

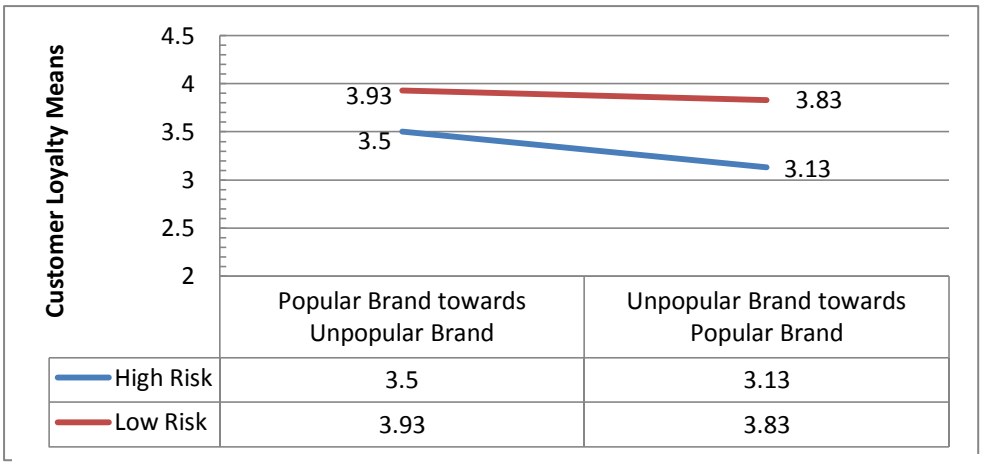

Figure 6 *Customer Loyalty difference between popular and unpopular brand for high risk and low risk application after another company is given a distrust factor*

Based on the results above, the means of customer loyalty for popular brand is lower than unpopular brand both from high risk and low risk application. Even though the difference is small and insignificant especially from the low risk application, there is a small hint and tendency that the bigger the brand, the more negative impact will occur when facing a distrust factor and it is affected by the level of risk. The significance level is measured by using a univariate general linear model as shown in the table below and the significance level of risk meaning the level of risk gives significant influence towards customer loyalty when another similar product from a different company is given a distrust factor.

Tests of Between-Subjects Effects

Dependent Variable: Another company within same industry is hacked

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	11.800[a]	3	3.933	4.517	.005	.105
Intercept	1555.200	1	1555.200	1786.170	.000	.939
Risk	9.633	1	9.633	11.064	.001	.087
Brand	1.633	1	1.633	1.876	.173	.016
Risk * Brand	.533	1	.533	.613	.435	.005
Error	101.000	116	.871			
Total	1668.000	120				
Corrected Total	112.800	119				

a. R Squared = .105 (Adjusted R Squared = .081)

Table 6 *Analysis of variance between subjects effect using univariate general linear model*

After getting the result from the second measurement for measuring the first hypothesis (H1), the next question is explained as the fourth measurement (M4) which will answer the third hypothesis (H3). This fourth measurement measures the transformation of customer loyalty after being given a distrust factor which comes from another product within the same company. The distrust factor that was used in the questionnaire is when another product from the same company who creates the product being used is hacked. Unfortunately, the result was not as expected. The likelihood level of continuing with the same product after being given a distrust factor for scenario 1 (high risk popular brand) is lower than scenario 2 (high risk unpopular brand) with the average mean 2.60 and 2.73 respectively. Whereas scenario 3 (low risk popular brand) is higher than scenario 4 (low risk unpopular brand) represented by the average mean of 3.17 and 2.20 respectively.

Fourth Measurement (M4)	Simple main effect test comparison of means			
	High Risk		Low Risk	
	Popular Brand (Scenario 1)	Unpopular Brand (Scenario 2)	Popular Brand (Scenario 3)	Unpopular Brand (Scenario 4)
Customer Loyalty *Likelihood of continue using same application*	2.60	2.73	3.17	2.20
Std. Deviation	1.221	.944	1.020	1.375

Table 7 *Descriptive Statistics for customer loyalty after another product within the same company is given a distrust factor*

From the above table, we can see the likelihood of continuing to use the same application if another product within the same company is given a distrust factor. The result from four scenarios can also be classified into two categories. The first one is high risk application and the other is low risk application. From high risk application, the possibility to keep continuing the same application is higher when the brand is not popular, however for the low risk application the possibility to keep continuing the same application is higher when the brand is popular. Interestingly, this observation result answers the third hypothesis which says that a product failure from a different product within a company might have a bigger negative effect towards customer loyalty of another product from the same company only if the level of risk is high (H3) as shown in Figure 7 below.

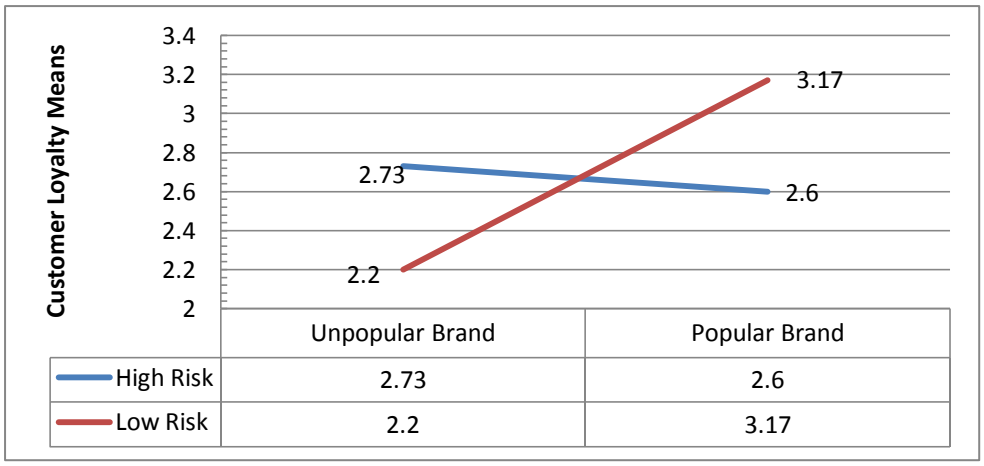

Figure 7 *Customer Loyalty difference between popular and unpopular brand for high risk and low risk application after another product within the same company is given a distrust factor*

