Ph. D. Dissertation in Engineering

The Study on Willingness to Pay for Cyber Insurance in Thailand

태국의 사이버보험 지불의사에 관한 연구

August 2023

Graduate School of Seoul National University

Technology Management, Economics, and Policy Program

Siriwan Chaichana

The Study on Willingness to Pay for Cyber Insurance in Thailand

지도교수 이종수

이 논문을 공학박사학위 논문으로 제출함
2023 년 8 월

서울대학교 대학원
협동과정 기술경영경제정책 전공
시리완 차이차나

시리완 차이차나의 공학박사학위 논문을 인준함
2023 년 8 월

위 원 장 김연배 (인)
부위원장 이종수 (인)
위 원 구윤모 (인)
위 원 신정우 (인)
위 원 김정훈 (인)

Abstract

The study on Willingness to Pay for Cyber Insurance in Thailand

Siriwan Chaichana

College of Engineering

Technology Management, Economics and Policy Program

The Graduate School

Seoul National University

In modern times, the growing concern of cyberattacks has emerged as a significant issue for businesses due to their growing dependence on digital technology for their everyday operations. Cybercriminals target vulnerable individuals and organizations, including critical infrastructure systems, resulting in potential disruptions and even fatalities. To enhance Thailand's competitiveness and instill trust in digital technologies, the government has implemented digital economy development policies, and the two digital lawsuit included the Cybersecurity Act, and the Personal Data Protection Act. Among various cybersecurity practices, cyber insurance stands out as an effective method to transfer risks to a third party, but its complexity in pricing and coverage considerations makes it relatively unfamiliar in the Thai market, particularly among Critical Information Infrastructure (CII) organizations.

This study aimed to gain valuable insights into the decision-making process and willingness to pay for cyber insurance among CII organizations in Thailand. To fulfill the research objective, the Contingent Valuation Method (CVM) was utilized in this study. The CVM is a well-established technique used to evaluate the economic worth of non-market goods, including cyber insurance. By utilizing this method, the researchers sought to understand the significant factors that influence CII organizations' purchasing decisions and their willingness to invest in cyber insurance coverage.

In light of the circumstances, cyber insurance has emerged as an effective method among various cybersecurity practices to mitigate risks by transferring them to a third-party insurer. This approach provides a much-needed safety net for organizations facing potential financial losses and reputational damage resulting from cyber incidents. However, despite its potential benefits, cyber insurance remains relatively unfamiliar in the Thai market, particularly among Critical Information Infrastructure (CII) organizations. The complexity involved in pricing and coverage considerations makes it a challenging product for these organizations to adopt.

To ensure a comprehensive analysis, the study integrated the Spike model, which effectively addresses situations where organizations might reject the idea of investing in cyber insurance. This approach allows for a more accurate estimation of the willingness to pay among potential adopters of cyber insurance, providing a deeper understanding of their risk management priorities.

The study's findings revealed a noteworthy willingness to pay for cyber insurance among CII organizations in Thailand. As determined by the Spike model, the average willingness to pay was found to be THB 207,455 (USD 6,694) per year. Additionally, the research highlighted the crucial role of understanding cyber insurance and the level of professionalism among key individuals within these organizations, particularly the chief cybersecurity officer. The willingness to pay was significantly influenced by their knowledge and expertise, with monetary values of THB 287,300 (USD 9,267) and THB 204,312 (USD 6,592) per year, respectively.

These findings hold valuable policy implications for the government and insurance companies, shedding light on the importance of the willingness to pay as determined by the Spike model. Furthermore, the study underscores the significance of raising awareness about cyber insurance and the need for qualified cybersecurity professionals in driving the demand for cyber insurance within the Thai market. Ultimately, the research aims to contribute to a more secure and resilient digital ecosystem in Thailand, where organizations can confidently embrace digital technologies while safeguarding their interests against cyber threats with cyber risk mitigation measures.

Keywords: cyber risk management, cyber insurance, willingness to pay, contingent valuation method, spike model, Thailand.

Student number: 2020-33021

Acknowledgement

First and foremost, I want to extend my sincere appreciation to my academic advisor, Professor Jongsu Lee, for his consistent support and mentorship during my academic voyage, spanning from my master's degree to my ongoing pursuit of a doctoral degree. Professor Lee's dedication to his students' achievements has been a tremendous source of inspiration and encouragement for me, fueling my determination to excel in both my studies and research endeavors. I am especially grateful for Professor Lee's understanding and support regarding the challenges I faced living in Korea. I am deeply grateful for his guidance, mentorship, and support, and consider myself fortunate to have worked under his tutelage.

I want to extend my heartfelt gratitude to my committee chair, Professor Yeonbae Kim, as well as to my esteemed dissertation committee members: Professor Yoonmo Koo, Professor Jungwoo Shin, and Professor Junghun Kim. Their continuous support, collective expertise, valuable insights, and helpful suggestions have played a pivotal role in the successful completion of this dissertation. It has been an absolute honor and privilege to collaborate with such an exceptional group of scholars.

I am immensely grateful to Professor Junseok Hwang and Professor Yoon Hyunyoung for their invaluable guidance, expertise, and unwavering support. Their kindness and motivation have profoundly influenced my academic and professional development. I will forever cherish the valuable lessons they imparted, as well as their time, patience, and dedication.

I would like to express my sincere appreciation to the National Cybersecurity Agency of Thailand for their invaluable support in facilitating the data collection process for this research. Their assistance has played a critical role in ensuring the success and effectiveness of this study.

I am deeply grateful to my ITPP2020 classmates and the ITPP family for an incredible three-year academic journey. Studying alongside such remarkable individuals has been a true blessing, providing me with diverse perspectives, lifelong friendships, invaluable lessons, unforgettable memories, and meaningful connections. Thank you all for making this experience transformative and unforgettable.

I am forever grateful for the unwavering support and motivation from my family, particularly my beloved mother, Ms. Thippawan Chaichana. Despite being alone for three years, she stood by me and patiently awaited my success. Your unwavering encouragement and love will always be cherished

Endless appreciation for those who, in deed and thought, have sustained my efforts and supported me. Thank you, Mr. Robert Liedl, Mr. Wittawat Mongkonnawatsatien, Mr. Tom Lennon, Ms. Kwankwi Yeong, ITPP Staffs, and Ms. Jiin Kim.

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Human Resource Development Project for Global R&DB Progeam (IITP-2019-0-01328) supervised by the IITP (Institute for information & communications Technology Planning&Evaluation)

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

This section provides an overview of various topics related to the implementation of cybersecurity policies and risk management measures. Specifically, it discusses the motivation behind Thailand's Digital Economy and Society Policy, as well as “the Cybersecurity Act” and “Personal Data Protection Act”, both of which encourage the adoption of cybersecurity measures pertaining to cyber insurance. This section states the problem, objectives, research questions, and the methodology employed in this study. Finally, a brief outline of the thesis is presented.

1.1 Research Background

The term cyber risk refers to any potential harm that could arise from the use or transmission of electronic data, encompassing technologies such as the internet and telecommunications networks (Forum, 2017). The global economy is vulnerable to significant damage resulting from cyberattacks. Although the world currently spends nearly $100 billion annually on cybersecurity (Wirth, 2017), and experts predict that global losses will exceed $1 trillion by 2020, reflecting a more than 50 percent increase in just two years (Malekos et al., 2020).

The impact of cyber catastrophes can include damage to physical and intangible assets, costs associated with business interruptions, and

various forms of liability to customers, suppliers, employees, and shareholders. Additionally, there are hidden costs associated with cyberattacks, such as opportunity costs, system downtime, time and money spent on cybersecurity decision-making, productivity loss, harm to brand reputation, and loss of consumer confidence (Forum, 2017).

To manage their cyber risk effectively, the organization implements cybersecurity policy, these policies may include guidelines for organizations to follow in order to protect against cyber threats, as well as laws and regulations that mandate certain security practices or impose penalties for non-compliance (Woods & Simpson, 2017). They must prioritize risk management practices and establish a comprehensive cybersecurity strategy that includes transferring risk through cyber insurance (Yang & Lui, 2014; Tosh et al., 2017; Bodin et al., 2018). By doing so, organizations can reduce the likelihood of cyber incidents, ensure compliance with cybersecurity and data privacy laws, and safeguard their reputation and financial well-being. Moreover, the Personal Data Protection Act aims to protect personal information or private information from leaking and adversely affecting the data subject which has a penalty for the data loss as well (The Kingdom of Thailand, 2019).

Risk management encompasses the process of identifying, evaluating, and mitigating potential threats that could impact the confidentiality, availability, and integrity of data or services (The Geneva Association,

2016; The NCSC, 2018; Kosseff, 2018). To maintain the confidentiality, integrity, and availability (CIA) triad, it is essential to allocate resources to security measures, including but not limited to antivirus software, firewalls, proxy servers, IT auditing, and disaster recovery plans. Information Security Management Systems (ISMS) are also employed to facilitate a secure and efficient risk management process by reducing associated risks and enhancing information security (Eling & Schnell, 2016).

Within the broader literature on cybersecurity policy, previous studies have extensively explored topics such as risk assessment, regulatory frameworks, and the economic impact of cyber threats. From an economic perspective, studies have examined the impact of cyber losses and have recommended organizations to consider investing in cyber insurance as part of their cybersecurity strategy. Cybersecurity policy handle IT security risk, businesses use a multiple approach including investing in security solutions and obtaining cyber insurance to cover remaining IT security risk (Bandyopadhyay & Mookerjee, 2019). They may also implement both self-insurance and cyber insurance to mitigate cyber risk (Tonn et al., 2019). Abdul Hamid et al. (2022) have directly examined the enabler and barrier of cyber insurance adoption, but there is still a lack of economic perspective, while other type of insurance, the monetary value has been determined and can be utilized for policy implications by both the government and the insurer.

Prior research also suggests that organizations should incorporate cyber insurance into their risk management strategies as a way to transfer cybersecurity risks associated with data breaches. Cyber insurance can be an effective measure for mitigating cyber risks (Yang & Lui, 2014; Tosh et al., 2017; Bodin et al., 2018). However, organizations should exercise caution in selecting the appropriate cyber insurance policy, as policies can vary widely in terms of coverage and exclusions.

To manage cyber risk is an essential aspect of modern organizational risk management (Bodin et al., 2018) . Effective risk management requires investment in security tools, implementation of risk management frameworks, and incorporation of cyber insurance into overall risk management strategies (Tosh et al., 2017). By adopting a comprehensive approach to managing cyber risk, organizations can reduce the likelihood and impact of cyberattacks and protect against potential financial and reputational damage (Yang & Lui, 2014).

Cyber risk and cyber loss become a National Agenda, to address these risks, the government has enacted cybersecurity and Personal Data Protection Act, to provide a legal framework for safeguarding personal information and regulating online activities. Compliance with these laws can pose a significant challenge for organizations operating in Thailand's digital economy, as they must ensure that their operations are in accordance with the country's complex and continually evolving cybersecurity and Personal Data Protection regulations (The Kingdom of

Thailand, 2019). Those laws are a part of Thailand and the Digital Economy and Society policy that aims to foster the country's digital transformation by harnessing the latest technological advancements to bolster economic growth, enhance public services, and improve the well-being of citizens (MDES, 2018).

