Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

THE FACTORS AFFECT PURCHASE INTENTION OF CYBERSECURITY PRODUCT IN SME MARKET OF HONG KONG

A dissertation submitted for the

Master of Business Administration (MBA) 2021

Submitted : April 2021

Student: Marco Lam

Student Number : 1913636

Supervisor : Dr. WONG, Chi Hong Arion

Declaration/Statements page

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed ..... (candidate)

Date .....14 April 2021.....

STATEMENT 1

This work is the result of my own investigations, except where otherwise stated.

Other sources are acknowledged by footnotes giving explicit references.
A bibliography is appended.

Signed ..... (candidate)

Date ..... 14 April 2021.....

STATEMENT 2

I hereby give consent for my work, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed ..... (candidate)

Date ..... 14 April 2021.....

NB: *Candidates on whose behalf a bar on access has been approved by the University (see Note1), should use the following version of Statement 2:*
I hereby give consent for my work, if accepted, to be available for photocopying and for inter-library loan **after expiry of a bar on access approved by the University.**

Signed ..... (candidate)

Date ..... 14 April 2021.....

NOTES

1 Provisions for Bars on Access to Higher Degree Dissertations

The University expects that research work accepted for a higher degree shall be openly available, and subject to no security classification or restriction of access. (Please note, however, that the University requires the reader of a dissertation to sign a declaration that in any statement or written work being prepared on the subject (or cognate subject) of the dissertation, due acknowledgement to the author will be made for any helpful information obtained from the dissertation.)

Nevertheless, in cases where there is an overriding need for a restriction of copying or access (for example where sponsored research has resulted in a dissertation which contains commercially-sensitive information) the University may place a bar on photocopying of and/or access to a dissertation for a specified period (normally three years in the first instance). It is the responsibility of your supervisor to make an application to the University for a bar to be sought as soon as is reasonably practicable, ideally at the outset of your candidature.

Please note that, in the event that a bar on photocopying and/or access is granted by the University, the signed statement to be included with each copy of the dissertation submitted should indicate that the dissertation may be made openly available *after the expiry of the bar on access.*

Normally, the title and summary of the dissertation will be made available.

2 Taught Master's Dissertation Archive

The University will keep a record of all dissertations successfully submitted for Part II of a taught Master's Degree. The record will include the student code, student name, the dissertation title and the mark awarded. The record will also include the title of the degree awarded and the year in which the award was conferred.

The University will keep one copy of each dissertation successfully submitted for Part II of a Taught Master's Degree. Following the successful outcome of the relevant

Progression/Award Examining Board, a printed copy of the dissertation will be sent to Library and Learning Resources for cataloguing and storage within the Library.
Dissertations will subsequently be available for reference use only.

An electronic copy of any dissertation deposited in the National Library of Wales will also be deposited in the University's digital repository.

3 National Library of Wales

In the event of the dissertation meeting the criteria for being deposited in the National Library of Wales, the candidate will be required to provide an additional copy in permanent, hardback binding.

Dissertations are only deposited in the National Library of Wales if:

(a) deemed by the examiners to be of Distinction standard
or

(b) if they are in the fields of Celtic Studies, Welsh or Welsh History;
or

(c) if they do not meet either of the above criteria, but are considered by the examiners to be of particular relevance to Wales.

Acknowledgements

Year 2019 to year 2021 are very special year for all the mankind in the world, we had much more chance to review our life and relationship with our friends and family. Despite this MBA program mostly conducted in virtual way, I still strongly feel the passion of all the professors and the professional support from the university.

I would like to take a few word to express my gratitude to my supervisor Dr. WONG, Chi Hong Arion for his insightful comments in this long journey of dissertation. His guidance is the lighthouse for me to finish this research. Finishing MBA will not be the end of the journey of improving myself, I hope there will be more to learn form him in the near future.

Lastly, I would like to mention the unconditional support from my family, my wife Yannie, my mother Tina, three of my kids, Tahlia, Theo and Taylor. Hoping in someday I can share the result of this thesis with them.

Abstract

The demand for cybersecurity solutions had been rising world-wide under the COVID-19 pandemic. The market size growth 7.6% in 2020 and would reach USD 366 billion in 2021. Although the world-wide SMEs market had an increasing demand for end-point security solutions, for example anti-virus and email protection, Hong Kong SMEs market seem didn't share the same trend. The cybersecurity readiness of Hong Kong SMEs had decrease 2.4 points in 2020. This study aim to explore factors that affect the purchase intention of Hong Kong SMEs toward cybersecurity product and service in order to help local service and product providers forming a better marketing plan to develop Hong Kong market.

This dissertation had included first-hand and second-hand researches. Three factors, perceived value, perceived risk and word-of-mouth had been identified would affect purchase intention of SMEs. Following up, there was a survey conducted which targeted the managements of SMEs in Hong Kong. In the process of developing the survey, focus group discussion and pilot test had been performed which helped the full scale survey conducted successfully. The survey collected responses from 126 managements from Hong Kong SMEs and the data had been fully analysis using SPSS with different statistical tools. The positive liner relationship between all three factors and purchase intention had been confirmed during the correlation analysis. In regression test, there were regression relationship found between perceived emotional value and perceived conditional value.

The recommendations to local cybersecurity product and service providers were to use more visualise materials in the sales process and to do more case study sharing on pervious attack in Hong Kong. For further study, the suggestion would be explore purchase intention by industry as this area of study was also important for local service and product providers to formulate marketing plans for SMEs market in Hong Kong.

Keywords: Cybersecurity, Purchase intention, Perceived value, Perceived risk, WoM

Contents

Acknowledgements v

Abstract vi

Contents vii

Tables List ix

Figure List xi

Appendix List xii

1. Introduction 1

1.1.Industry overview 1

1.2.Cybersecurity 6

1.3.Small and medium enterprise (SME) 7

1.4.Research rationale 8

1.5.Research question 9

1.6.Objective of the research 10

1.7.Contribution of research 10

1.8.Structure overview 12

1.9.Summary 13

2. Literature review 14

2.1.Perceived value 14

2.2.Perceived risk 19

2.3.Word of mouth (WOM) 25

2.4.Purchase intention 28

2.5.Relationship with purchase intention 31

2.6.Literature review summary 32

3. Methodology 33

3.1.Research framework 33

3.2.Hypotheses 33

3.3.Research type 34

3.4.Research target 35

3.4.1.Sampling method 35

3.4.2.Sampling size 36
3.5.Analysis methods 38
3.6.Correlation 39
3.7.Regression 40
3.8.Questionnaire design 41
3.8.2.Perceived value 41
3.8.3.Perceived risk 42
3.8.4.Word of mouth 44
3.8.5.Purchase intention 44
3.9.Survey 45
3.10.Summary 47
4. Research Results 48
4.1.Descriptive statistics 48
4.2.Reliability 57
4.3.Correlation analysis 59
5. Conclusion and recommendation 69
5.1.Conclusion 69
5.2.Recommendation 70
5.3.Limitation of the study 72
5.4.Impact of business 73
5.5.Recommendation on further study 74
Reference 76
Bibliography 78
Appendix 85

Tables List

Table 1.1.1 List of some international cybersecurity service and product providers that provide service in Hong Kong 4
Table 1.1.2 List of some local cybersecurity service and product providers 5
Table 1.2.1 The definition of SMEs 8
Table 2.1.1 Definition of perceived value 15
Table 2.1.2 Measurement of perceived value 17
Table 2.2.1 Definition of perceived risk 20
Table 2.2.2 Measurement of perceived risk 22
Table 2.3.1 Definition of WoM 25
Table 2.3.2 Measurement of WoM 27
Table 2.4.1 Definition of purchase intention 29
Table 2.4.2 Measurement of purchase intention 30
Table 3.5.1 Relationship between Cronbach's alpha and internal consistency 39
Table 3.6.1 Relationship between Pearson coefficient and r 40
Table 3.8.1 Screening questions 41
Table 3.8.2 Questions on perceived value 42
Table 3.8.3 Question on perceived risk 43
Table 3.5.2 Question on WoM 44
Table 3.5.3 Question on Purchase intention 44
Table 3.9.1 Focus group study result 46
Table 3.9.2 Reliability test result of pilot test 47
Table 4.1.1 Descriptive statistics of perceived functional value 49
Table 4.1.2 Descriptive statistics of perceived social value 50
Table 4.1.3 Descriptive statistics of perceived emotional value 50
Table 4.1.4 Descriptive statistics of perceived epistemic value 51
Table 4.1.5 Descriptive statistics of perceived conditional value 51
Table 4.1.6 Descriptive statistics of perceived value 52
Table 4.1.7 Descriptive statistics of perceived time risk 53
Table 4.1.8 Descriptive statistics of perceived privacy risk 53

Table 4.1.9 Descriptive statistics of perceived financial risk 54
Table 4.1.10 Descriptive statistics of perceived functional risk 54
Table 4.1.11 Descriptive statistics of perceived psychological risk 55
Table 4.1.12 Descriptive statistics of perceived value 55
Table 4.1.13 Descriptive statistics of WoM 56
Table 4.1.14 Descriptive statistics of purchase intention 56
Table 4.2.1 Reliability test result on perceived value 57
Table 4.2.2 Reliability test result on perceived risk 58
Table 4.2.3 Reliability test result on WoM 58
Table 4.2.4 Reliability test result on purchase intention 58
Table 4.3.1 Correlation analysis between perceived value and purchase intention 59
Table 4.3.2 Correlation analysis between perceived risk and purchase intention 60
Table 4.3.3 Correlation analysis between WoM and purchase intention 60
Table 4.3.1 Correlation analysis of all independent variables and purchase intention 61
Table 4.4.1 Model summary for regression analysis (First-run) 62
Table 4.4.2 ANOVA of the regression analysis (First-run) 62
Table 4.4.3 Regression coefficient of analysis (First-run) 63
Table 4.4.4 Model summary for regression analysis (Second-run) 63
Table 4.4.5 ANOVA of the regression analysis (Second-run) 64
Table 4.4.5 Regression coefficient of analysis (Second-run) 64
Table 4.4.6 Model summary for regression analysis (Final-run) 65
Table 4.4.7 ANOVA of the regression analysis (Final-run) 65
Table 4.4.8 Final Element eliminated from the regression test 65
Table 4.4.9 Regression coefficient of analysis (Final-run) 66
Table 4.5.1 Research hypothesis test result 68

Figure List

Figure 1.1.1 Financial loss from cyberattack in Hong Kong 3
Figure 1.1.2 Cyber Security incident reported to HKCERT 3
Figure 3.1.1 Research framework 33
Figure 4.1.1 Distribution of the participants 49
Figure 4.4.1 Re-run correlation analysis of construct of perceived risk 66
Figure 4.4.2 Re-run correlation analysis of construct of perceived risk 67
Figure 4.5.1 The research framework 67
Figure 5.2.1 Network attack map 71

Appendix List

Appendix i Draft questionnaire 85
Appendix ii Details of Focus group interview 89
Appendix iii Final questionnaire 90
Appendix iv Proposal 93
Appendix v Ethic Form 112
Appendix vi Media article by Capital Magazine 118

1. Introduction

This introduction explained fundamental information and background of the topic. Within the first part of the introduction session, an industry overview of cybersecurity had been covered. Also current market size, market players and elaboration of a few cybersecurity cases had been discussed. After that, there were some definitions of key concepts and news that would help readers who are not familiar with the topic to have a ground of understand. Then it reviewed the research rationale and research question by looking into some facts of Hong Kong Small and Medium size Enterprises with other trends.

1.1. Industry overview

The demand of cybersecurity solutions had been rising world-wide under the COVID-19 pandemic. Governments and large enterprises promote Work-form-home policy to protect staff from getting inflated (News HKGOV, 2020; Davis, 2020). For example 75% of staff in Standard Charter bank had been work from home during the pandemic. The arrangement has increased the cybersecurity solution needs world-wide (Fortune Business insights, 2021).

The impact of pandemic created an opportunity for companies to speed up their digital transformation (German Industry and Commerce Ltd., 2020). Companies in all different size were getting their business operations more relay on computer systems and moving faster to setup online stores that keep customers engaged. The cybersecurity risks for companies were increasing as the number of systems and customer's information were growing towards their business growth. In details, adopting new technologies such as machine learning, internet of things (IoT), cloud

computing and big data had increased the needs of cybersecurity solutions for all size of companies.

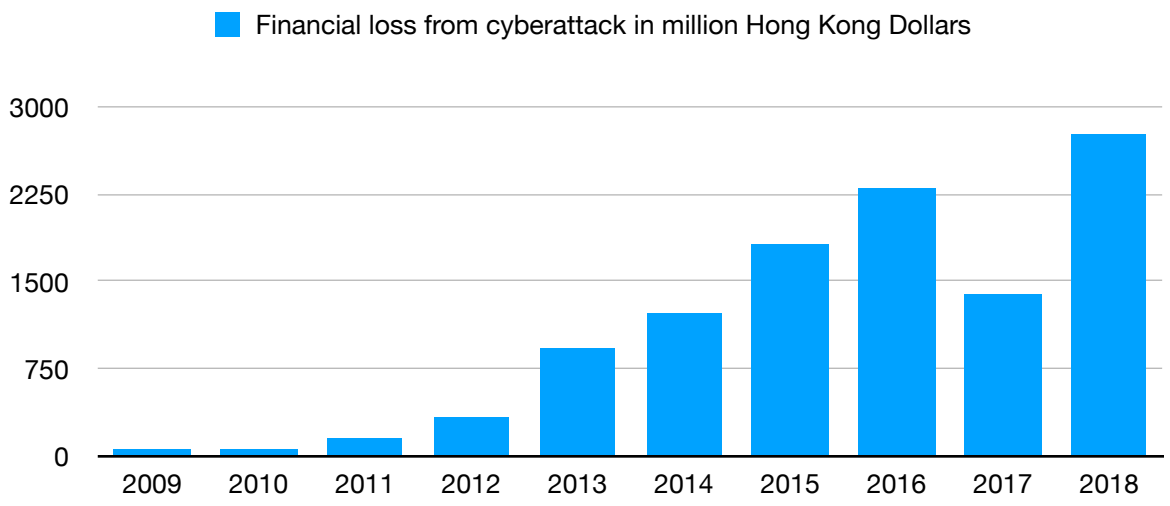
Recent researches supported the forecast about the pandemic, the market size growth 7.6% in 2020 and would reach USD 366 billion in 2021. The growth not only reflected in enterprises but more on SMEs. The world-wide SMEs market has an increasing demand for end-point security solutions, for example anti-virus and email protection, which has seen to be one of the major driving forces to the industry growth (Fortune Business insights, 2021).

Looking into regional growth, Asia Pacific was expected to have the most compound annual growth rate in 2021 - 2028 which meant the SMEs market in Asia Pacific were expected to have a high growth rate in coming years.

Hong Kong is an international city with the largest stock market in Asia. However, the SMEs market of cybersecurity in Hong Kong seems not share the same trend with the rest of the world.

The cybersecurity readiness of Hong Kong SMEs has decreased 2.4 points in 2020. In an annual survey, conducted by HKPC, indicated that the Hong Kong SMEs only have 56.3 point in the readiness of cybersecurity and only less than 60% of SMEs think they can handle a cyberattack (HKCERT, 2020a). The readiness of basic element were decreasing by 2.4 point compare to 2019 (HKCERT, 2020a). That meant over 343,313 small and medium sized enterprises (SMEs) in Hong Kong were not quite ready for cyber attack.

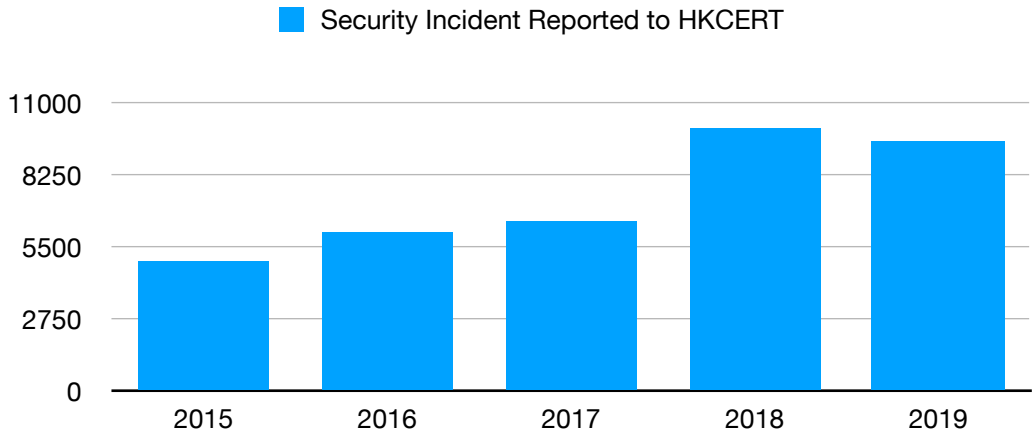
Figure 1.1.1 Financial loss from cyberattack in Hong Kong



Sources: Lai (2020)

The Figure 1.1 provided a concept of the overall cybersecurity environment in Hong Kong. The total cost of cyber crime in 2018 was the record high since 2009 (Lai, 2020). The reported loss growth over 300000% in the past 10 years.

Figure 1.1.2 Cyber Security incident reported to HKCERT



Sources: HKCERT (2020b)

Table 1.1.2 showed that the reported cybersecurity cases in Hong Kong. the number of attacks handled by HKCERT reached 9,458 in 2019, draped 6% compared to 2018 as shown in figure 1.2. The dropping is caused by the attackers shifted their focus from mass volume attack to attacking for profit which meant their

attack methods changed from malware to Botnet and Phishing email (HKCERT, 2020).

Table 1.1.1 List of some international cybersecurity service and product providers that provide service in Hong Kong

Company name	Head office location
BM Corporation	United States
Check Point Software Technologies	Israel
Cisco Systems Inc.	United States
Cloudflare Inc.	United States
Cloudstrike Inc.	United States
FireEye Inc.	United States
Fortinet Inc.	United States
Kaspersky Lab	Russia
McAfee Inc.	United States
Oracle Corporation	United States
SonicWall	United States
Splunk Inc.	United States

Sources: Writer construct the table

There were cybersecurity service and product providers operating in Hong Kong and there were more companies put their focus in Hong Kong market.

The importance of cybersecurity is also recently reflected in the stock price in major market players in the industry, such as Splunk, Cloudstrike and Cloudflare, all have reached their record high in number of transitions and company valuations (Cohen, 2021). Table 1.1.1 showed some of the international cybersecurity service and product providers that provide service in Hong Kong.

Table 1.1.2 List of some local cybersecurity service and product providers

Company name	Head office location
Binary Solutions	Hong Kong
Digitpol	
Dual Layer IT Solutions	
Edvance International Holdings	
EIRE Systems	
Ensign InfoSecurity	
Maximus Consulting	
Nearby	
Nexusguard	
StormEye.io	
Velocity Technology	

Sources: Writer construct the table

Apart from international enterprises, there were also some local companies providing cybersecurity services and products in Hong Kong as list in table 1.1.2. Both international firms and local firms were now looking for ways to take full advantage of growth of SMEs cybersecurity service and product market in Hong Kong (Goldstein research, 2020).

1.2. Cybersecurity

Cybersecurity was a concept to protect information being unwanted access. The industry had began in 1990s, which meant to provide services to protect client's systems and databases not to damage and misuser by attackers (Cisco 2021). The first cyber threat started at 1978, a programmer found a way to access a mainframe data base without permission. The area of cybersecurity had changed a lot since then.

There are many literatures discuss and define the concept of cybersecurity. Definition of cybersecurity was a discipline base on computer that use different technology, people, information and process to make sure system information is not being misused (CISA USGOV, 2019). The process involved creation, operation, analysis and testing a specific system. Von Solms and Van Niekerk (2013) suggested the definition of cybersecurity was more than the boundaries mentioned above, it also included personal asset in digital forms.

As one of the uniqueness of cybersecurity, attackers were able to laugh attacks beyond organisational and geographical boundaries, and often untraceable (, their risks and impacts were more far-reaching (Jaccard-Jaccard and Nepal, 2014; Hovav and Gray ,2014).

Common types of attacks included Phishing, Ransomware, Malware and Social engineering. "I Love You" virus was one of the well known virus in 1990s, it gained access to victim contact lists and forward a simple wording of "I Love You" with a phishing link and cause chain damaged.

Cyber attack was a potential threat to all companies and/or organisations. According to a report from Rudow (2020), there were 205,280 organisations had been successfully attacked by hacker be ransomware, compared to 2018, that was 41% increased with average payment of USD 111,605. Not like the virus or attack

like “I Love You”, attackers found ways to damage victim’s systems and gain financial benefits from the attack. Acer, a Taiwan computer manufacturer, faced with a USD 100 Millions Ransomware attack recently and it was the largest reported (Mathews, 2021). It showed that hackers are spending more effort and resources to attack enterprise and/or organisations as they tend to be willing to pay for ransom demand in order to reduce damage.

Backed in May 2017, a cyber attack targeted on Windows operation system “Wannacry” spread in over 150 countries worldwide and costed USD 4B losses across the globe.

Guta (2019) state that the trend of cyber attack were switched to very small and medium size enterprises as targets. In 2019, Broadcom reported at least 4,818 different business websites have been form jacking each month in 2018. SMEs may face different types of threats, both direct or indirect in nature which increases the challenge to get ready and identify attacks (Ilvonen and Virtanen, 2013).

The range of cybersecurity products and services were relatively wide, compared to other commodity products. Firewall and anti-virus software are some of the examples that SMEs’ owner had knowledge of.

Cybersecurity products and services were limited to computer base software and hardware, policies, law and regulation are equally important in this study (Kosseff, 2019).

1.3.Small and medium enterprise (SME)

International companies and/or listed companies had more resources to handle cyber threat, yet for SMEs cyber risk was challenging issue due to limited resources. This research focused on the decision makers in SMEs . There were definitions of Small and medium enterprise in different countries.

Table 1.2.1 The definition of SMEs

	The definition of SMEs	
	Companies have under	
Hong Kong	50 employees for non-industrial	100 for industrial companies
European Union	250 employees	
USA	500 employees	

Sources : Table construct by writer

The definition of SMEs varies by country, in European Union companies had under 250 employees were categories as SME. In America, SMEs were the backbone of U.S. Economy, 30 million of SME created 2/3 of new jobs created in last decades (Office of the United States Trade Representative, 2021). While in USA, the limite was up to 500 employees, Hong Kong set the SME definition to a company has less than 50 employees for non-industrial and less than 100 for industrial companies (TID HKSAR, 2021). In Hong Kong, there were more than 95% of the total company was SMEs (SUCCESS HKSAR, 2021).

1.4. Research rationale

In Hong Kong, there were lots of international and local market players as mentioned. They both have certain groups of target audiences. For international cybersecurity firms like Splunk and IBM, their primary target segments were enterprises with different operation locations and using lots of systems to run their businesses. Their primary target were local public listed companies and/or large enterprises.

For local cyber security enterprises, they might had insufficient resources to serve those large organisations and usually placed themselves as a system integrator who helped to resell and implement security products. SMEs were their target customers. HKCERT (2020b) stated that there are 51% more phishing cases in 2020 compared to 2019 due to the pandemic. Most of the phishing emails used

fake government funding site to attack SMEs. And the fundings were often for support SMEs this indicted that hackers are targeting on SMEs. Thus, more cybersecurity service and product providers tended to target the same group of people as the demand in SME market is increasing.

There were more than 340,000 of SMEs x in Hong Kong, constituting more than 98% of business unite and 45% of workforce in private (Kosseff, 2019). As a result, SMEs could be one of the most potential market for the industry to explore and invest for.

In today's competitive business environment, the industry should understand the target segments purchasing behaviour in order to differentiate their marketing strategies.

This study aimed to explore factors that affect the purchase intention of Hong Kong SMEs toward cybersecurity product and service in order to help local service and product providers forming a better marketing plan to develop Hong Kong market.

1.5.Research question

This dissertation would like to use different research methods to find out what is the factors that affect the purchase intention of SME in Hong Kong toward cybersecurity products or services. The research questions of the discretion would focus on three areas to provide full picture for readers.

To be more specifically answering the research questions, the dissertation will try to answer the questions below.

a. What is the driver when SMEs purchase cybersecurity products or service?
b. How those factors affect the decision make?
c. What are the motivations to attract SMEs to purchase cybersecurity product and service ?

1.6. Objective of the research

The main purpose of this research was to explore the factors that affect purchasing intention of small and medium size businesses towards purchasing cybersecurity product. To answer the research question, the objective expended into the three objectives accordingly.

a. Identification of the concepts and components of factors that affect purchasing behaviour of SME in cybersecurity product.
b. To identify the relationship between factors that apply to SME market in Hong Kong.
c. Development of recommendation of effective market expansion plans.

To achieve the above objective A, the dissertation first performed literature review on some factors that might relate, for example, perceived value, perceived risk and word of month. For objective B, some hypothesis would be formulated that act as an independent variable which affect purchase intention of SMEs. By using quantitive research such as questionnaire, there would be some relationships that affect purchase intention that identified. From the results of the factors and hypothesis, this study provided some suggestions for cybersecurity service or product providers that can help them to promote more effectively.

1.7.Contribution of research

There were contributions this research aimed to provide that benefit different parts of the society. There were three layers of stake holder might benefit from this study.

1.7.1. Contribution to individual

The purchase discussion of SMEs was decided by a few management, as their companies structure were less complicated compare to larger enterprises. For the management of SMEs, there would be time-consuming

to read through all marketing material from cybersecurity service and product providers Ozmen (2014). This study provided the necessary information for cybersecurity service and product provider to simplify their sales process and promotion materials. Also, the findings would help the sales process more focus on the topics that managements concerned about. It would help the management of SMEs to save time and more easy to make a purchase.