Based on the observation result above, the means of customer loyalty for popular brand is lower than unpopular brand only from high risk application. Even though the significance level of the brand is quite high in this observation, the result cannot answer the third hypothesis completely because it only works when the risk is high. In other words, a company who does not have a popular brand might face a bigger negative impact to all of their products if one of them fail especially if the product that fails is a common product which do not handle any credential or important data, meaning the risk of the product is low. On the other hand, a company who has a popular brand has more advantage because people tend to continue using their product even though the company makes several failures with their product which has low risk. However for the high risk application the third hypothesis might be correct (H3) even though it is insignificant. From this observation we can also see that the mean of customer's loyalty in an unpopular brand is higher when the product has a bigger risk

represented by 2.73 for high risk and 2.2 for low risk. It means there is a signal that a high risk application has more trust if the brand is unpopular. The significance level is also measured by using a univariate general linear model as shown in the table below and the significance level of brand, which is the level of brand gives a significant influence towards customer loyalty when another product from the same company is given a distrust factor.

Tests of Between-Subjects Effects

Dependent Variable: Same company different product is hacked

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	14.292[a]	3	4.764	3.588	.016	.085
Intercept	858.675	1	858.675	646.654	.000	.848
Risk	.008	1	.008	.006	.937	.000
Brand	5.208	1	5.208	3.922	.050	.033
Risk * Brand	9.075	1	9.075	6.834	.010	.056
Error	154.033	116	1.328			
Total	1027.000	120				
Corrected Total	168.325	119				

a. R Squared = .085 (Adjusted R Squared = .061)

Table 8 *Analysis of variance between subjects effect using univariate general linear model*

The last measurement for measuring the transforming effect towards own product is explained as the sixth measurement (M6) which will answer the fifth hypothesis (H5). This sixth measurement measures the change in customer loyalty after facing a product failure. The combination will also be based on the high risk and low risk application from both popular brand and unpopular brand. From the observation, the result was partially good. The likelihood level of continuing with the same product after being given a distrust factor for scenario 1 (high risk

popular brand) is lower than scenario 2 (high risk unpopular brand) with the average mean 1.77 and 1.90 respectively. Whereas scenario 3 (low risk popular brand) is higher than scenario 4 (low risk unpopular brand) represented by the average mean of 2.50 and 1.77 respectively.

Sixth Measurement (M6)	**Simple main effect test comparison of means**			
	High Risk		**Low Risk**	
	Popular Brand (Scenario 1)	**Unpopular Brand (Scenario 2)**	**Popular Brand (Scenario 3)**	**Unpopular Brand (Scenario 4)**
Customer Loyalty *Likelihood of continue using same application*	1.77	1.90	2.50	1.77
Std. Deviation	1.104	.960	.861	1.135

Table 9 *Descriptive Statistics for customer loyalty after the product failure*

From the above table, we can see that the likelihood of continuing with the same application if the product is given a distrust factor. The results from the four scenarios can also be classified into two categories. The first one is high risk application and the other is low risk application. From high risk application, the possibility to keep continuing the same application is higher when the brand is not popular, however for the low risk application the possibility to keep continuing the same application is higher when the brand is popular. Interestingly, this observation result answers the fifth hypothesis which says that the tolerance level for a product failure from a popular brand is lower if the company has bigger brand popularity (H5) only when the product has high risk as shown in Figure 8 below.

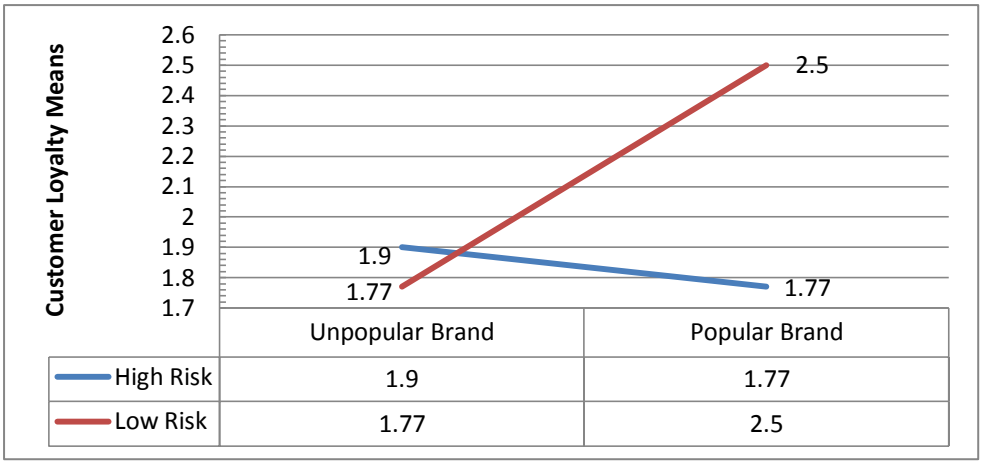

Figure 8 *Customer Loyalty difference between popular and unpopular brand for high risk and low risk application after the product failure*

Based on the observation result above, the means of customer loyalty for popular brand is lower than unpopular brand only from high risk application. Even though the significance level of the brand is quite high in this observation, the result cannot answer the fifth hypothesis completely because it only works when the risk is high. In another words, a company who does not have a popular brand might face a bigger negative impact to all of their products if one of them fail especially if the product that fails is a common product which do not handle any credential or important data, meaning the risk of the product is low. On the other hand, a company who has a popular brand has more advantage because people tend to continue using their product even though the company makes several failures with their product which has low risk. However for the high risk application, the fifth hypothesis might be true (H5) even though it is insignificant. From this observation we can also see that the mean of customer's loyalty in an unpopular brand is higher when the product has a bigger risk represented by 1.9

for high risk and 1.7 for low risk. It means that there is a signal that a high risk application has more trust if the brand is unpopular. The significance level is also measured by using a univariate general linear model as shown in the table below and the significance level of brand, which is the level of brand gives a significant influence towards customer loyalty when another product from the same company is given a distrust factor.