Moreover, Thailand's cybersecurity legislation emphasizes the safeguarding of Critical Information Infrastructure (CII) organizations, encompassing sectors like national security, essential public services, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, and public health. According to the law, CIIs are obligated to uphold their cybersecurity measures, and non-compliance can lead to significant consequences, including imprisonment, fines, or the revocation of licenses. (Cybersecurity Act B.E. 2562 (2019), 2019). Both “Cybersecurity law” and “Personal Data Protection law” are enforced in both public and private organization’s to maintain cybersecurity and secure personal data.

Cyber insurance is a modern method of transferring risks to a third party, which can be effective in mitigating cyber threats to an acceptable level. However, it is a complex product that involves both pricing and coverage considerations. Since it is still relatively new in the Thai market, CIIs organization may not have a sufficient empirical understanding of itIn order to advance the growth of the cyber insurance market and establish

effective policies surrounding cyber insurance, it is crucial to delve into a comprehensive examination of user preferences and choices concerning cyber insurance in Thailand. This holds particular significance considering the potential impact of cyber insurance within Critical Information Infrastructure (CII) organizations in the nation. Consequently, it becomes imperative to identify the factors that influence a user's inclination to invest in cyber insurance and their willingness to pay for it.

Moreover, academic research on insurability typically concentrates on factors related to insurance supply on demand is limited (Eling & Schnell, 2016). According to several studies (Bodin et al., 2018; Yang & Lui, 2014; Tosh et al., 2017), cyber insurance should be considered as a crucial aspect of a comprehensive risk-management strategy to mitigate the cyber risks related to potential breaches. However, the cost of cyber insurance can vary based on the type of organization, the severity of cyber threats, the size of the company, and its annual revenue (Ozawa, 2021; Malekos et. Al., 2020; Pooser et al., 2018), which can affect the likelihood of purchasing cyber insurance. As such, they recommend that companies evaluate cyber insurance products proactively by examining factors such as price and coverage. Despite the potential benefits, cyber insurance has not been widely adopted (Vakilinia & Sengupta, 2019) due to factors such as costly premiums and policy limitations, particularly outside the US, where the awareness and utilization of cyber insurance coverage remain limited and underexplored (Eling & Schnell, 2016).

Consequently, introducing cyber insurance to new markets may be challenging due to the product's complexity and limited awareness. Therefore, it is important for governments to establish policies and guidelines to promote effective measures for cyber risk transfer, including the use of cyber insurance, which can reduce the burden on organizations responding to losses caused by cyberattacks, benefiting both the public and private sectors.

The previous study reveals the amount of money that the individual wants to pay for non-life insurance, and identify the determinantss that influenced the Willingness to Pay. The study on cyber insurance is limited, therefore this study comparative from non-life insurance such as flood insurance (Paopid et al., 2020), motor insurance (Dragos & Dragos, 2017), house insurance (Hansen et al., 2016), and earthquake insurance (Tian & Yao, 2015). However, the direct payment for cyber insurance is not available in academic literature only can be found the extra payment for block chain and smart contact in cyber insurance (Nam, 2018).

1.2 Motivation

The increasing frequency of cyber-attacks and their detrimental impact on organizational losses in today's digital landscape, where cyber risks pose significant threats, highlights the crucial need for organizations to have effective cybersecurity measures in place. Cyber insurance

provides a valuable method for organizations to enhance their cybersecurity policies and effectively transfer unexpected losses.

Although cyber insurance has been acknowledged as an effective cybersecurity tool (Bodin et al., 2018; Yang & Lui, 2014; Tosh et al., 2017) and popular in many countries. However, there are limitations in the current cyber insurance market, particularly in Thailand, regarding price and adoption rate. In the initial phases of the cyber insurance market in Thailand, understanding the demand side's perspective and gaining insights into pricing is crucial. This knowledge is essential for both the government and insurance providers to collaborate and drive the growth of the cyber insurance market. Moreover, while numerous studies have explored various types of insurance, research on the Willingness to Pay for cyber insurance remains limited, including in Thailand. Consequently, the determinants influencing Willingness to Pay in the context of cyber insurance remain unknown.

Prior study on cybersecurity policy have extensively explored topics such as risk assessment, regulatory frameworks, and the economic impact of cyber threats. From an economic perspective, studies have examined the impact of cyber losses and have recommended organizations to consider investing in cyber insurance as part of their cybersecurity strategy. And the various studies on cyber insurance primarily focus on mitigating challenges stemming from asymmetric information, including moral hazard and adverse selection (Dou et al., 2020). These challenges significantly impact insurers and directly

influence insurance premiums. Additionally, various studies have investigated pricing models to enable pricing transparency and assess the cost of damages (Romanosky et al., 2019). However, these studies indirectly approach the topic from the customer perspective. In contrast, other domains of insurance dealing with uncertain risks similar to cyber risk, such as flood insurance (Paopid et al., 2020), insurance (Dragos & Dragos, 2017), house insurance (Hansen et al., 2016), and earthquake insurance (Tian & Yao, 2015), and the extra payment for block chain and smart contact in cyber insurance (Nam, 2018) have initially focused on studying willingness to pay and identifying the factors influencing the decision to pay, providing implications for both the government and insurance companies.

Conducting a study on willingness to pay in cyber insurance would provide valuable insights on the policy implication, help shape effective policy interventions, and enable insurance providers to design tailored products that align with customer preferences and demands. Through a comprehensive understanding of the Willingness to Pay for cyber insurance, policymakers and insurance providers can make well-informed decisions to facilitate the growth and advancement of the cyber insurance market.

Moreover, there is currently no evidence-based study on the demand for cyber insurance in Thailand. This issue has significant implications for policymakers and insurers. Despite the importance of addressing this

issue, limited research has been conducted to tackle this problem. This thesis aims to fill this gap by enhancing the understanding of the factors that influence Willingness to Pay for cyber insurance and the socioeconomic and behavioral determinants that impact the demand for cyber insurance in Thailand. This contribution will expand the wider academic discussion on the demand for cyber insurance in emerging markets and have the potential to contribute to the development of effective strategies for managing cyber risks.

Additionally, conducting a research on the Willingness to Pay for cyber insurance in Thailand will not only address the gaps in understanding factor affecting demand of cyber insurance, but also align with the country's cybersecurity laws and personal data privacy laws. It will shed light on the financial considerations of Critical Information Infrastructure organizations regarding cyber insurance, and promote cyber insurance as effective cybersecurity mechanism accordingly to factors influenced the Willingness to Pay.

1.3 Problems statement

Exploring the background of cyber insurance products can significantly enhance a comprehension of how the insurance market approaches cybersecurity, as well as how the government regulates and advances cybersecurity measures. This highlights the crucial role that cyber

insurance plays as a cybersecurity mechanism to reduce risk, and increase cybersecurity.

It is acknowledged that the number of cyber-attacks is exponentially rising, but the demand for cyber insurance remains relatively low, and many organizations are hesitant to purchase it (Eling & Schnell, 2016). Since cyber insurance is a voluntary form of insurance with no legal requirement to purchase it, some organizations consider it a niche product.

Therefore, introducing cyber insurance to a new market, it is essential to understand consumer behavior and their preference of purchasing for such a product, which can inform policy decisions related to the regulation and promotion of cyber insurance to drive market demand, as well as the insurance company can setup strategy to generate demand.

Previous theoretical background of cyber insurance product suggested that the primary reason for low demand is a lack of understanding of the potential risks and benefits of cyber insurance (Abdul Hamid et al., 2022). Additionally, perceived costs, lack of suitable insurance policies, and the difficulty of quantifying cyber risks have also hindered demand for this type of insurance. As well as the complexity of the product and its relative obscurity have contributed to its lack of popularity (Eling & Schnell, 2016). The same study also noted that comparatively fewer

studies have been conducted in behavioral economics study than in the IT domain.

Therefore, to increase the acceptance of cyber insurance products and their prices, further research is necessary to focus on the economic aspects of the demand side. The decision criteria for firms to purchase cyber insurance policies are not well established from academic so without a deeper understanding of why firms decide to pay for cyber insurance policies, the insurance industry may not be able to meet the demands of its client. As a result, the cyber insurance market may not reach its full potential, and companies may not be able to use cyber insurance effectively as a risk management tool as the government is looking for.

To address this knowledge gap, this study will start by gathering organizations' perceptions of this unique form of cyber insurance. This will involve conducting literature reviews on consumer behavior regarding the purchase of insurance and their willingness to pay, and affective method to analyzing it.

1.4 Research objective and questions.

This study has a specific objective, which is to examine the preferences of customers for cybersecurity mechanisms and risk transfer-based cyber insurance. It aims to identify the determinants that influence the

purchasing behavior of customers in this area. To achieve this objective, the study utilizes a survey questionnaire that targets CIIs organizations and other relevant organizations identified by law in Thailand.

By answering specific research questions, the study will help identify the factors that influence customers' willingness to purchase cyber insurance and the amount that they are willing to pay for such coverage. The insights gained from the study will be useful for insurance companies and policymakers in developing pricing strategies that align with customers' preferences and increasing the uptake of cyber insurance. To achieve this goal, the following research questions will be addressed:

1. What is the extent of organizations' willingness to pay for cyber insurance to transfer cyber risk to the insurance company?
2. What are the key factors that affect their decision to invest in cyber insurance?

1.5 Methodology

The survey will use a contingent valuation approach to examine the significant factors that influence customers' decision-making processes when purchasing cyber insurance and their Willingness to Pay for such coverage. A survey-based approach like the Contingent Valuation

Method is that relies on respondents to determine the economic value that they place on non-market goods or services.

In addition, in the case of assessing Willingness to Pay for unfamiliar goods or services, such as cyber insurance, individuals may respond with zero willingness to pay. To address this issue, the study will also use the Spike model, which can adjust zero willingness-to-pay responses statistically to provide better estimates of the average willingness to pay value.

1.6 Research outline

This thesis consists of five chapters. Next, Chapter 2 presents the Literature review, covering topics such as cyber risk, cyber loss, cybersecurity laws, liability, and cyber insurance, the empirical evidence on insurance and willingness to pay, factors affecting the demand for cyber insurance, limitations of previous literature, and the contribution. Chapter 3 describes the methodology, including the use of Random Utility Theory and a Contingent Valuation Method with a Willingness to Pay estimate. The chapter also covers the basic components of a CV survey, the estimation of optimal bid value for Double Bound Dichotomous Choice. Additionally, the chapter examines the Spike Model in Double Bound Dichotomous Choice. Chapter 4 focuses on the experimental design and empirical study, including survey design and data collection, descriptive summary statistics, bid distribution, and empirical study results. The chapter presents the estimation results of the

Willingness to Pay model, and Spike Model. Finally, Chapter 5 concludes the thesis, highlighting the key findings, policy implications and, limitation.

Chapter 2. Literature review

This chapter serves to lay the theoretical foundation for the research through a comprehensive literature review encompassing relevant fields, with a particular focus on the domain of cyber insurance. The literature review aims to offer a comprehensive comprehension of cyber insurance as a mechanism for transferring risks. It explores the notions of cyber risk and cyber loss in the context of cyber insurance, with a particular emphasis on Risk Management—a cybersecurity protection approach that accentuates risk transfer for efficient cyber risk management.

The review encompasses several key aspects. Firstly, it presents an overview of the cyber risks and losses faced by organizations, as well as the legal obligations stemming from these risks. Furthermore, it explores the cybersecurity mechanisms employed by organizations to establish effective cybersecurity measures. In addition, it delves into existing studies on cyber insurance, including research on consumer behavior and the factors influencing decisions related to purchasing it.