1.7.2. Contribution to company

Cybersecurity service and product providers in Hong Kong had faced hard time to promote cybersecurity service and products to local SMEs, as the readiness of them is not high and the business forecast was not good (HKE HKSAR, 2021). Together with the impact to the business from the COVID-19 pandemic, the service and product providers were seeking ways to improve their sales effectiveness. This research would help them understand the most important factor that SMEs concern about and adjust the marketing angle accordingly. As the SME market in Hong Kong was big and not yet fully developed, local service and product providers might get benefit from the market development and kept their business growth.

StormEye as an example, they were a local start-up supported by Hong Kong Cyberport incubation program, they faced difficulty in developing new sales lead as they didn't understand what the client needs (Capital, 2020). Marco and Windham stated that they were looking for new tech angles to attract new clients (Capital, 2020). This study can help them to understand what was the client needs.

1.7.3. Contribution to industry

Cybersecurity was one of the most important topics to concern in this high digitalise business environment. The product and service development

required the most up-to-date front line information as the threat from hackers was changing every day (Kaspersky, 2021). To encourage more SMEs using their service and product, there would collect different information by the network traffic generated by SMEs. A large amount of traffic would provide important sources of threat for service and product providers to update their threat database and lead to more secure protection to their service provided.

1.8. Structure overview

this research performed a classic 5 chapters structure in the dissertation in order to best demonstrated this MBA program study target.

Chapter 1 was the introduction which provides essential information for readers to understand the research topic and the rationale behind. Some definition of terms and concepts stated in this chapter. The main research question with objective were also be discussed in this chapter.

Chapter 2 was literature review, there was 4 major research areas. The main focus designed according to the review result. The first review highlight is on research method, review article and peer reviewed research which provide some insights to find out how this discretion questionnaire should design. The second review highlight focused on different factors, as there are many factors would affect purchase intention in certain market. This review aimed to find out some of the most important factors we should focus on. At the end of the chapter, there would be a list of hypotheses formed in the process of literature review.

Chapter 3 discussed the methodology of this dissertation from the result of the literature review. This chapter provided a clear plan for readers to understand how specific studies were valid to answer the specific research questions. Next, research methods such as which type of data and target segment classification would be discussed. To answer the research questions there were discussions on

major factors that this dissertation concerned, and how the factors would be construct along the research and analysis. Each of the hypotheses examined and properly define with literature support. After the hypotheses discussion, there we re information that stated the statistical support on in the proposed questionnaire questions. At the end of the chapter, there were lists of questions used in the questionnaire provided with proper explanation.

Chapter 4 is the chapter performed a data analysis on the survey, SPSS would be used as a main analysis tools. Different methods would be consider according to result of literature review. At the end of this chapter, the result of the factors that affect SMEs purchase intention were stated.

Chapter 5 was the chapter to conclude the assessment of the dissertation. Suggestions for industry players and further research were elaborated in this chapter.

1.9. Summary

This dissertation introduction provided essential background knowledge of the research topic, by highlighting key industry trends, like market size and recent trend of growth. These showed the importance of the research and the research rationale. The research aimed to provide supports to answer three research questions and its objective accordingly. Next, there was a showcase that explained overall roadmap of the process and method needed to be taken to achieve the result. In the next chapter, literature review chapter would identify academic supports of different factors and components that used to answer the research questions.

2. Literature review

This part of the dissertation explored a wide range of literatures that related to the research topic to find a suitable angle on how should the topic be better discussed. After that, three factors that affected purchase intention were discussed. The discussed factors also helped to form the hypotheses at the end of this literature review session.

During the research, there were lack of literatures focus on purchasing behaviour on cybersecurity services and products. As a result, this review section reviewed the general review purchase intention.

2.1.Perceived value

The terms perceived value had been mentioned in an article in 1960 (Levitt, 1960), it defined as base functions of a products. Despite there were lots of researches under the topic, the concept of perceived value has often being confused with other similar words. Khalifa (2004) stated that the concept has become one of the most overused and misused concepts in social sciences field and in the management literature.

2.1.1.Definition

Berry and Yadav (1996) pointed out that perceived value was described as the main consideration when purchasing a product or service. The following table summaries some of the definitions made by different literatures.

Table 2.1.1 Definition of perceived value

Literture	Definition
Zeithaml (1988)	A list of consideration and comparison between the value and the costs they need to pay
Sheth, Newman and Gross (1991)	The perceived value appears when customers are considering their purchase on a service or product
Berry and Yadav (1994)	It is the main consideration when purchasing a product or service
Kotler (1994)	The value can be gain socially
Woodruff (1997)	Customers overall assessment of a perception of what is received and given by providers
Snoj, Aleksandra,and Mumel (2004).	Perceived value can be tangible and intangible

Sources : Table construct by writer

As showed in table 2.1.1, Zeithaml (1988) stated that the perceived value was not a textbook theory, but a list of considerations and comparisons between the value and the costs they need to pay. Consumers took all the sub-value in to their consideration, such as internal and external value toward the service or product. As a result, There were particle usage in the real-world.

Kotler (1994) suggested the value can be gain socially. It means that individual or group could fulfil their needs and desire by share value among them. It also suggested that when consumers choosing products or services, they would always try to reach the highest value with the lowest cost (Kotler, 1994).

Woodruff (1997) defined that value is customers overall assessment of a perception of what was received and given by providers. It also mentioned that the perceived value was unique and personal (Woodruff, 1997). According to the definition, consumers would have different considerations when they were given different

scenarios. The same product or service would have changed its value with the usage of the consumers.

Snoj, Aleksandra and Mumel (2004) gave a different dimensions to perceived value that were tangible and intangible. Sheth, Newman and Gross (1991) did a comprehensive summary research and study on this topic. They suggested that the perceived value appears when customers were considering their purchase on a services or product and it can divided into five constructs. They brought up a clear view on how study could effectively measures and increases the value of a product.

2.1.2. Measurement

Different literatures pointed out some different angles of perceived value, some of them suggested that the perceived value should be divided into several elements.

Table 2.1.2 Measurement of perceived value

Literture	Definition
Sheth et al. (1991)	1. Functional value 2. Social value 3. Emotional value 4. Epistemic value 5. Conditional value
Hallowell (1996)	1. Economic benefit 2. Perceived benefit 3. Emotional benefit
Holbrook (1999)	1. Interactive 2. Relativistic 3. Preferential 4. Experience
Parasuraman and Grewal (2000)	1. Acquisition value 2. Transaction value 3. In-use value 4. Redemption value
Sweeney and Soutar (2001)	1. Emotional value 2. Social value 3. Functional value (price/value for money) 4. Functional value (performance/ quality)
Petrick and Backman (2002)	1. Quality 2. Monetary Value 3. Behavioural price 4. Emotional response 5. Reputation

Sources : Table construct by writer

Table 2.1.2 listed some of the measurement. Sheth et al. (1991) said that the perceived value was construct by five elements which included functional value, social value, emotional value, epistemic value and conditional value.

Functional value should be defined as the actual usage of the product. This value was presumed to be the major driver of the customer choice and can be measured on a serious of choice attributes.

Holbrook (1999) elaborated value as consumer value and proposed a framework of the nature and types of consumer value, which included interactive, relativistic, preferential and experience.

Social value means a service or product helps customers to enhance their social acceptance when using the product or service (Holbrook, 1999). Social acceptance could further expend as the sense of belonging to a specific groups of people. Customers would focus more on social value if a product is visible or can be share to others, like jewellery and video games.

Emotional value can be interpreted as the feeling that associated with emotional responses and it is usually intangible (Holbrook, 1999). In some cases, emotional values can be tangible, for example souvenirs in tourist attraction point.

Epistemic value is described as the value fulfil customers curiosity, satisfy and desire for knowledge (Holbrook, 1999). A customer might purchase similar products with new brands or new taste. The value can be measured by questionnaire items that referring to curiosity, knowledge and novelty.

Conditional value related to a situation or a serious of circumstance to the customers (Holbrook, 1999). The conditional value can related with different kinds of circumstances including physical or social contingencies which enhance its functional or social value of a product or service.

Parasuraman and Grewal (2000) proposed that there are four constructs, including acquisition value, transaction value, in-use value and redemption value.

Acquisition value described as the consumer believe they gain by acquiring a product or service. Transaction value means the happiness of getting a good deal. In-use value can interpreted as the actual usage value from using a product or service. Redemption value represented the remind value when a product in the end-of life state. Those values are used to study the relationship between customers loyalty, reliability, product quality and price.

2.1.3.Summary

All the above values mentioned are independence in most cases, customers were likely to accept less of one of the above values to obtain more of the rest (Seth et al.,1991). At the same time, some customers would consider all five values, when the product or service is a major decision to make, like buying the first car or renting an office for his new start-up. After the overview of literature above, Seth's (1991) proposed five ways of construct would be used in the following discussion.

2.2. Perceived risk

The concept of perceived risk was first presented in the 1960s, Bauer (1960) described perceived risk as a sense of unpleasant feeling that customers would feel before they took the action to purchase a service and/or product. The feeling came from uncertainty some factor of risk. Since the first introduction, the researcher almost obsessed with exploring the concept. In this part of the review, we looked into some concept worth discussing.

2.2.1.Definition

The perceived risk appeared whenever consumers could not subjectively make their purchase decisions. Cox (1967) divided the risk into two parts, before purchase and after purchase. Consumers would have different feelings in these two parts. Before purchase, consumers could only guess what would happen and hope it would not happen. After purchase, consumers would see and feel the risk happened, which made them subjectively evaluate the consequences. The following table surmises some of the definitions made by different pieces of literature.

Table 2.2.1 Definition of perceived risk

Literture	Definition
Bauer (1960)	A sense of unpleasant feeling
Cox (1967)	Before purchase, consumer can only guess what would happen and hope it would not happen. After purchase, consumer can see and feel the risk happened
Cunningham (1967)	The risk is related to the chances of happening, another parts is related to the consequence of the damaged caused
Stone and Grønhaug (1993)	The expected loss of each purchase, the higher the expectation, the perceived risk would be higher
Sheth and Parvatiyar (1995)	The greater perceived risk, the easier for consumer to manifest behaviour
Sweeney et al. (1999)	The relationship between perceived risk, value and quality is negative related
Tzavlopoulos et al. (2019)	The higher the perceived risk, the more likely the customer would play their second visit to the same service

Sources : Table construct by writer

As Showed in table 2.2.1, Cunningham (1967) added two more parts to the definition. He suggested one part of the risk is related to the chances of happening, another part is related to the consequence of the damage caused.

Murray and Schlachter (1990) examined the perceived risk in the area of service marketing, showing evidence of linkage to such topics. Einhorn and Hogart (1985) proposed the following factor that builds perceived risk. They started by measuring the expected product or service damage with how likely it would happen. Following by if the damage occurred, would it do the same damage as expected. Last to examine there any unforeseen damages and ask if the damage is controllable.

Stone and Grønhaug (1993) pointed out that the perceived risk is talking about the expected loss of each purchase, the higher the expectation, the higher the perceived risk.

Some other studies about the perceived risk suggested the relationship between perceived risk, value and quality are negative (Sweeney et al., 1999). A study by Sheth and Parvatiyar (1995) shared the point of view that the greater perceived risk, the easier for consumers to manifest behaviour.

Tzavlopoulos et al. (2019) suggested that the higher the perceived risk, the more likely customers would play their second visit to the same service provider that fulfil their satisfaction. In contrast, if the service or product has a relativity low perceived risk, customers would be more likely to switch their option to other product or service providers when the option has better quality or at a more attractive price.

2.2.2. Measurement

There were different ways to measure which involved different constructs to form perceived risk. The following table summarised some constructions.

Table 2.2.2 Measurement of perceived risk

Literture	Definition
Cox (1967)	1. Financial 2. Social-psychological
Perry and Hamm (1969)	1. Psychological consequences 2. Social consequences
Roselius (1971)	1. Time loss 2. Hazard loss 3. Ego loss 4. Money loss
Jacoby and Kaplan (1972)	1. Financial Risk 2. Functional/Performance Risk 3. Physical Risk 4. Psychological Risk 5. Social Risk
Peter and Tarpey (1975)	1. Financial Risk 2. Functional/Performance Risk 3. Physical Risk 4. Psychological Risk 5. Social Risk 6. Time Risk
Stone and Grønhaug (1993)	1. Time Risk 2. Privacy Risk 3. Financial Risk 4. Functional Risk 5. Psychological Risk 6. Physical Risk

Sources : Table construct by writer

As listed in table 2.2.2, Cox (1967) suggested the perceived risk included financial risk and social psychological risk, which meant putting the perceived risk into two constructs. Different literature adopted the concept. Jacoby and Kaplan (1972) proposed five dimensions categorised construct in the perceived risk. The constructs are performance risk, financial risk, time risk, social risk, psychological risk and privacy risk. Peter and Tarpey (1975) added time risk in the measurement.

According to Stone and Grønhaug (1993), there was a full discussion on all risks that would be used in the study. As this study was about cybersecurity, the physical risk would not be discussed.

Time risk defined as the time consume may lose when making the purchase decision, also included the time to use the product and/or service. We can explain the concept of time invested as the time customers spent to accomplish a specific goal (Carter. and Belanger, 2005). The time risk might appear in different steps in the purchasing process. The communication lead time would be the most significant in this researches.

Privacy risk included the potential loss of the right to control their personal information. In other words, the risk described the protection level of a product and/or service categorised the risk of losing their self-identity as privacy risk (Aimeur and Schönfeld, 2011) . The sense of privacy risk would be developed and identified when there are different managerial and technological tools are implemented to protect customers during the purchasing process and which gain their trust to lower privacy risk (Pavlou and Reichiert, 2004).

Financial risk included the potential of paying extra cost apart from the initial cost and also the potential loss due to fraud (Grewal, Gotlieb and Marmorstein 1994). Zeilke and Dobbelstein (2007) explained financial risk is the chance of a monetary loss from a poor purchase. The extended meaning of the financial risk is share as the product's quality does not match its price (Schiffman and Kanuk, 2000).

Functional risk is further associated with the possibility of product malfunctioning or not work as it was designed and advertised to (Gerwal et al., 1994). The risk can also be described as functional risk and expressed as the uncertainty of products or services purchased would not meet consumers expectation.

Psychological risk is the potential loss of self-esteem after purchasing a product (Mitchell, 1992). A related concept suggested by Shareef et al. (2018) further elaborated the concept of psychological risk as anxiety risk. A similar feeling would appear in e-commerce purchasing processes which demonstrated the feeling produced in customers mind to certain degrees (Anderson et al., 2008). We can also put the state of consumer's disappointment in making a bad selection of products as a psychological risk (Ueltschy et al, 2004).

2.2.3. Summary

After this literature review, there was a larger range of literature thought differently on preceded risk. Stone and Gronhaug (1993) pointed that the perceived risk would adopt in this dissertation. Their point of perceived risk provided a suitable discussion ground for further data analysis. As this study was about cybersecurity, the service and product usually wouldn't involve daily usage of hardware, the physical risk would not be discussed.

2.3.Word of mouth (WOM)

There are some studies provided factors forming the word of mouth, as the volume of information of a product can be relatively high for one product, consumers cannot read all the comment or statement posted.

2.3.1.Definition

The word Word of Month (WoM), is defined as how consumers share conversation about a product and/or service experiences (Sen and Lerman, 2007).

Table 2.3.1 Definition of WoM

Literture	Definition
Arndt (1967)	The informal communication on product information
Richins (1984)	The information exchange initial by consumers
Westbrook (1987)	An informal communication between consumers and the company
Bone (1995)	WoM contribute toward consumer purchase behaviour
Balasubramanian and Mahajan (2001)	WOM appear in different forum, comment section under specific online shop or products
Bickart and Schindler (2001)	WoM is convenient and perceived to have higher credibility
Hennig-Thurau et al. (2004)	The statement of comment made in a publicly available platform about a product or service
Dellarocas and Narayan (2006)	WOM behaviors satisfied their need to share something important with other consumers
Sen and Lerman, (2007)	How consumers share conversation about a product or service experience

Sources : Table construct by writer

As shown in table 2.3.1, the earlier definition was defined by Arndt (1967), which meant informal communication on product information. Richins (1984) used another point of view to describe WoM, which proposed WoM was the information exchange process that initial by consumers. Westbrook (1987)

suggested that all informal interactions between companies and consumers can be one of WoM behaviour. Bone (1995) stated that WoM contributed toward consumers purchase behaviours.

Hennig-Thurau et al. (2004) gave us a definition of WoM as all comments gave by potential, actual or former consumers toward a product and/or service via internet platforms.

With technological platforms taking over the marketing channels, the meaning of word of mouth expanded to the internet and defined as a statement of comments made on a publicly available platform about a product and/or service and the comment can be positive or negative (Hennig-Thurau et al., 2004).

2.3.2. Measurement

There are numerous researches suggested that WoM played an important role in forming the purchasing behaviour of a customer. Studies showed customers would intend to be involved in the process of contributing to WoM because of the desire to help others make better purchase decisions and avoid unwanted experiences (Dellarocas and Narayan, 2006). The summarised review has listed in table 2.1.3 for further discussion.

Table 2.3.2 Measurement of WoM

Literture	Measurement
Hovland, Janis and Kelley (1953)	1. The source of information 2. The quality of information 3. The receiver factor
Gilly et al. (1998)	1. The authoritative of source 2. The personal character of source and receiver 3. The receiver preference of WoM
Silverman (2001)	1. Informal communication 2. Noncommercial comment 3. The flow of information exchanged
Sweeney, Soutar and Mazzarol (2008)	1. Personal 2. Interpersonal 3. Message characteristics 4. Situational characteristics
Goyette et. al (2010)	1. The intensity of the discussion, 2. The positive valence of the company, 3. The negative valance of the company, 4. The content discussed in the conversation

Sources : Table construct by writer

As listed in 2.3.2, Hovland, Janis & Kelley (1953) suggested WoM can be measured by the source of information, the quality of information and the receiver factors which may lead to a long discussion after that. Gilly et al. (1998) suggested a similar concept with the authoritative of source, the personal character of source and receiver and the receiver preference to WoM.

Goyette et. al (2010) listed out a range of measurement on WoM and suggested the WoM can be measured by the intensity of the discussion, the positive valence of the company, the negative valance of the company and the content discussed in a conversation.

Other literature like Silverman (2001) suggested WoM should measure informal communication, non-commercial comment and the flow of information exchanged. Sweeney, Soutar and Mazzarol (2008) proposed that

WoM should be measured by personal, interpersonal, message characteristics and Situational characteristics.

2.3.3.Summary

There were different definitions of WoM that might consider to include in this study. Dodds, Monroe and Grewal (1991) point of view was the one using in the following discussion. The measurements were suitable for performing the survey via electronic methods, as there was less information needed to provide to participants.

2.4.Purchase intention

When performing a wide range of literature review, researchers reference a wide range of articles and studies about factors that affect customer purchase behaviour and intention.

2.4.1.Definition

Ajzen and Fishbein (1975) stated that purchase intention is a prediction of the chance that customers would buy a product or not and the intention is a subjective concept. Dodds, Monroe and Grewal (1991) described the intention included elements like satisfaction toward a product and/or service. Mazumdar and Monroe (1992) pointed out that the intention should be a subjective feeling but not an objective feeling, which can be influenced by external factors.

Table 2.4.1 Definition of purchase intention

Literture	Definition
Ajzen and Fishbein (1975)	A prediction of the chance to purchase
Dodds et al. (1991)	A subjective feeling to choose a service or product
Mazumdar and Monroe (1992)	A personal feeling that might affect by external factor
Keller (1993)	A preference of consumer to purchase a product or service
Morinez et al.(2007)	A situation when a consumer more willing to buy a certain product in a particular situation
Shah et al. (2012)	A kind of decision making process behind consumer's mind

Sources : Table construct by writer

Table 2.4.1 listed some of the definitions of purchase intention. Purchase intention defined as the preference of consumer to buy a product or service (Keller, 1993). To further explains, it means the evaluation before customers decided to do the purchase. Shah et al. (2012) described purchase intention as a decision-making process behind consumer's mind when they buy a particular brand. A different view from Morinez et al.(2007) suggested that the purchase intention was a situation when a consumer more willing to buy a certain product in a particular situation.

Purchase intention discussed above can be summarised as a subjective feeling that measurement of the chance of a consumer buying a specific product and/or service.

2.4.2. Measurement

Different literature suggested different methods to measure purchase intention from customers. Table 2.4.2 listed some of the literature suggestions by the year published.

Table 2.4.2 Measurement of purchase intention

Literture	Measurement
Zeithaml (1988)	1. Are they considering to purchase 2. Do they want to purchase 3. Are they going to purchase
Dodds, Monroe and Grewal (1991)	1. Would they consider to buy 2. Would they buy 3. Would they recommend to others
Heskett et al. (1994)	1. Retention rate 2. Re-visit rate 3. Recommandation rate
Schiffman and kanuk (2000)	1. They would purchase 2. They are likely to purchase 3. They are not sure would they purchase 4. They are not likely to purchase 5. They would not purchase
Zia (2012)	1. Website quality 2. Commitment factor 3. Customer service 4. Security

Sources : Table construct by writer

Dodds, Monroe and Grewal (1991) suggested asking three target questions: would they consider buying, would they buy, would they recommend to others, that could measure the level of purchase intention. Zeithaml (1988) used different approaches to measure the level of intention by asking: are they considering, willing or might buy a product. Heskett et al. (1994) proposed a statistical measurement tool like customer retention rate, re-visit rate and recommendation rate to calculate intention level. Schiffman and Kanuk (2000) developed another measurement tool base on the Likert scale (Likert, 1932). The tool used a 5-point-scale to measure the purchase

intention of an audience. Zia (2012) did an investigation on the main factor which would influence customer behaviour and stated that overall website quality, customer service, commitment and security are the most important factors when customers consider their purchase decision.

2.4.3.Summary

The purchase intention in this study referenced the point of view and measurement by Dodds, Monroe and Grewal (1991) as the measurement method have a wider range of answer. The questions included the “Would they consider to buy?”, “ Would they buy?” and “Would they recommend to others?”.

2.5.Relationship with purchase intention

From the point of view by different literature, different factors affected the purchase intention of customers. This session provided a detailed explanation of the relationship between the mentioned factors.

2.5.1. Relationship between perceived value and purchase intention

Payne and Holt (2001) described that perceived value is one of the factors that related to consumer’s purchasing intention and a product. Tung (2013) provided a conclusion that perceived value and purchase intention has a strong positive relationship. Dodds, Monroe and Grewal (1991) proposed a conceptual model in willingness to buy and a linkage between perceived quality, evaluation and choice has been found. Similar to the statement previous made, the perception of value would directly turn in to willingness to buy (Dodds, Monroe and Grewal, 1991).

2.5.2. Relationship between perceived risk and purchase intention

There is a weak direct relationship between perceived risk and purchase intention found in the Malaysian e-commerce sector (Mei, Ling and Piew,

2012). However, when purchasing online airline tickets, Kim, Kim and Leong (2005) found there was a strong negative relationship. Kim, Lennon (2013) proposed similar results that customer purchase intention would decrease when perceived risk is relatively high.

2.5.3. Relationship between WOM and purchase intention

Sa'ait, Kanyan and Nazrin (2016) provided a good view on a strong positive relationship between WOM and purchase intention as it is one of the most effective ways to influence other purchase intention. The same result appeared in the local culinary business sector in the Indonesian SMEs market (Hamdani and Maulani 2018).

2.6. Literature review summary

In previous literature research, three independent variables that proposed to affect purchase intentions of SMEs cybersecurity were identified, they were perceived value, perceived risk and WoM.

Different literature's point of view on the above three independent variables and one dependant variable had been discussed. After the discussion, the relationship of each factor with the dependant variable has been reviewed. There were different research conducted by literature that suggested that the perceived value and WoM formed a positive relationship with purchase intention and the perceived risk negativity affect the purchase intention.

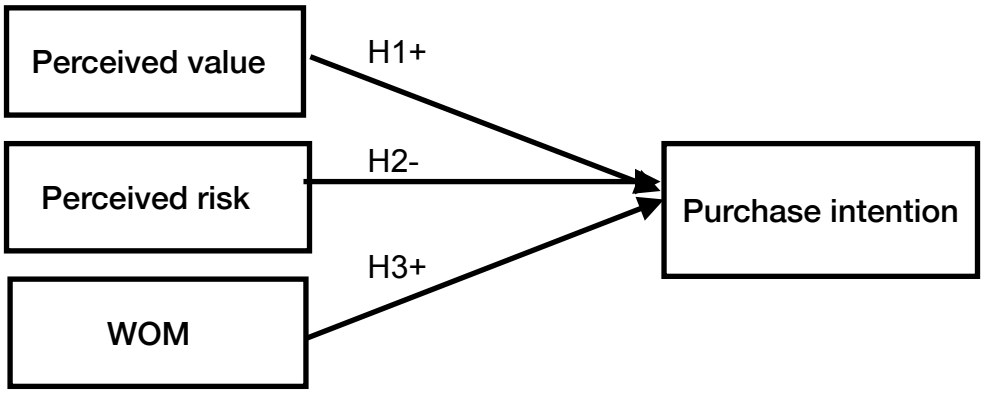
Furthermore, among all point of view studied in this chapter, many of them promised some factors to construct those factors. Perceived values were suggested to have five constructs (Seth et al.,1991; Stone and Gronhaug, 1993). David, Bozkurt and Russo (2019) stated some ways of measuring WOM.