Tests of Between-Subjects Effects

Dependent Variable: The product is hacked

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	11.033[a]	3	3.678	3.528	.017	.084
Intercept	472.033	1	472.033	452.777	.000	.796
Risk	2.700	1	2.700	2.590	.110	.022
Brand	2.700	1	2.700	2.590	.110	.022
Risk * Brand	5.633	1	5.633	5.404	.022	.045
Error	120.933	116	1.043			
Total	604.000	120				
Corrected Total	131.967	119				

a. R Squared = .084 (Adjusted R Squared = .060)

Table 10 *Analysis of variance between subjects effect using univariate general linear model*

5.2. Product Failure and Carryover Effect

To measure the carryover effect towards industry in total, three measurements was done. The analysis itself starts from the fourth question second scale which is explained as the third measurement (M3). This third measurement measures the carryover effect towards trust within the industry in total after another product which has similar functionality from another company is hacked (H2). The result turns out not as expected, the safety perception of using cloud service is pretty much the same between all combinations as seen in scenario 1 (high risk popular brand) which is slightly lower than scenario 2 (high risk unpopular brand) with the average mean 3.07 and 3.13 respectively. Whereas scenario 3 (low risk popular brand) is slightly higher than scenario 4 (low risk unpopular brand) represented by the average mean of 3.50 and 3.47 respectively.

Third Measurement (M3)	**Simple main effect test comparison of means**			
	High Risk		**Low Risk**	
	Popular Brand (Scenario 1)	**Unpopular Brand (Scenario 2)**	**Popular Brand (Scenario 3)**	**Unpopular Brand (Scenario 4)**
Carryover Effect *Safety perception towards Cloud Service Industry*	3.07	3.13	3.50	3.47
Std. Deviation	1.112	1.008	.861	.819

Table 11 *Descriptive Statistics of trust for industry in total after another company is given a distrust factor*

From the above table, we can see the safety perception of using cloud service has no significant difference for popular brand and unpopular brand.

Looking from both high risk and low risk application, it is obvious that the means for high risk will be lower than the low risk. Therefore, the result from this observation cannot prove the second hypothesis which mentions that a product failure from a popular brand may have bigger negative impact towards trust for the industry in total (H2), the difference is very small as shown in Figure 9 below.

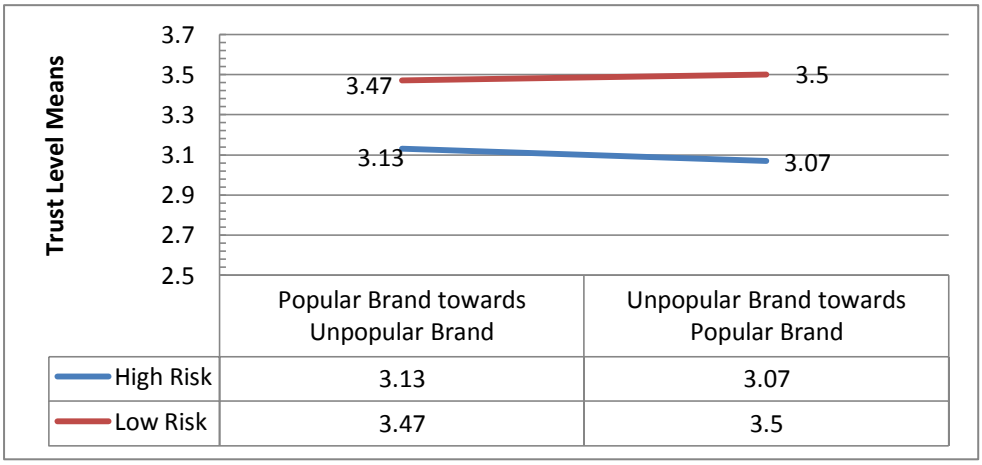

Figure 9 *Trust for industry in total between popular and unpopular brand for high risk and low risk application after another company is given a distrust factor*

Based on the observation result above, the means of trust level for popular brand is slightly lower than unpopular brand only when the risk of application is high. However it is considered as the same and insignificant. The significance level is measured by using a univariate general linear model as shown in the table below.

Tests of Between-Subjects Effects

Dependent Variable: Reaction towards CS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	4.492[a]	3	1.497	1.634	.185	.041
Intercept	1300.208	1	1300.208	1418.854	.000	.924
Risk	4.408	1	4.408	4.811	.030	.040
Brand	.008	1	.008	.009	.924	.000
Risk * Brand	.075	1	.075	.082	.775	.001
Error	106.300	116	.916			
Total	1411.000	120				
Corrected Total	110.792	119				

a. R Squared = .041 (Adjusted R Squared = .016)

Table 12 *Analysis of variance between subjects effect using univariate general linear model*

After getting the result from the third measurement for measuring the second hypothesis (H2), the next question is explained as the fifth measurement (M5) which will answer the fourth hypothesis (H4). The analysis comes from the result of the fifth question second scale which is explained as the fifth measurement (M5). This fifth measurement measures the carryover effect towards trust within industry in total after different product within the same company is hacked. The result turns out not as expected, the safety perception of using cloud service is better when the popularity of the brand is higher as seen in scenario 1 (high risk popular brand) which is slightly higher than scenario 2 (high risk unpopular brand) with the average mean 2.50 and 2.47 respectively. Whereas scenario 3 (low risk popular brand) is extremely higher than scenario 4 (low risk unpopular brand) represented by the average mean of 2.87 and 2.37 respectively.