Considering the limited research specifically focused on cyber insurance, this review expands its scope to include investigations into individual behavior in purchasing non-life insurance and the factors that impact willingness to pay for it. By examining these related areas, the

review aims to fill the gaps in the existing literature and provide valuable insights for this study.

2.1 Cyber Risks and cyber loss

Cyber risks are operational risks that compromise the confidential, integrity, or availability of information technology (IT) assets. It refers to any risk associated with potential financial loss, disruption, or harm to an organization's reputation arising from the failure, unauthorized access, or improper use of its information systems (PwC, 2017). As Internet is the primary source of cyber threats (Eling & Schnell, 2016), it may cause criminal and non-criminal activity in modern organizations that utilize digital technology for their business operations, they are constantly exposed to cyber risks, and it is the most critical risk for their business operations. Cyber risk is primarily a possible cyber threat associated with an asset, there are many types of cyber threats that harm assets due to asset vulnerabilities (PwC, 2017). There exist various types of cyber threats, including Distributed Denial of Service (DDoS) attacks, GUI intrusion tools, hacking, phishing, worms, spoofing, Trojans, viruses, spam, malware, ransomware, web application attacks, credential compromise, data theft, manipulation, destruction, eavesdropping, and zero-day exploits (Elnagdy, 2017; Noor et al., 2020), financial fraud, system penetration, theft of proprietary information, and unauthorized access (Mukhopadhyay et al., 2019), Critical information infrastructure

disruptions can have both short and long term socioeconomic effects from those cyber risk (Tonn et al., 2019). Companies are witnessing a rise in the frequency of cyberattacks, consequently leading to substantial costs associated with these incidents (Berkman et al., 2018).

Trends in cyber risk are regularly discussed in academic research and journal articles, organizations are aware of them and are making efforts to reduce cyber risks in response to these trends. Insurance companies are affected by cyber risks as they rely heavily on their IT infrastructure, but writing a cyber risk policy appears to be an attractive business opportunity for them as well (Eling & Schnell, 2016). Insureds are also affected by cyber risk, and when the cyber risk policy is written, it is difficult for them to estimate the compensation they should receive from cyber insurance.

Cyber risks are strongly connected and happen all over the world, in Thailand, operational technology organizations are facing cyber risk as the number of cyber risks increases worldwide, leading to an increase in cyberattacks. ThaiCERT reported Thailand incident statistics in 2021, showing that there were 2,069 incidents, with vulnerabilities accounting for 674 cases, malicious code accounting for 479 cases, and information gathering accounting for 248 cases. The rest are intrusion attempts, fraud, intrusions, information security, abusive content, and availability, which account for 668 cases (ThaiCERT, 2022).

As the occurrences of cyber threat events continue to escalate, the cost of cyber risk to organizations is experiencing a rapid surge. Cyber risks refer to catastrophic scenarios in which key information infrastructure fails due to technological failure or illegal activity, resulting in significant economic losses. These risks can cause both first-party and third-party losses with short or long-term effects (Eling & Schnell, 2016). First-party losses may include damage to an institution's reputation, monetary loss, data breaches, privacy accusations, and reputation damage (Elnagdy, 2017), regulatory, liability, and operational losses (Pooser et al., 2018), and may have a negative effect on a company's profit margins, market capitalization, and brand image (Mukhopadhyay et al. (2013); Tonn et al. (2019)). On the other hand, third-party losses are caused by a data breach that affects clients' privacy, which can result in liability from a customer data breach (Tonn et al., 2019).

Cyber events can result in a range of losses, including damage to tangible and intangible assets, costs associated with business disruption, and liabilities to customers, suppliers, employees, and shareholders. The hidden costs of cyberattacks consist of opportunity costs, system unavailability, and the time and money spent on cybersecurity decisions. The effects of system downtime on productivity loss, brand harm, and trust erosion are significant (Forum, 2017). Moreover, reputational, regulatory, liability, and operational losses and events are the sorts of cyber losses and events that have an impact on businesses as well (Pooser

et al., 2018). Cyber insurance policies protect those who expect to incur costs as a result of cyberattacks.

Due to their unpredictability, it can be challenging to estimate the financial impact of threats that target digital assets (Rees et al., 2011). The cost of cyber losses is rising rapidly, with annual worldwide cybersecurity investment exceeding $100 billion (Wirth, 2017), Despite this investment, global losses from cyber risks are projected to reach almost $1 trillion in 2020 (Malekos et al., 2020) and could escalate to $10 trillion in 2025 (Sausalito, 2020). The projected expenses per data breach for a hacked corporation can range between $2.1 and $3.8 million (Eling & Schnell, 2016).

The case of cyber risk and loss is often exemplified by the ransomware extortion of the WannaCry attack that infected 150 countries in May 2017. The initial ransom demand was for $300 in bitcoins, but the attackers eventually raised it to $600. This cybercrime is estimated to have cost the world $4 billion. In the same event, NHS institutions in Britain had to spend approximately $99 million on following up on 19,000 cancelled appointments caused by the WannaCry attack. Following the NotPetya ransomware attack on companies in North America and Asia in June 2017, the total damage cost was $10 billion (Wolff, 2022b), causing FedEx's TNT division and significant firms in Latin America, Australia, and Europe to lose $300 in Bitcoin. The

attackers sought to extort other companies. FedEx cited a $300 million drop in quarterly earnings due to the interruptions (Forum, 2017).

The global cyber loss cases have demonstrated that cyber responsibility encompasses a financial penalty derived from associated legislation. One such example is the 2011s hacking of Sony's PlayStation Network, which exposed personally identifiable information for 77 million PlayStation user accounts. For twenty-three days, the vulnerability prevented PlayStation console owners from accessing the service. The incident resulted in significant financial losses for Sony, with the company incurring costs in excess of $171 million. This included the costs of the forensic investigation, remediation of the attack, legal fees, and compensation paid to affected customers. A portion of these costs may have been covered by a cyber insurance policy, but Sony's insurance policy at the time only covered physical property loss, leaving Sony accountable for the full cost of the cyber losses. In addition to financial losses, Sony also suffered reputational damage and had to rebuild trust with its customers following the breach. The incident highlights the importance of having comprehensive cyber insurance coverage that includes both first-party and third-party losses, as well as coverage for business interruption and cyber liability (Wolff, 2022c) .

In 2020, a Hana Tour Service Inc. privacy officer was held legally responsible for failing to prevent a data breach that affected over 465,000 clients and 29,000 employees. The court penalized the privacy officer

around $8,500, while the Ministry of the Interior and Safety separately fined the corporation nearly $280,000. There is no evidence that Hana Tour Service Inc. has cyber insurance or is accountable for the full cost of cyber losses (Hunton Andrews Kurth, 2020).

2.2 Cyber Law and Liability

Cyberattacks and data breaches are increasingly recognized as major concerns for national security and the economy (Kosseff, 2018). As the sophistication of cyberattacks continues to grow, so do regulations around cybersecurity (Tonn et al., 2019). Governments are taking measures to enforce laws mandating organizations to establish cybersecurity programs and demonstrate compliance in their annual reports (Berkman et al., 2018). In the United States, entities operating in regulated industries, such as healthcare, telecommunications, and defense, are obliged to report any breaches they encounter. Furthermore, this requirement has been extended to encompass other sectors as well (Eling & Schnell, 2016). The European Union has also introduced regulations that mandate a wide variety of businesses to report any breaches they encounter (Berkman et al., 2018). Additionally, in the US, state regulators are required to investigate and disclose data breaches, and federal banking authorities have imposed regulatory requirements on banks. China has established a cybersecurity policy aimed at providing trusted e-government services. The China National Cybersecurity Law

encompasses a diverse array of industrial sectors, which includes energy, transportation, and information networks (Zhang et al., 2018).

The Thai government recently established the National "Cybersecurity Act B.E. 2562 (2019)", which aims to protect the Critical Information Infrastructure (CII) and respond to cyber threats effectively. By law, the National Cybersecurity Agency (NCSA) is responsible for national cybersecurity and is tasked with enforcing regulations for CII organizations, It includes industries vital to national security, public services, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, as well as public health. To cope with cybersecurity threats, the NCSA has established minimum guidelines based on risk management and self-assessment measures, which are aimed at maintaining cybersecurity. This includes any measures or procedures established to prevent and mitigate the risk of cyber threats (Cybersecurity Act B.E. 2562 (2019), 2019). Moreover, "Personal Data Protection Act, B.E. 2562 (2019)" aim to protect personal information or private information from leaking and adversely affecting the data subject which has a penalty for the data loss as well (The Kingdom of Thailand, 2019).

It is probable that corporate directors and officers are anxious about the possible liabilities they or their company may face in the case of a catastrophic incident (Pooser et al., 2018), The effects of cybersecurity and data protection laws encompassed several actions, such as

appointing directors with IT backgrounds, employing Chief Information Security Officers, establishing IT committees within the Board, acquiring or developing new systems with improved security measures, and investing in insurance coverage (Berkman et al., 2018). According to Berkman et al. (2018), the implementation of cybersecurity laws and the emergence of cyber liability have contributed to an upsurge in the potential legal ramifications of security breaches. Consequently, this has fostered the expansion of the cyber insurance industry.

2.3 Cybersecurity policy

Cybersecurity policy refers to the measures and regulations put in place to ensure the security of digital systems and networks. These policies may include guidelines for organizations to follow in order to protect against cyber threats, as well as laws and regulations that mandate certain security practices or impose penalties for non-compliance (Woods & Simpson, 2017).

According to the study of (Chronopoulos et al., 2017), cybersecurity policy is affected to the investment in cybersecurity. Cybersecurity investment refers to the financial and operational decision made by companies to mitigate the losses arising from cyber-attacks is of paramount importance. It serves as a critical determinant for the success or failure of companies heavily reliant on information systems. The

paper suggests that investment in cybersecurity is crucial for mitigating risks in cyberspace and increasing welfare.

Within the broader cybersecurity policy literature, previous studies have extensively explored topics such as risk assessment, regulatory frameworks, and the economic impact of cyber threats. However, a limited number of studies of cybersecurity mechanism specifically focusing on the cyber insurance and Willingness to Pay, however, study on Willingness to Pay will provides valuable insights into the economic dimensions of cyber insurance and its role in cybersecurity policy. While previous studies have recognized the importance of economic considerations in cybersecurity policy, few have directly examined the factors affecting the decision-making adoption in cyber insurance. Our research offers a unique perspective on the economic factors shaping cybersecurity decision-making, specifically focusing on the role of insurance as a risk management tool.

The cybersecurity policy literature, this research builds upon theories of risk management, insurance economics, and behavioral economics. Works by Smith & Paté-Cornell (2018) and Johnson and Brown (2020) have shed light on economic evaluation and decision-making in cybersecurity. However, these studies have primarily focused on cost estimation and regulatory aspects, rather than explicitly examining the relationship between cyber insurance and Willingness to Pay. This research extends the understanding of economic factors in cybersecurity

policy by investigating the role of insurance and its influence on organizations' decision-making processes.