3. Methodology

This chapter further developed the research questions by using some of the basic concepts explored in chapter two. Firstly the hypotheses were introduced. Secondly, a questionnaire and research framework would be discussed. The result of the hypotheses discussed in the next chapter.

3.1.Research framework

Figure 3.1.1 Research framework



Sources : Figure construct by writer

The research framework, shown in figure 3.1.1, was drafted according to the research rationale and objective in chapter 1 and the literature review in the last chapter. Perceived value, perceived risk and WOM are independent variables while the purchase intention is the dependant variable. The following session discussed their relationship.

3.2.Hypotheses

After the literature review, this dissertation suggested the hypotheses below.

H1 : Perceived value positively influence the purchase intention of SME in purchasing cybersecurity products or services (Payne and Holt, 2001).

H2 : Perceived risk negatively influence the purchase intention of SME in purchasing cybersecurity products or services (Kim, Kim and Leong, 2005).

H3 : WOM positively influence the purchase intention of SME in purchasing cybersecurity products or services (Sa'ait, Kanyan and Nazrin 2016).

3.3.Research type

There were two common methods of research that is qualitative and quantitative research. These two research method would be used in this dissertation and the result discussed in different chapter accordingly.

Qualitative research aimed to research by looking into a problem without an actual number (Emmel, 2013; Bernard, 2017). Not using number doesn't mean qualitative doesn't apply in the real world. These methods put focus on relating different theories and develop an academic system by different means like literature review and second-hand data analysis. This method required the researcher to clearly understand the research topic and form an opinion by cross-reference a wide range of peer-reviewed paper written by experts from their specialities (Queirós et al., 2017). Other qualitative research methods included focus groups interview and experimental research.

The quantitative research method adopted statistical analysis to study social phenomena (Brannen, 2017). There were some common applications in quantitive research, for example, a questionnaire would be used to collect comments and point of views from a specific target audience; experimental was eliminating the influence of disturbing variables when collecting data; structured observation provided an event or a series of event that observe participant react and behave to study (Rahman, 2017).

This research involved both qualitative quantitative research methods.

3.3.1.Data type

For qualitative research, this dissertation used literature review and analyses second-hand data. For quantitative research methods included a questionnaire that collected first-hand data that helped understand the purchase intention for SME business in Hong Kong towards cybersecurity products.

3.4. Research target

The research question of this research was the purchase intention for SME business in Hong Kong towards cybersecurity products. Most of the company nowadays used computer system and network to process clients request and daily operation, there were no differences in terms of cybersecurity risk, the research object was the SME in Hong Kong of any industry. The questionnaire would be answered by the management of SMEs in Hong Kong.

3.4.1.Sampling method

Blumberg, Cooper and Schindler (2014) stated that sampling is the choice of sub-set of examples of a large number of units the can interpret the choice of the population. When performing research with a large population, two sampling methods can effectively draw a sample from a large population, that was probability sampling and non-probability sampling. Probability sampling picked samples from the whole population, usually required the researcher had access to the full list of the population. In this dissertation, a non-probability sampling method would be used. There were 4 major sampling methods for non-probability sampling, convenience sampling, quota sampling, snowball sampling and purposeful sampling (Cochran, 1977, Setia, 2016).

Convenience sampling helped the researcher to do sampling quick by access the easiest to reach the target. Quota sampling picked a sample within a specific segment of the whole population, this method first placed the entire population into several groups. purposeful. Purposeful sampling was the methods that the targets would be picked by the researcher by their judgement. The Snowball sampling method would require the researcher to reach the first tier of their targets and leverage their network to reach more of the samples until the sampling size target met. Snowball sampling was suitable for the list of population is not available.

To understand the purchase intention of SMEs in Hong Kong, the best choice is to send a survey to all SMEs in Hong Kong. The total number of SMEs in Hong Kong was over 340,000, which was almost impossible to ask all the companies on this research considering the resources involved in this dissertation. Therefore, the snowball sampling method would be used to support this study.

The upcoming questionnaire used Google form as a tool to collect feedback from SMEs managements response.

3.4.2. Sampling size

In the most recent data, there were over 350,000 SMEs in Hong Kong (SUCCESS HKSAR, 2021). The sampling size was calculated by the formulation below (Cochran, 1977).

$$n = [Z^2 * p * (1 - p)]/e^2$$

Where n is sample size, 1- e was the confidence level and p is the sample ratio. Confidence level mean the probability of samples will fall in to this

sample range. When confidence level set to 95%, e = 0.05, z = 1.96 and p = 0.5.

The equation was

$$n = [1.96^2 * 0.5 * (1 - 0.5)]/0.05^2$$

$$n = 384$$

The number of samples targeted to collect would be 384 under Cochran (1977) suggestion.

Green (1991) suggested an alternative method to calculate the sample size. The method had considered the sampling size calculation for multiple regression like the case in this surveys.

The equation is :

$$n > 50 + 8p$$

Where n was the sample size, p is the number of predictors involved in the calculation process. This research defines three hypotheses, which are perceived value, perceived risk and WoM.

The equation became :

$$n > 50 + 8(3)$$

$$n > 74$$

The suggested sample size is larger than 74 according to Green (1991) suggestion.

Combining both sampling methods, the most ideal target sample number in this survey was larger than 384.

This survey designed to collect purchase intention on cybersecurity product or service of SMEs in Hong Kong. The questionnaire filtered participant in serval way to achieve the goal. In the stage of invitation, the invitation message specific defined the audience. The audience limited to who has the

right to make the discussion on buying new cybersecurity service or products. As the survey is anonymous which aim to protect the participants' identity, there was no method to prevent different participants fill in the survey on behalf of the same company.

To ensure the participants' company is SMEs, there is an introduction and question to ask whether their company size falls into the SMEs category. If their company doesn't, they cannot continue the surveys.

3.5.Analysis methods

The questionnaire result was analysed using SPSS version 27. The following section had discussed some critical tools.

3.5.1. Descriptive statistics

Descriptive statistics used to describe the data in many ways (Bickel and Lehmann, 2012). The tools measures of central tendency included the mean and average, at the same time measures of variability include standard deviation. This study used descriptive statistics to present data.

Means and standard deviation were used to describe the data collected from the survey. Means reflected the targets opinion towards the questions asked. In some questions, there was a comparison between means. Standard deviation showed the diversity of the answer, the ideal value of standard deviation is less than 1. The larger the value, the more diverse the data was.

3.5.2. Reliability test

To ensure the survey was properly developed and the data collection can represent a certain level of the truth, reliability test considered one of the most important tests every survey should pass (Fink and Litwin, 1995). Cuieford (1965) set up a scale to define the internal consistency of the

survey questions. In this reliability test, Cronbach's alpha methods would be used.

Table 3.5.1 Relationship between Cronbach's alpha and internal consistency

Internal consistency of the scope	Cronbach's alpha
Excellent	$0.9 \leq \alpha$
Good	$0.8 \leq \alpha < 0.9$
Acceptable	$0.7 \leq \alpha < 0.8$
Questionable	$0.6 \leq \alpha < 0.7$
Poor	$0.5 \leq \alpha < 0.6$
Unacceptable	$\alpha < 0.5$

Sources : Cronbach (1951)

Table 3.5.1 showed the relationship between Cronbach's alpha and internal consistency, the research question had to reach 0.7 to prove the internal consistency.

3.6. Correlation

Kafle (2019) and Aboubaima et al. (2020) pointed out Pearson correlation is a good tool to analyses the correlation relationship between two or more variable in the same data set. The tool was used to analyse the relationship among three variable and one independent variable.

Table 3.6.1 Relationship between Pearson coefficient and r

Pearson coefficient	Relationship
r = 1	Perfect positive relationship
0.7 ≤ r < 1	Strong positive linear relationship
0.3 ≤ r < 0.7	Moderate positive linear relationship
0 < r < 0.3	Weak positive linear relationship
r = 0	No linear relationship
0 > r > - 0.3	Weak negative linear relationship
-0.3 ≥ r > -0.7	Moderate negative linear relationship
-0.7 ≥ r > -1	Strong negative linear relationship
r = -1	Perfect negative relationship

Sources : Pearson (1938)

Table 3.6.1 listed of the meaning of the relationship according to a different value in the range 1 to -1. As our variable content both positive and negative relationship, the result of the survey fell into this range.

3.7. Regression

Regression analysis was a statistical tool used to estimate the relationship between a dependent variable and independent variables (Brook and Arnold, 2018). There were three sets of regression, linear regression, multiple linear regression and non-linear regression.

Linear regression meant to estimate the relationship with the single dependent variable and single independent(Long and Ervin, 2000). Multiple linear regression was used to handle the estimation of more than one independent variable with a single dependent variable (Baños et al.,2019).

$$Y = a + bX_1 + cX_2 + dX_3 + \ldots + \epsilon$$

Where Y = Dependent variable, X_1 ,X_2 , X_3 = dependent variable, a = coefficient, b,c,d = regression coefficient, ϵ = error.

3.8. Questionnaire design

Related to the research framework of this study and literature reviewing, the construct of dependant variable would be discussed in the following sections (Baños et al., 2019). For easy reference and process using SPSS, this study assigned a number for each construct.

3.8.1. Screening questions

The questions confirming the participants' suitability to join the survey was placed at question 1. The question asked about the number of employees and the industry of the company they worked in.

Table 3.8.1 Screening questions

No.	Number of employee	Industry
1	1-49	Manufacturing firms
2	over 50	Manufacturing firms
3	1-99	Non-manufacturing firms
4	over 100	Non-manufacturing firms

Sources : Table construct by writer

The target of the survey were those working in SMEs in Hong Kong. For participants who answered answer number 2 or 4, the survey came to the end as showed in table 3.8.1.

3.8.2. Perceived value

Related to Chapter 2.1, this research took Seth et al.(1991) point of view to design the questionnaire. Seth et al. (1991) suggested 5 constructs from perceived value.

Table 3.8.2 Questions on perceived value

	When I purchase a cybersecurity product/ service for my company, I expect, the product/service is/are/will ：	
Functional Value	VF1	Ease to use.
	VF2	Increase the productivity of my company.
	VF3	Enhance our service quality.
Social value	VS1	Increase our acceptance by clients.
	VS2	Differentiate our product/ service from the competitors.
	VS3	Build a positive image.
Emotional value	VE1	Provide a safety feeling.
	VE2	Provide a joyful experience.
	VE3	Provide a new service environment.
	When I purchase a cybersecurity product/ service for my company:	
Epistemic value	VEP1	I am willing to try a new product/service
	VEP2	It will satisfy my curiosity.
	VEP3	I am willing to try new auxiliary product/ service.
Conditional Value	VC1	If my company was being hacked, we will be more willing to try a cybersecurity product/ service.
	VC2	If there is a promotions campaign, we will be more willing to try.
	VC3	If there is news about the hacking of companies, we will be more willing to try.

Sources : Table construct by writer

As showed in table 3.8.2, there were fifteen questions asking the perceived value in the questionnaire.

3.8.3.Perceived risk

Related to Chapter 2.2, this research took Stone and Grønhaug (1993) point of view to design the questionnaire. There were 6 constructs that form perceived risk.

Table 3.8.3 Question on perceived risk

	When I purchase a cybersecurity product/ service for my company, I am afraid I will / there is:	
Time Risk	RT1	Spend lots of time to look for a suitable product/ service.
	RT2	Take me lots of time to communicate with the supplier.
	RT3	Take lots of time to install.
	RT4	Needs lots of time to learn how to use.
Privacy Risk	RP1	Share my company information to others without our consent.
	RP2	Our data will be out of control after installation.
	RP3	Our client's data will be stolen.
	RP4	Insured on the online payment method
Financial Risk	RF1	Pay a higher initial cost than the market price.
	RF2	Pay a higher maintenance cost than the market price
	RF3	Unexpected huge surcharge on additional service.
	RF4	Pay more than the market price.
Functional Risk	RFC1	Insufficient in technical support while facing a technical issue.
	RFC2	Different product/ service in the promotion martial.
	RFC3	Insufficient network protection of my company.
	RFC4	Difficult to compare the product/service before purchase.
Psychological Risk	RPC1	Dislike the product/service
	RPC2	Have an unpleasant feeling when my company is using the product/service.
	RPC3	I will feel the anxiety to install the product/service.

Sources : Table construct by writer

To simplify the analysis process, the questions used a reverse format. All the questions were asked in negative wordings as showed as 3.8.3.

3.8.4.Word of mouth

According to Dodds, Monroe and Grewal (1991), there were 4 questions exploring the relationship in the objective of this research.

Table 3.5.2 Question on WoM

	When I purchase cyber security product/service for my company,	
WOM	W1	I will seek advice from my friends.
	W2	I will seek advice from my business partners.
	W3	I trust the comments from different social media.
	W4	I trust the user comments from the official website of the product/ service provider.

Sources : Table construct by writer

As showed in table 3.5.2, there were four questions asking the WoM in the questionnaire.

3.8.5.Purchase intention

After the discussion on the literature review, this research will use the reference from Dodds, Monroe and Grewal (1991) in the questionnaire questions.

Table 3.5.3 Question on Purchase intention

Purchase intention	PI1	I will purchase a cybersecurity product in the near future.
	PI2	I will recommend my friends or partners to purchase cybersecurity product/service in the near future.
	PI3	I will purchase a cybersecurity product in the near future, even when the price goes up.

Sources : Table construct by writer

As showed in table 3.5.3, there were three questions asking the purchase intention in the questionnaire.

3.9.Survey

In the survey, there were be five options for most of the question which is the Likert scale (Likert, 1932). From 1-5, that meant strongly disagree, partly disagree, neutral, partly agree and strongly agree.

After drafting the questionnaire, there are different process and tools had been used to improve the accuracy of the data to be collected. In the below section, we will discuss the focus group test, pilot test and other tools in SPSS that show the survey results are correct.

3.9.1.Focus group

O'Brien (1993) suggested that focus groups help develop a quantitative survey in two ways. Focus group can provide an idea of how to improve the word choice and content to fit the style of the targeted audience. These provided a better understanding and better delivery of the key message of the questionnaire and gain better results.

During the focus group discussion, participants suggested some changes to the numbering methods made confusion when answering the questions. Some wording, like question 4, which was " I will believe the comments from different social media", was changed to " I trust the comments from different social media".

Table 3.9.1 Focus group study result

Questions	Before	After	Improvement
4	I will believe the comments from different social media.	I trust the comments from different social media.	Deliver the message in. a more direct way.
8	The product/service will take lots of time to install.	Take lots of time to install.	Shorten the sentence and make it easier to read
11	Once we installed the product/ service, our data will be out of control.	Our data will be out of control after installation	Shorten the sentence and make it easier to read
18	My company will not get technical support while facing a technical issue.	Insufficient in technical support while facing a technical issue.	Replace “will not get” by “insufficient” to provide more accurate meaning
31	The product/ service brings a sense of safety to my company	Provide a safety feeling.	Use direct sentence to send clear message.
33	My company staff will feel confident about network safety.	Provide a new service environment.	Replace the staff’s feeling using the new service environment.

Sources : Table construct by writer

In this surveys, there was one round of focus group performed. The six focus group participants were members of the Junior Chamber of Commerce, they provided some key improvements to the survey questions. For example, they suggest replacing most of the question with more simple wordings to make them more reader-friendly. Table 3.9.1 showed some of the examples of the changes.

3.9.2. Pilot test

A pilot test was an invaluable component of survey research that helped researcher avoid error, reflected their questions and wording before official launch (Rothgeb, 2008). The pilot test could perform in different research, for example, experimental research would do several rounds of tests to test if the briefing notes were clear and easy to understand base on the educational background of the participants.

In this surveys, the pilot test had been performed 1 month before the official launch.

Table 3.9.2 Reliability test result of pilot test

	Cronbach's α	Number of items
Perceived Value	0.902	15
Perceived Risk	0.919	19
WOM	0.745	4
Purchase intention	0.857	3

Sources : Table construct by writer

There were 20 participants in the pilot test (Isaac and Michael, 1995). The result was positive and passed the reliability test as showed in table 3.9.2.

3.10.Summary

This chapter showcased the tools used to design the survey to collect the data from targets. From the questions asked, the analysis methods and the survey drafting process. The survey had been translated to Traditional Chinese to provide a better understanding of questions to targets. After the translation, the question had been turned into digital formation and uploaded to google drive and sent out.

4. Research Results

In this chapter of the study, the tools mentioned above was used to bring out the result of the survey done. The survey conducted from January to March 2021. There are a total of 126 responses collected from targets. There are no missing data or answer in the samples.

4.1. Descriptive statistics

Due to COVID -19 and the lockdown of Hong Kong, the chance of having business or social meeting decrease, the ways of collecting response is limited. The sample size of the survey failed to reach the ideal target, which was larger than 384.

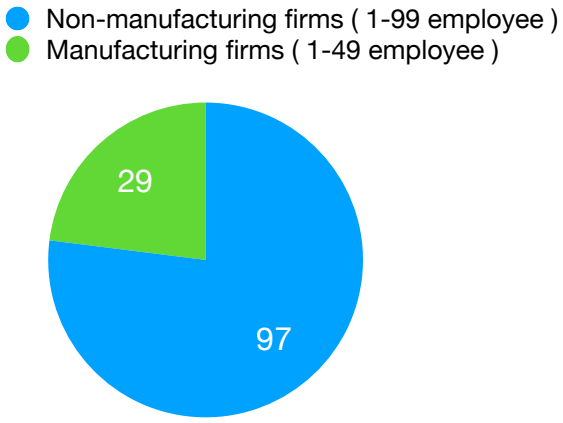
Refer to section 3.4.2, Green (1991) suggested the sampling size had to be larger than 74 in the context of this survey. As the total number of responses is 126, which is larger than 74, the sample counted as an effective sample.

The case summary showed the mean, standard deviation of the constructs proposed to put an effect on purchase intention. The average of all questions had been used to provide a better picture in further discussion.

4.1.1. Demographic

There were questions of the survey to understand the industry and company size of the participants. All the participants that finished the surveys were assumed to work at SME in Hong Kong and had the right to decide which cybersecurity product or service that their company might purchase. This was the filtering question to only allow the participants were answering on behalf of a Hong Kong SME. The results listed as follow.

Figure 4.1.1 Distribution of the participants



Sources : Figure construct by writer

For all participants who joined the survey, 97 (77%) of the participants' company is non-manufacturing firms and 28 (23%) is manufacturing as shown in figure 4.1.1. Compare with the data listed in SUCCESS HKSAR (2021), there were 2.8% of the whole pool of SMEs is manufacturing firm in Hong Kong.

4.1.2.Perceived value

The result of each construct was discussed separately to provide a better understanding to readers. The summary listed at the end of this section.

Table 4.1.1 Descriptive statistics of perceived functional value

	Code	Questions	Mean	Standard deviation
Functional Value	**VF1**	Ease to use.	4.35	0.823
	VF2	Increase the productivity of my company.	4.3	0.879
	VF3	Enhance our service quality.	4.29	0.859

Sources : Table construct by writer

Listed in table 4.1.1, there are three questions asking the participants about the perceived functional value with the average range of 4.29 to 4.35. The higher average score was " VF1, Ease to use" which meant user-friendly is

important for cybersecurity product or service. The range of standard deviation was 0.823 to 0.79, which was in the acceptable range (Ali and Bhaskar, 2016). All result are high, meaning functional value was an important concern in cybersecurity service/ product.

Table 4.1.2 Descriptive statistics of perceived social value

	Code	Questions	Mean	Standard deviation
Social value	**VS2**	Differentiate our product/ service from the competitors.	4.18	0.871
	VS3	Build a positive image.	4.17	0.956
	VS1	Increase our acceptance by clients.	4.07	0.931

Sources : Table construct by writer

As shown in Table 4.1.2, three questions were asked about the perceived social value that the participants perceived. The range is 4.07 to 4.18 with the highest average is VS3 Build a positive image. The standard deviation ranged from 0.871 to 0.956, which is lower than 1. The result is acceptable (Ali and Bhaskar, 2016). As the means of all 3 question is above 4, meaning more than average participants think social value is a concern when making discussion.

Table 4.1.3 Descriptive statistics of perceived emotional value

	Code	Questions	Mean	Standard deviation
Emotional value	**VE1**	Provide a safety feeling.	4.4	0.792
	VE2	Provide a joyful experience.	4.06	0.927
	VE3	Provide a new service environment.	3.72	1.017

Sources : Table construct by writer

For emotional value, there are also 3 questions, the range is between 3.72 to 4.4, with the standard deviation ranged 0.792 to 1.017. For “VE3 Provide a new service environment “, the standard deviation is higher than 1 and the lowest mean among these three questions. As shown in table 4.1.3, the

standard deviation of emotional value is under 1, the case classified as acceptable (Ali and Bhaskar, 2016).

Table 4.1.4 Descriptive statistics of perceived epistemic value

	Code	Questions	Mean	Standard deviation
Epistemic value	**VEP3**	I am willing to try new auxiliary product/ service.	3.97	1.085
	VEP1	I am willing to try a new product/ service	3.94	1.017
	VEP2	It will satisfy my curiosity.	3.37	0.817

Sources : Table construct by writer

For epistemic value, 3 questions had been included in the questionnaire listed in table 4.1.4, the range is between 3.37 to 3.94, with the standard deviation ranged 0.817 to 1.085. In these three questions, there are two questions " VEP1 I am willing to try a new product /service" and " VEP3 I am willing to try new auxiliary product/service" with standard deviation higher than 1, which mean the distribution was widen but acceptable (Ali and Bhaskar, 2016) .

Table 4.1.5 Descriptive statistics of perceived conditional value

	Code	Questions	Mean	Standard deviation
Conditional Value	**VC1**	If my company was being hacked, we will be more willing to try a cybersecurity product/ service.	4.33	0.810
	VC3	If there is news about the hacking of companies, we will be more willing to try.	4.17	0.728
	VC2	If there is a promotions campaign, we will be more willing to try.	3.82	1.023

Sources : Table construct by writer

There were 3 questions that had been included in the questionnaire for conditional value as shown in table 4.1.5, which set the range between 3.82 to 4.33 and the standard deviation ranged 0.810 to 1.023. The question" VC2

if there is a promotion campaign, we will be more willing to try" had a standard deviation larger than 1, the result means the data is disturbed in a wider range and acceptable (Ali and Bhaskar, 2016). The question " VC1 If my company was being hacked, we will be more willing to try a cybersecurity product/ service." had the highest mean that participants took this conditional seriously.

Table 4.1.6 Descriptive statistics of perceived value

	Mean		Standard deviation	
Social value	4.14	4.16	0.780	0.58
Functional value	4.13		0.761	
Conditional value	4.11		0.694	
Emotional value	4.06		0.767	
Epistemic value	3.76		0.757	

Sources : Table construct by writer

Table 4.1.6 showed that the means of all results related to perceived value is 4.16 and the standard deviation of the sum of all questions is 0.58, which is less than 1, state that the distribution of the answer is normal. Among all the individual questions, some of those had a standard deviation of over 1. The maximum mean of all question under perceived value is 4.4 and the minimum is 3.37, which made the range is 3.37 to 4.4.

4.1.3. Perceived risk

The result of each construct was discussed separately to provide a better understanding to readers. The summary listed at the end of this section.

Table 4.1.7 Descriptive statistics of perceived time risk

	Code	Questions	Mean	Standard deviation
Time Risk	**RT1**	Spend lots of time to look for a suitable product/ service.	3.94	0.842
	RT2	Take me lots of time to communicate with the supplier.	3.67	0.978
	RT4	Needs lots of time to learn how to use.	3.52	1.164
	RT3	Take lots of time to install.	3.33	1.003

Sources : Table construct by writer

Time risk was measured by 4 questions and the result listed in table 4.1.7. The range set between 3.33 to 3.94. The lowest value is “RT3 Take lots of time to install”. The question asked them about the time might spend got the highest mean among these 4 questions reflecting the importance. The standard deviation value is from 0.842 to 1.164, which can support the analysis(Ali and Bhaskar, 2016).

Table 4.1.8 Descriptive statistics of perceived privacy risk

	Code	Questions	Mean	Standard deviation
Privacy Risk	**RP2**	Our data will be out of control after installation.	3.56	1.197
	RP1	Share my company information to others without our consent.	3.52	1.249
	RP3	Our client’s data will be stolen.	3.37	1.306
	RP4	Unsecured online payment method	3.17	1.151

Sources : Table construct by writer

There were four questions measuring privacy risk in the survey and the result listed in table 4.1.8 with the range between 3.37 to 3.56. The largest value is “RP2 Our data will be out of control after installation” while the lowest is “RP4 Insured on the online payment method.” The standard deviation value of all four questions was higher than 1, which is from 1.151 to 1.306 can be used in further analyses (Ali and Bhaskar, 2016).

Table 4.1.9 Descriptive statistics of perceived financial risk

	Code	Questions	Mean	Standard deviation
Financial Risk	**RF3**	Unexpected huge surcharge on additional service.	3.63	1.108
	PF2	Pay a higher maintenance cost than the market price	3.61	0.980
	RF1	Pay a higher initial cost than the market price.	3.51	0.970
	RF4	Pay more than the market price.	3.46	1.025

Sources : Table construct by writer

The financial risk was asked through 4 questions in the questionnaire as showed in table 4.1.9. The highest average is 3.63 and the lowest is 3.46. Participants were most concerned about the unexpected cost of cybersecurity product and service. The standard deviation of RF1 and RF2 were lower than 1 and higher than 1 in RF3 and RF4. All four result were in the acceptable range for analysis (Ali and Bhaskar, 2016).