Fifth Measurement (M5)	Simple main effect test comparison of means			
	High Risk		Low Risk	
	Popular Brand (Scenario 1)	Unpopular Brand (Scenario 2)	Popular Brand (Scenario 3)	Unpopular Brand (Scenario 4)
Carryover Effect *Safety perception towards Cloud Service Industry*	2.50	2.47	2.87	2.37
Std. Deviation	1.009	.937	.900	.1.033

Table 13 *Descriptive Statistics of trust for industry in total after different product within the same company is given a distrust factor*

From the above table, we can see the safety perception of using cloud service is better when the brand has higher popularity. Therefore, the result from this observation cannot prove the fourth hypothesis which mentions that a product failure from different product in the same company has bigger negative impact towards trust for the industry in total if the brand popularity is higher (H4), the difference is shown in Figure 10 below.

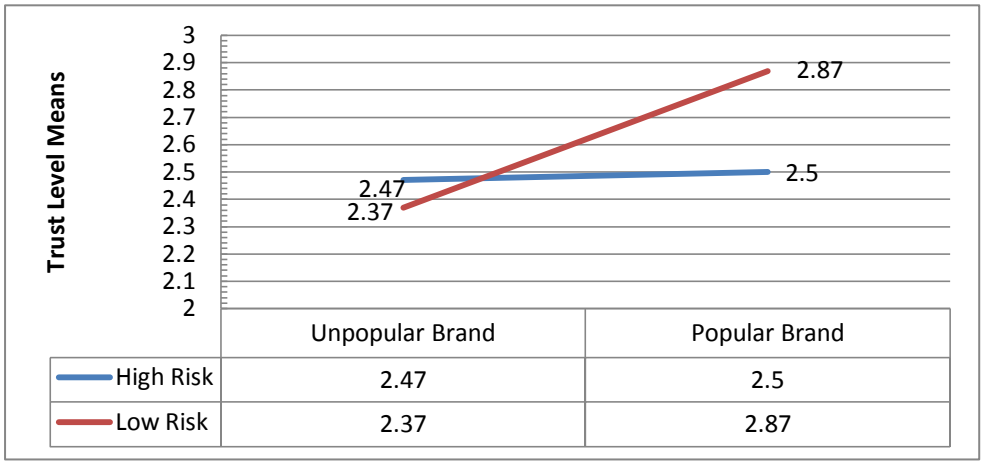

Figure 10 *Trust for industry in total between popular and unpopular brand for high risk and low risk application after different product within the same company is given a distrust factor*

Based on the observation result above, the means of trust level for popular brand is extremely higher than unpopular brand when the risk of application is low while for the high risk application the difference is less and insignificant. The significance level is measured by using a univariate general linear model as shown in the table below.

Tests of Between-Subjects Effects

Dependent Variable: Reaction towards CS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	6.158[a]	3	2.053	2.176	.095	.053
Intercept	785.408	1	785.408	832.538	.000	.878
Risk	.075	1	.075	.080	.778	.001
Brand	3.675	1	3.675	3.896	.051	.032
Risk * Brand	2.408	1	2.408	2.553	.113	.022
Error	109.433	116	.943			
Total	901.000	120				
Corrected Total	115.592	119				

a. R Squared = .053 (Adjusted R Squared = .029)

Table 14 *Analysis of variance between subjects effect using univariate general linear model*

The last measurement for measuring the carryover effect is represented by the seventh measurement (M7), this measurement will answer the sixth hypothesis (H6). The analysis comes from the responses of the sixth question second scale. This seventh measurement measures the carryover effect towards trust within industry in total after the product is hacked. The result is partially good, the safety perception of using cloud service is better when the popularity of the brand is lower only when the risk level is high as seen in scenario 1 (high risk popular

brand) which is lower than scenario 2 (high risk unpopular brand) with the average mean 1.87 and 2.03 respectively. Whereas scenario 3 (low risk popular brand) is higher than scenario 4 (low risk unpopular brand) represented by the average mean of 2.50 and 2.30 respectively.

Seventh Measurement (M7)	**Simple main effect test comparison of means**			
	High Risk		**Low Risk**	
	Popular Brand (Scenario 1)	**Unpopular Brand (Scenario 2)**	**Popular Brand (Scenario 3)**	**Unpopular Brand (Scenario 4)**
Carryover Effect *Safety perception towards Cloud Service Industry*	1.87	2.03	2.50	2.30
Std. Deviation	.937	.999	1.042	.1.112

Table 15 *Descriptive Statistics of trust for industry in total after the product failure*

From the above table, we can see the safety perception of using cloud service is better for unpopular brand only when the level of risk is high. Therefore, the result from this observation may only prove the sixth hypothesis which mentions that a product failure from a popular brand may have bigger negative impact towards trust for the industry in total (H6) if the level of risk is high. The difference is quite big as shown in Figure 11 below.

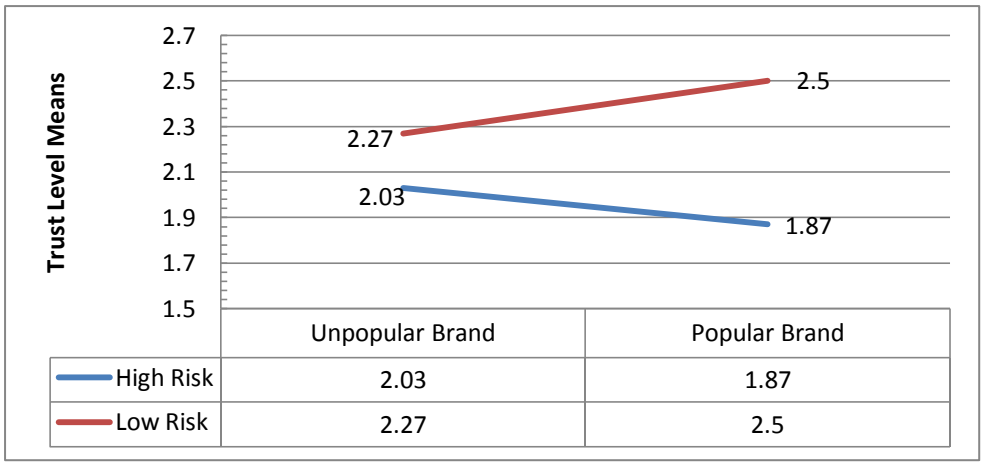

Figure 11 *Trust for industry in total between popular and unpopular brand for high risk and low risk application after a product failure*

Based on the observation result above, the means of trust level for popular brand is slower than unpopular brand when the risk of application is high and for the low risk application the effect is the other way around. The significance level is measured by using a univariate general linear model as shown in the table below.