In conclusion, this research on cyber insurance and willingness to pay contributes to the existing cybersecurity policy literature by providing empirical evidence and insights into organizations' economic valuation of cyber insurance coverage. By addressing the specific gap in literature and situating our work within the broader cybersecurity policy context that aim to inform policymakers, insurance providers, and stakeholders about the economic dimensions of cyber insurance decision-making.
Organizations typically use risk analysis processes to assess business risks and determine how to manage them based on priorities and internal and external constraints. They interactively manage risk as part of their operations, often relying on enterprise risk management systems and strategies to align risk management with their business goals (Eling & Schnell, 2016). Cybersecurity risk management takes various forms to mitigate and manage risks, depending on the organization's needs (Yang & Lui, 2014). Establishing a risk strategy has become a crucial challenge in international relations, and cybersecurity strategies protect information systems' confidentiality, availability, and integrity, minimizing asset loss due to cybersecurity threats (Rees et al., 2011), A technical approach to risk strategy aims to ensure the CIA triad operates effectively within an organization (Mukhopadhyay et al., 2013).

Cybersecurity policy handle IT security risk, businesses use a multiple approach including investing in security solutions and obtaining cyber insurance to cover remaining IT security risk (Bandyopadhyay & Mookerjee, 2019). They may also implement both self-insurance and cyber insurance to mitigate cyber risk (Tonn et al., 2019). Implementing design approaches that strengthen system architecture and activities, along with operational methods that modify business processes, can prove highly effective. Employing countermeasures such as security software, system design and operational enhancements, and investments in the cyber workforce are common practices. Additionally, protective techniques like firewalls, software encryption, virus detection, and system compartmentalization are employed. Institutional cyber risk management measures can take various forms, including structural, procedural, and responsive strategies.

A suggested approach to enhance the cyber resilience of transportation infrastructure within the US government was the adoption of cyber insurance as a means to transfer any remaining cyber risk (Tonn et al., 2019). Cyber insurance can be an alternative option for financial organizations to reduce cybersecurity risks. To make well-informed choices on security mitigation strategies, including cyber insurance, policymakers and security staff must have a greater understanding of the relationship between cost and security and risk (Meland et al., 2015). Institutions have the flexibility to decide how to manage cyber risks, including investing in mitigation, transferring risk, avoiding risk, or

accepting risk, based on the potential business implications. While acquiring cyber insurance can be a crucial component of a cyber risk management plan, it represents an alternative option to reduce cyber risks (Elnagdy, 2017).

2.4 An overview of cyber insurance.

Threats, security breaches, and IT disruptions cannot be avoided only via technological methods, financial risk management through so-called cyber insurance has become a hot topic of discussion. Various terms have been used in literature to refer to cyber insurance, including cyber insurance, cyber insurance, cyber risk insurance, liability insurance, and cybersecurity insurance (Mukhopadhyay et al., 2013; Meland et al., 2015; Eling & Schnell, 2016; Elnagdy, 2017; Tonn et al., 2019). As per the U.S. Department of Homeland Security, cyber insurance is a risk transfer and mitigation strategy, but Franke (2017) Stated findings suggest that cyber insurance serves not only as a risk transfer mechanism but also encompasses risk avoidance and mitigation aspects. In this approach, insurers compensate policyholders for monetary losses and expenses incurred due to cyber incidents defined in the insurance policy.

Cyber Insurance is often utilized to bridge the gap between the service provider's insurance coverage and contractual limits and the client's complete loss. Cyber Insurance coverage includes data breach charges, such as lost income due to company disruption, cyber extortion costs,

and forensic and investigative costs. Additionally, products protect third-party liability arising from data and privacy breaches. However, some insurers do not cover non-malicious events such as human mistake or power outages (Franke, 2017).

Financial service firms can leverage cyber insurance to minimize risks by transferring them to third parties that provide cybersecurity protection (Elnagdy, 2017). Cyber insurance is a type of insurance that offers coverage for losses arising from cyberattacks. Cyber insurance policies typically cover losses resulting from cyberattacks and cause computer system down, network unavailability, data breaches (Chase, 2021).

Cyber insurance is a contemporary risk management technique that helps organizations transfer financial risks resulting from network and computer events to a third party, and to blend risk management to balance security investments and acceptable loss (Yang & Lui 2014; Meland et al. 2015). It also plays a crucial role in managing risks associated with cyber incidents by transferring them and facilitating business recovery (Jason Nurse et al., 2020). The use of cyber insurance can mitigate expenses associated with cyber events such as cyberattacks, malicious conduct, network flaws, information leaking, and business interruption (Elnagdy, 2017). However, as cyber insurance is a relatively new concept in both practical and research domains (Jason Nurse et al., 2020), several questions remain unanswered, such as how the data and

economic models influence it, what coverage options and premiums are available, and what procedural policy-related aspects are involved.

Cyber Insurance has been regarded as an efficient method of enhancing resilience since it expedites the process of recovering from financial losses sustained as a result of significant cyber-attack occurrences. Adopting a collaborative approach to exchanging cyber-threat information may help firms remain on top of cyber dangers (Tosh et al., 2017). It concerns as a risk management strategy for the financial sector that involves shifting part of the risk to an insurance provider. It has grown in popularity as a means of recouping part of the financial damages incurred as a result of cybersecurity accidents (Gai et al., 2017). Cyber insurance solutions on the market typically cover three broad categories of risk: (a) data theft loss and responsibility, (b) breach response forensics and cleanup costs, and (c) coverage for fines and penalties imposed by law and regulation (Bandyopadhyay & Mookerjee, 2019). Cybersecurity insurance has evolved into a critical instrument for many firms in minimizing financial risks associated with data breaches (Kabir et al., 2020). This is a way for businesses to shift some of the risk associated with Cybersecurity (Young et al., 2016).

Cyber insurance coverage helps to mitigate the financial damages caused by cyber events and incidents. According to the literature, cyber insurance policies have covered a wide range of cyber catastrophes, from hacking to fraud. Such coverage can extend to direct losses incurred from

cybersecurity breaches and costs related to notifying affected individuals about privacy breaches (Tonn et al., 2019). First-party cyber insurance coverage is designed to help an organization respond to data breaches that occur on its own network or systems, such as legal fees, investigations, crisis specialists, and public relations services. In contrast, third-party cyber insurance coverage is meant to assist in paying for lawsuits that may result from data breaches on a client's network or systems, including settlement costs and media liability (Gai et al., 2017). From the study of Romanosky et al., (2019) also mentioned that insurance companies offer coverage for liability arising from data breaches, network security breaches, and privacy violations. The policies analyzed often include coverage for legal fees, settlements, judgments, and regulatory fines and penalties related to third-party claims.

2.4.1 The evolution of cyber insurance

The evolution of cyber insurance is a relatively recent phenomenon, driven by the increasing prevalence and severity of cyber-attacks and data breaches (World Economic Forum, 2018). During the initial stages of the Internet's development, cyber insurance was virtually non-existent because the Internet was still a relatively new technology and the risks associated with it were not yet fully understood (Romanosky et al., 2019). The first insurance company to introduce a cyber insurance policy was American International Group (AIG), which covered losses related to computer hacking, denial of services, and other forms of cybercrime

(Granato & Polacek, 2019a). In the early 1990s, cyber insurance policies were created to cover liability arising from the transmission of viruses, hacking, and other computer-related crimes (First-party), these policies were primarily purchased by technology companies and other businesses that relied heavily on computer systems (Majuca et al., 2006). During the late 1990s, the Y2K scare triggered a significant increase in the demand for cyber insurance policies. Businesses were apprehensive about potential computer system failures when the year 2000 arrived, and they sought protection against potential losses (Chase, 2021). Furthermore, during the early 2000s, cyber-attacks became more sophisticated, originating from online activities. Consequently, cyber insurance policies underwent evolution to encompass a broader spectrum of risks, such as data breaches and network security failures (both First and Third-Party) (Kshetri, 2020). The mid-2000s saw a resurgence of interest in cyber insurance as businesses began to recognize the growing threat of cyber-attacks. The emergence of new types of cyber threats, such as phishing scams and ransomware attacks, made it clear that traditional insurance policies were not adequate to cover these risks (Camillo, 2017). GlobalData Thematic Research (2020) note that after the dot-com bubble bloom in 2001 the use of internet increasing, demand for cyber insurance policies declined. This led to an increased demand for cyber insurance as businesses looked for ways to mitigate their risk and protect themselves from potential liabilities. In 2013, a data breach was a turning point for the cyber insurance industry, as it highlighted the potential for large-scale data breaches to cause significant financial losses for

businesses. Many companies began to see cyber insurance as a necessity rather than a niche product and, in 2014, the target breach highlighted the need for cyber insurance coverage. Target's insurance policy did not cover losses resulting from a cyber-attack, and the company faced significant costs related to the breach (Camillo, 2017).

The WannaCry and NotPetya cyber-attacks were highly destructive and impacted the evolution of cyber insurance. In May 2017, WannaCry targeted Microsoft Windows computers in more than 150 countries, demanding ransom for encrypted data. NotPetya occurred in June 2017 and spread quickly, affecting many industries. Both attacks led to a reevaluation of cyber insurance policies, with insurers offering new products to cover losses resulting from state-sponsored cyber-attacks. Today, cyber insurance policies cover data breaches, cyber extortion, and business interruption (Wolff, 2022c). The cyber insurance industry needs to be agile and responsive to new and evolving threats to protect businesses effectively.

Table 1. Summary evolution of cyber insurance.

Period	Evolution	Literature
1990s	First cyber insurance policy was introduced by add-ons to existing liability covers.	(Wolff, 2022c)
Mid 1990s	Cyber insurance policies for the first-party lost were created.	(Majuca et al., 2006)
Late 1009s	The Y2K scare led to a surge in demand for cyber insurance policies.	(Chase, 2021)
2000s	Cyber insurance policies began to evolve to cover a wider range of risks, cover first and	(Kshetri, 2020)

Period	Evolution	Literature
	third-party lost.	
2017s	The emergence of malware and ransomware attacks has prompted insurance companies to expand their coverage policies to meet the growing demand for protection against these types of cyber threats.	(Wolff, 2022c)
Present	Cyber insurance policies cover data breaches, cyber extortion, and business interruption.	(Chen, 2021)

2.4.2 Determining cyber insurance premium.

Today, cyber insurance is a rapidly growing industry, with more and more insurers offering policies tailored to the needs of businesses of all sizes. Cyber insurance policies generally encompass a broad array of risks, including data breaches, network security failures, cyber extortion, and business interruption losses. Nonetheless, it is important to note that cyber insurance is a relatively new and continually evolving field (Jason Nurse et al., 2020), and there is no standardization of policies and coverage (Toregas & Zahn, 2014). As such, to ensure sufficient protection in case of a cyber-attack or data breach, it is essential for organizations to verify that they are adequately covered by cyber insurance policies (Abdul Hamid et al., 2022).

The premiums for cyber insurance policies vary based on individual circumstances , to determining the appropriate premiums for cyber insurance usually involves considering various factors, including the organization's size, type, industry sector, history of cyber incidents,

existing security measures, and the desired level of coverage (Chen, 2021), so it was challenging for them to determine the appropriate coverage needed and understand the specific coverage provided by different options available in the market (Toregas & Zahn, 2014).