Table 4.1.10 Descriptive statistics of perceived functional risk

	Code	Questions	Mean	Standard deviation
Functional Risk	**RFC1**	Insufficient in technical support while facing a technical issue.	3.64	1.099
	RFC3	Insufficient network protection of my company.	3.56	1.121
	RFC4	Difficult to compare the product/service before purchase.	3.52	1.122
	RFC2	Different product/ service in the promotion martial.	3.46	1.017

Sources : Table construct by writer

Table 4.1.10 showed that functional risk was asked through four questions in the questionnaire. The highest average was 3.64 and the lowest is 3.46. Overviewing the standard deviation, all 4 questions' standard deviation value is around 1, the answer was representing the population (Ali and Bhaskar,

2016). In functional risk, participants were seen to care about the technical support most as the mean value was the highest.

Table 4.1.11 Descriptive statistics of perceived psychological risk

	Code	Questions	Mean	Standard deviation
Psychological Risk	**RPC2**	Have an unpleasant feeling when my company is using the product/ service.	3.33	1.049
	RPC1	Dislike the product/service	3.10	1.155
	RPC3	I will feel the anxiety to install the product/service.	3.07	1.121

Sources : Table construct by writer

The psychological risk was asked through four questions in the questionnaire. The highest average is 3.10 and the lowest is 3.33. The question asked about unpleasant feeling had the highest mean compare to the other two questions. As showed in table 4.1.11 that overviewing the standard deviation, all 3 questions' standard deviation value is near 1, the answer can use the represent the population (Ali and Bhaskar, 2016).

Table 4.1.12 Descriptive statistics of perceived value

	Mean		Standard deviation	
Time Risk	3.61	3.46	0.764	0.691
Financial Risk	3.55		0.88	
Functional Risk	3.55		0.867	
Privacy Risk	3.36		0.984	
Psychological Risk	3.16		1.00	

Sources : Table construct by writer

Table 4.1.12 shown that the means of all results related to perceived risk is 3.46 and the standard deviation of the sum of all questions is 0.691, which is less than one, state that the distribution of the answer is normal. Among all the individual questions, some of those had a standard deviation equal to 1.

The maximum mean of all question under perceived value is 3.61 and the minimum is 3.16, which made the range is 3.16 to 3.61. The time risk had the highest mean of all construct which is 3.61.

4.1.4.WoM

Table 4.1.13 Descriptive statistics of WoM

Code	Questions	Mean		Standard deviation	
W2	I will seek advice from my business partners.	4.29	3.95	0.747	0.566
W1	I will seek advice from my friends.	4.26		0.671	
W3	I trust the comments from different social media.	3.64		0.805	
W4	I trust the user comments from the official website of the product/service provider.	3.63		0.758	

Sources : Table construct by writer

Table 4.1.13 shown that the means for WoM is 3.95. The standard deviation of all four questions is under 1, that means the data is in acceptable range in term of distribution (Ali and Bhaskar, 2016). The range of mean is from 3.63 to 4.29. The WoM factor defined in chapter 3 related it to 4 questions. Questions W1 and W2 had a higher mean which is above 4.2 compare to W3 and W4 which is around 3.63.

4.1.5.Purchase intention

Table 4.1.14 Descriptive statistics of purchase intention

Code	Questions	Mean		Standard deviation	
PI1	I will purchase a cybersecurity product in the near future.	3.89	3.83	0.751	0.730
PI2	I will recommend my friends or partners to purchase cybersecurity product/service in the near future.	3.90		0.798	
PI3	I will purchase a cybersecurity product in the near future, even when the price goes up.	3.80		0.858	

Sources : Table construct by writer

Table 4.1.14 displayed the descriptive statistics of the response of purchase intention. The mean of the purchase intention is 3.83, with the range of each question is 3.8 to 3.9. The standard deviation of the average purchase intention is 0.73, the distribution is a normal distribution as the value is under 1 which is acceptable (Ali and Bhaskar, 2016).

4.2. Reliability

There are in total 42 questions asked in this survey, forty-two questions fell into 3 independent variable and one dependant variable. The result of all four independent variables passed 0.7 at the reliability test. The result was consistent with the data collected from the pilot test performed before the surveys. Cronbach's α was the tools used to test the reliability.

Table 4.2.1 Reliability test result on perceived value

Construct	Number of Question	Cronbach's α	
Functional value	3	0.872	0.920
Social value	3	0.805	
Emotional value	3	0.788	
Epistemic value	3	0.787	
Conditional value	3	0.727	

Sources : Table construct by writer

As shown in table 4.2.1, there are 3 questions for each construct to develop the factor of perceived value. In total 15 questions, the range of the Cronbach’s α value was 0.727 to 0.872. The reliability of the perceived value is 0.920. For all the value result that passed 0.7, the result stated to be reliable.

Table 4.2.2 Reliability test result on perceived risk

Construct	Number of Question	Cronbach's α	
Time risk	4	0.758	0.916
Privacy risk	4	0.815	
Financial risk	4	0.887	
Functional risk	4	0.806	
Psychological risk	3	0.871	

Sources : Table construct by writer

In table 4.2.2, we can see there are in total 19 questions asked about perceived risk. The range of the Cronbach's α value is from 0.758 to 0.887, while the value of time risk is the lowest. The Cronbach's α of the perceived risk is 0.926 so that all the result passed the reliability test.

Table 4.2.3 Reliability test result on WoM

Factor	Number of Question	Cronbach's α
WoM	4	0.703

Sources : Table construct by writer

Table 4.2.3 showed there were four questions to review the point of view on WoM related to cybersecurity product or service. The question passed the reliability test with Cronbach's α value higher than 0.703.

Table 4.2.4 Reliability test result on purchase intention

Factor	Number of Question	Cronbach's α
Purchase intention	3	0.828

Sources : Table construct by writer

Listed in table 4.2.4, there are three questions asked the participants about their view of purchase intention. As a dependant variable, the reliability test result shows the Cronbach's α is 0.828, passed the test, implying that the result was consistent with the pilot test result.

4.3. Correlation analysis

This chapter explored the correlation between the independent variable and dependant variable. Pearson 2-tailed analysis was used in this analysis.

Table 4.3.1 Correlation analysis between perceived value and purchase intention

		Average of PI	Average of VF	Average of VS	Average of VE	Average of VEP	Average of VC
Average of PI	Pearson Correlation	1	.341**	.384**	.465**	.432**	.536**
	Sig. (2-tailed)		.000	.000	.000	.000	.000
	N	126	126	126	126	126	126
Average of VF	Pearson Correlation	.341**	1	.749**	.628**	.435**	.497**
	Sig. (2-tailed)	.000		.000	.000	.000	.000
	N	126	126	126	126	126	126
Average of VS	Pearson Correlation	.384**	.749**	1	.729**	.581**	.441**
	Sig. (2-tailed)	.000	.000		.000	.000	.000
	N	126	126	126	126	126	126
Average of VE	Pearson Correlation	.465**	.628**	.729**	1	.654**	.499**
	Sig. (2-tailed)	.000	.000	.000		.000	.000
	N	126	126	126	126	126	126
Average of VEP	Pearson Correlation	.432**	.435**	.581**	.654**	1	.526**
	Sig. (2-tailed)	.000	.000	.000	.000		.000
	N	126	126	126	126	126	126
Average of VC	Pearson Correlation	.536**	.497**	.441**	.499**	.526**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	
	N	126	126	126	126	126	126

**. Correlation is significant at the 0.01 level (2-tailed).

Sources : Table construct by writer

Table 4.3.1 showed the correlation between all construct that forms perceived value. All the construct appeared to have a relationship with perceived value, as all the sig. (2-tailed) value is 0.000. The result showed all the proposed are relevant to the purchase intention of the participants. Among all the constructs, conditional value showed the highest relationship with perceived value with the value 0.536.

There was also a strong correlation between individual construct. As the relations had no contribution to the research topic and objective, there would not be any discussion about those relationships.

Table 4.3.2 Correlation analysis between perceived risk and purchase intention

		Average of PI	Average of RT	Average of RP	Average of RF	Average of RFC	Average of RPC
Average of PI	Pearson Correlation	1	.100	.011	.269**	.174	.129
	Sig. (2-tailed)		.264	.902	.002	.052	.150
	N	126	126	126	126	126	126
Average of RT	Pearson Correlation	.100	1	.284**	.449**	.450**	.188*
	Sig. (2-tailed)	.264		.001	.000	.000	.035
	N	126	126	126	126	126	126
Average of RP	Pearson Correlation	.011	.284**	1	.570**	.492**	.416**
	Sig. (2-tailed)	.902	.001		.000	.000	.000
	N	126	126	126	126	126	126
Average of RF	Pearson Correlation	.269**	.449**	.570**	1	.665**	.576**
	Sig. (2-tailed)	.002	.000	.000		.000	.000
	N	126	126	126	126	126	126
Average of RFC	Pearson Correlation	.174	.450**	.492**	.665**	1	.612**
	Sig. (2-tailed)	.052	.000	.000	.000		.000
	N	126	126	126	126	126	126
Average of RPC	Pearson Correlation	.129	.188*	.416**	.576**	.612**	1
	Sig. (2-tailed)	.150	.035	.000	.000	.000	
	N	126	126	126	126	126	126

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Sources : Table construct by writer

Table 4.3.2 listed the correlation between all constructs that form perceived risk suggested in chapter 2. The only correlation that showed a positive relationship is the relationship between perceived financial risk and purchase intention. The Pearson correlation value is 0.269, interpreted as a weak positive relationship between perceived financial risk and purchase intention. Same as perceived value, this section was not meant to discuss the relationship among all the constructs under perceived risk.

Table 4.3.3 Correlation analysis between WoM and purchase intention

		Average of PI	Average of WoM
Average of PI	Pearson Correlation	1	.412**
	Sig. (2-tailed)		.000
	N	126	126
Average of WoM	Pearson Correlation	.412**	1
	Sig. (2-tailed)	.000	
	N	126	126

**. Correlation is significant at the 0.01 level (2-tailed).

Sources : Table construct by writer

Table 4.3.3 showed the correlation between WoM and purchase intention. As the Sig. value was 0, there was a correlation relationship between WoM and purchase intention.

As there were different construct involved in this surveys and the above correlation test supported that not all the construct in a single factor have correlated with the purchase intention. In the coming discussion, the average value of all the construct of perceived value and perceived risk would be used. For the test of significance, a two-tailed analysis would be performed.

Table 4.3.1 Correlation analysis of all independent variables and purchase intention

		Average of PI	Average of WoM	Average of PV	Average of PR
Average of PI	Pearson Correlation	1	.412**	.590**	.181*
	Sig. (2-tailed)		.000	.000	.043
	N	126	126	126	126
Average of WoM	Pearson Correlation	.412**	1	.514**	.031
	Sig. (2-tailed)	.000		.000	.734
	N	126	126	126	126
Average of PV	Pearson Correlation	.590**	.514**	1	.244**
	Sig. (2-tailed)	.000	.000		.006
	N	126	126	126	126
Average of PR	Pearson Correlation	.181*	.031	.244**	1
	Sig. (2-tailed)	.043	.734	.006	
	N	126	126	126	126

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Sources : Table construct by writer

The statistical result shown in 4.3.1 provided an overview of correlation among all the variable. The purchase intention as a dependant variable had a positive relationship with both WoM and perceived value by having 0.000 in Sig. (2-tailed) which is less than 0.05. The relationship of both WoM and perceived value with purchase intention is a moderate positive linear relationship. There was a relationship between perceived risk and purchase value which were a weak positive relationship, with the Sig (2-tailed) was less than 0.05. As the questions of

perceived risk were in reserve as mention in chapter 3, the relationship was a weak negative linear relationship.

Other than purchase intention, there was also a strong relation between WoM with perceived value and perceived risk with perceived value. The Pearson correlation of WoM with perceived value was 0.590, with Sig. (2-tailed) 0.000.

4.4. Regression analysis

This section presented the regression analysis from the data collected in the surveys. Building a regression model helped to achieve the research objective, to identify the relationship between factors that apply to the SMEs market in Hong Kong. There were three rounds of a regression performed in this section and all the regression used the average value of all the factors.

Table 4.4.1 Model summary for regression analysis (First-run)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.625[a]	.391	.332	.59656

a. Predictors: (Constant), Average of VC, Average of RP, Average of WoM, Average of RT, Average of RPC, Average of VE, Average of VF, Average of VEP, Average of RF, Average of RFC, Average of VS

b. Dependent Variable: Average of PI

Sources : Table construct by writer

The first step of performing a regression is to check the data variation that could be interpreted by the model. As shown in Table 4.4.1, the R2 value was 0.332 which imply that the model had 33.2% of data that could be interpreted by this regression.

Table 4.4.2 ANOVA of the regression analysis (First-run)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	26.037	11	2.367	6.651	.000[b]
	Residual	40.571	114	.356		
	Total	66.608	125			

a. Dependent Variable: Average of PI

b. Predictors: (Constant), Average of VC, Average of RP, Average of WoM, Average of RT, Average of RPC, Average of VE, Average of VF, Average of VEP, Average of RF, Average of RFC, Average of VS

Sources : Table construct by writer

The next step was to check the Sig, as showed in table 4.4.2, the Sig = 0.000, which was less than 0.05 as shown in table 4.4.2. The regression medal was overall significant in this study.

Table 4.4.3 Regression coefficient of analysis (First-run)

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	.610	.504		1.211	.228		
	Average of WoM	.288	.118	.223	2.449	.016	.642	1.557
	Average of RT	-.103	.087	-.108	-1.179	.241	.642	1.558
	Average of RP	-.053	.074	-.072	-.724	.470	.542	1.845
	Average of RF	.130	.098	.157	1.322	.189	.380	2.632
	Average of RFC	.064	.103	.076	.624	.534	.359	2.789
	Average of RPC	-.009	.079	-.012	-.107	.915	.450	2.222
	Average of VF	-.075	.119	-.078	-.627	.532	.348	2.874
	Average of VS	-.037	.128	-.040	-.289	.773	.286	3.499
	Average of VE	.233	.121	.245	1.925	.057	.329	3.037
	Average of VEP	.008	.111	.009	.076	.940	.406	2.461
	Average of VC	.357	.107	.339	3.343	.001	.519	1.928

a. Dependent Variable: Average of PI

Sources : Table construct by writer

In table 4.4.3, the regression model showed the only average condition value had a sig lower than 0.05, which implied the result was not significant to the regression model upon purchase intention. Some element was deleted in the next round of regression analysis. Due to the number of element, the first element perceived epistemic value which had the Sig value as 0.940 would be deleted in the re-run.

Table 4.4.4 Model summary for regression analysis (Second-run)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.625[a]	.391	.338	.59398

a. Predictors: (Constant), Average of VC, Average of RP, Average of WoM, Average of RT, Average of RPC, Average of VE, Average of VF, Average of RF, Average of RFC, Average of VS

b. Dependent Variable: Average of PI

Sources : Table construct by writer

Table 4.4.5 ANOVA of the regression analysis (Second-run)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	26.035	10	2.603	7.379	.000[b]
	Residual	40.573	115	.353		
	Total	66.608	125			

a. Dependent Variable: Average of PI

b. Predictors: (Constant), Average of VC, Average of RP, Average of WoM, Average of RT, Average of RPC, Average of VE, Average of VF, Average of RF, Average of RFC, Average of VS

Sources : Table construct by writer

In the re-run test result showed in table 4.4.4, the R2 was valued 0.338, similar to the first run, which implied the regression result can represent 33.8% of the result. With the Sig value was 0.000 as showed in table 4.4.5, the re-run test result was a result is significant in this run.

Table 4.4.5 Regression coefficient of analysis (Second-run)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.609	.501		1.215	.227		
	Average of WoM	.290	.114	.225	2.550	.012	.680	1.470
	Average of RT	-.102	.087	-.107	-1.181	.240	.644	1.552
	Average of RP	-.054	.073	-.073	-.738	.462	.547	1.828
	Average of RF	.129	.098	.157	1.326	.187	.380	2.630
	Average of RFC	.063	.101	.075	.622	.535	.368	2.720
	Average of RPC	-.007	.076	-.009	-.090	.928	.488	2.050
	Average of VF	-.076	.116	-.079	-.653	.515	.359	2.787
	Average of VS	-.035	.126	-.038	-.282	.778	.293	3.418
	Average of VE	.237	.109	.249	2.165	.032	.399	2.503
	Average of VC	.359	.102	.341	3.511	.001	.560	1.784

a. Dependent Variable: Average of PI

Sources : Table construct by writer

Table 4.4.5 listed the result in the re-run. The Sig value of all the elected elements was higher than 0.05 except the perceived conditional value, which was not significant to the model. All the elements that had over 0.05 Sig value were be deleted one by one in the coming regression test. For the clear presentation, the

process would not be shown in the coming section, only the final result would be discussed.

Table 4.4.6 Model summary for regression analysis (Final-run)

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.582[a]	.339	.328	.59831

a. Predictors: (Constant), Average of VC, Average of VE

b. Dependent Variable: Average of PI

Sources : Table construct by writer

Table 4.4.7 ANOVA of the regression analysis (Final-run)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	22.577	2	11.288	31.534	.000[b]
	Residual	44.031	123	.358		
	Total	66.608	125			

a. Dependent Variable: Average of PI

b. Predictors: (Constant), Average of VC, Average of VE

Sources : Table construct by writer

Table 4.4.8 Final Element eliminated from the regression test

Order to eliminate	Construct
1	**Perceived Psychological Risk**
2	**Perceived Social Value**
3	**Perceived Functional Risk**
4	**Perceived Privacy Risk**
5	**Perceived Financial Value**
6	**Perceived Time Risk**
7	**Perceived Financial Risk**
8	**WoM**

Sources : Table construct by writer

Table 4.4.6 showed the final run result of the regression analysis, the R2 value is 0.328, which meant 32.8 % of the result can be explained by this analysis. The Sig value showed in table 4.4.7 stated that the regression is 0.000, which meant the model can represent the data. The order of element deleted as shown in table 4.4.8

Table 4.4.9 Regression coefficient of analysis (Final-run)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.064	.352		3.021	.003		
	Average of VE	.251	.080	.264	3.116	.002	.751	1.332
	Average of VC	.425	.089	.404	4.775	.000	.751	1.332

a. Dependent Variable: Average of PI

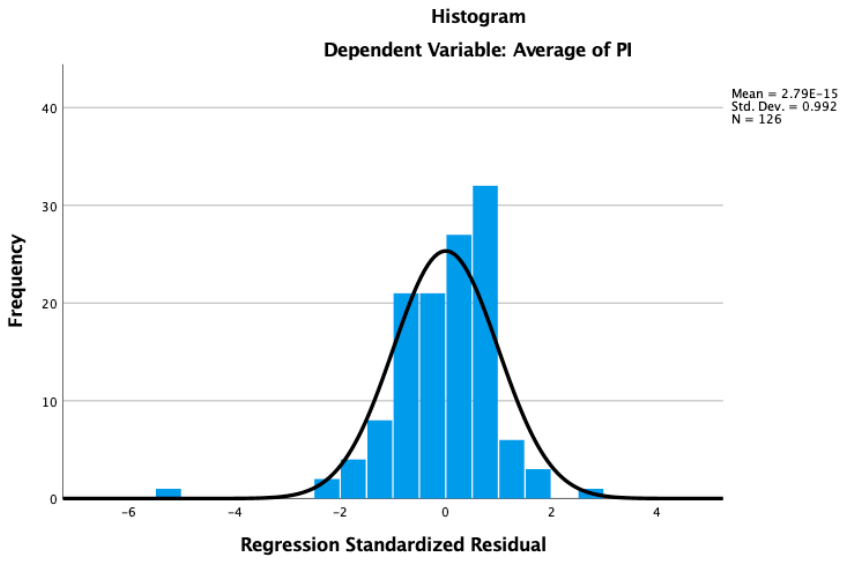
Sources : Table construct by writer

In the final run analysis test result listed in table 4.4.9, the perceived emotional value had a perceived conditional value from regression relationship with the purchase intention with the Sig value 0.002 and 0.00. In this case, the question of the analysis presented as below :

$$PI = 1.064 + 0.251VE + 0.425VC$$

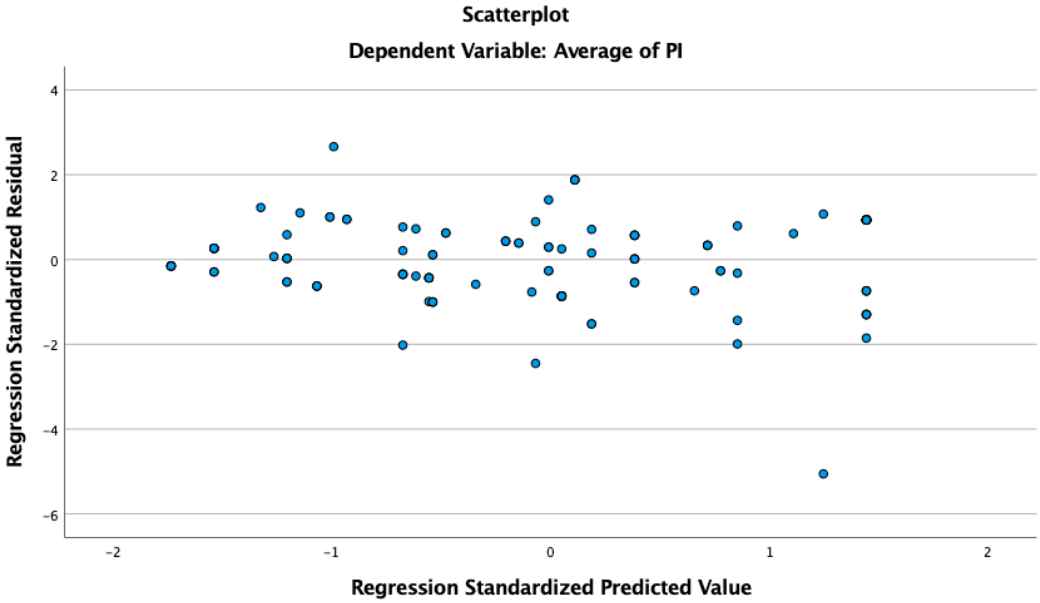
Where PI = Purchase intention, VE = Perceived Emotional Value and VC = Perceived Conditional Value.

Figure 4.4.1 Re-run correlation analysis of construct of perceived risk



Sources : Figure construct by writer

Figure 4.4.2 Re-run correlation analysis of construct of perceived risk

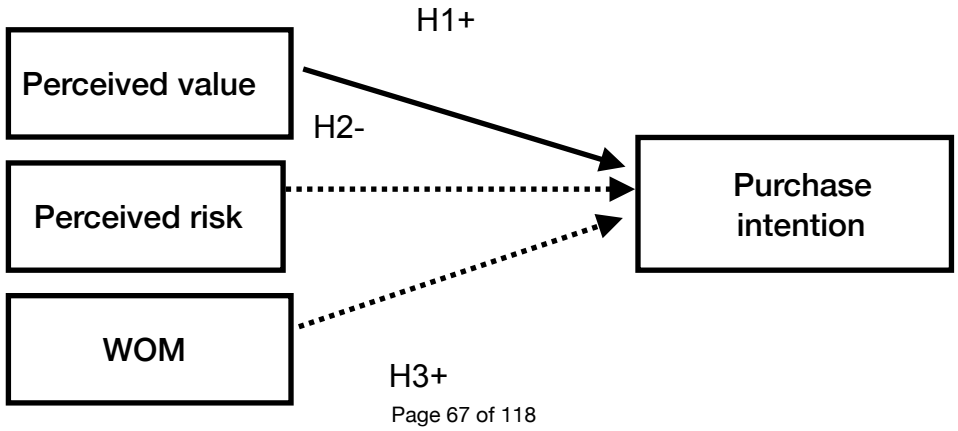


Sources : Figure construct by writer

Figure 4.4.1 showed the distribution of the result. By observation, the result was appeared to be right skewness. The skewness was caused by one outliner on the left. Apart from the outliner, the distribution appeared to be a normal distribution. Figure 4.4.2 showed the scatterplot graphic is averagely spread in the session. There was no significant linear relationship shown in figure 4.4.2.

4.5. Hypothesis

Figure 4.5.1 The research framework



Sources : Figure construct by writer

Table 4.5.1 Research hypothesis test result

Code	Research hypothesis	Test result
H1+	Perceived value positively influence the purchase intention of SME in purchasing	Partially Passed
H2 -	Perceived risk negatively influence the purchase intention of SME in purchasing	Not Passed
H3+	WOM positively influence the purchase intention of SME in purchasing cybersecurity products or services	Not Passed

Sources : Table construct by writer

Figure 4.5.1 showed the summary of the surveys. Table 4.5.1 showed the result of the test, H1: Perceived value positively influence the purchase intention of SME in purchasing (Payne and Holt, 2001) was partially passed the assumptions. However others two ass H2: Perceived risk negatively influence the purchase intention of SME in purchasing (Kim, Kim and Leong, 2005) and H3: WOM positively influence the purchase intention of SME in purchasing cybersecurity products or services had no data to pass the regression test (Sa'ait, Kanyan and Nazrin 2016).

5. Conclusion and recommendation

The research question of this dissertation was to explore the factor that affects the purchase intention of SMEs on cybersecurity product or service. In chapter 1, the background overview with the research question had been stated. The literature review discussed different literature point of view on factors related to the research topic. A survey was designed that aim to collect first-hand data of SMEs on the purchase intention about the research questions.

In chapter 4, SPSS was used to perform a series of analysis to test the reliability and the relationship of all 3 independent variables with dependant variable. There were recommendations and a summary of this dissertation presented in this chapter. The detailed summary of surveys, research objective and research questions were presented in the coming section.