Tests of Between-Subjects Effects

Dependent Variable: Reaction towards CS

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared
Corrected Model	6.867[a]	3	2.289	2.180	.094	.053
Intercept	563.333	1	563.333	536.508	.000	.822
Risk	5.633	1	5.633	5.365	.022	.044
Brand	.033	1	.033	.032	.859	.000
Risk * Brand	1.200	1	1.200	1.143	.287	.010
Error	121.800	116	1.050			
Total	692.000	120				
Corrected Total	128.667	119				

a. R Squared = .053 (Adjusted R Squared = .029)

Table 16 Analysis of variance between subjects effect using univariate general linear model

5.3. The transformation of customer loyalty on each distrust case

The transformation of customer loyalty on each distrust case was measured by the second, fourth and sixth measurement (M2, M4 and M6). This part shows the changing of between means from each measurement and will be categorized into two sections which explain the changing in low risk application and the changing in high risk application.

The observation result for low risk application shows the change of customer loyalty has bigger negative impact during the fourth and sixth measurement. This concludes that in a low risk application, brand gives more positive impact.

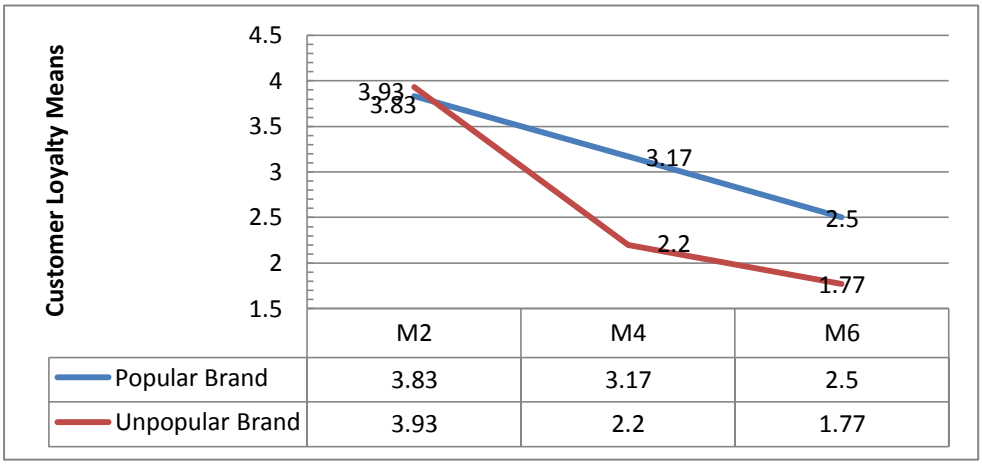

Figure 12 *The change of customer loyalty means between M2, M4 andM6 on a low risk application*

From the figure above, the observation fails to confirm the third and fifth hypothesis (H3 & H5). The first hypothesis (H1) has a possibility to be confirmed

but because the difference is small and insignificant, hence, the observation cannot be considerably confirmed.

The observation result for high risk application turns out as expected. Because the difference between popular and unpopular brand is also very small and insignificant, this observation cannot clearly confirm the first, third and fifth hypothesis. However the researcher assumes that there is a tendency that the result could be more significant with a bigger sample group. This concludes that after giving a distrust factor there might be a tendency that popular brand is affected negatively more than unpopular brand.

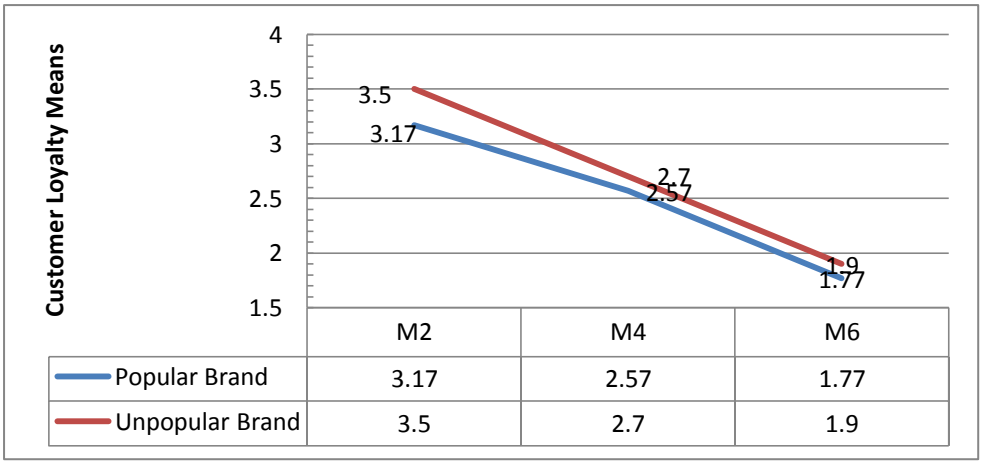

Figure 13 *The change of customer loyalty means between M2, M4 andM6 on a high risk application*

This observation above might confirm the first, third and fifth hypothesis (H1, H3 and H5). However due to the small and insignificant difference of the result, the observation cannot confirm it significantly.

5.4. Carryover effect of trust for industry in total on each distrust case

The carryover effect of trust for industry in total on each distrust case was measured by the third, fifth and seventh measurement (M3, M5 and M7). This part shows the changing between means from each measurement and will be categorized into two sections which explain the changing of customer's trust in low risk application and high risk application.

The result of observation based on low risk application shows the confidence level of using cloud service is bigger when the product has bigger popularity. This concludes that in a low risk application, unpopular product has bigger carryover effect towards trust for industry in total.