Cyber insurance policy writing is similar to other insurance but with some unique considerations (Biener et al., 2015). The underwriting process for cyber insurance, the insurance company assesses the risk of a potential policyholder, including their exposure to cyber threats, the effectiveness of their cybersecurity measures, and their history of cyber incidents (Biener et al., 2015). The insurer conducts a thorough assessment of the potential risks and threats that the policyholder may face, such as data breaches, cyber-attacks, or system failures (Romanosky et al., 2019). One unique aspect of the underwriting process for cyber insurance is the importance of understanding the policyholder's cybersecurity posture. This includes assessing their security policies and procedures, their employee training programs, and their technical controls such as firewalls and antivirus software. Once the insurance company has assessed the risk of the potential policyholder, they will determine the policy terms and conditions, including the coverage amount, premiums, and any exclusions or limitations (Franke, 2017). The way prices are structured for these policies is often based on how cyber liability and first-party expenses are offered in the real world (Gai et al., 2017). Assessing a potential policyholder's cyber-risk profile and comparing it to the insurer's risk tolerance is a vital task for cyber

insurance underwriters. It allows them to determine an accurate level of risk associated with the policyholder and set an appropriate premium rate that aligns with this risk profile. An accurate evaluation of cyber-risk is essential to ensure fairness and adequacy in the premium charged (Kshetri, 2020). However, Determining the appropriate premiums for cyber insurance remains more of an art than a science (Toregas & Zahn, 2014). Toregas & Zahn (2014) also highlight the difficulties involved in accurately calculating cyber insurance premiums, including the lack of historical data, the ever-changing nature of cyber threats, and the challenges of quantifying potential losses resulting from a cyber incident.

Therefore, as part of the underwriting policy process, insurers proposal forms, which are used to gather information from clients during the underwriting process, include information regarding management, and policy/compliance practices, (Jason Nurse et al., 2020). The objective of the questions is to acquire a comprehensive or approximate understanding of the insured's overall security posture. Essentially, these questionnaires serve as a crucial tool for assessing an organization's cybersecurity posture and differentiating risks across different applicants, then insurance companies use risk assessments to determine premiums (Talesh, 2018).

The underwriting process for cyber insurance entails conducting a comprehensive evaluation of the policyholder's cybersecurity posture. This evaluation helps to determine the policyholder's risk profile and

enables the development of appropriate coverage terms, which are reflected in the premiums charged. The insurer drafts the policy language, including the coverage limits, exclusions, and definitions, based on the risk assessment, the insurer determines what types of coverage to offer the policyholder, such as first-party coverage for losses suffered by the policyholder, third-party coverage for claims made against the policyholder by others, or both. The insurer evaluates the policyholder's risk profile, including their security protocols and risk management practices, to determine the appropriate premium and terms for the policy. Once the policy is approved, the insurer issues the policy to the policyholder, along with any endorsements or amendments. However, the underwriting process for cyber insurance is complex and involves a thorough evaluation of the policyholder's cyber risk profile (Romanosky et al., 2019).

2.4.3 Challenges and opportunities of cyber insurance.

There are many proponents of cyber insurance, the market for it is confronted with several challenges, with determining the appropriate premiums being one of the most significant obstacles (Toregas & Zahn, 2014). The emerging cyber insurance market encounters several distinct challenges in its development (Marotta et al., 2017). The dynamic and ever-changing nature of cyber risks poses uncertainty, making it challenging for insurers to accurately evaluate and price cyber insurance policies. This can lead to coverage gaps and disputes over claims

(Aziz et al., 2020). The lack of standardization poses a significant challenge in the cyber insurance industry. The absence of a uniform framework for measuring cyber risk makes it challenging for insurers to compare risks effectively and develop consistent policies. This can also make it difficult for insured to understand what is and isn't covered by their policy (Granato & Polacek, 2019; Aziz et al., 2020). Limited data: cyber insurance is a relatively new product, which means that there is limited data available to insurers to help them understand and price cyber risk. This can lead to conservative underwriting practices and higher premiums (Gai et al., 2017; Tonn et al., 2019). Complexity of cyber-attacks: Cyber-attacks is complex and could be hard to understand, which can make it difficult for insurers to accurately assess the impact of a breach and develop appropriate coverage. The unique attributes of cyber risks, in contrast to other operational risks, underscore significant obstacles that impede the establishment of a sustainable cyber insurance market (Biener et al., 2015). Changing regulatory environment: As cyber risks continue to evolve; governments and regulators are also evolving their approach to cyber risk management. This can create uncertainty for insurers and customers around what is required to comply with regulations and how insurance policies fit into this framework (Granato & Polacek, 2019b). To minimize confusion, most cyber insurance policies cover major cyber incidents, but existing cyber insurance plans seldom cover this expanding risk due to the difficulty of establishing cyber events' causes (Elnagdy, 2017).

Cyber insurance presents several opportunities for businesses including: risk transfer: cyber insurance allows individuals and businesses to transfer some of the financial risk associated with cyber-attacks to insurers. This can help protect against the potentially significant costs of a cyber-attack, such as data loss, business interruption, and legal expenses (Elnagdy, 2017; Yang & Lui 2014; Meland et al. 2015). Increased awareness: the process of obtaining cyber insurance can help raise awareness of cyber risks and encourage individuals and businesses to take proactive steps to improve their cybersecurity posture (Mazzoccoli & Naldi, 2020; Meland et al., 2015). Customized coverage is a key aspect of cyber insurance policies, allowing them to be tailored to the unique requirements of individuals or businesses. These tailoring options are based on various factors, including the industry, size, and type of data handled by the insured entity. This can help ensure that the policy covers the most relevant risks and provides the appropriate level of protection (Tonn et al., 2019). Access to resources: Many cyber insurance policies come with access to resources such as breach response services, which can help individuals and businesses respond to a cyber-attack more effectively. In order to minimize claim payouts, insurance companies offer assistance to insured individuals or businesses in preventing cyberattacks. They provide on-staff and outsourced resources, such as lawyers to handle class-action lawsuits, security professionals to offer advice on safeguarding measures before breaches occur, and incident response support after breaches. Additionally, credit monitoring services are provided to assist customers affected by

breaches. Cyber Insurance is an excellent method for smaller companies without cybersecurity resources to get security expertise (Meland et al., 2015). Competitive advantage: In some industries, having cyber insurance can be a competitive advantage, as it demonstrates to customers and partners that the individual or business takes cyber risks seriously and is taking steps to protect against them. Disclosure information regarding a company's cybersecurity awareness makes investors perceive its business favorably (Berkman et al., 2018). Overall, cyber insurance offers businesses an effective means of managing their cyber risks and can serve as a crucial component of a comprehensive cybersecurity strategy.

2.5 Cyber insurance market trends.

Cyber insurance has rapidly grown in response to the increasing need for financial organizations to mitigate cyber losses (Gai et al., 2017). By 2025, cyber insurance is projected to become a major line of business for insurance companies (Tonn et al., 2019). As consumers show growing interest, insurance companies are boarding the trend, making cyber insurance a significant industry. Notably, cyber insurance is the specialty insurance product with the highest rate of growth in the United States and is also gaining popularity in Europe (Meland et al., 2015). In the United States, a specialist insurance market for cyber risks has emerged (Eling & Schnell, 2016). While cyber insurance is now available,

coverage is still restricted. There is a need to expand cyber insurance coverage to deal with the growing risk (Tonn et al., 2019).

Presently, the annual gross premiums for cyber insurance in the United States amount to $2.75 billion, with a consistent growth rate of 26% to 50% each year. The anticipated premium volume in continental Europe stands at approximately $192 million, and it is estimated that the global cyber insurance premium volume will reach $5.9 billion by 2023. The U.S. market is more developed compared to its European counterpart, primarily due to the existence of reporting rules for cyberattacks, which have been in place for several years, accompanied by strict penalties for noncompliance (Eling & Schnell, 2016). The market for cyber insurance is growing rapidly and is estimated to be worth over $20 billion by 2025 (KPMG International, 2018).

Smaller businesses that generate more revenue and have more interest payments are often the early adopters of cyber insurance. These businesses also have stronger growth, rely less on outside reinsurance, and have higher premium concentrations in lines of insurance that may be standard and have more insureds. However, cyber risk perception in the United States is high, indicating that large financial institutions and businesses in other industries are vulnerable to cyberattacks. Many insurers admit that they purchase cyber insurance coverage to manage cyber threats (Pooser et al., 2018). Larger companies usually employ a chief information officer and other cybersecurity professionals to make

strategic decisions, which may inform cyber insurance purchases to minimize catastrophic situations (Meland et al., 2015). Infrastructure leaders have protected their organizations with cyber insurance, but they believe that current cyber insurance products are unable to adequately satisfy their demands, despite acquiring cyber insurance. Broader coverages and larger limitations are preferred. Trends in cyber insurance purchasing are probably influenced by the liabilities associated with customer data breaches (Tonn et al., 2019), and companies are more inclined to purchase insurance after a significant cyberattack (Eling & Schnell, 2016).

The cyber insurance industry is currently in its early stages of development; however, as the market progresses, it is expected to witness significant growth and expansion (Eling & Schnell, 2016). IT Governance reported trend of Cyber statistics for 2022, recently cyber-attacks target small organizations because of cybersecurity immaturity, and weakness of incident response, and it is also hard to recover from cyberattack according to lack of finances.

2.6 Behavioral study in the insurance industry.

The behavioral study has offered valuable insights into how individuals make decisions to hold insurance policies. There are studies on the insurance products that provide insight into incurred decision-making that would guide understanding cyber insurance adoption, and its

barrier. These studies identified key pain points in the insurance industry that are influenced by behavioral economics from both supply and demand side, including risk aversion, moral hazards, and adverse selection (Pal (2012); D Bailey (2014); Bodin et al. (2018); Talesh (2018); Abdul Hamid et al. (2022)).

The potential benefits and challenges of cyber insurance in mitigating the risks associated with cyber-attacks, and it is an effective tool for risk-sharing (Bodin et al., 2018). In cyber insurance industry, the concept of information asymmetry is significant in the context of cyber insurance, as it refers to the situation where the insurer has limited information about the insured's security measures compared to the insured themselves. This lack of information can cause adverse selection and moral hazard issues. The insured may not take adequate measures to protect their systems because they have insurance coverage, and the insurer may find it challenging to price the insurance policy accurately (Pal, 2012).

2.6.1 Risk aversion

In the context of the insurance industry, risk aversion pertains to the policyholders' inclination to transfer the financial risk to an insurance company by paying a premium. This enables them to safeguard themselves against potential losses (Abdul Hamid et al., 2022). The organization must determine the ideal level of investments in cyber

insurance and self-protection, considering its level of risk aversion (Simoni et al., 2020). Additionally, Fahad et al. (2018) discovered that consumers who exhibit higher levels of risk aversion are more inclined to adopt insurance as a strategy for managing risks. Nevertheless, according to Lyu & Barré (2017), when insured amounts are substantial, risk aversion may no longer influence decisions, suggesting that consumers might be more willing to accept higher risks if the potential losses are not financially significant. Individuals tend to display decreasing absolute risk aversion and increased downside risk aversion, implying that they are less averse to risk when facing small probabilities of large losses and more averse to risk when encountering large probabilities of small losses. This can create a problem for insurers, as they may end up with a pool of policyholders who are more likely to file claims, which can lead to higher costs for the insurer (Majuca et al., 2006).