5.1. Conclusion

The research questions had been answered throughout this dissertation. On the question “Which was what is the driver when SMEs purchase cybersecurity products or service?” By industry overview and literature review performed in chapter 1 and 2, the key driver of SMEs to purchase cybersecurity intention are perceived value, perceived risk and Word-of month.

On how those factors affect the decision making, there was a hypothesis setup which is perceived value and WoM form a positive relationship with purchase intention yet perceived risk form negative relationship with purchase intention. In the survey performed to test the hypothesis, the survey supported that there was a strong regression relationship between perceived value and purchase intention. That meant for more value SMEs perceived to have the higher the intention for them to purchase such service. Looking into the survey's result of 5 constructs of

perceived conditional value and perceived emotional value appeared to forms the strongest positive relationship with the purchase intention. The question VC1, which is “If my company was being hacked, we will be more willing to try a cybersecurity product/ service.” show the highest marks among the three questions asked. For perceived emotional value, the question “VE1 Provide a safety feeling.” ranked the first among the three questions asked.

The result showed SMEs might only consider investing more on purchase cybersecurity if they got hacked by hacker and need a sense of safety, which consistent with the behaviour described in different news and research. Trend Micro (2020) shared the same insight, which was company will only realise the importance of enhancing cybersecurity after they faced the loss of cyberthreat. Former FBI director Stacy Cowley used the statement to warn the company saying that there were two types of company in the worlds, those have been hacked and those will be (Cowley and July 2012). The result of the research aligned with the point of view of different service provider and regulator worldwide.

There was a recommendation on each factor that service provider should consider take to help them promote cybersecurity service more effectively.

5.2. Recommendation

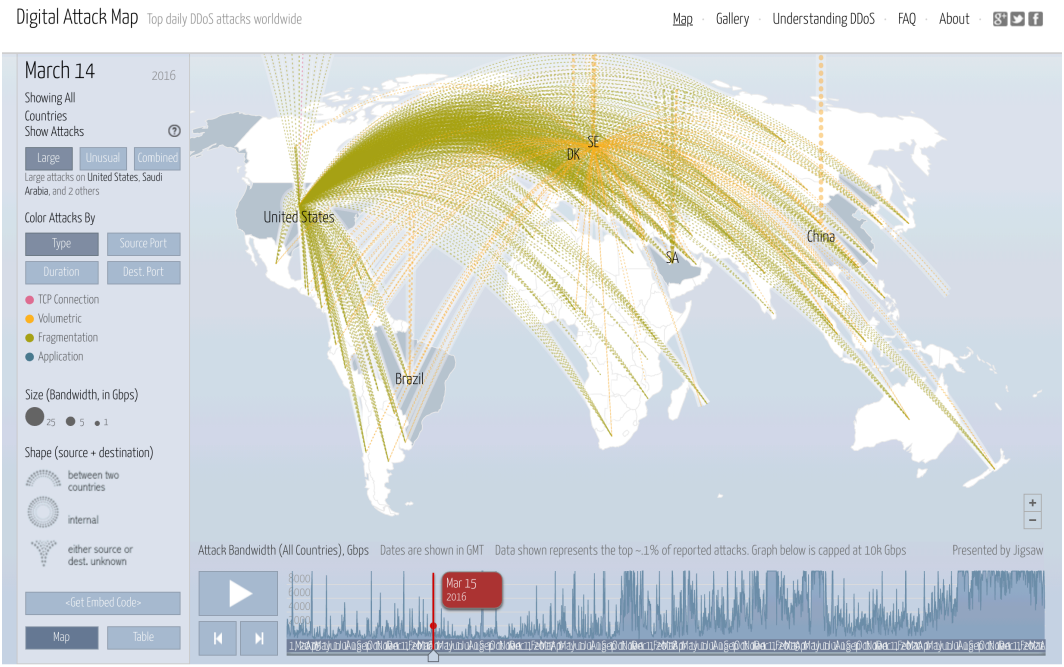
As there are proofed relationship between purchase intention and perceived value, service or product provider are suggested to take a deeper look of the benefits customer can feel before their purchase.

The topic ranking related to the perceived value was feeling safe in emotional value (4.4) and consider to purchase if they got hacked in conditional value (4.35).

For the emotional value, the service provider can consider doing more case sharing of existing customer. Take Hong Kong Hospital Authority as an example, in February 2019, they got an organised cyber-attack (Hospital Authority HKSAR,

2019). They successfully stop the attack after two weeks of searching and system upgrade. While they are busy handling the event after the attack, they give out their case details for the public to study and investigate. Case sharing is one of the tools to make the potential client trust their brand and work (Liou, 2016). Also, they can consider setting up a physical area to provide a sense of safety when a client comes to visit their office.

Figure 5.2.1 Network attack map



Sources : Checkpoint (2021)

Companies can consider building more visual effect on the protection model. Take Checkpoint, DDoS data and FireEye as an example, they provide a live map for the public to see the attack happening. This live attack map is like eye candy (Ragan, 2017). Ragan also suggested that a map is a good tool to helps the potential customer visualise the attack to increase their sense of perceived conditional value.

To add the above element into sales flow, service providers can consider doing more visual demo on the attack flow, the live demo not necessary a system, but can be recording stream video. The streaming video will help non-industry customer to understand the real-life case happing in the world.

To provide a further sense of safety, service and product providers might consider getting certificates to accredit their service and staff level.

Table 5.2.1 List of accreditation to enhance customer sense of safety

Name	Content	For
Offensive Security Certified Professional (OSCP)	A certification that focuses on hands-on offensive information security skills.	Staff
Certified Information Systems Security Professional (CISSP)	an information assurance professional who defines the architecture, design, management and/or controls that assure the security of business	Staff
Certified Information Systems Auditor (CISA)	A globally recognized certification for IS audit control, assurance and security professionals.	Staff
ISO 27001	A widely known ISO, providing requirements for an information security management system (ISMS),	Company

Sources : Table construct by writer

As listed in table 5.2.1, getting the accreditation would help customer to understand the skill level of the service provider’s staff, which would enhance the sense of safety.

There were many others action could be taken to tackle the customers' needs. One of the key elements was to educate customers on the cybersecurity industry and events that happened in other countries, which overall increased the awareness of SMEs.

5.3.Limitation of the study

There are some limitation and factors that might affect the result of the study, To highlight them in this section would provide suggestion to improve the accuracy of the research.

First, the research topic is the purchase intention of SMEs toward cybersecurity service or product in Hong Kong. The number of literature and news about the

market of Hong Kong is limited. Since most of the purchase intention study in Asia were focus on China or Southeast Asia market, the differences in culture and business operation will lead to not accurate target factor to consider.

Secondly, the sampling methods may not be generalised according to a specific population. Other factors such as the industry of the company, the actual size of the company might also affect the answer of the questionnaire. Some study suggested that the education background, company cybersecurity history will also affect the purchasing behaviour of companies(Madahi and Sukati, 2012). Yet, due to the limitation of scale and research method, the detailed relationship between these factors will not be discussed in this dissertation.

The year 2020 to 2021, the business sector was heavily impacted by the COVID-19. The impact on the business can seriously affect the purchasing behaviour of service and product. As the impact on the company will be different by industry, this research will not be cover the impact of COVID-19. Further research on COVID-19 should be conducted since the pandemic of COVID-19 is one of the biggest game changers in the last decades.

Also, the researcher conducted these experiments by using hypothetical scenarios, it may not fully represent purchasing behaviour on cybersecurity product and service. Other researchers are suggested to conduct more related research using other hypotheses.

5.4. Impact of business

The I.T. industry of Hong Kong has always been left behind (Hammond and Ruehl,2020). Together with its cybersecurity education, Hong Kong Government had been promoting public awareness of cybersecurity (CIFO HKGOV, 2021).

However, the cybersecurity readiness of SMEs in Hong Kong is decreasing (Chik, 2019).

This dissertation would provide insights that benefit product and service providers, for examples StormEye.io, Maximus Consulting and Guardforce. The insight included the key movers of the purchase and concerns. Furthermore, this dissertation also helps to eliminate some factors the general public may think will affect purchase intention, like the time risk and financial risk. Service and product provide wouldn't have to consider to put sales and promotion on their service as the result of this discretion.

For service and product provider currently not in Hong Kong, this insight can help them to put a key element on their overall planning to start a business in Hong Kong, for example, Splunk and IBM. When they consider expanding the Hong Kong market, they might consider their perceived value toward the SMEs market.

As mentioned, local company like Stormeye can take a deeper look into this study and help them to better develop their business and take advantage of the potential growth of the cybersecurity industry.

5.5. Recommendation on further study

There are a few recommendations for further study, the first few will be on the sampling method and some will be on other researchers who want to explore more in some idea inspired by this discretion.

For sampling methods, rather than using snowball methods to collect a sample, the further researcher should consider engaging with a larger business organisation in Hong Kong, for example, Hong Kong Chinese Industry & Commerce Association or Hong Kong Management Association. With their help, the survey can collect response from the more specific target and make sure there is a unique response

for each company. They can also help to increase the sampling size, reaching 385 as mentioned in chapter 3.

Another suggestion would be to perform a focus group test to collect response from the management of SMEs with more background information. The test suggested the aim to find the relationship between cybersecurity knowledge and purchase intention. For example, there should be a 5-10 minutes video before the focus group test, explained the financial impact and related law and regulations. As Aggarwal et al (2020) suggested that the knowledge of customer would affect the purchase intention from cybersecurity product.

For a new angle to study, further studies were recommended to study the relationship between industry and company size. Also, the relationship between the number of exiting product and service with purchase intention can be studied in order to help business to expand in the Hong Kong SMEs market.

Reference

Cisco (2021). 'What Are the Most Common Cyber Attacks?' Available at : https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Accessed: 1 February 2021).

Cohen J. (2021) '2021年，这3只领先网络安全股票有望继续大涨', Investing.com. Available at: https://cn.investing.com/analysis/article-200460318 (Accessed: 2 March 2021).

Fortune Business insights (2021) 'Cyber Security Market Size, Share & COVID-19 Impact Analysis, By Component (Solution and Services), By Deployment Type (Cloud and On-Premise), By Enterprise Size (Small & Medium Enterprise and Large Enterprise), By Industry (BFSI, IT and Telecommunications, Retail, Healthcare, Government, Manufacturing, Travel and Transportation, Energy and Utilities and Others) and Regional Forecast, 2021-2028'. Available at: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 (Accessed :1 April 2021).

Gaul V. (2020). 'Cyber Security Market By Component (Solutions and Services), Solution/Offering (Identity & Access Management; Infrastructure Security; Governance, Risk, & Compliance; Unified Vulnerability Management Service Offering; and Data Security & Privacy Service Offering; and Others), Deployment Type (Cloud and On-premise), User Type (Large Enterprises and Small & Medium Enterprises), and Industry Vertical (Telecom, Automotive, BFSI, Public Sector, Retail, Healthcare, IT, Energy & Utilities, Manufacturing, and Others): Global Opportunity Analysis and Industry Forecast, 2020–2027'. Available at : https://www.alliedmarketresearch.com/cyber-security-market (Accessed : 5 January 2021).

Goldstein research (2020). 'Asia-Pacific (Apac) Cyber Security Market Outlook : Market Segmentation Based On Security Type, Based On Solutions, Based On Services, Based On Deployment Mode, Based On End-User & By Region With Covid-19 Impact | Forecast Period 2017-2030'. Available at :https://www.goldsteinresearch.com/report/asia-pacific-apac-cyber-security-market-outlook-2024-opportunity-assessment-and-demand-analysis-market-forecast-2016-2024/ (Accessed: 5 March 2021).

HKCERT (2020a) 'SSH Hong Kong Enterprise Cyber Security Readiness Index Survey Down 2.4 Points to 46.9 Staying Vigilant for Cyber Threats in Stormy Times'. Available at: https://www.hkcert.org/blog/ssh-hong-kong-enterprise-cyber-security-readiness-index-survey-down-24-points-to-469-staying-vigilant-for-cyber-threats-in-stormy-times (Accessed: 10 March 2021).

HKCERT (2020b). 'Security Incidents Reported to Us'. Available at : https://www.hkcert.org/statistic (Accessed: 8 Nov 2020).

Lai, L.T. (2020) 'Financial loss due to computer crime in Hong Kong from 2009 to 2018' Available at : https://www.statista.com/statistics/786989/hong-kong-financial-loss-caused-by-computer-crime/ (Accessed 10 October 2020).

News HKSAR (2020) 'Government extends social distancing measures'. Available at : https://www.info.gov.hk/gia/general/202008/10/P2020081000774.htm (Accessed: 6 March 2021).

SUCCESS HKSAR (2021). ‘Small and medium enterprises (SMEs)’. Available at: https://www.success.tid.gov.hk/english/aboutus/sme/service_detail_6863.html (Accessed: 6 March 2021).

TID HKSAR (2021). *Support to Small and Medium Enterprises.* Available at: https://www.tid.gov.hk/english/smes_industry/smes/smes_content.html (Accessed: 6 March 2021).

Trend Micro (2020). ‘The sprawling reach of complex threats’. Available at : https://www.trendmicro.com/zh_hk/about/newsroom/press-releases/2020/2020-02-26.html (Accessed: 8 November 2020).

Bibliography

Abounaima, M. C. et al (2020). 'The Pearson Correlation Coefficient Applied to Compare Multi-Criteria Methods: Case the Ranking Problematic'. 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET) (pp. 1-6). IEEE.

Aimeur, E. & Schönfeld, D. (2011). 'The ultimate invasion of privacy: Identity theft. 2011 9th Annual International Conference on Privacy'*, Security and Trust, PST 2011*. pp.24-31.

Ajzen, I., and Fishbein, M. (1975). *Intention and Behavior: An Introduction to Theory and Research*. MA: Addison-Wesley.

Ali, Z. and Bhaskar, S. B. (2016). 'Basic statistical tools in research and data analysis'. *Indian journal of anaesthesia*, 60(9), pp. 662.

Arndt, J. (1967). 'Role of product-related conversations in the diffusion of a new product', *Journal of marketing Research*, 4(3), pp. 291-295.

Balasubramanian, S. and Mahajan, V. (2001). 'The economic leverage of the virtual community'*. International journal of electronic commerce*, 5(3), pp.103-138.

Balasubramanian, S. V. M. (2001). The economic leverage of the virtual community. *International journal of electronic commerce*, *5*(3), 103-138.

Baños, R. F. et al. (2019). 'Influencia de las competencias del profesorado de secundaria en los comportamientos disruptivos en el aula' .*Influence of the competencies of secondary teachers on disruptive behavior in the classroom*. 12 pp. 3–10. 10.25115/ecp.v12i24.21.

Bauer, R. A. (1960). *Consumer behavior as risk taking*. Chicago, IL, pp. 384-398.

Bernard, H. R. (2017). *Research methods in anthropology: Qualitative and quantitative approaches*. Rowman & Littlefield.

Berry, L. and Yadav, M.S. (1996). 'Capture and Communicate Value in the Pricing of Services'*, MIT Sloan Management Review 1996.* Available at: https://sloanreview.mit.edu/article/capture-and-communicate-value-in-the-pricing-of-services/ (Accessed :1 February 2021).

Bhukya, R. and Singh, S. (2015). 'The effect of perceived risk dimensions on purchase intention', *American Journal of Business,* 30(4), pp. 218-230.

Bickart, B. & Schindler, R.M. (2001). 'Internet forums as influential sources of consumer information', *Journal of Interactive Marketing*, 15(3), pp. 31-40.

Bickart, Barbara and Robert M.S. (2001). "'nternet forums as influential sources of consumer information'. *Journal of interactive marketing* 15(3), pp.31-40.

Bickel, P. J., and Lehmann, E. L. (2012). 'Descriptive statistics for nonparametric models' *I. Introduction. In Selected Works of EL Lehmann*. Springer, Boston, MA. pp. 465-471

Blumberg, B., Cooper, D.R. , Schindler P.S., (2014) *Business Research Methods.*

Bone, P. F. (1995). 'Word-of-mouth effects on short-term and long-term product judgments*', Journal of business research*, 32(3), pp. 213-223.

Brannen, J. (Ed.). (2017). *Mixing methods: Qualitative and quantitative research,* Routledge.

Brook, R. J., and Arnold, G. C. (2018). *Applied regression analysis and experimental design,* Routledge.

Carter, L. and Bélanger, F. (2005). 'The utilization of e−government services: citizen trust, innovation and acceptance factors', *Information Systems Journal*, 15, pp.5-25. https://doi.org/10.1111/j.1365-2575.2005.00183.x.

Capital (2020). '網絡保安輕量化', *Capital Magazine, December pp. 40. A*vailable at Appendix vi.

Chik, H. (2019) 'Hong Kong's smaller companies are not ready to face cybersecurity threats, warns Chubb Insurance', *South China Morning Post Publishers Ltd*. Available at: https://www.scmp.com/tech/big-tech/article/3126072/apple-warns-against-unauthorised-iphone-tracking-chinese-firms (Accessed 1 March, 2021).

CIFO HKGOV (2021) 'Cybersec Infohub'. Available at: https://www.cybersechub.hk/en/aboutus/programme' (Accessed 1 March, 2021).

CISA USGOV (2019) *What is Cybersecurity?* Available at : https://us-cert.cisa.gov/ncas/tips/ST04-001 (Accessed: 1 Feb 2021).

Cochran, W. G. (1977). *Sampling Techniques*. 3rd edition. New York: John Wiley & Sons.

Columbus L. (2020) *2020 Roundup Of Cybersecurity Forecasts And Market Estimates,* Forbes. Available at: https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurityforecasts-and-market-estimates/#504da95a381d (Accessed: 8 June 2020) .

Cowley, S., and July, C. (2012). 'Former FBI cyber cop worries about a digital 9/11'. *CNN Money*, *25*.

Cox, D. F. (1967). 'Risk handling in consumer behavior: An intensive study of two cases'. *Risk taking and information handling in consumer behavior*, pp. 34-81.

Cronbach L.J. (1915) *Coefficient alpha and the internal structure of tests,* pp. 97–334(1951).

Cuieford, J. P. (1965). *Fundamental Statistics in Psychology and Education, 4th (Ed)*, NY McGraw Hill.

Cunningham, S.M. (1967). 'The Major Dimensions of Perceived Risk', *Risk Taking and Information Handling in Consumer Behavior*, pp. 82-108.

David, G., Bozkurt, S., Russo I.,(2019) 'Achieving customer engagement with social media: A qualitative comparative analysis approach', *Journal of Business Research* ,Volume 101, 2019, pp. 59-69, ISSN 0148-2963, https://doi.org/10.1016/j.jbusres.2019.04.006.

Davis, R. (2020). *COVID-19: The world's biggest ever technology pilot,* Standard Chartered. Available at : https://www.sc.com/en/navigate-the-future/covid-19-the-worlds-biggest-ever-technology-pilot/ (Accessed: 5 Oct 2020).

Day, R.L. (1977). 'Extending the Concept of Consumer Satisfaction'*, Advances in Consumer Research Volume 4, 1977*. pp.149-154.

Dellarocas, C., and Narayan, R. (2006). 'What motivates consumers to review a product online? A study of the product-specific antecedents of online movie reviews'. *WISE* pp. 1-6.

Dodds, W. B., Monroe, K. B., and Grewal, D. (1991). 'Effects of price, brand, and store information on buyers' product evaluations', *Journal of marketing research*, 28(3), pp. 307-319.

Einhorn, H. J., & Hogarth, R. M. (1985). 'Ambiguity and uncertainty in probabilistic inference', *Psychological Review*, 92(4), pp. 433–461. https://doi.org/10.1037/0033-295X.92.4.433

Emmel, N. (2013). *Theoretical or purposive sampling. Sampling and choosing cases in qualitative research: a realist approach*, pp.45-66.

Fink, A. and Litwin, M. S. (1995). *How to measure survey reliability and validity* (Vol. 7). Sage.

German Industry and Commerce Ltd. (2020). *'*Driving Digital Transformation: Business after Covid-19*'.* Available at: *https://hongkong.ahk.de/news/news-details/driving-digital-transformation-business-after-corona* (Accessed : 5 January 2021).

Gilly, M. et al. (1998). 'A Dyadic Study of InterpersonalInformation Search', J*ournal of The Academy of Marketing Science*, 26. pp. 83-100. 10.1177/0092070398262001.

Goyette, I. et al. (2010). 'e-WOM Scale: Word-of-Mouth Measurement Scale for e-Services Context*: Revue Canadienne des Sciences de l'Administration', *Canadian Journal of Administrative Sciences,* 27(1), pp. 5-23.

Green, S.B. (1991). 'How Many Subjects Does It Take To Do A Regression Analysis', *Multivariate Behavioral Research*, 26:3, pp. 499-510, DOI: 10.1207/s15327906mbr2603_7

Grewal, D., Gotlieb, J., & Marmorstein, H. (1994). 'The moderating effects of message framing and source credibility on the price-perceived risk relationship*', Journal of consumer research*, 21(1), pp. 145-153.

Guta M. (2019) '43% of Cyber Attacks Still Target Small Business while Ransomware Stays On the Rise*', Small Business Trends*. Available at: https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html (Accessed: 5 January 2021).

Hallowell, R. (1996) 'The Relationships of Customer Satisfaction, Customer Loyalty, and Profitability: An Empirical Study*', International Journal of Service Industry Management*, 7, pp. 27-42. https://doi.org/10.1108/09564239610129931.

Hamdani, N. & Maulani, A.F.G. (2018). 'The influence of E-WOM on purchase intentions in local culinary business sector', *International Journal of Engineering and Technology(UAE)*. 7. 246-250. 10.14419/ijet.v7i2.29.13325.

Hennig-Thurau, T. et al. (2004). 'The impact of new media on customer relationships', *Journal of Service Research*, 13(3), pp. 311-330.

Heskett, J. L.,et al. (1994). 'Putting the service-profit chain to work', *Harvard business review*, 72(2), pp. 164-174.

HKE HKSAR (2021) 'Latest Developments'. Available at: https://www.hkeconomy.gov.hk/en/situation/development/index.htm (Accessed: 9 April 2021).

Holbrook, M. (1999) ‘Consumer Value: A Framework for Analysis and Research*’, Routledge,* New York. http://dx.doi.org/10.4324/9780203010679.

Hospital Authority HKSAR (2019). *HAS Link*. Issue 1 2020. Available at: https://www3.ha.org.hk/ehaslink/issue108/HASLink_1.pdf (Accessed: 1 Feb 2021).

Hovav, A. and Gray, P. (2014). ‘The ripple effect of an information security breach event: A stakeholder analysis’*, Communications of the Association for Information Systems. 34*(1), pp.50.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). ‘Communication and persuasion; psychological studies of opinion change’. *Yale University Press*.

Ilvonen, I. and Virtanen, P. (2013) ‘Preparing for Cyber Threats in Companies With Information Security Policies’*, The 12th European Conference on Information Warfare and Security*, ECIW 2013, 11.-12.7.2013.

Isaac, S., and Michael, W. B. (1995). *Handbook in research and evaluation: A collection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences*. Edits publishers.

Jacoby, J. and Kaplan, L. B. (1972). ‘The components of perceived risk’, ACR Special Volumes.

Jang-Jaccard, J. and Nepal, S. (2014). ‘A survey of emerging threats in cybersecurity’, *Journal of Computer and System Sciences. 80*(5), pp. 973-993.

Kafle, S. C. (2019). ‘Correlation and Regression Analysis Using SPSS. Management', *Technology & Social Sciences*, pp126.

Kaspersky (2021). ‘Regular, Frequent Antivirus Updates’ Available at: https://www.kaspersky.com/resource-center/preemptive-safety/antivirus-updates (Accessed: 5 January 2021).

Keller, K. L. (1993). ‘Conceptualizing, measuring, and managing customer-based brand equity’. *Journal of marketing*, 57(1), pp 1-22.

Khalifa, A.S. (2004) ‘Customer Value: A Review of Recent Literature and an Integrative Configuration’*, Management Decision,* 42, pp. 645-666. Available at : http://dx.doi.org/10.1108/00251740410538497 (Accessed : 7 October 2020).

Kim, L. H., Kim, D.J. and Leong, J.K. (2005). 'The Effect of Perceived Risk on Purchase Intention’, *Purchasing Airline Tickets Online, Journal Of Hospitality & Leisure Marketing*, 13(2), pp 33-53, DOI: 10.1300/J150v13n02_04.

Kosseff, J. (2019). *Cybersecurity Law, 2nd Edition.* ISBN: 978-1-119-51720-7.

Kotler, P. (1994) *Marketing Management Analysis, Planning, Implementation, and control Eight Edition (prentice hall international edition).* pp. 173.

Levitt, T. (1960). ‘Marketing myopia’*, Harvard Business Review, 38,* 45–56.

Likert, R. (1932). ‘A technique for the measurement of attitudes’, *Archives of psychology*.

Liou H.M. (2016). ‘Endorsements And Testimonials In Advertising - In The Perspective Of Competition Law. Journal of Legal*’, Ethical and Regulatory Issues,* 19(1), pp. 79-99.

Long, J. S. and Ervin, L. H. (2000). ‘Using heteroscedasticity consistent standard errors in the linear regression model’,*The American Statistician*, 54(3), pp. 217-224.

Madahi, A., and Sukati, I. (2012). 'The effect of external factors on purchase intention amongst young generation in Malaysia', *International Business Research*, *5*(8), pp. 153.

Mahmud, A.S. et al. (2019). 'Purchase intention in an electronic commerce environment', *Information Technology & People,* 32(6), pp. 1345-1375.