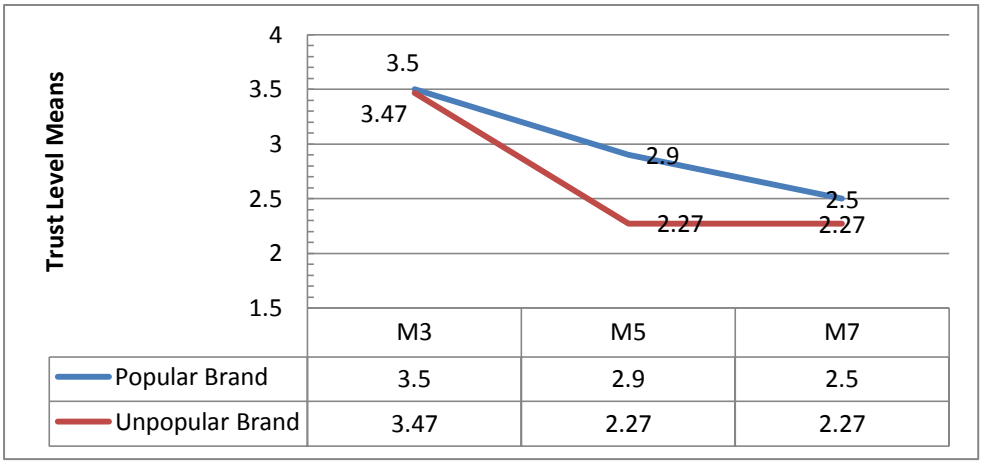

Figure 14 *The change of trust for industry in total means between M3, M5 andM7 on a low risk application*

This observation fails to confirm the second, fourth and sixth hypothesis (H2, H4 and H6). The biggest carryover effect is occurred during the fifth measurement, meaning the confidence level of using cloud service industry falls

down drastically when there is a product failure from another product within one company which has a low level of risk.

The observation result for high risk application shows that the effect is the same for both popular product and unpopular product because the difference between the means for each measurement is small and insignificant. This concludes that after giving a distrust factor, the level of trust for industry in total is insignificantly affected by the level of brand.

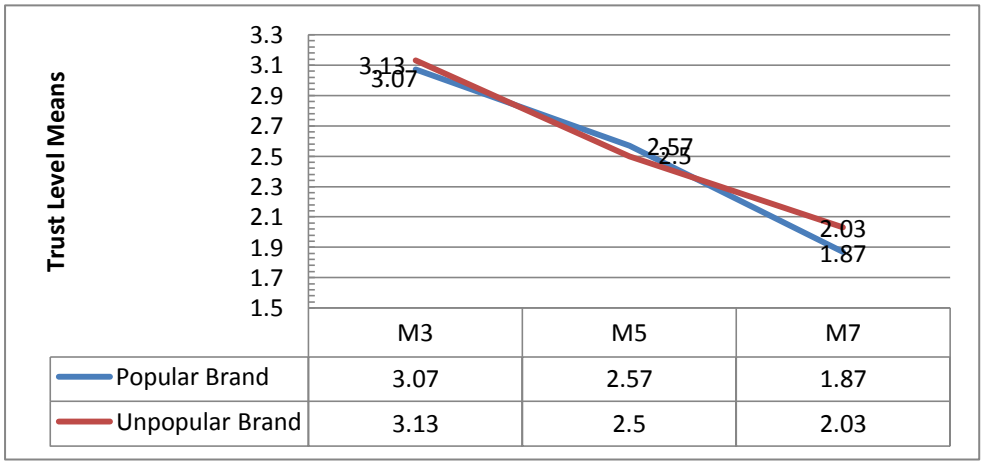

Figure 15 *The change of trust for industry in total means between M3, M5 andM7 on a high risk application*

This observation fails to confirm the second, fourth and sixth hypothesis (H2, H4 and H6). The carryover effect on each case has no influence from the level of brand. It means no matter the brand is, the carryover effect will be the same.

CHAPTER 6 DISCUSSION AND MANAGERIAL APPLICATION

6.1. Discussion

This research identifies the transformation of customer loyalty towards a high and low risk cloud computing application after being given several distrust factors in sequence. This study demonstrates that only in high risk application, the outcome turns out as expected although it is insignificant. It can be assumed that there is a possibility that the higher the brand, the higher the negative feedback towards the company. The tolerance level from the customer is smaller when the brand has more popularity which is explained in the sixth measurement in this study. It can be assumed that the expectation from the consumer is higher when the brand is well known. Giving an expectancy disconfirmation towards a branded company will give bigger negative feedback to the company compared to the same impact on the non-branded company.

The carryover effect from the given distrust factor could be confirmed only during the third and seventh measurement. Regardless of the significance level from the findings, it can be assumed that there is a tendency that a product failure from the similar product in a branded company may give bigger negative attention to the similar product within the industry. However, the effect is applied only when the level of the risk is high. The carryover effect of a product failure from a branded cloud computing company may influence the consumer's perception towards the cloud computing service industry in total and this can also become the

basic reason answering the question of why several people are reluctant to adapt the cloud computing technology up to now.

However, this study fails to confirm the hypotheses when the research object has low level of risk. Both impact towards own company and carryover effect towards the whole industry are not influenced by the level of the brand. Regardless of the brand, the negative impact towards the company is on the same level. This also applies for the carryover effect from the low risk research object. Consumer's perception towards the whole industry is not influenced by the level of the brand.

6.2. Managerial Application

Based on the above discussion, the researcher can confirm that this study can only be effectively measured when the research object has high level of risk. Thus, all cloud companies who are handling high risk information might use this study to be more selective and careful on managing their brand. When allocating financial budget for advertisement or marketing strategy in order to attract new customers, a cloud computing service company should consider the possibility of attracting negative attention due to the chosen strategy which may give more disadvantages for the company itself.