Majuca et al. (2006) mentioned that risk aversion can lead to adverse selection, which occurs when higher-risk individuals or organizations are more likely to purchase insurance, while those with lower risk avoid it (Bodin et al., 2018). Lyu & Barré (2017) mentioned that more risk-averse consumers being more likely to buy insurance protect themselves from the financial consequences of risks they are faced. Majuca et al. (2006) suggests that insurers are need to addressing adverse selection by offering more comprehensive cyber insurance policies that are tailored to specific business needs. By offering policies that are more

customized to individual organizations, insurers can better manage their risk and avoid adverse selection

Abdul Hamid et al. (2022) found that many organizations in developing countries, may view cyber insurance as an unnecessary expense, as they may believe that the likelihood of a cyber-attack is low and that they can manage the risks on their own. Additionally, some organizations may be hesitant to adopt cyber insurance because they may not fully understand the risks involved or the potential benefits of coverage. The study suggests that addressing these concerns and increasing awareness about the benefits of cyber insurance may help to overcome risk aversion and encourage adoption. Therefore, the concept of risk aversion is important in understanding the behavior of policyholders, insurers, and regulators in the insurance industry, as it can influence the design of insurance policies, pricing strategies, and regulatory frameworks.

2.6.2 Moral hazards

Moral hazards is the consequences of cyber insurance to insurance company, it occur when people or organizations change their behavior in response to having insurance (Majuca et al., 2006), they take less care in protecting their systems and data because they are insured against the financial losses caused by cyber-attacks (Bodin et al., 2018). This can lead to a lack of incentive for businesses to invest in robust

cybersecurity measures and may even result in an increase in cyber incidents (Talesh, 2018). The anticipated losses are impacted, resulting in an increase in the insurance premium (Visscher et al., 2018).

Insurers can use appropriate pricing strategies and risk assessment techniques to mitigate adverse selection and moral hazard problems. Talesh (2018) noted that insurance companies can mitigate the risk of moral hazard by requiring policyholders to implement specific security measures and adhere to various cybersecurity standards as a condition of coverage. In addition, insurers should consider providing incentives for organizations to improve their cybersecurity posture, such as offering lower premiums for organizations that have implemented security best practices.

Education and awareness campaigns are essential to promote a culture of cybersecurity and encourage organizations to take a proactive approach to risk management. Bodin et al. (2018) and D Bailay (2014) highlight the importance of such campaigns. D Bailey (2014) also explores various strategies that insurance companies can use to mitigate moral hazard, including risk-based pricing, loss control services, and contractual limitations on coverage. The article emphasizes the importance of underwriting expertise in identifying and managing moral hazard in cyber-risk insurance as well.

To implement risk-based pricing, insurance companies need to assess the risk profile of each policyholder accurately. This involves gathering data on the policyholder's cybersecurity measures, such as firewalls, antivirus software, and employee training programs. Insurance companies may also use external data sources, such as third-party risk assessments or public data breaches, to supplement the policyholder's information. Loss control services refer to the measures that insurance companies provide to help policyholders reduce their exposure to loss or damage from cyber-attacks by implementing risk assessment to identify areas of vulnerability in their cybersecurity measures, training program, and incident response planning.

However, contractual limitations on coverage can also be a double-edged sword. If the limitations are too severe, policyholders may feel that they are not getting adequate protection for their premiums, which can discourage them from buying cyber-risk insurance at all. Insurance companies need to strike a balance between limiting their liability and providing meaningful coverage that meets their policyholders' needs (D Bailey, 2014).

In summary, the prior behavioral study sheds light on how individuals make the decision to obtain a cyber insurance policy based on their risk profile and their tolerance for potential loss. The issues of risk aversion, adverse selection, and moral hazard present significant challenges for

both insurers and the insured when it comes to determining appropriate pricing.

2.7 Factors affecting the Willingness to Pay for insurance.

There is limitation of study on a Willingness to Pay for cyber insurance in academic literature. However, Wolff (2022) notes that auto insurance and flood insurance are commonly used as reference points when discussing cyber insurance, as they are non-life insurance, and also share many similarities. Like auto insurance, cyber insurance policies have deductibles, limits, and premiums based on risk. Factors such as a company's industry, size, and cybersecurity practices can impact their cyber insurance rates, similar to how a driver's age, driving record, and vehicle can affect their auto insurance rates.

Additionally, floods and cyberattacks can both cause substantial financial losses and damage. While flood insurance covers physical property damage due to a flood, cyber insurance covers financial losses resulting from cyberattacks. Both policies may also offer additional coverage for specific risks, such as cyber insurance policies that cover data breaches or ransomware attacks and flood insurance policies that may need additional coverage for events like sewer backup or mudflow. Cyber insurance is not mandatory by law as opposed to auto insurance. Furthermore, unlike health insurance, there is no legislation at the state

or federal level regulating the specifics of policies and the expenses they must cover. The flood insurance models provide a helpful reference for cyber insurance because both types of insurance cover risks that do not occur frequently and can vary in scale from small to large (Wolff, 2022a).

Insurance is a vital tool for managing risk and providing financial security against unexpected events. However, the decision to purchase insurance can be influenced by a variety of factors. Comprehending the correlation between insurance and the Willingness to Pay holds significant importance for policymakers and insurance providers. Such understanding can aid in making informed decisions concerning pricing, product design, and marketing strategies. To explore cyber insurance, other types of insurance such as auto insurance, and flood insurance have been studied and compared for any valuable insights or ideas they may provide for this study.

This study explore the previous literature included cyber insurance domain, Nam (2018), uses Contingent Valuation Method to estimate consumer Willingness to Pay for extra cost in cyber insurance when using smart contract and Blockchain technology for claim processing. The result show that price is influence the decision to pay for extra payment in cyber insurance.

Study on flood insurance with the Contingent Valuation Method's Single Bound Dichotomous Choice framework to determine individuals' willingness to pay for this type of coverage. The study findings indicate that the flood insurance premium and factors such as house type and prior flood experience significantly influence the decision to pay for it (Paopid et al., 2020).

In Pakistan, flood insurance is available, and evidence suggests that factors influencing rural households' willingness to pay for flood insurance encompass the age of the household head, landownership, off-farm income sources, and preconceptions about the effectiveness of flood insurance. Surprisingly, the perceived risk of flooding does not have a significant impact on rural families' willingness to pay for an insurance premium; however, their financial position does play a crucial role in this regard (Abbas et al., 2015).

Dragos & Dragos (2017), explored motor insurance domain, they study the state preference with the discrete choice models, to analyze the impact of various factors, including price, coverage, deductible, and insurer reputation on consumer behavior in motor insurance policy selection. The results show that price is the most crucial factor influencing consumers' decisions, followed by coverage level, deductible, and insurer reputation.

The Contingent Valuation Method was employed to examine the crucial factors influencing the willingness to pay for various types of insurance, such as car, house, and home insurance. The study outcomes demonstrated that age, income, education level, and risk perception were significant factors in determining individuals' inclination to pay for insurance. Notably, the study indicated that older individuals, those with higher income, and higher education levels exhibited a greater willingness to pay for insurance coverage (Hansen et al., 2016).

A study utilizing the Contingent Valuation Method to explore the Willingness to Pay for insurance, particularly disaster insurance, aimed to identify the factors that influence household inclination to pay for earthquake insurance. These factors included household income, risk perception, knowledge of earthquake insurance, and personal experience with earthquakes. The study's findings revealed that risk perception, knowledge of earthquake insurance, and personal experience with earthquakes significantly influenced households' willingness to pay for earthquake insurance (Tian & Yao, 2015).

In today's digital age, cyber insurance coverage has gained immense significance by offering protection against losses and damages resulting from cyber-attacks, data breaches, and other cyber-related risks. Despite its advantages, several factors influence the demand for cyber insurance and the willingness of individuals to invest in it. Prior literature has identified these factors, which encompass the perceived

cost of cyber insurance, the level of cybersecurity awareness and education regarding potential cyber risks, the perceived value of cyber insurance products, misunderstandings about the necessity for coverage, and potential discrepancies between offered coverage and companies' requirements. Additionally, individual demographic and socioeconomic attributes play a role in the decision-making process related to cyber insurance payment.

For the better understanding those factors that influence consumer preferences and impact the uptake of cyber insurance, insurers and policymakers can identify potential barriers and develop strategies to address them. This can help to increase the demand for cyber insurance and improve the overall cybersecurity posture of individuals and organizations. The previous study has identified several factors that are valuable for this study, including:

One of the key concerns in the realm of cyber insurance is the high premiums for insurance coverage and their variability. Cyber insurance is designed to safeguard businesses against financial losses stemming from cyber-attacks. However, the high premiums for insurance coverage and variability can influence the adoption of new products and services, and cyber insurance is no exception. Studies by Gai et al. (2017), Bodin et al. (2018), and Vakilinia & Sengupta (2019) have found that the high premium of cyber insurance is a key factor that affects the demand for it. A high premium can deter businesses from purchasing insurance, as

it may be seen as too expensive relative to the perceived likelihood and potential impact of a cyber-risk (De Smidt & Botzen, 2018). The cost of coverage is reasonable and the extent of coverage is comprehensive, the likelihood of making a purchase increases (Vakilinia & Sengupta, 2019). The same as another type of insurance, Dragos & Dragos (2017) use state preference method to explored the motor insurance, the results show that price is the most crucial factor influencing consumers' decisions. Nam (2018) uses Contingent Valuation Method to estimate consumer Willingness to Pay for extra cost in cyber insurance when using smart contract and Blockchain technology for claim processing and the result show that expensive additional premiums were less attractive to respondents so the only 65 percent of the respondent are willing to pay for it. Study of Paopid et al. (2020), also show that the flood insurance premium is affect to the decision to pay.

Therefore, finding the right balance between the premium and the coverage offered is important in order to encourage organization to purchase cyber insurance and mitigate cyber risks effectively. While cyber insurance is becoming more common for large firms that may fairly anticipate facing a cyber-attack at some time, it may be more difficult to justify for smaller businesses that may want to self-insure rather than pay a high insurance premium (Pooser et al. (2018); Zhanna Malekos, Smith; Eugenia & Lewis, (2020)).

Several sub-factors, such as industry, law and regulation, and cybersecurity measures, can impact the price of cyber insurance. For example, businesses in the healthcare industry are often a prime target for cyberattacks as they possess unique vulnerabilities that make them attractive to malicious cyber actors (Kabir et al., 2020), so they are more likely to face cyber-attacks than those in the retail industry, and may therefore face higher insurance premiums (Gai et al., 2017). The location of a business can also impact its exposure to cyber risks, with businesses located in areas with higher rates of cybercrime may face higher premiums.

While Eling & Schnell (2016), found the insufficient data breaches to compute premiums, capital, or reserves, increasing the available insurance capacity and the level of competition can drive down premiums. To alleviate some of the issues associated with cyber risk insurance, it is crucial to develop standards for cyber risk definitions, coverage, and pre-coverage risk assessment, and insurance companies can establish and report cybersecurity best practices that will result in a better premium (Meland et al., 2015).

In summary, the high premium of cyber insurance remains a challenge in encouraging organization to purchase it. Finding the right balance between the premium and the coverage offered is important, as well as considering sub-factors such as industry, law and regulation, and

cybersecurity measures. Developing standards for cyber insurance can also help to alleviate some of the issues associated with cyber insurance.