Mathews, L. (2021) 'Acer Faced With Ransom Up To $100 Million After Hackers Breach Network'. Available at : https://www.forbes.com/sites/leemathews/2021/03/21/acer-faced-with-ransom-up-to-100-million-after-hackers-breach-network/?sh=505c2ff3750f (Accessed : 21 March 2021).

Mazumdar, T., and Monroe, K. B. (1992). 'Effects of inter-store and in-store price comparisons on price recall accuracy and confidence', *Journal of Retailing,* 68(1), pp. 66.

Mccollough, M., Leonard, B and Manjit. Y. (2000). *An Empirical Investigation of Customer Satisfaction after Service Failure and Recovery, Journal of Service Research* - J SERV RES. 3. 121-137. 10.1177/109467050032002.

Mei, O.J. , Ling K.C and Piew, T.H. (2012) 'The Antecedents of Green Purchase Intention among Malaysian Consumers'. doi:10.5539/ass.v8n13p248.

Mitchell, V. W. (1992). 'Understanding consumers' behaviour: can perceived risk theory help?'. *Management Decision.*

Morinez, C. et al.(2007). 'High yield ofnmannosylglycerate production by upshock fermentation and bacterial milking of trehalose-deficient mutant Thermus thermophilus '*RQ-1*. *Applied microbiology and biotechnology* 75(5): pp. 1039-1045.

Murray, K. B., and Schlacter, J. L. (1990). 'The impact of services versus goods on consumers' assessment of perceived risk and variability', *Journal of the Academy of Marketing science*, 18(1), pp. 51-65.

Aggarwal, N. et al. (2020). 'Risk knowledge and concern as influences of purchase intention for internet of things devices', *Technology in Society*. pp. 62. 101311. 10.1016/ j.techsoc.2020.101311.

O'Brien, K. (1993). 'Improving survey questionnaires through focus groups', *Successful focus groups: Advancing the state of the art*, *156*, pp. 105-117.

Office of the United States Trade Representative (2021). 'Small Business'. Available at : https://ustr.gov/issue-areas/small-business (Accessed : 1 February 2021).

Ozmen, E. et al. (2014). 'SMEs' Purchasing Habits: A Procurement Maturity Model for Stakeholders', *Sage Open*. 4. 1-19. 10.1177/2158244014536405.

Parasuraman, A., and Grewal, D. (2000). 'The impact of technology on the quality-value-loyalty chain: a research agenda', *Journal of the academy of marketing science*, 28(1), pp. 168-174.

Pavlou, A. K., & Reichert, J. M. (2004). 'Recombinant protein therapeutics—success rates, market trends and values to 2010'. *Nature biotechnology, 22(12)*, pp. 1513-1519.

Payne, A. and Holt, S. (2001). 'Diagnosing customer value: integrating the value process and relationship marketing', *British Journal of management*, *12*(2), pp. 159-182.

Pearson, E. S. (1938). *Mathematical Statistics and Data Analysis (2nd ed.)*, Belmont, CA: Duxbury.

Perry, M.P. and Hamm, C.H. (1969) *Canonical Analysis of Relations between Socioeconomic Risk and Personal Influence in Purchase Decisions.* https://doi.org/10.1177/002224376900600311 .

Peter, J. P., and Tarpey Sr, L. X. (1975). 'A comparative analysis of three consumer decision strategies', *Journal of consumer research,* 2(1), 29-37.

Petrick, J. & Backman, S. (2002). 'An Examination of the Construct of Perceived Value for the Prediction of Golf Travelers' Intentions to Revisit'. *Journal of Travel Research - J TRAVEL RES.* 41. pp. 38-45. 10.1177/0047287502041001005.

Queirós, A., Faria, D., and Almeida, F. (2017). 'Strengths and limitations of qualitative and quantitative research methods', *European Journal of Education Studies*.

Ragan, S. (2017). '8 top cyber attack maps and how to use them'. Available at: https://www.csoonline.com/article/3217944/8-top-cyber-attack-maps-and-how-to-use-them.html (Accessed: 10 March 2021).

Rahman, M. S. (2017). 'The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language Testing and Assessment" Research: A Literature Review', *Journal of Education and Learning*, 6(1), pp. 102-112.

Richins, M. L. (1984). 'Word of mouth communication as negative information'. *ACR North American Advances.*

Roselius, T. (1971). 'Consumer rankings of risk reduction methods', *Journal of marketing*, 35(1), pp. 56-61.

Rothgeb, M. K. (2008). 'Creating a nursing simulation laboratory: A literature review', *Journal of Nursing Education*, *47*(11), pp. 489-494.

Rudow C. (2020) 'The cost of ransomware attacks'. Available at: https://www.nationwide.com/cps/cic/blog/cost-of-ransomware-attacks.html (Accessed: 10 March 2021).

Sa'ait, N., Kanyan, A. and Nazrin, M. F. (2016). 'The effect of e-WOM on customer purchase intention', *International Academic Research Journal of Social Science*, *2*(1), pp.73-80.

Schiffman, L. G., and Kanuk, L. (2000). *Consumer Behavior*, PrenticeHall. Upper Saddle River, NJ.

Sen, S. and Lerman, D. (2007). 'Why are you telling me this? An examination into negative consumer reviews on the web'*, Journal of Interactive Marketing, 21(4), pp. 76-94.*

Setia, M. S. (2016). 'Methodology series module 5: Sampling strategies', *Indian Journal of Dermatology*, 61(5), pp. 505.

Shah, S. S. H. et al. (2012). 'The impact of brands on consumer purchase intentions'*, Asian Journal of Business Management*, 4(2), pp.105-110.

Sheth, J. and Parvatiyar, A. (1995). 'The Evolution of Relationship Marketing'. *International Business Review*. 4. 397-418. 10.1016/0969-5931(95)00018-6.

Sheth, J. N., Newman, B. I., and Gross, B. L. (1991). 'Why we buy what we buy: A theory of consumption values'. *Journal of business research,* 22(2), pp. 159-170.

Silverma, D. (2001). *Interpreting Qualitative Data: Methods forAnalysing Talk,* Text and Interaction (second edition). London / ThousandOaks / New Delhi: Sage, 325 pages, ISBN 0-7619-6864-4 .

Snoj, B., Aleksandra, P. and Mumel, D. (2004). 'The relationships among perceived quality, perceived risk and perceived product value', *Journal of Product & Brand Management*. 13. pp. 156-167. 10.1108/10610420410538050.

Stone, R. N. and Grønhaug, K. (1993). 'Perceived risk: Further considerations for the marketing discipline'. *European Journal of marketing*, 27(3), pp. 39-50.

Sweeney, J. and Soutar, G. (2001). 'Consumer Perceived Value: The Development of a Multiple Item Scale', *Journal of Retailing*. 77. pp. 203-220. 10.1016/S0022-4359(01)00041-0.

Sweeney, J.C., Soutar, G.N. and Mazzarol, T. (2008), 'Factors influencing word of mouth effectiveness: receiver perspectives', *European Journal of Marketing*, 42 (3), pp. 344-364. https://doi.org/10.1108/03090560810852977 .

Tung, C. (2013). 'Customer satisfaction, perceived value and customer loyalty: the mobile services industry in China', African Journal of Business Management. 7. 1730-1737. 10.5897/AJBM10.383.

Tzavlopoulos, I. et al. (2019). 'Determining the impact of e-commerce quality on customers' perceived risk, satisfaction, value and loyalty', *International Journal of Quality and Service Sciences,* 11(4), pp. 576-587.

Verhoef, et al. (2015). 'From multi-channel retailing to omni-channel retailing: introduction to the special issue on multi-channel retailing', *Journal of retailing* 91(2): pp.174-181.

Von, S.R. and Van, N.J. (2013). *From information security to cyber security, Computers & security.* Vol *38*, page 97-102.

Westbrook , R. A. (1987) 'Product/Consumption-Based Affective Responses and Postpurchase Processes', *Journal of Marketing Research*, 24: pp. 258-270.

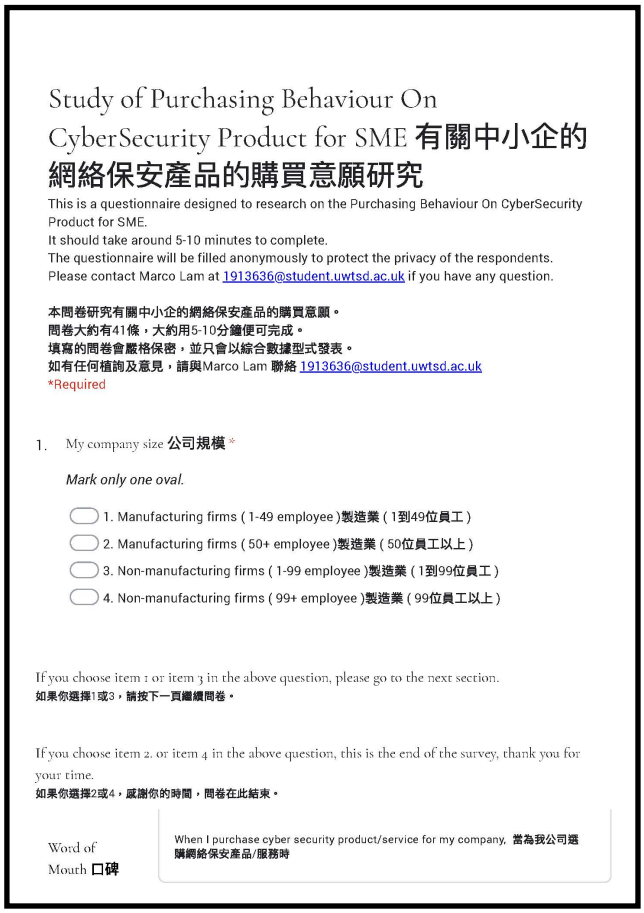
Woodruff, R. B. (1997). 'Customer value: the next source for competitive advantage', *Journal of the academy of marketing science*, 25(2), pp. 139.

Zeithaml, V. A. (1988). 'Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence', *Journal of marketing*, 52(3), pp. 2-22.

Zia, M. (2017). 'Impact of Product Attributes on Purchase Decision: A Study of Processed Food Consumer in India'.

Appendix

Appendix i Draft questionnaire



Study of Purchasing Behaviour On CyberSecurity Product for SME 有關中小企的網絡保安產品的購買意願研究

This is a questionnaire designed to research on the Purchasing Behaviour On CyberSecurity Product for SME.
It should take around 5-10 minutes to complete.
The questionnaire will be filled anonymously to protect the privacy of the respondents.
Please contact Marco Lam at 1913636@student.uwtsd.ac.uk if you have any question.

本問卷研究有關中小企的網絡保安產品的購買意願。
問卷大約有41條，大約用5-10分鐘便可完成。
填寫的問卷會嚴格保密，並只會以綜合數據型式發表。
如有任何查詢及意見，請與Marco Lam 聯絡 1913636@student.uwtsd.ac.uk
*Required

1. My company size 公司規模 *

Mark only one oval.

- 1. Manufacturing firms (1-49 employee)製造業 (1到49位員工)
- 2. Manufacturing firms (50+ employee)製造業 (50位員工以上)
- 3. Non-manufacturing firms (1-99 employee)製造業 (1到99位員工)
- 4. Non-manufacturing firms (99+ employee)製造業 (99位員工以上)

If you choose item 1 or item 3 in the above question, please go to the next section.
如果你選擇1或3，請按下一頁繼續問卷。

If you choose item 2. or item 4 in the above question, this is the end of the survey, thank you for your time.
如果你選擇2或4，感謝你的時間，問卷在此結束。

Word of Mouth 口碑

When I purchase cyber security product/service for my company, 當為我公司選購網絡保安產品/服務時



2. 1. I will ask for the opinions from my friends. 我會問朋友的意見。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

3. 2. I will ask for the opinions from my business partners. 我會問生意伙伴的意見。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

4. 3. I will believe the comments from different social media. 我會相信在不同社交媒體上的評語。 *

Mark only one oval.

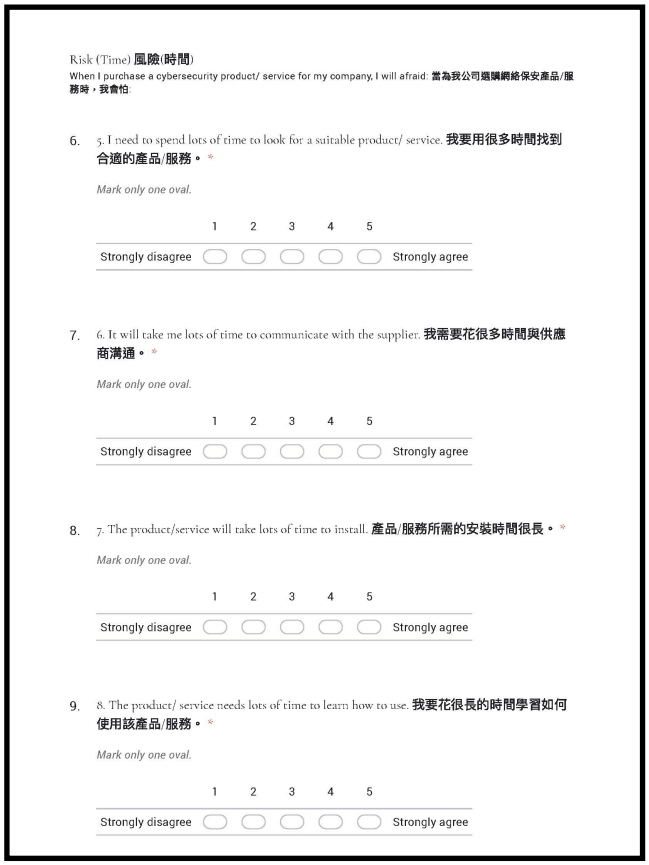
	1	2	3	4	5	
Strongly disagree						Strongly agree

5. 4. I will believe the user comments from the offical website of the product/service provider. 我會相信產品/服務商的官方網站上的用家評語。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

Risk 風險



Risk (Time) 風險(時間)
When I purchase a cybersecurity product/ service for my company, I will afraid: 當為我公司選購網絡保安產品/服務時，我會怕:

6. 5. I need to spend lots of time to look for a suitable product/ service. 我要用很多時間找到合適的產品/服務。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

7. 6. It will take me lots of time to communicate with the supplier. 我需要花很多時間與供應商溝通。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

8. 7. The product/service will take lots of time to install. 產品/服務所需的安裝時間很長。 *

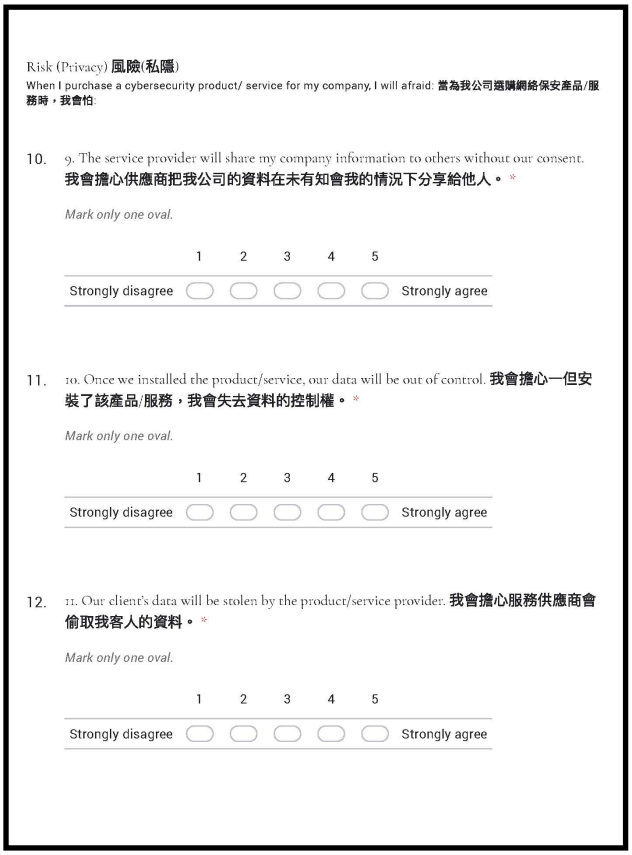
Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

9. 8. The product/ service needs lots of time to learn how to use. 我要花很長的時間學習如何使用該產品/服務。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree



Risk (Privacy) 風險(私隱)
When I purchase a cybersecurity product/ service for my company, I will afraid: 當為我公司選購網絡保安產品/服務時，我會怕:

10. 9. The service provider will share my company information to others without our consent. 我會擔心供應商把我公司的資料在未有知會我的情況下分享給他人。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

11. 10. Once we installed the product/service, our data will be out of control. 我會擔心一但安裝了該產品/服務，我會失去資料的控制權。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

12. 11. Our client's data will be stolen by the product/service provider. 我會擔心服務供應商會偷取我客人的資料。 *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

13. 12. The online payment method for the product/service is not safe. **產品/服務的網上付款方式不安全。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Risk (Financial) **風險(金錢)**

When I purchase a cybersecurity product/ service for my company, I will afraid: **當為我公司選購網絡保安產品/服務時，我會怕:**

14. 13. My company will pay a higher initial cost than the market price. **我公司支付的安裝費用比市場價格貴。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

15. 14. My company will pay a higher maintenance cost than the market price. **我公司支付的維護費用比市場價格貴。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

16. 15. There will be unexpected surcharge appeared during the service. **在服務期間會有額外的突發費用。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

17. 16. My Company will pay more than market price. **我公司支付的比市場價格更多。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Risk (Functional) **風險(功能)**

When I purchase a cybersecurity product/ service for my company, I will afraid: **當選購網絡保安產品/服務時，我會怕:**

18. 17. My company will not get technical support while facing a technical issue. **我公司有技術問題時未能找到技術支援。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

19. 18. My company will not get the same product/ service described in the promotion martial. **我公司不能得到與宣傳物上介紹相同的產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

20. 19. The product cannot help to protect the network of my company. **產品/服務不能保護我公司的網絡。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

21. 20. I cannot compare the function of the product/service with other product/service provider. **我不能比較不同的公司產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Risk (Psychological) **風險(心理)**

When I purchase a cybersecurity product/ service for my company, I will afraid: **當選購網絡保安產品/服務時，我會怕:**

22. 21. I will not like the product/service **我公司不喜歡該產品/服務** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

23. 22. I will have an unpleasant feeling when my company is using the product/service. **使用產品/服務時會令我不愉快。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

24. 23. I will feel the anxiety to install the product/service. **使用產品/服務時會令我不安。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value **價值**

Value(Functional) **價值 (功能性)**

When I purchase a cybersecurity product/ service for my company, I will expect: **當選購網絡保安產品/服務時，我會期望:**

25. 24. The product/service is easy to use. **產品/服務操作容易。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

26. 25. The product/service will increase the efficiency of my company. **產品/服務能提高我公司的工作效率。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

27. 26. The product/service will increase my quality of life. **產品/服務能提高我的生活質素。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value(Social value) **價值 (社會性)**
When I purchase a cybersecurity product/ service for my company, I will expect: **當選購網絡保安產品/服務時，我會期望:**

28. 27. The product/ service will increase my company social acceptance. **產品/服務能提高我公司的社會認同。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

29. 28. The product/ service will help my company differentiate from the competitors. **產品/服務能令我公司比競爭對手優勝。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

30. 29. The product/ service will help my company to build a positive image. **產品/服務能令我公司建立正面型像。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value (Emotaional) **價值(情感)**
When I purchase a cybersecurity product/ service for my company, I will expect: **當選購網絡保安產品時，我會期望:**

31. 30. The product/ service brings a sense of safety to my company. **產品/服務能令人感到我公司是安全的** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

32. 31. I will enjoy using the product/service. **我會享受使用該產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

33. 32. My company staff will feel confident about network safety. **我公司同事會對網絡保安有信心。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value (Epistemic) **價值(嘗新性)**
When I purchase a cybersecurity product/ service for my company: **當選購網絡保安產品時:**

34. 33. I will want to try a new product/service. **我希望試到新的產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

35. 34. I will want the product/service provider that can satisfy my curiosity. **產品/服務提供者可以滿足我的好奇心。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

36. 35. My company will like to try a new add-on about the product/service. **我公司願意嘗試產品/服務新的附加功能。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value (Conditional) **價值(條件性)**

37. 36. If my company has been hacked before, my company will be more willing to purchase a cybersecurity product/ service. **若我公司的網絡曾被入侵，我公司將更有意願購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

38. 37. If there is a discount campaign, my company will be more willing to purchase a cybersecurity product/service. **若有折扣活動，我公司會更有意願購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

39. 38. If there is more news on the network of the different companies being attacked, my company will be more willing to purchase a cybersecurity product/service. **若有更多公司的網絡被攻擊的新聞，我公司會更有意願購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Purchase intention (**購買意願**)

40. 39. I will purchase cybersecurity product in the near future. **在未來我會購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

41. 40. I will recommend my friends or partners to purchase cybersecurity product in the near future. **在未來我會推薦朋友購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

42. 41. I will purchase cybersecurity product in the near future, even when the price goes up. **即使價格上調，我依舊會在未來購買更多網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

43. 42. I will recommend my friends to purchase cybersecurity product in the near future even if the price goes up. **即使價格上調，我依舊會推薦朋友在未來購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Thank you for your time, this is the end of the survey. **問卷完成，感謝你的參與。**

Appendix ii Details of Focus group interview

Details of the focus group

Date conduct	8 November 2020
Venue	An office in Lai Chi Kok
Participant	6 People
Duration	1 hour

Interview questions

	Questions	**Answer summary**
Question asked	1. Do you understand the instruction of the survey?	The instruction is clear and easy to understand
	2. Do you understand this survey target audience are the manager of Hong Kong SMEs?	Yes, the inviting message by Whatapp is clear and polite
	3. Do you understand all question clearly?	Questions are too long and meaning might be confused. The details comment list in the
	4. Are there any improvement ?	Suggested that the survey should add some wordings that state the participants can leave the surveys anytime they feel like too

Questions revised

No.	**Draft**	**After adjusted**	**Improvement**
4	I will believe the comments from different social media.	I trust the comments from different social media.	Deliver the message in. a more direct way.
8	The product/service will take lots of time to install.	Take lots of time to install.	Shorten the sentence and make it easier to read
11	Once we installed the product/ service, our data will be out of control.	Our data will be out of control after installation	Shorten the sentence and make it easier to read
18	My company will not get technical support while facing a technical issue.	Insufficient in technical support while facing a technical issue.	Replace “will not get” by “insufficient” to provide more accurate meaning
31	The product/ service brings a sense of safety to my company	Provide a safety feeling.	Use direct sentence to send clear message.
33	My company staff will feel confident about network safety.	Provide a new service environment.	Replace the staff’s feeling using the new service environment.

Appendix iii Final questionnaire

Study of Purchasing Behaviour On Cybersecurity Product/Service for SME 有關中小企的網絡保安產品/服務的購買意願研究

This is a questionnaire designed for the research of the Purchasing Behaviour On Cybersecurity Product/service for SME.
It should take around 5-10 minutes to complete.
You might leave the survey whenever you feel like to.
The questionnaire will be filled anonymously to protect the privacy of the respondents.
Please contact Marco Lam at 1913636@student.uwtsd.ac.uk if you have any question.

本問卷研究有關中小企的網絡保安產品/服務的購買意願。
問卷大約有42條，大約用5-10分鐘便可完成。
你可按自己意願隨時離開此問卷。
填寫的問卷會嚴格保密，並只會以綜合數據型式發表。
如有任何垂詢及意見，請與Marco Lam 聯絡 1913636@student.uwtsd.ac.uk

*Required

1. My company size **公司規模** *

Mark only one oval.