CHAPTER 7 FUTURE RESEARCH AND LIMITATION

Future research should consider the variation of the distrust factors and the model of the experiment. In this study, the experiment was done by questionnaires which only measure the respondent's intention, not the real action. The future research is suggested to examine the real natural reaction from the people who have already experienced the distrust factor in a real situation. The number of the respondent in this study was 120 in total which is divided into 4 scenarios. This number is the minimum possible for measuring the impact of a mass product. Another limitation for measuring the carryover effect also comes from the measurement combination of the brand level. Current observation only includes the loyalty carryover effect from popular brand towards unpopular brand and vice versa. There might be a different result if the combination of the brand level also considers the impact from the similar brand. The future research is suggested to observe more sample group in order to increase the significance level of the difference between the impact of popular brand and unpopular brand and measure the carryover effect from the same level of brand.

The finding of this study suggests that companies who are engaged in cloud service industry have possibility to attract more negative impact by increasing the brand popularity rather than positive impact because it might increase the vulnerability and reduce the customer tolerance level when the company facing distrust factors such as product failure. On the other hand, the brand itself does not really give a financial benefit to the company because by using a freemium business model, most of the attracted people by awareness of the brand will

reconsider their decision when it comes to commercial or paid by subscription business model. More over the observation in this study cannot prove most of the hypotheses significantly due to the limitations that have been mentioned above. These limitations await further research.

REFERENCES

Ahluwalia, R., & Gurhan-Canli, Z. (2000). The effects of extensions on the family brand name: An accessibility-diagnosticity perspective. *Journal of Consumer Research* , 371-381.

Ahluwalia, R., Burnkrant, R., & Unnava, R. (2000). Consumer response to negative publicity: the moderating role of commitment. *Journal of Marketing Research* , 203-214.

Banda, B. (2011). *The Marketing Report: Building a strong brand.*

Barone, M. J., Shimp, T. A., & Sprott, D. E. (1999). Product Ownership as a Moderator of Self-Congruity Effects. *Marketing Letters* , 75-85.

Benedicktus, R. L., Brandy, M. K., Darke, P. R., & Voorhees, C. M. (2010). Conveying Trustworthiness to online consumers: Reactions to Consensus, Physical Store Presence, Brand Familiarity and Generalized Suspicion. *Journal of Retailing* , 322-335.

Chuah, G. (2010). Owning a luxury car.

Coi, C. r., & Jeong, H. y. (2014). Quality evaluation and best service choice for cloud computing based on user preference and weights of attributes using the analytic network process. *Electronic Commerce Research* , 245-270.

Cumming, D., & Johan, S. (2010). The Differential Impact of the Internet on Spurring Regional Entrepreneurship. *Entrepreneurship Theory and Practice , 34*, 857-883.

Darke, P. R., & Ritchie, R. J. (2007). The Defensive Consumer; Advertising Deception, Defensive Processing, and Distrust. *Journal of Marketing Research* , 114-127.

Darke, P. R., Ashworth, L., & Main, K. J. (2009). Great expectation and broken promises; misleading claims, priduct failure, expectancy disconfirmtion and customer distrust. *Academic of Marketing Science* , 347-362.

Dolich, I. J. (1969). Congruence Relationships Between Self Images and Product Brands. *Journal of Marketing Research 6* , 80-84.

Doney, P., & Cannon, J. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing* , 35-51.

Edmonds, J. (2005). Comment: The importance of building a strong brand identity. *Technical Textiles International : TTI* , 2.

Ehrenberg, A., & Goodhardt, G. (2000). New brands: newar instat loyalty. *Journal of Marketing Management* , 07-17.

Froberg, P. (2015). *What is freemium ?* Retrieved from What is freemium ?: http://www.freemium.org/what-is-freemium-2/

Huang, E., & Liu, C.-C. (2010). A Study on Trust Building and Its Derived Value in C2C E-Commerce. *Journal of Global Business Management* , 1-9.

ITU, I. T. (2014). *Number of Internet User & Growth*. Retrieved 02 2015, from http://www.internetlivestats.com/internet-users/

Kakaomerlioglu, D. C., & Carlsson, B. (1999). Manufacturing in decline? A matter of definition. *Economics of Innovation and New Technology , 8*, 175-196.

Lee, M., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce* , 75-91.

Maras, M.-H. (2012). Computer forensics: Cybercriminals, laws, and evidence. *Jones & Bartlett Learning* , 1.

McBrayer, J. (2014). Exploiting the digital frontier: Hacker typology and motivation. 83.

Mell, P. &. (2011). The NIST definition of cloud computing.

Mimoso, M. (2015, January 27). *GHOST glibc Remote Code Execution Vulnerability Affects All Linux Systems*. Retrieved from https://threatpost.com/ghost-glibc-remote-code-execution-vulnerability-affects-all-linux-systems/110679

Mittal, B., & Lassar, W. (1998). Why do customers switch? The dynamics of sarisfaction versus loyalty. *The Journal of Servies Marketing* , 177-94.

Rogowsky, M. (2013, 11). *Dropbox Is Doing Great, But Maybe Not As Great As We Believed*. Retrieved 2015, from Forbes: http://www.forbes.com/sites/markrogowsky/2013/11/19/dropbox-makes-hundreds-of-millions-so-why-is-it-only-asking-for-an-8b-price/

Shah Alam, S., & Mohd Yasin, N. (2010). What factors influence online brand trust: evidence from online tickets buyers in Malaysia. *Journal of Theoretical and Applied Electronic Commerce Research* , 78-89.

Sheikh, S. U., & Beise-Zee, R. (2011). Corporate social responsibility or cause-related marketing? The role of cause specify of CSR. *Journal of Consumer Marketing* , 27-39.

Tellis, G. (1988). Advertising exposure, loyalty and brand purchase: a two-stage modelof choice. *Journal of Marketing Research* , 34-44.

Zetter, K. (2014, December 3). *Sony Got Hacked Hard: What We Know and Don't Know So Far*. Retrieved from http://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

APPENDIX

Scenario 1

You are a business man or business woman who is currently looking for a solution to help managing your credential data (customers pin, bank accounts, passwords, security keys and many more). Your work requires you to remember all the credential data, however you cannot just write it down on your note because it is too risky. One of the solutions is to keep it inside a very secure cloud application which can be accessed from everywhere. “Cloud application means any data that you store will be saved on the server via internet, enabling you to access it from any devices, anywhere and anytime.” Imagine you found a Sony application and you are using it.