The lack of risk perception is a significant consideration when it comes to the decision-making process for purchasing cyber insurance. Risk perception refers to how individuals or organizations perceive the potential risks associated with cyber threats. The level of perceived cyber threats tends to rise with personal experience and awareness of cybersecurity breaches (Nam, 2019). This perception is influenced by various factors such as previous experiences and overall risk tolerance, and the salience, or accessibility, of information has a significant effect on risk perception (De Smidt & Botzen, 2018). However, despite the increasing awareness of cyber risks, the lack of risk perception is still a significant barrier to cyber insurance adoption, as many individuals and organizations may not see cyber risks as a priority (Abdul Hamid et al., 2022). In another insurance domain (Tian & Yao, 2015), also Hansen et al. (2016), found risk perception affect the decision to hold insurance policy as it played significant roles in determining individuals' willingness to pay for car, house, and home insurance.

In summary, lack of risk perception is a major barrier to cyber insurance adoption, as it influences how individuals and organizations perceive the level of risk associated with cyber threats. This perception is influenced by various factors, such as previous experiences and overall risk tolerance. The accessibility of information also has a significant

effect on risk perception. Therefore, efforts should be made to improve risk awareness and increase the salience of information to encourage greater adoption of cyber insurance.

Lack of perceive benefit: the perceived benefits of cyber insurance play a significant role in the decision to purchase insurance. However, despite the high potential value of losses resulting from cyberattacks in comparison to the cost of cyber risk insurance, there is still hesitation among many individuals and organizations to purchase it (Visscher et al., 2018). This is a concerning issue, given the increasing frequency and severity of cyber-attacks.

A key obstacle to the adoption of cyber insurance is the lack of perceived value. Individuals and organizations may not fully comprehend the advantages that cyber insurance can offer, such as protection against financial losses arising from cyber incidents. Abdul Hamid et al. (2022) conducted a study that highlighted this lack of perceived value as one of the primary barriers to the adoption of cyber insurance.

In addition to the lack of perceived value, there is also a knowledge gap regarding cyber insurance. Many individuals and organizations may not understand the coverage offered by cyber insurance policies, which can lead to a potential mismatch between the coverage offered and what they seek. Gai et al. (2017), noted that a primary challenge is the

difficulty of optimizing insurance returns by prudent selection of covered objects within a certain financial budget. This highlights the need for individuals and organizations to have a better understanding of the coverage offered by cyber insurance policies before making a decision to purchase.

In summary, the perceived benefits of cyber insurance are crucial in the decision to purchase insurance. Individuals and organizations must have a better understanding of the coverage offered by cyber insurance policies and the potential value it can provide to effectively manage cyber risks.

The experience of a cyber-attack can significantly influence a company's inclination to acquire cyber insurance. The potential financial losses and business disruptions resulting from a cyber-attack can make a company more aware of the need for protection against such events. In fact, research by Eling & Schnell (2016) suggests that companies are more inclined to purchase cyber insurance after experiencing a significant cyber-attack. This is because the experience provides a real-world understanding of the potential consequences of a cyber-attack, which may not have been fully appreciated before. The experience may also increase the perceived value of cyber insurance, as companies realize the financial and operational benefits of having a policy in place. It is the same as study of Paopid et al. (2020), that prior flood experience significantly influence Willingness to Pay for flood insurance.

In summary, the companies may perceive insurance as more valuable and necessary after experiencing the consequences of risk, which can result in significant financial losses.

The level of regulatory pressure: It is a significant factor that influences the decision of organizations to purchase cyber insurance. Laws and regulations have been established, and they have raised the potential for fines, penalties, and other obligations on organizations in the event of a data breach or cyber-attack (Talesh, 2018). Organizations that understand the consequences of these laws and regulations tend to look for ways to manage their cyber risks effectively, and one of the mechanisms they use is transferring those risks to third parties such as cyber insurance providers.

Gai et al. (2017), stated that the primary challenge for organizations in purchasing cyber insurance is the difficulty of optimizing insurance returns by prudent selection of covered objects within a certain financial budget. This challenge highlights the importance of understanding the regulatory landscape and ensuring that the organization is adequately covered under the relevant laws and regulations. Trends in cyber insurance purchasing are also influenced by the liabilities associated with customer data breaches. Research conducted by Tonn et al. (2019), demonstrated that the heightened emphasis on data privacy and security regulations, such as the General Data Protection Regulation (GDPR) in

the European Union, has resulted in an upsurge in cyber insurance purchases by organizations aiming to safeguard themselves against potential fines and other liabilities related to data breaches.

In summary, laws and regulations play a significant role in driving organizations to purchase cyber insurance. With the potential for significant fines and penalties associated with data breaches, organizations are recognizing the importance of transferring cyber risks to third parties such as cyber insurance providers. Understanding the regulatory landscape and ensuring adequate coverage is crucial for organizations looking to maintain their cyber risks effectively.

The lack of IT security awareness is another critical factor that may impede the adoption of cyber insurance: According to Abdul Hamid et al. (2022), lack of IT security awareness is one of the significant barriers to cyber insurance adoption. The absence of awareness can be attributed to several factors, including a lack of comprehension regarding the value of cyber insurance and the perception that cyber risks are not a primary concern. These factors contribute to the overall lack of understanding and awareness of the importance of cyber insurance as a risk management tool. Organizations may not realize the severity of potential losses associated with cyberattacks, including the type of data they hold and the potential impact of a data breach on their reputation and customer trust.

In addition to awareness, organizational culture also influenced in the adoption of cyber insurance. Companies with a culture of risk management and proactive security measures are more likely to consider cyber insurance as part of their overall risk management strategy. On the other hand, companies with a reactive approach to security may be more reluctant to invest in cyber insurance until after they have experienced a significant data breach.

Experienced purchasing cyber insurance: the claim history of a company can affect its cyber insurance premiums. If a company has a record of filing claims for cyber-attacks, it may be perceived as a higher risk and may face higher insurance premiums. The claim history of a company is a crucial factor in determining its cyber insurance premiums. Companies with a history of filing claims for cyber-attacks may be viewed as higher risk and face higher premiums (Eling & Schnell, 2016).

Professionalism in cybersecurity: The level of professionalism in cybersecurity is critical for effective risk management and cyber insurance purchasing decisions. Professionals, particularly risk managers, who have firsthand experience with a cyber incident are more inclined to consider purchasing cyber insurance. The personal experience of dealing with a cyber-incident often leads to a better understanding of the potential risks involved and the benefits of having cyber insurance coverage (Biener et al., 2015), while larger companies

usually employ a chief information officer and other cybersecurity professionals to make strategic decisions, which may inform cyber insurance purchases to minimize catastrophic situations (Meland et al., 2015). However, research indicates that decision-makers have a tendency to overestimate the likelihood of a successful cyberattack while underestimating its potential financial impact. This results in a certain reluctance to obtain cyber insurance coverage to protect against cyber risks (De Smidt & Botzen, 2018). Despite the high expected value of cyberattack losses, decision-makers are hesitant to purchase cyber insurance. Top management of enterprises recognizes cyber threats as one of the most hazardous risks (Uuganbayar et al., 2021), while assessing and managing risks in emerging cyber systems presents significant challenges for risk assessors and managers (Ganin et al., 2020).

Demographic and socioeconomic factor: Research exploring the factors influencing the willingness to pay for insurance typically incorporates demographic, socioeconomic, and industry-specific elements, such as sex, age, and other relevant variables (Abbas et al. (2015); Hansen et al. (2016), income, the university education are statistically insignificant for predicting future voluntary insurance participation (Dragos & Dragos, 2017), company profile such as size, revenue, organizations that hold significant amounts of customer information are more likely to purchase cyber insurance (Ozawa, 2021; Pooser et al., 2018; Tal

Pavel, 2020; Franke, 2017), industry (Bandyopadhyay & Mookerjee, 2019).

Abdul Hamid et al. (2022), identified enablers such as government regulations and incentives, industry standards and best practices, and the role of insurance brokers. However, the adoption of cyber insurance in developing countries like Malaysia is influenced by a complex interplay of factors that include organizational culture, leadership commitment, and stakeholder engagement. Insurance companies face challenges in meeting the evolving preferences, expectations, and demands of their clients. As a result, they must continually innovate to reach customers and promote their products. The role of insurance brokers is also crucial in facilitating the adoption of cyber insurance. In addition to promoting insurance products, companies should prioritize increasing client risk awareness (Dragos & Dragos, 2017).

Table 2**.** Factors influence Insurance purchasing

Factors	**Correlation with WTP**	**Literature Citation**
Socioeconomic		
1. Education Level	High education likely to purchase insurance	(Dragos & Dragos, 2017)
2. Age		(Pooser et al., 2018)
3. Position	In transportation study the manager is decide to transfer risk to insurers	
4. A size of the company	Large companies are more likely to purchase cyber insurance.	(Ozawa, 2021), (Pooser et al., 2018), (Tal Pavel, 2020), (Franke, 2017)
5. Annual revenue	Individual income affects their decision to pay.	(Ozawa, 2021)
6. Industrial	Cyber insurance is initially growing in financial industry.	(Franke, 2017) (Elnagdy et al., 2016)

Factors	Correlation with WTP	Literature Citation
Purchasing behaviors		
1. Premium	The adoption of new products and services is influenced by their pricing, and cyber insurance is not an exception.	(Bodin et al., 2018), (Gai et al., 2017), (Vakilinia & Sengupta, 2019)
2. Coverage	The more extensive the coverage offered at a reasonable price, the higher the likelihood of purchasing insurance.	(Vakilinia & Sengupta, 2019)
3. Awareness	Respondents who are aware of the potential risks are more likely to purchase insurance.	(Tal Pavel, 2020) (Hansen et al., 2016)
4. Knowledge	Respondents who possess extensive knowledge about cyber insurance would demonstrate a higher willingness to pay compared to those with limited understanding of cyber insurance.	(Tal Pavel, 2020) (Tian & Yao, 2015)
5. Assessment of IT or Awareness of cyber risks	Respondents with a clear understanding of their cyber risk level and risk assessment are more likely to purchase insurance.	(Franke, 2017)
6. Information security maturity	A company that has a high level of information security maturity is more likely to obtain cyber insurance.	(Franke, 2017)

Factors	Correlation with WTP	Literature Citation
7. Experiences	Companies that have prior experience purchasing insurance or currently hold insurance are more inclined to acquire additional insurance policies.	(Tian & Yao, 2015) (Paopid et al., 2020) (Nam, 2018)
8. Awareness of relative law	Cyber insurance is an optional value, so respondents who are aware of its legal impact will choose to pay for it.	(Berkman et al., 2018) (De Smidt & Botzen, 2018)

2.8 Identification of gaps in previous literature.

Behavioral studies have provided valuable insights into the overall cyber insurance industry and its challenges and opportunities. Meanwhile, the alarming increase in cyber risks is projected to drive exponential growth in the cyber insurance market over the next decade. However, despite its potential benefits, cyber insurance acceptance levels are relatively low and it is currently only popular in America and Europe. Cyber Insurance is currently in its exploratory phase; therefore, a variety of aspects are being discovered by current applications. Itis becoming a feasible alternative for financial institutions and other businesses to protect business environments and financial processes (Gai et al., 2017). According to its unique characteristic in specific market so, it is crucial to identify effective ways to increase the growth of the cyber insurance market in these regions.

While prior studies have made efforts to identify factors impacting consumers' willingness to pay for various insurance types, the existing research pertaining to cyber insurance primarily concentrates on the extension of coverage and additional payments. To comprehend the economic value of cyber insurance, researchers have employed the Contingent Valuation Method, a validated approach for determining the amount of money individuals are willing to invest in non-market products or services.

Table 3. Identification gap in previous literature.