- 1. Manufacturing firms (1-49 employee)**製造業 (1到49位員工)**
- 2. Manufacturing firms (50+ employee)**製造業 (50位員工以上)**
- 3. Non-manufacturing firms (1-99 employee)**非製造業 (1到99位員工)**
- 4. Non-manufacturing firms (99+ employee)**非製造業 (99位員工以上)**

If you choose item 1 or item 3 in the above question, please go to the next section.
如果你選擇1或3，請按下一頁繼續問卷。

If you choose item 2 or item 4 in the above question, this is the end of the survey, thank you for your time.
如果你選擇2或4，感謝你的時間，問卷在此結束。

Word of Mouth
口碑

When I purchase cyber security product/service for my company, **當為我公司選購網絡保安產品/服務時**

2. I will seek advice from my friends. **我會問朋友的意見。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

3. I will seek advice from my business partners. **我會問生意伙伴的意見。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

4. I trust the comments from different social media. **我會相信在不同社交媒體上的評語。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

5. I trust the user comments from the official website of the product/service provider. **我會相信產品/服務商的官方網站上的用家評語。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

Risk **風險**

Risk (Time) **風險(時間)**
When I purchase a cybersecurity product/ service for my company, I am afraid I will /there is: **當為我公司選購網絡保安產品/服務時，我擔心我會:**

6. Spend lots of time to look for a suitable product/ service. **我要用很多時間找到合適的產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

7. Take me lots of time to communicate with the supplier. **我需要花很多時間與供應商溝通。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

8. Take lots of time to install. **所需的安裝時間很長。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

9. Needs lots of time to learn how to use. **花很長的時間學習** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

Risk (Privacy) **風險(私隱)**
When I purchase a cybersecurity product/ service for my company, I am afraid I will /there is: **當為我公司選購網絡保安產品/服務時，我會怕:**

10. Share my company information to others without our consent. **我公司的資料在未有知會我的情況下分享給他人。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

11. Our data will be out of control after installation. **我會在安裝產品/服務後失去資料的控制權。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

12. Our client's data will be stolen. **我的客人資料會被偷取。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

13. Insured on the online payment method. **網上付款方式不安全。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

Risk (Financial) **風險(金錢)**
When I purchase a cybersecurity product/ service for my company, I am afraid I will /there is: **當為我公司選購網絡保安產品/服務時，我會怕:**

14. Pay a higher initial cost than the market price. **支付的安裝費用比市場貴。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

15. Pay a higher maintenance cost than the market price. **支付的維護費用比市場價格貴。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

16. Unexpected huge surcharge on additional service. **在服務期間會有額外巨額突發費用。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

17. Pay more than the market price. **支付的比市場價格貴。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Risk (Functional) **風險(功能)**
When I purchase a cybersecurity product/ service for my company, I am afraid i will /there is: **當選購網絡保安產品/服務時，我會怕:**

18. Insufficient in technical support while facing a technical issue. **有技術問題時未能找到足夠技術支援。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

19. Different product/ service in the promotion martial. **與宣傳物上介紹的產品/服務有所不同。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

20. Insufficient network protection of my company. **產品/服務不能保護我公司的網絡。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

21. Difficult to compare the product/service before purchase. **在購買前不能比較同類產品。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Risk (Psychological) **風險(心理)**
When I purchase a cybersecurity product/ service for my company, I will afraid: **當選購網絡保安產品/服務時，我會怕:**

22. Dislike the product/service **我公司不喜歡該產品/服務** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

23. I have an unpleasant feeling when my company is using the product/service. **使用產品/服務時會令我不愉快。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

24. I will feel the anxiety to install the product/service. **使用產品/服務時會令我不安。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value **價值**

Value(Functional) **價值 (功能性)**
When I purchase a cybersecurity product/ service for my company, I expect, the product/service is/are/will ：**當選購網絡保安產品/服務時，我會期望產品/服務:**

25. Ease to use. **操作容易。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

26. Increase the productivity of my company. **能提高我公司的工作效率。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

27. Enhance our service quality. **能提高我公司的服務質素。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value(Social value) **價值 (社會性)**
When I purchase a cybersecurity product/ service for my company, I expect, the product/service is/are/will ：**當選購網絡保安產品/服務時，我會期望:**

28. Increase our acceptance by clients. **能提高我客戶的認同。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

29. Differentiate our product/ service from the competitors. **產品/服務能令我公司比競爭對手優勝。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

30. Build a pisitive image. **令我公司建立正面型像。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value (Emotional) **價值(情感)**

When I purchase a cybersecurity product/ service for my company, I expect, the product/service will ：**當選購網絡保安產品時，我會期望:**

31. Provide a safety feeling. **感到我公司是安全的** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

32. Provide a joyful experience. **享受使用該產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

33. Provide a new service environment. **提供新的工作環境。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value (Epistemic) **價值(嘗新性)**

When I purchase a cybersecurity product/ service for my company: **當選購網絡保安產品時:**

34. I am willing to try a new product/service. **我願意試新的產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

35. It will satisfy my curiosity. **可以滿足我的好奇心。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

36. I am willing to try new auxiliary product/ service. **願意嘗試產品/服務新的附加功能。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Value (Conditional) **價值(條件性)**

37. If my company was being hacked, we will be more willing to try a cybersecurity product/ service. **若我公司的網絡曾被入侵，我公司將更有意願購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

38. If there is a promotions campaign, we will be more willing to try. **若有推廣活動，我公司會更有意願購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

39. If there is news about the backing of companies, we will be more willing to try. **若有公司網絡被攻擊的新聞，我公司會更有意願購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Purchase intention (**購買意願**)

40. I will purchase a cybersecurity product in the near future. **在未來我會購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

41. I will recommend my friends or partners to purchase cybersecurity product/service in the near future. **在未來我會推薦朋友購買網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

42. I will purchase a cybersecurity product in the near future, even when the price goes up. **即使價格上調，我依舊會在未來購買更多網絡保安產品/服務。** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

Thank you for your time, this is the end of the survey. **問卷完成，感謝你的參與。**

This content is neither created nor endorsed by Google.

Google Forms

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

THE FACTORS AFFECT PURCHASE INTENTION OF CYBERSECURITY PRODUCT IN SME MARKET OF HONG KONG

A proposal submitted for the

Master of Business Administration (MBA) 2021

Submitted : Oct 2020

Student: Marco Lam

Student Number : 1913636

Supervisor : Dr. WONG, Chi Hong Arion

I

Abstract

The demand for cybersecurity solutions had been rising world-wide under the COVID-19 pandemic which recorded a market size growth 7.6% in 2020 which. Although the world-wide SMEs market had an increasing demand for end-point security solutions, for example anti-virus and email protection, Hong Kong SMEs market seem didn't share the same trend. The cybersecurity readiness of Hong Kong SMEs had decrease 2.4 points in 2020. This study aim to explore factors that affect the purchase intention of Hong Kong SMEs toward cybersecurity product and service in order to help local service and product providers forming a better marketing plan to develop Hong Kong market.

This dissertation will include first-hand and second-hand researches. Factors will be identified which will affect purchase intention of SMEs. Following up, there will be a survey to conduct which targeted the managements of SMEs in Hong Kong. In the process of developing the survey, focus group discussion and pilot test will be performed which might help the full scale survey conducted successfully. The survey targeted to collect responses from 356 managements from Hong Kong SMEs and the data will be analysed using SPSS with different statistical tools. The positive liner relationship and regression test will be performed to look for regression relationship between factors and purchase intention.

The recommendations to local cybersecurity product and service providers will be stated For further study, the suggestion would be made and the limitation will be stated to provide information for further study .

Table of content

Abstract	II
Table of content	III
1. Introduction	1
1.1.Industry overview	1
1.2.Research rationale	3
1.3.Research question	4
1.4.Objective of the research	5
1.5.Structure overview	5
2. Literature review	8
2.1.Perceived value	8
2.2.Perceived risk	8
2.3.Word of mouth (WOM)	8
2.4.Purchase intention	9
3. Methodology	10
3.1.Research framework	10
3.2.Research type	10
3.3.Research target	11
3.4.Sampling method	11
3.5.Analysis methods	11
3.5.3.Correlation	12
3.5.4.Regression	12
4. Conclusion	13
4.1.Recommendation	13
4.2.Limitation of the study	13
4.3.Recommendation on further study	13
5. Conclusion	14
Reference	15
Bibliography	16

1. Introduction

This introduction will provide fundamental information and background of the topic. Within the first part of the introduction session, an industry overview of cybersecurity will be covered. Also current market size, market players and elaboration of a few cybersecurity cases will be discussed. After that, there were some definitions of key concepts and news that will help readers who are not familiar with the topic to have a ground of understand. Then it will review the research rationale and research question by looking into some facts of Hong Kong Small and Medium size Enterprises with other trends.

1.1.Industry overview

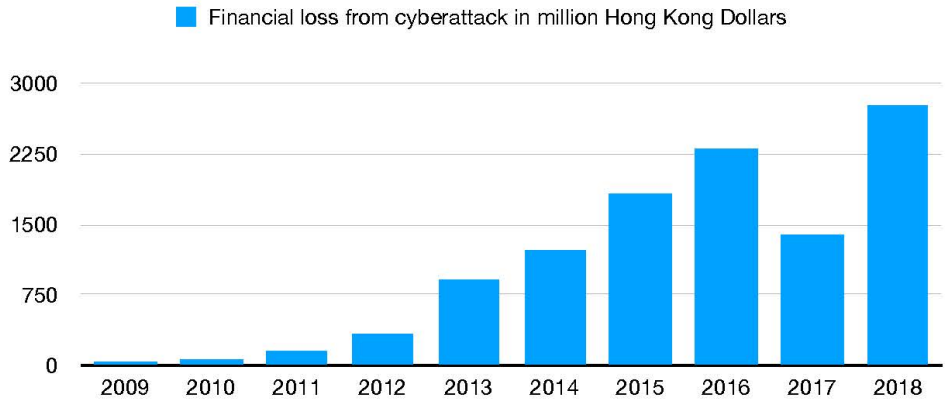
The demand of cybersecurity solutions had been rising world-wide under the COVID-19 pandemic. Governments and large enterprises promote Work-form-home policy to protect staff from getting inflated (News HKGOV, 2020; Davis, 2020). For example 75% of staff in Standard Charter bank had been work from home during the pandemic.

The impact of pandemic created an opportunity for companies to speed up their digital transformation (German Industry and Commerce Ltd., 2020). Companies in all different size were getting their business operations more relay on computer systems and moving faster to setup online stores that keep customers engaged. The cybersecurity risks for companies were increasing as the number of systems and customer's information were growing towards their business growth. In details, adopting new technologies such as machine learning, internet of things (IoT), cloud computing and big data had increased the needs of cybersecurity solutions for all size of companies.

Hong Kong is an international city with the largest stock market in Asia. However, the SMEs market of cybersecurity in Hong Kong seems not share the same trend with the rest of the world.

The cybersecurity readiness of Hong Kong SMEs has decreased 2.4 points in 2020. In an annual survey, conducted by HKPC, indicated that the Hong Kong SMEs only have 56.3 point in the readiness of cybersecurity (HKCERT, 2020a) and only less than 60% of SMEs think they can handle a cyberattack. The readiness of basic element were decreasing by 2.4 point compare to 2019 (HKCERT, 2020a). That meant over 343,313 small and medium sized enterprises (SMEs) in Hong Kong were not quite ready for cyber attack.

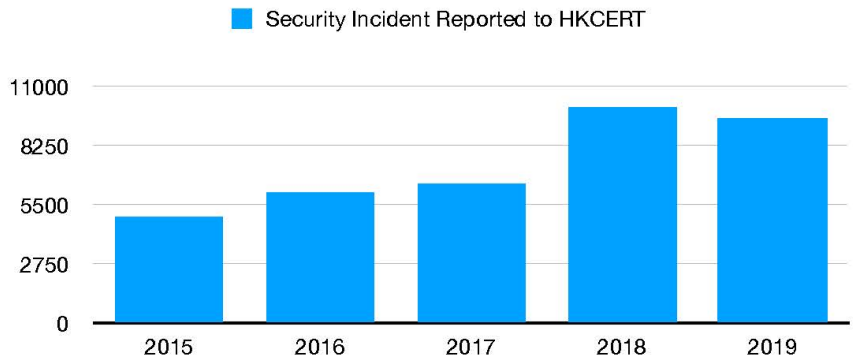
Figure 1.1.1 Financial loss from cyberattack in Hong Kong



Sources: Lai (2020)

The Figure 1.1 provided a concept of the overall cybersecurity environment in Hong Kong. The total cost of cyber crime in 2018 (Lai, 2020) was the record high since 2009. The reported loss growth over 300000% in the past 10 years.

Figure 1.1.2 Cyber Security incident reported to HKCERT



Sources: HKCERT (2020b)

Table 1.1.2 showed that the reported cybersecurity cases in Hong Kong. the number of attacks handled by HKCERT reached 9,458 in 2019, draped 6% compared to 2018 as shown in figure 1.2. The dropping is caused by the attackers shifted their focus from mass volume attack to attacking for profit which meant their attack methods changed from malware to Botnet and Phishing email (HKCERT, 2020b).

Apart from international enterprises, there were also some local companies providing cybersecurity services and products in Hong Kong. Both international firms and local firms were now looking for ways to take full advantage of growth of SMEs cybersecurity service and product market in Hong Kong (Goldstein research, 2020).

1.2.Research rationale

In Hong Kong, there are lots of international and local market players as mentioned. They both have certain groups of target audiences. For international cybersecurity firms like Splunk and IBM, their primary target segments are enterprises with

different operation locations and using lots of systems to run their businesses. Their primary target are local public listed companies and/or large enterprises.

For local cyber security enterprises, they might have insufficient resources to serve those large organisations and usually placed themselves as a system integrator who helps to resell and implement security products. SMEs are usually their target customers. HKCERT (2020) stated that there are 51% more phishing cases in 2020 compared to 2019 due to the pandemic. Most of the phishing emails used fake government funding site to attack SMEs. And the fundings are often for support SMEs this indicted that hackers are targeting on SMEs. Thus, more cybersecurity service and product providers tend to target the same group of people as the demand in SME market is increasing.

There are more than 340,000 of SMEs (SUCCESS HKSAR, 2020) in Hong Kong, constituting more than 98% of business unite and 45% of workforce in private. As a result, SMEs could be one of the most potential market for the industry to explore and invest for.

In today's competitive business environment, the industry should understand the target segments purchasing behaviour in order to differentiate their marketing strategies.

This study aim to explore factors that affect the purchase intention of Hong Kong SMEs toward cybersecurity product and service in order to help local service and product providers forming a better marketing plan to develop Hong Kong market.

1.3.Research question

This dissertation would like to use different research methods to find out what is the factors that affect the purchase intention of SME in Hong Kong toward cybersecurity

products or services. The research questions of the discretion will focus on three areas to provide full picture for readers.

To be more specifically answering the research questions, the dissertation will try to answer the questions below.

a. What is the driver when SMEs purchase cybersecurity products or service?
b. How those factors affect the decision make?
c. What are the motivations to attract SMEs to purchase cybersecurity product and service ?

1.4. Objective of the research

The main purpose of this research is to explore the factors that affect purchasing intention of small and medium size businesses towards purchasing cybersecurity product. To answer the research question, the objective expend into the three objectives accordingly.

a. Identification of the concepts and components of factors that affect purchasing behaviour of SME in cybersecurity product.
b. To identify the relationship between factors that apply to SME market in Hong Kong.
c. Development of recommendation of effective market expansion plans.

From the results of the factors and hypothesis, this study will provide some suggestions for cybersecurity service or product providers that can help them to promote more effectively.

1.5.Structure overview

In this research, the researcher will perform a classic 5 chapters structure in the dissertation in order to best demonstrate this MBA program study target.

Chapter 1 will be the introduction which provides essential information for readers to understand the research topic and the rationale behind. Some definition of terms and concepts will be stated in this chapter. The main research question with objective will also be discussed in this chapter.

Chapter 2 is literature review, there will be some major research areas. The main focus will be designed according to the review result. The first review highlight is on research method, review article and peer reviewed research which provide some insights to find out how this discretion questionnaire should design. The second review highlight will focus on different factors, as there are many factors would affect purchase intention in certain market. This review aims to find out some of the most important factors we should focus on. At the end of the chapter, there will be a list of hypotheses formed in the process of literature review.

Chapter 3 will discuss the methodology of this dissertation from the result of the literature review. This chapter will also provide a clear plan for readers to understand how specific studies are valid to answer the specific research questions. Next, research methods such as which type of data and target segment classification will be discussed. To answer the research questions we will also discuss the major factors that this dissertation concern, and how the factors will be construct along the research and analysis. Each of the hypotheses will be examined and properly define with literature support. After the hypotheses discussion, there will be information that stated the statistical support on in the proposed questionnaire questions. At the end of the chapter, there are list of question used in the questionnaire provided with proper explanation.

Chapter 4 is the chapter we will perform a data analysis on the survey, SPSS will be used as the main analysis tools. Different methods will be consider according to

result of literature review. At the end of this chapter, the result of the factors that affect SMEs purchase intention will be stated

Chapter 5 will be the chapter to conclude the assessment of the dissertation. Suggestion for industry players and further research will also be elaborate in this chapter.

2. Literature review

This part of the dissertation will explore a wide range of literature that related to the research topic to find a suitable angle on how should the topic be better discussed. After that, three factors that affect purchase intention will be discussed. The discussed factors also will help to form the hypotheses at the end of this literature review session.

2.1.Perceived value

The terms perceived value had been mentioned in an article in 1960 (Levitt, 1960), it defined as base functions of a products. Despite there were lots of researchs under the topic, the concept of perceived value has often being confused with other similar words. Khalifa (2004) stated that the concept has become one of the most overused and misused concepts in social sciences field and in the management literature.

2.2.Perceived risk

The concept about perceived risk was first presented at 1960s, Bauer (1960) described perceived risk as a sense of unpleasant feeling, that customer would feel before they took the action to purchase a service and a product. The feeling came from uncertainty some factor of risk. Since the first introduced, researcher almost obsessed in explore the concept. In this part of the review, we will look into some concept worth discussing.

2.3.Word of mouth (WOM)

The word Word of Month (WOM), is defined as how consumers share conversation about a product or service experience (Sen and Lerman, 2007). There are some study provide factors forming the word of month, as the volume of information of

product can be relatively high for one product, consumers cannot read all the comment or statement posted.

2.4.Purchase intention

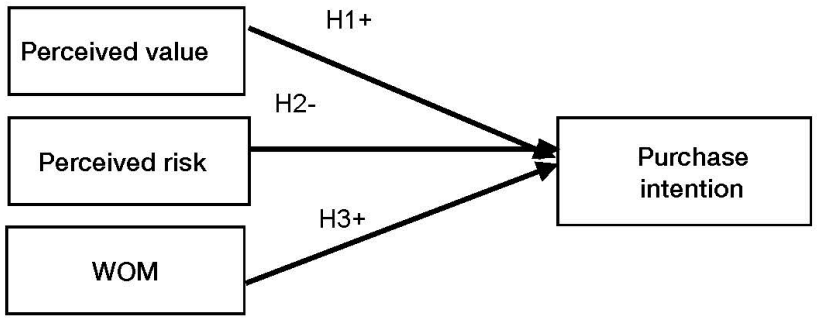
Dodds, Monroe and Grewal (1991) described the intention included element like satisfaction toward the product or service. Mazumdar and Monroe (1992) pointed out that the intention should be a subjective feeling but not an objective feelings, which can be influenced by external factor. When performing a wide range of literature review, researcher take reference in wide range of article and study about factor that affect customer purchase behaviour and intention.

3. Methodology

This chapter will further develop the research questions by using some of the basic concept explored in chapter 2. Firstly the hypotheses will be carried out. Secondly questionnaire and research framework will be discussed. The result of hypotheses will be discussed in the next chapter.

3.1.Research framework

Figure 3.1.1 Research framework



Sources : Figure construct by writer

The research framework, shown in figure 3.1.1, are drafted according to the research rationale and objective in chapter 1 and literature review in the last chapter. Perceived value, perceived risk and WOM are independent variable while the purchase intention is the dependant variable. The following session will discuss their relationship.

3.2.Research type

For qualitative research, this dissertation will use literature review and analyses second-hand data while for quantitative research methods will include a questionnaire that collect first-hand data to help understand the purchase intention for SME business in Hong Kong towards cybersecurity products.

3.3.Research target

Research question of this research is the purchase intention for SME business in Hong Kong towards cybersecurity products. Most of the company nowadays use computer system and network to process clients request and daily operation, The questionnaire will answered by the management of SMEs in Hong Kong.

3.4.Sampling method

To understand the purchase intention of SEMs in Hong Kong, the best choice is to send survey to all SMEs in Hong Kong. The total number of SMEs in Hong Kong is over 340,000, that is almost impossible to ask all the company on this research topic considering the resources involved in this dissertation. Therefore, snowball sampling method will be use to support this study.

The up coming questionnaire will use Google form as a tools to collect feedback from SEMs management response.

3.5.Analysis methods

The questionnaire result will be analysed using SPSS version 27. The following section will discuss some critical tools.

3.5.1. Descriptive statistics

Descriptive statistics will be used to describe the data (Bickel and Lehmann, 2012) in many ways.

3.5.2.Reliability test

To ensure the survey is properly develop and the data collect can represent a certain level of the truth, reliability test is consider one of the most important test every survey should pass (Fink and Litwin, 1995), which will be included in this session.

3.5.3. Correlation

The tool will be used to analyse the relationship among three variable and one independent variable.

3.5.4.Regression

Regression analysis is a statistical tools used to estimate the relationship between a dependent variable and independent variables (Brook and Arnold, 2018), which will be used in the session.

4. Conclusion

The research question of this dissertation will explore the factor that affect the purchase intention of SMEs on cybersecurity product or service. In chapter 1, the background overview with the research question had been stated. Literature review will discuss different literature point of view on factors related to research topic. A survey will be conducted that aim to collect first-hand data of SMEs on the purchase intention about the research questions.

In chapter 4, SPSS was used to perform a series of analysis to test the reliability and the relationship of all 3 independent variables with dependant variable. There was recommendations and summary of this dissertation presented in this chapter.

4.1.Recommendation

As there will be proofed relationship between purchase intention and perceived value, service or product provider are suggested to take a deeper look of the benefits customer can feel before their purchase.

4.2.Limitation of the study

There are some limitation and factors that might affect the result of the study, To highlight them in this section would provide suggestion to improve the accurate of the research.

4.3.Recommendation on further study

There are few recommendation of further study, first few will be on sampling method and some will be on other researcher who want to explore more in some idea inspired by this discretion.

5. Conclusion

The research question of this dissertation will explore the factor that affect the purchase intention of SMEs on cybersecurity product or service. The details summary of surveys, research objective and research questions will be presented in this section.

Reference

Goldstein research (2020). 'Asia-Pacific (Apac) Cyber Security Market Outlook : Market Segmentation Based On Security Type, Based On Solutions, Based On Services, Based On Deployment Mode, Based On End-User & By Region With Covid-19 Impact | Forecast Period 2017-2030'. Available at :https://www.goldsteinresearch.com/report/asia-pacific-apac-cyber-security-market-outlook-2024-opportunity-assessment-and-demand-analysis-market-forecast-2016-2024/ (Accessed at : 5 October 2020).

HKCERT (2020a) 'SSH Hong Kong Enterprise Cyber Security Readiness Index Survey Down 2.4 Points to 46.9 Staying Vigilant for Cyber Threats in Stormy Times'. Available at: https://www.hkcert.org/blog/ssh-hong-kong-enterprise-cyber-security-readiness-index-survey-down-24-points-to-469-staying-vigilant-for-cyber-threats-in-stormy-times (Accessed: 8 October 2021).

Lai, L.T. (2020) 'Financial loss due to computer crime in Hong Kong from 2009 to 2018' Available at : https://www.statista.com/statistics/786989/hong-kong-financial-loss-caused-by-computer-crime/ (Accessed 10 October 2020).

News HKSAR (2020) 'Government extends social distancing measures'. Available at : https://www.info.gov.hk/gia/general/202008/10/P2020081000774.htm (Accessed: 6 October 2021).

HKCERT (2020b). 'Security Incidents Reported to Us'. Available at : https://www.hkcert.org/statistic (Accessed: 8 October 2020).

SUCCESS HKSAR (2020). 'Small and medium enterprises (SMEs)'. Available at: https://www.success.tid.gov.hk/english/aboutus/sme/service_detail_6863.html (Accessed: 16 October 2021).

Bibliography

Bauer, R. A. (1960). *Consumer behavior as risk taking*. Chicago, IL, pp. 384-398.

Brook, R. J., and Arnold, G. C. (2018). *Applied regression analysis and experimental design*, Routledge.

Bickel, P. J., and Lehmann, E. L. (2012). 'Descriptive statistics for nonparametric models' *I. Introduction. In Selected Works of EL Lehmann*. Springer, Boston, MA. pp. 465-471

Davis, R. (2020). *COVID-19: The world's biggest ever technology pilot*, Standard Chartered. Available at : https://www.sc.com/en/navigate-the-future/covid-19-the-worlds-biggest-ever-technology-pilot/ (Accessed: 5 Oct 2020).

Dodds, W. B., Monroe, K. B., and Grewal, D. (1991). 'Effects of price, brand, and store information on buyers' product evaluations', *Journal of marketing research*, 28(3), pp. 307-319.

Fink, A. and Litwin, M. S. (1995). *How to measure survey reliability and validity* (Vol. 7). Sage.

German Industry and Commerce Ltd. (2020). 'Driving Digital Transformation: Business after Covid-19'. Available at: https://hongkong.ahk.de/news/news-details/driving-digital-transformation-business-after-corona (Accessed : 5 November 2020).

Levitt, T. (1960). 'Marketing myopia', *Harvard Business Review, 38,* 45–56.

Mazumdar, T., and Monroe, K. B. (1992). 'Effects of inter-store and in-store price comparisons on price recall accuracy and confidence', *Journal of Retailing*, 68(1), pp. 66.

Sen, S. and Lerman, D. (2007). 'Why are you telling me this? An examination into negative consumer reviews on the web', *Journal of Interactive Marketing, 21(4), pp. 76-94.*

Appendix v Ethic Form

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically. A researcher may not be covered by the University's insurance if ethical approval has not been obtained prior to commencement.

The University follows the OECD Frascati manual definition of **research activity**: "creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications". As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the "principal researcher".

Ethical approval is not required for routine audits, performance reviews, quality assurance studies, testing within normal educational requirements, and literary or artistic criticism.

Please read the notes for guidance before completing ALL sections of the form.

This form must be completed and approved prior to undertaking any research activity. Please see Checklist for details of process for different categories of application.