Scenario 2

You are a business man or business woman who is currently looking for a solution to help managing your credential data (customers pin, bank accounts, passwords, security keys and many more). Your work requires you to remember all the credential data, however you cannot just write it down on your note because it is too risky. One of the solutions is to keep it inside a very secure cloud application which can be accessed from everywhere. “Cloud application means any data that you store will be saved on the server via internet, enabling you to access it from any devices, anywhere and anytime.” Imagine you found a password manager application called DataVault and you are using it.

Scenario 3

You are a truly movie lover, you do not want to miss any single movie that will be premiered in the cinema or television. In order to do that, you are looking for a solution to help managing your movie to-do-list or watch-list. You want a simple and informative application that can help reminding your movie watch-list anytime and anywhere, so you decided to search a cloud application for that. "Cloud application means any data that you store will be saved in the server via internet, enabling you to access it from any devices, anywhere and anytime." Imagine you found this below Sony Movie List application and you are using it. This application only safe your movie title, premiered date and other information. It does not safe your movie.

Scenario 4

You are a truly movie lover, you do not want to miss any single movie that will be premiered in the cinema or television. In order to do that, you are looking for a solution to help managing your movie to-do-list or watch-list. You want a simple and informative application that can help reminding your movie watch-list anytime and anywhere, so you decided to search a cloud application for that. "Cloud application means any data that you store will be saved in the server via internet, enabling you to access it from any devices, anywhere and anytime." Imagine you found this below Movie List application and you are using it. This application only safe your movie title, premiered date and other information. It does not safe your movie.

Question 1 on each scenario

Scenario 1: Imagine you are using it, How would you feel using Sony Password Manager?

Scenario 2: Imagine you are using it, How would you feel using DataVault Password Manager?

Scenario 3: Imagine you are using it, How would you feel using Sony My Movie List Application?

Scenario 4: Imagine you are using it, How would you feel using My Movie List Application?

Question 2 on each scenario

Scenario 1: What do you feel about putting your credential data into Sony Password Manager?

Scenario 2: What do you feel about putting your credential data into DataVault Password Manager?

Scenario 3: What do you feel about putting your movie list into Sony My Movie List Application?

Scenario 4: What do you feel about putting your movie list into My Movie List Application?

Question 3 on each scenario

Scenario 1: Do you familiar with the company who creates this application? Sony Corporation.

Scenario 2: Do you familiar with the company who creates this application? DataSecure Corporation.

Scenario 3: Do you familiar with the company who creates this application? Sony Corporation.

Scenario 4: Do you familiar with the company who creates this application? Movie Media Corporation.

Question 4 on each scenario

Scenario 1: You have been using Sony Password Manager for a while and suddenly news rises. The news says that another company, DataSecure Inc. has been hacked for the first time and their password manager application data is leaked and spread through the internet. However your application and its data are SAFE. What will you do?

Scenario 2: You have been using DataVault Password Manager for a while and suddenly news rises. The news says that another company, Sony Corp. has been hacked for the first time and their password manager application data is leaked and spread through the internet. However your application and its data are SAFE. What will you do?

Scenario 3: You have been using Sony My Movie List Application for a while and suddenly news rises. The news says that another company, Movie Media Corp. has been hacked for the first time and their similar movie list application's data has lost. However your application and its data are SAFE. What will you do?

Scenario 4: You have been using My Movie List Application for a while and suddenly news rises. The news says that another company, Sony Corp. has

been hacked for the first time and their similar movie list application's data has lost. However your application and its data are SAFE. What will you do?

Question 4 Second Scale on each scenario

Scenario 1 & 2: How would you feel about storing your credential data inside the internet (Cloud Computing)?

Scenario 3 & 4: How would you feel about storing your data inside the internet (Cloud Computing)?

Question 5 on each scenario

Scenario 1: You have been using this Sony Password Manager a while. Suddenly you received an apology message from Sony Corp. informing that theirs payment system was hacked. However your application and its data are safe. What will you do?

Scenario 2: You have been using this DataVault Password Manager a while. Suddenly you received an apology message from DataSecure Corp. informing that theirs payment system was hacked. However your application and its data are safe. What will you do?

Scenario 3: You have been using this Sony My Movie List Application for a while. Suddenly you received an apology message from the company. informing that theirs payment system was hacked. However your application and its data are safe. What will you do?

Scenario 4: You have been using this My Movie List Application for a while. Suddenly you received an apology message from the company. informing

that theirs payment system was hacked. However your application and its data are safe. What will you do?

Question 5 Second Scale on each scenario

Scenario 1 & 2: After above incident, how would you feel about storing your credential data inside the internet (Cloud Computing)?

Scenario 3 & 4: After above incident, how would you feel about storing your data inside the internet (Cloud Computing)?

Question 6 on each scenario

Scenario 1: You have been using Sony Password Manager without problem, but then suddenly you loss all of your data because it has been hacked. The company (Sony Corp.) will refund your money and apologize because of the inconvenience, they promise to improve the service. What will you do?

Scenario 2: You have been using DataVault Password Manager without problem, but then suddenly you loss all of your data because it has been hacked. The company (DataSecure Corp.) will refund your money and apologize because of the inconvenience, they promise to improve the service. What will you do?

Scenario 3: You have been using Sony My Movie List Application without problem, but then suddenly you loss all of your data because it has been hacked. The company (Sony Corp.) apologizes because of the inconvenience and they promise to improve the service. What will you do?

Scenario 4: You have been using My Movie List Application without problem, but then suddenly you loss all of your data because it has been hacked.

The company (Movie Media Corp.) apologizes because of the inconvenience and they promise to improve the service. What will you do?

Question 6 Second Scale on each scenario

Scenario 1 & 2: After all of above tragedies, How would you feel about storing your credential data inside the internet (Cloud Computing)?

Scenario 3 & 4: After all of above tragedies, How would you feel about storing your data inside the internet (Cloud Computing)?