Delete the Guidance Notes at the end of the form BEFORE submitting your application

SECTION A: About You (Principal Researcher)

1	Full Name:	Lam Wai Yeung				
2	Tick all boxes which apply:		Member of staff:	□	Honorary research fellow:	□
3	Undergraduate Student	□	Taught Postgraduate Student	√	Postgraduate Research Student	□

4	Institute/Academic Discipline/Centre:	MBAMBA-HK
5	Campus:	Hong Kong
6	E-mail address:	marco.lam@stormeye.io
7	Contact Telephone Number:	+85290508670
	For students:	
8	Student Number:	1913636
9	Programme of Study:	MBAMBA-HK
10	Director of Studies/ Supervisor:	Dr. WONG, Chi Hong Arion

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

SECTION B: Approval for Research Activity

1	Has the research activity received approval in principle? (please check the Guidance Notes as to the appropriate approval process for different levels of research by different categories of individual)		YES	√	NO □
					Date
2	If Yes, please indicate source of approval (and date where known): ***Approval in principle must be obtained from the relevant source prior to seeking ethical approval***	Research Degrees Committee	√		
3		Institute Research Committee	□		
4		Other (write in)	□		

SECTION C: Internal and External Ethical Guidance Materials

	Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines.	
1	**UWTSD Research Ethics & Integrity Code of Practice**	√
2	**UWTSD Research Data Management Policy**	√
3		□

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

SECTION D: External Collaborative Research Activity

1	Does the research activity involve collaborators outside of the University?		YES	□	NO	√
2	If Yes, please provide the name of the external organisation and name and contact details for the main contact person and confirmation this person has consented to their personal data being shared as part of this collaboration.					
3	Institution					
4	Contact person name					
5	Contact person e-mail address					
6	Has this individual consented to sharing their details on this form?		YES	□	NO	□
7	Are you in receipt of a KESS scholarship?		YES	□	NO	□
8	Is your research externally funded		YES	□	NO	□
9	Are you specifically employed to undertake this research in either a paid or voluntary capacity?	Voluntary	YES	□	NO	□
10		Employed	YES	□	NO	□
11	Is the research being undertaken within an existing UWTSD Athrofa Professional Learning Partnership (APLP)	If YES then the permission question below does not need to be answered.	YES	□	NO	□
12	Permission to undertake the research has been provided by the partner organisation	(If YES attach copy) If NO the application cannot continue	YES	□	NO	□

Where research activity is carried out in collaboration with an external organisation

13	Does this organisation have its own ethics approval system?	YES	□	NO	□
14	If Yes, please attach a copy of any final approval (or interim approval) from the organisation				

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

SECTION E: Details of Research Activity

1	Indicative title:	Study of Purchasing Behaviour On Cybersecurity Product/Service for SME		
2	Proposed start date of your research (not your course start date):	10 Oct 2020	Proposed end date:	19 March 2021
3	**Introduction to the Research (maximum 300 words)** **Ensure that you write for a Non-Specialist Audience when outlining your response to the three points below:** • *Purpose of Research Activity* • *Proposed Research Question* • *Aims of Research Activity* • *Objectives of Research Activity* Demonstrate, briefly, how **Existing Research** has informed the proposed activity and explain • *What the research activity will add to the body of knowledge* • *How it addresses an area of importance.*			
4	**Purpose of Research Activity** To collect the point of view on purchase intention on SMEs (this box should expand as you type)			

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

5	**Research Question** When I purchase a cybersecurity product/ service for my company, I expect, the product/service is/ are/will : VF1 Ease to use. VF2 Increase the productivity of my company. VF3 Enhance our service quality. VS1 Increase our acceptance by clients. VS2 Differentiate our product/ service from the competitors. VS3 Build a positive image. VE1 Provide a safety feeling. VE2 Provide a joyful experience. VE3 Provide a new service environment. When I purchase a cybersecurity product/ service for my company: VEP1 I am willing to try a new product/service VEP2 It will satisfy my curiosity. VEP3 I am willing to try new auxiliary product/ service. VC1 If my company was being hacked, we will be more willing to try a cybersecurity product/ service. VC2 If there is a promotions campaign, we will be more willing to try. VC3 If there is news about the hacking of companies, we will be more willing to try. When I purchase a cybersecurity product/ service for my company, I am afraid I will /there is: RT1 Spend lots of time to look for a suitable product/ service. RT2 Take me lots of time to communicate with the supplier. RT3 Take lots of time to install. RT4 Needs lots of time to learn how to use. RP1 Share my company information to others without our consent. RP2 Our data will be out of control after installation. RP3 Our client's data will be stolen. RP4 Insured on the online payment method RF1 Pay a higher initial cost than the market price. RF2 Pay a higher maintenance cost than the market price RF3 Unexpected huge surcharge on additional service. RF4 Pay more than the market price. RFC1 Insufficient in technical support while facing a technical issue. RFC2 Different product/ service in the promotion martial. RFC3 Insufficient network protection of my company. RFC4 Difficult to compare the product/service before purchase. RPC1 Dislike the product/service RPC2 Have an unpleasant feeling when my company is using the product/service. RPC3 I will feel the anxiety to install the product/service. When I purchase cyber security product/service for my company, W1 I will seek advice from my friends. W2 I will seek advice from my business partners. W3 I trust the comments from different social media. W4 I trust the user comments from the official website of the product/service provider. (this box should expand as you type)

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

6	**Aims of Research Activity** a. Identification of the concepts and components of factors that affect purchasing behaviour of SME in cybersecurity product. b. To identify the relationship between factors that apply to SME market in Hong Kong. c. Development of recommendation of cost effective market expansion plan (this box should expand as you type)
7	**Objectives of Research Activity** a. Get first-hand data on SMEs view on research topic (this box should expand as you type)
8	**Proposed methods (maximum 600 words)** Provide a brief summary of all the methods that **may** be used in the research activity, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed.
9	Activity : Survey , Focus group Sampling methods : snowball sampling Sample size : Target 385 Total number of question : 42 Scale : 1-5 Way to analysis the result : SPSS a. Focus group test b. Pilot test c. Reliability test d. Correlation analysis e. Regression analysis The server will be uploaded to a privacy google form for participant to fill in. All the data will be deleted after the result of the discretion. (this box should expand as you type)

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

10	**Location of research activity** Identify all locations where research activity will take place.
11	Hong Kong (this box should expand as you type)
12	**Research activity outside of the UK** If research activity will take place overseas, you are responsible for ensuring that local ethical considerations are complied with and that the relevant permissions are sought. Specify any local guidelines (e.g. from local professional associations/learned societies/ universities) that exist and whether these involve any ethical stipulations beyond those usual in the UK (provide details of any licenses or permissions required). Also specify whether there are any specific ethical issues raised by the local context in which the research activity is taking place, for example, particular cultural and/or legal sensitivities or vulnerabilities of participants.
13	The research will be performed in Hong Kong *(this box should expand as you type)*

14	Use of documentation not in the public domain: Are any documents **NOT** publicly available?	**NO**	√
		YES	□
15	If Yes, please provide details here of how you will gain access to specific documentation that is not in the public domain and that this is in accordance with prevailing data protection law of the country in question and England and Wales. *(this box should expand as you type)*		

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

SECTION F: Scope of Research Activity

	Will the research activity include:	**YES**	**NO**
2	Use of a questionnaire or similar research instrument?	√	□
3	Use of interviews?	√	□
4	Use of diaries?	□	√
5	Participant observation with their knowledge?	□	√
6	Participant observation without their knowledge?	□	√
7	Use of video or audio recording?	□	√
8	Access to personal or confidential information without the participants' specific consent?	□	√
9	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	□	√
10	Performance of any acts which may cause embarrassment or affect self-esteem?	□	√
11	Investigation of participants involved in illegal activities?	□	√
12	Use of procedures that involve deception?	□	√
13	Administration of any substance, agent or placebo?	□	√
14	Working with live vertebrate animals?	□	√
15	Other primary data collection methods, please explain in this box For example, 'focus groups'. Please indicate the type of data collection method(s) in this box and tick the accompany box.		
16	Details of any other primary data collection method: (this box should expand as you type)	□	√

If NO to every question, then the research activity is (ethically) low risk and **may** be exempt from **some** of the following sections (please refer to Guidance Notes).

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

SECTION G: Intended Participants

	Who are the intended participants:	**YES**	**NO**
2	Students or staff at the University?	□	√
3	Adults (over the age of 18 and competent to give consent)?	√	□
4	Vulnerable adults?	□	√
5	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	□	√
6	Prisoners?	□	√
7	Young offenders?	□	√
8	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	□	√
9	People engaged in illegal activities?	□	√
10	Others (please identify specifically any group who may be unable to give consent) please indicate here and tick the appropriate box.		
11	Other – please indicate here: (this box should expand as you type)	□	√

12	**Participant numbers and source** Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
13	How many participants are expected?	More than 74 number of SMEs company in Hong Kong *(this box should expand as you type)*
14	Who will the participants be?	Representative of SMEs in Hong Kong *(this box should expand as you type)*
15	How will you identify the participants?	N/A *(this box should expand as you type)*

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

PG2 / E1 FORM

	Information for participants:	**YES**	**NO**	**N/A**
17	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	√	□	□
18	Will you tell participants that their participation is voluntary?	√	□	□
19	Will you obtain written consent for participation?	□	□	√
20	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	□	□	√
21	If the research is observational, will you ask participants for their consent to being observed?	□	□	√
22	Will you tell participants that they may withdraw from the research at any time and for any reason?	√	□	□
23	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	□	√	□
24	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	√	□	□
25	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	□	√	□
26	If NO to any of above questions, please give an explanation			
27	The main survey is a online questionnaire, the participant may leave anytime without any record. Therefore the answer will be No for questions 23 and 25. *(this box should expand as you type)*			

	Information for participants:	**YES**	**NO**	**N/A**
29	Will participants be paid?	□	√	□
30	Is specialist electrical or other equipment to be used with participants?	□	√	□
31	Are there any financial or other interests to the investigator or University arising from this study?	□	√	□
32	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	□	√	□
33	If YES to any question, please provide full details			
34	*(this box should expand as you type)*			

SECTION H: Anticipated Risks

1	**Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.** If you have completed a full risk assessment (for example as required by a laboratory, or external research collaborator) you may append that to this form.		
2	**Full risk assessment completed and appended?**	**Yes**	□
		No	√
3	**Risks to participants** For example: emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information		
4	Risk to Participant: *(this box should expand as you type)*	*How will you mitigate the Risk to Participant* *(this box should expand as you type)*	
5	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities		
	N/A *(this box should expand as you type)*		
6	**Risks to investigator** For example: personal safety, physical harm, emotional distress, risk of accusation of harm/ impropriety, conflict of interest		
	Risk to Investigator: N/A *(this box should expand as you type)*	*How will you mitigate the Risk to Investigator:* *(this box should expand as you type)*	
7	**University/institutional risks** For example: adverse publicity, financial loss, data protection		
	Risk to University: N/A *(this box should expand as you type)*	*How will you mitigate the Risk to University:* *(this box should expand as you type)*	

8	**Disclosure and Barring Service**			
9	If the research activity involves children or vulnerable adults, a Disclosure and Barring Service (DBS) certificate must be obtained before any contact with such participants.	**YES**	**NO**	**N/A**
10	Does your research require you to hold a current DBS Certificate?	□	□	√

SECTION I: Feedback, Consent and Confidentiality

1	**Feedback** What de-briefing and feedback will be provided to participants, how will this be done and when?
	N/A *(this box should expand as you type)*
2	**Informed consent** Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.
	N/A *(this box should expand as you type)*
3	**Confidentiality / Anonymity** Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.
	All name of participants or companies are anonymous. *(this box should expand as you type)*

SECTION J: Data Protection and Storage

In completing this section refer to the University's Research Data Management Policy and the extensive resources on the University's Research Data Management web pages (http://uwtsd.ac.uk/library/research-data-management/).

1	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 "GDPR" and the Data Protection Act 2018 "DPA")?	**YES**	**NO**
	"Personal data" *means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*	□	√
2	If YES, provide a description of the data and explain why this data needs to be collected:		
	(this box should expand as you type)		
3	Does it involve special category data (as defined by the GDPR)?	**YES**	**NO**
	"Special category data" *means sensitive personal data consisting of information as to the data subjects' –* *(a) racial or ethnic origin,* *(b) political opinions,* *(c) religious beliefs or other beliefs of a similar nature,* *(d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),* *(e) physical or mental health or condition,* *(f) sexual life,* *(g) genetics,* *(h) biometric data (as used for ID purposes),*	□	√
4	If YES, provide a description of the special category data and explain why this data needs to be collected:		
	(this box should expand as you type)		

5	Will the research activity involve storing personal data and/or special category data on one of the following:	**YES**	**NO**
6	Manual files (i.e. in paper form)?	□	√
7	University computers?	□	√
8	Private company computers?	□	√
9	Home or other personal computers?	√	□
10	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	□	√
11	"Cloud" storage or websites?	√	□
12	Other – specify:	□	√

13	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of password protection, encryption, anonymisation and pseudonymisation:		
	All file are stored in a strong password protected storage, the personal computer had install suitable protection software, the cloud storage will also be password protected and will not share to any third party. *(this box should expand as you type)*		
14	**All Data Storage**		
15	Will the research activity involve any of the following activities:	**YES**	**NO**
16	Electronic transfer of data in any form?	□	√
17	Sharing of data with others at the University?	□	√
18	Sharing of data with other organisations?	□	√
19	Export of data outside the European Union or importing of data from outside the UK?	□	√
20	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	□	√
21	Publication of data that might allow identification of individuals?	□	√
22	Use of data management system?	□	√
23	Data archiving?	□	√
24	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and DPA (and/or any international equivalent):		
	(this box should expand as you type)		
25	List all who will have access to the data generated by the research activity:		
	All name of participants or companies are anonymous. The data will only be present in summarised format. The university, researcher and markers may have the access of the above information. *(this box should expand as you type)*		
26	List who will have control of, and act as custodian(s) for, data generated by the research activity:		
	All name of participants or companies are anonymous. The data will only be present in summarised format. The university, researcher and markers may have the custody of the above information. *(this box should expand as you type)*		
27	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form. Will data be archived – if so how and if not why not.		

	The data collect will store in password protected drive, the data will deleted after the final confirmation on the reserch had been approved. *(this box should expand as you type)*		
28	Please indicate if your data will be stored in the UWTSD Research Data Repository (see https://researchdata.uwtsd.ac.uk/). If so please explain. (*Most relevant to academic staff*) No *(this box should expand as you type)*		
29	Confirm that you have read the UWTSD guidance on data management (see https://www.uwtsd.ac.uk/library/research-data-management/)	YES	√
		NO	□
30	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	YES	√
		NO	□

SECTION K: Declaration

31	The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/		
	Signature of applicant:	Lam Wai Yeung	**Date:** 19 Oct 2020

For STUDENT Submissions:

32	Director of Studies/ Supervisor:	Dr Wong, Chi Hung Arion	**Date:** 19 Oct 2020
33	Signature:		

For STAFF Submissions:

34	Academic Director/ Assistant Dean:		**Date:**
35	Signature:		

Checklist: Please complete the checklist below to ensure that you have completed the form according to the guidelines and attached any required documentation:

√	I have read the guidance notes supplied before completing the form.
√	I have completed **ALL RELEVANT** sections of the form in full.
√	I confirm that the research activity has received approval in principle
□	I have attached a copy of final/interim approval from external organisation (where appropriate)
□	I have attached a full risk assessment (and have NOT completed Section H of this form) (where appropriate) *ONLY TICK IF YOU HAVE ATTACHED A FULL RISK ASSESSMENT*
√	I understand that it is my responsibility to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice.
√	I understand that before commencing data collection all documents aimed at respondents (including information sheets, consent forms, questionnaires, interview schedules etc.) must be confirmed by the DoS/Supervisor, module tutor or Academic Director.
√	I have deleted the guidance notes before submitting the PG2 for consideration

RESEARCH STUDENTS AND STAFF ONLY
All communications relating to this application during its processing must be in writing and emailed to pgresearch@uwtsd.ac.uk , with the title 'Ethical Approval' followed by your name. You will be informed of the outcome of your claim by email; therefore it is important that you check your University and personal email accounts regularly.

~~**STUDENTS ON UNDERGRADUATE OR TAUGHT MASTERS PROGRAMMES**~~ should submit this form (and receive the outcome) via systems explained to you by the supervisor/module leader.

This form is available electronically from the Academic Office web pages: https://www.uwtsd.ac.uk/academic-office/appendices-and-forms/

Application Process

All staff research projects and all research students must submit the Ethical Approval Form to the **University Research Ethics Committee** via the Academic Office (pgresearch@uwtsd.ac.uk). Staff research directly in relation to personal study for taught undergraduate or Masters programmes should be submitted via the Institute procedures explained below.

Taught masters and taught undergraduate research Ethical Approval Forms are considered **within Institutes.** Institutes will provide details of the specific processes for this. Where the Ethical issues within any single ethical application are of particular concern the Institute will refer these to the University Research Ethics Committee. Any student activity that involves the collection of primary data needs to undergo Ethical approval, this includes assignment work as well as dissertations.

Notes for guidance in completion of this form

Section A: About You
Please complete all relevant sections

Section B: Approval for research activity
Research proposals must be approved in principle before applying for Ethical Approval. The proposal approval only becomes final when the ethical approval is received.

The process for proposal approval varies according the individual and programme of study:
- Research students, by application on form PG1 to the Research Degrees Committee
- Taught students by review of research proposal within Institutes (Institutes provide specific details of these processes)
- Staff, by agreement by the Academic Director/Assistant Dean

Section C: External Ethical Guidance materials
Many discipline areas are required to operate with the discipline specific codes of research ethics (for example health, psychology, education etc.), any such codes must be listed and you must tick to confirm that you have consulted with these.

Section D: External Collaborative Research Activity
Provide details of the external collaborative partners, where appropriate you might want to submit a copy of the external collaboration agreement with the Ethical Approval Form. If the partner requires the research to be subject to its own internal Ethical approval process then please provide details of that process and a copy of any final (or interim) approvals received from the organisation.

Section E: Details of Research Activity
Remember that the individuals reviewing this Ethical Approval Form may not have seen your research proposal, and also may not be experts in the specific area of your research. The information provided should therefore be jargon free and clearly stated.

Indicative Title: please use the same title as used on the research proposal.

Purpose: the Ethical approval process will want to ensure that the methods you propose are adequate and appropriate to address the research aims and objectives. Excessive additional data collection can be seen as unethical.

Proposed Methods: the Ethical approval process seeks to ensure that you understand the methods that are intended, and that the implementation of those methods will be appropriate and without unnecessary impact on respondents. This section must explain how the methods described will lead to the collection of necessary and sufficient data, but not excessive data. Please be specific.

Location: this needs to mention geographical location and also local situation (for example, within Local Authority Offices in Cardiff, using a private room but close to other individuals). If you are collecting data within an organisational setting then you need to explain the permissions that you have obtained to do this.

Research Activity outside of the UK: please complete this section in detail, and note any guidance you have received. Also describe your own familiarity (or not) with the location that you will be utilising.

Section F: Scope of Research Activity
Please tick ALL of the research activities that might be undertaken. If any additional types of activity are intended then please add an extra box and describe these.

If you have answered no to all questions in F then sections G and I do not need to be completed. . Signatures are still required in section K.

Section G: Intended Participants
Please tick all categories that might apply.

Numbers & Source: if you are using a series of different methods or research activities please list numbers for each stage/phase. Be clear about how you will find respondents. Will you use intermediaries, and if so how? How will you ensure compliance with your sampling strategy?

Information for participants: all participants should be appropriately informed about the research, what is expected of them and what will happen to the information that they provide. The Ethical review process does not ask to see this documentation, but requires this to be reviewed and approved by the Director of Studies in the case of research students, the supervisor/module tutor in relation to students on taught programmes and the Academic Director/Assistant Dean in relation to staff research.

Section H: Anticipate Risks
All research carries some level of risk. The answers you provide to questions in this section will be reviewed to ensure that you have an appropriate understanding of the type of risks involved and how you can mitigate against these risks. If you have completed a full risk assessment, as required for example for laboratory work, field work, clinical tests, diving operations, or by a collaborative partner, you may append that to this form. In that case, please tick the box indicating this has been provided. You will not then be required to complete Section H.

Risk to participants Think very carefully about how your actions/questions/discussions might affect the people you are involving as participants. You might identify the risk as small but it would still be a risk. Many types of question have the potential to make respondents less content with their life / job; you need to recognise and try to ameliorate any such effects
If these are business owners, time with you may reduce profit.
In some locations physical risk is very real to both participants and yourself, please consider this.

Risk to you, the researcher Think about where you will meet people, if there are any dangers involved in the location. If you are meeting people as individuals think about using a public place. In general do not visit people in their own homes or remote locations. If you are talking to individuals about certain issues think about how their responses might affect you emotionally. What about the risk of collecting insufficient data?

Risk to the University When undertaking your research, you are acting as a member of the University (student or staff). Professionalism is important, so it is important to be well organised and well prepared. Punctuality, clarity etc. are all part of this. What will you do to ensure this? You must ensure you do not harm the good name of the University in any way and do nothing to undermine the reputation of the research it conducts and sponsors. Upholding high standards of conduct and integrity are vital in this regard. You must also conduct the research in such a way to minimise the potential for claims of negligence made against the University, its researchers and any collaborating individual or organisation. In this respect you should always comply with ethical, legal and professional frameworks, obligations and standards as required by statutory and regulatory authorities, as well as the university's Research Integrity and Ethics Code of Practice. Research misconduct in this respect can take many forms, including:
- fabrication: making up results or other outputs (eg, artefacts) and presenting them as if they were real
- falsification: manipulating research processes or changing or omitting data without good cause
- plagiarism: using other people's material without giving proper credit

- failure to meet ethical, legal and professional obligations: for example failure to declare competing interests; misrepresentation of involvement or authorship; misrepresentation of interests; breach of confidentiality; lack of informed consent; misuse of personal data; and abuse of research subjects or material
- improper dealing with allegations of misconduct: failing to address possible infringements such as attempts to cover up misconduct and reprisals against whistle-blowers

Adverse Outcomes. Think carefully about the possibilities, and cover here

Section I: Feedback, Consent and Confidentiality

Feedback to participants: outline your approach. Will interview transcripts be shared with respondents to check accuracy? Will summaries of questionnaire analysis be made available to respondents in some way? Will an overview report be provided? How and when?

Informed consent: Draft letter / e-mail / or heading (or footer) section of questionnaire must be approved by DoS/supervisor (if research student), supervisor/module tutor if taught student, or Academic Director / Assistant Dean if a member of staff.
Confidentiality/Anonymity. Explain clearly how you will ensure confidentiality and anonymity.

Section J: Data Protection and Storage
Before completing this section it is necessary to read the University's Research Data Management information. The questions that follow are designed to ensure compliance with the Data Protection Act as well as established research protocols.

Many research activities will involve electronic transfer of data and use of data management systems in the summarisation and analysis of data. You will need to explain these in relation to compliance with the Data Protection Act.

Think carefully about who will have access to your data, this will include supervisors and examiners. Also that a thesis will be made available via the University library and the British Library system. If you are seeking an access bar for a period of time after completion then mention it here. If you will provide a copy of your findings, or intend to give a presentation, to a facilitating/ supporting/accessing organisation then explain that in this section. But also think about the general principle of data sharing, as explained in the Research Data Management information.

In terms of storage of data please ensure security, and also mitigate against loss of data.

Section K: Declaration
Ensure the appropriate countersignatures have been provided
Look carefully at the checklist and ensure that you comply with and tick all that are relevant to your research.



在企業新常態下，網絡應用例如人力資源管理、採購、會議和客服系統日益普及，但同時保安的挑戰亦越來越嚴峻，面對每日不同的勒索軟件、軟件漏洞，而人手及資源不同，企業管理層往往會出現無力感，本欄的兩位主角林煒揚（Marco）及黃永亨（Windham），正正了解到企業的需要，創立了 StormEye，用創新並具前瞻性的技術為企業減輕公司內部的壓力，專注發展。

兩位創辦人於在學時期相識，畢業後分開發展，Marco 原為跨國軟件公司區域代理，及後以合伙人身份創立網上教育平台並獲得多個創業獎項；Windham 在畢業後到英國著名大學攻讀網絡保安，並在畢業後加入英國龍頭網絡保安監察中心工作多年。兩人深深體會到亞洲區的網絡發達，但網絡保安的產品往往來自外國，欠缺對本地企業用家的支援及客製化，企業在應用上難以入手，亦大大增加成本及管理。

自主研發 不走捷徑

隨大數據及物聯網的普及，StormEye 深明網絡安全的綜合監察系統將成為未來網絡保安的中心，而市面上的相關系統未有加以運用最新的大數據處理科技，難以實時處理大量並多變的數據，自主研發乃解決此問題的最佳方法。StormEye 研發的資訊與事件管理系統，運用了近兩三年成熟的數據串流處理框架，實時以極少的資源處理大量數據，並增強了硬件擴充的可能性，類似的框架原先用於協助提高大型的社交媒體處理、檢查及發佈的即時性。自主研發的系統更令在應對不同客戶的客製需求時，反應更快，時間及管理成本大大降低，企業運作更具效率！

香港創立 放眼全球

在亞洲區，概念上只有銀行及跨國企業才有資訊與事件管理系統，StormEye 的系統不但可以為銀行、跨國企業降低現有系統對硬件及人力資源的需求，更可以服務本地中小企保護現有網絡。透過收集及分析不同的網絡儲存設備（NAS）及防毒軟件的數據，StormEye 同時協助中小企的 IT 部門了解系統弱點及處理入侵。「全系統化令黑客入侵基本上無成本，因此不會因為公司規模細而放棄入侵！」創辦人 Marco 經常會提醒中小企要留意網絡安全。

隨住歐盟一般資料保障條例（GDPR）及巴西一般資料私隱法（LGPD）等條例相繼實施，兩位創辦人預視在網絡保安問題上，香港並不能獨善其身，因此在本年度，他們與在歐盟中研究相關法規的 De Groote – De Man 律師事務所組成聯盟，為亞洲地區的客戶提供網絡保安的相關法律顧問服務；亦在早前與馬來西亞一間會計師樓合作推出網絡保安訓練課程，在提供服務同時，亦希望可以將經驗帶給本地及世界各地的客戶。【C】

STORMEYE.io

01 StormEye 聯合創辦人林煒揚（Marco）。
02 StormEye 聯合創辦人黃永亨（Windham）。

Sources : Capital (2020)