	Domain	**Origin**	**Factor**	**Methodology**	**Research Gap and relevant**
Paopid et al. (2020)	Flood insurance	Thailand	House type and prior flood experience.	CVM SBDC	-Specific insurance domain - Not considering a zero WTP
Nam (2018)	Cyber insurance *(Extra payment)*	Korea	Prior experience in purchasing insurance contracts.	CVM OOHB	-Indirect insurance premium - Not considering a zero WTP
Hansen et al. (2016)	House insurance and Auto insurance	Denmark	Aware of risk	CVM	-Specific insurance domain
Tian & Yao (2015)	Earthquake insurance	China	Knowledge of earthquake insurance and Experience with earthquakeare.	CVM	-Specific insurance domain - Not considering a zero WTP
This study	Cyber insurance	Thailand	Add the relevant factors, position in field (Tonn et al., 2019), and the impact of cybersecurity and data protection laws on organizations (Berkman et al., 2018)	CVM and Spike model	- Study in Organization level. - New insurance domain.

Interestingly, prior literature has revealed that a significant portion of people express zero Willingness to Pay for hypothetical insurance, which negatively impacts the mean Willingness to Pay. To address this issue, a spike model is recommended to account for these respondents. As such, it becomes crucial to investigate consumers' Willingness to Pay for cyber insurance and identify the key factors influencing their decision-making process. To bridge this gap, this study aims to employ the Contingent Valuation Method in the first part to identify factors affecting consumers' Willingness to Pay for cyber insurance. In the second part of the study, a spike model will be utilized to address respondents with zero Willingness to Pay and uncover the actual economic value of cyber insurance. This model will be instrumental in determining the true value of cyber insurance payments by adjusting for the zero-value responses from respondents who are not willing to pay.

This study will significantly contribute to the literature by providing a demand-side perspective on the cyber insurance market. This study addition estimate the study on cyber risk and cyber lost (Meland et al., 2015) found the larger companies usually employ a chief information officer and other cybersecurity professionals to make strategic decisions, which may inform cyber insurance purchases to minimize catastrophic situations. And Berkman et al. (2018) examines the impact of cybersecurity and data protection laws on organizations and reveals that these laws have prompted various measures, appointing directors with IT backgrounds, hiring Chief Information Security Officers, forming IT

committees of the Board, enhancing security in new systems, and purchasing insurance thus this study will also contribute these two additional explanatory variables.

Chapter 3. Methodology

This chapter consists of the theories, models, and methodologies used in previous studies that are relevant to the research objectives. This section will cover key economic theories, the Contingent Valuation Method, and the Spike Model, which will be utilized to determine the users' Willingness to Pay for Cyber Insurance in Thailand.

3.1 Random Utility Theory

The economic value of goods and services, whether they are market or non-market goods, is based on the level of well-being that people derive from what they want, which is determined by their preferences and choices. Various stated preference methods, including Contingent Valuation, discrete choice experiments, and best-worst scaling, are employed to investigate consumers' preferences for different products or services within hypothetical markets. These methods allow researchers to analyze how individuals make choices and express their preferences in situations where real market transactions may not be feasible or practical. The background of Contingent Valuation is derived from the random utility theory (Aizaki et al., 2015). In Contingent Valuation studies, there are two different approaches, such as utility differences and cost functions (Huh et al., 2015), with the Double Bound Dichotomous Choice when respondents answer that they are unwilling to pay at all

derived from an individual's utility (Yoo & Kwak, 2002). However, this study uses random utility theory.

Aizaki et al. (2015) have presented a model of random utility, which suggests that in a choice set (S) an individual n derives utility U_{ni} from alternative i This utility function can be expressed as:

$U_{ni} = V_{ni} + e_{ni}$ ..... Eq. (4.1)

Where, V_{ni} represents a random parameter vector that has an impact on the attribute, while e_{ni} represents a random component of utility.

The authors also assume that for individual n, alternative i in the choice set provides the highest utility among all the alternatives available, such that $\forall_i \neq$ j , we have

$U_{ni} > U_{nj}$ ..... Eq. (4.2)

which is equivalent to

$V_{ni} - V_{nj} > e_{ni} - e_{nj}$ ..... Eq. (4.3)

The random utility concept for Contingent Valuation can be explained as follows: When the first question is asked, there are two possible answers yes or no. If the respondent answers yes, we can interpret that

the utility of this respondent is greater than that of the other alternative. However, we cannot observe $e_{ni} - e_{nj}$. only $V_{ni} - V_{nj}$ can be calculated to estimate the probability, and it is shown that $V_{ni} - V_{nj} > e_{ni} - e_{nj}$. Consequently, the likelihood of individual n selecting alternative i from the choice set can be represented as follows:

$$P_n(i) = \Pr(U_{ni} > U_{nj})$$
$$= \Pr(V_{ni} - V_{nj} > e_{ni} - e_{nj}), \forall_i \neq j \quad \text{Eq. (4.4)}$$

3.2 Method to measure Willingness to Pay

According to Jagpal & Jedidi (2009), estimating reservation prices can be accomplished through either purchase data or survey/experimental data. Frequently employed approaches based on survey/experimental data encompass self-stated Willingness to Pay, contingent valuation, conjoint analysis, and experimental auctions. These methods serve as valuable tools to assess individuals' preferences and willingness to pay for various products or services in research and market scenarios. When evaluating these measurement methods, several factors come into play. The first factor to consider is incentive compatibility, which refers to how effectively the method encourages consumers to disclose their true Willingness to Pay. The second factor is hypothetical bias, which relates to the method's ability to accurately replicate real-life purchasing contexts. The third factor pertains to the method's capability to estimate

reservation prices for new products with attributes that have not yet been introduced to the market or have not exhibited sufficient variation among existing products, making reliable estimation challenging. The fourth factor focuses on the method's capacity to measure Willingness to Pay for multiple brands within a specific category or for multiple products across different categories.

Actual purchase data is not subject to hypothetical bias; however, it requires knowledge of the actual purchase amounts. The utilization of purchase data is not feasible for determining the optimal price for a new product or implementing an optimal product line policy (Wertenbroch & Skiera, 2002).

Table 4 Methods based on survey/experimental data.

Method	Approaches	Challenges	References
Contingent Valuation	Provide hypothetical scenarios and capture non-market values that lack a readily observable price.	- Prone to hypothetical bias.	(Sajise et al., 2021)
Conjoint Analysis	Individuals make trade-offs between different attributes or features of a product or service, which involves presenting them with a series of choices.	- requires careful design. - Need the product details/feature.	(Jedidi & Zhang, 2002)

The choice of research method depends on various factors, including the research objectives, context, and trade-offs between accuracy, cost, and practicality. In the case of cyber insurance in Thailand, as it is a relatively new and option value product in the market, the selection of an appropriate method becomes crucial. While the Contingent Valuation Method has found diverse applications in areas such as flood insurance, earthquake insurance, motor insurance, and house insurance, applying the Choice Experiment Method to cyber insurance in Thailand may present limitations. This is because the Choice Experiment Method requires individuals to make trade-offs between different attributes or features of a product or service, which may not be well-defined or readily available in the case of cyber insurance.

Therefore, the Contingent Valuation Method has a great advantage in flexibly creating virtual market scenarios without actual cost benefit to be evaluated and inducing the willingness to pay through surveys, thereby enhancing preservation value (optional value) goods measure (Sajise et al., 2021). Moreover, Hanemann (1989) has highlighted that the Contingent Valuation Method is an effective approach to investigate individuals' Willingness to Pay for non-market goods and products.

3.3 A Contingent Valuation Method

The Contingent Valuation Method (CVM) is a stated preference approach widely employed to assess the intangible and non-market value

associated with optional value goods (Aizaki et al., 2015). The Contingent Valuation Method is a frequently employed approach utilized by policymakers and economists (Song et al., 2019), that establishes a hypothetical market for the transaction of non-market goods and directly expresses Willingness to Pay for goods or services expected (Rahmatian, 2005). The Contingent Valuation Method has a great advantage in flexibly creating virtual market scenarios without actual cost benefit to be evaluated and inducing the willingness to pay through surveys, thereby enhancing the stated preference of the optional value goods measure (Sajise et al., 2021). However, it is important to note that the Contingent Valuation Method derives the Willingness to Pay by relying on a virtual market setting and conducting a questionnaire survey (Honu, 2007), it is important to design the questionnaire in a way that increases the accuracy of the Willingness to Pay per household measured from the sample, and to conduct surveys and analyze survey data at each stage to secure the reliability and validity of the research results (Zainudin et al., 2016; Sajise et al., 2021).

Given that the Contingent Valuation Method is employed to measure the total value of insurance markets, encompassing optional value, which is still in its early stages, it is susceptible to various forms of bias. Therefore, this study aims to apply the Contingent Valuation Method after thoroughly comparing and reviewing the applicable techniques from previous literature. This study has identified previous research works that have utilized the Contingent Valuation Method to estimate

the value of flood insurance (Paopid et al., 2020), and the additional premium for smart contracts and blockchain for claims processing in cyber insurance (Nam, 2018).

The term Contingent Valuation (CV) refers to a technique used to assess the value an individual place on goods or services that do not have a market price. In the process of evaluating the value of non-market goods and services, the Contingent Valuation Method involves individuals declaring their willingness to pay (WTP) or willingness to accept (WTA) for such products and services. As a widely used approach, the Contingent Valuation Method plays a crucial role in assessing the value of intangible and non-market goods and services.

Numerous studies have showcased the suitability and adaptability of the Contingent Valuation Method for non-market goods, building upon prior research endeavors in the insurance sector. An illustrative example is the application of the Contingent Valuation Method to assess the feasibility of incorporating blockchain and smart contracts for claim processing in the domain of cyber insurance (Nam, 2018), flood insurance (Paopid et al., 2020), car insurance (Dragos & Dragos, 2017), and house insurance (Hansen et al., 2016).

3.3.1 A Willingness to Pay

When consumers make purchasing decisions in the market, they typically compare the market price of goods or services with their individual Willingness to Pay (WTP). In situations where the WTP is greater than or equal to the price, consumers proceed to make the purchase. Thus, the WTP for a good is composed of the amount actually paid in the market (market price) and the surplus above the price (consumer surplus). The maximum WTP, expressed in monetary units, reflects consumers' preferences for the product and represents its economic value.

The extension of the Willingness to Pay (WTP) concept aims to estimate the consumer's WTP for non-market goods. the Contingent Valuation Method are popular estimation tools with several survey types introduced, such as the Single Bound method (Sajise et al., 2021), and the Double Bound Dichotomous Choice format (Song et al., 2019).

One common method of estimating Willingness to Pay is by calculating the ratio of factors, and the ratio zero of the Willingness to Pay from a Contingent Valuation questionnaire, where individuals provide a dichotomous answer, $Ans_i = 0$ if the answer is no, and $Ans_i = 1$ if the answer is yes (Alejandro, 2012). To estimate the WTP for non-market goods such as optional value insurance, the linear WTP estimation method has been most commonly used in preliminary feasibility studies.

Alejandro (2012) explained the economic estimation of Dichotomous Choice format, where WTP_i is the willingness of an individual i to pay for non-market goods. The WTP can be expressed as follows:

$$WTP_i(z_i, u_i) = z_i\beta + \varepsilon_i \quad \text{Eq. (4.5)}$$

In this context, the notation used is as follows: z_i represents the vector of independent variables, β denotes the vector of estimated parameters, and ε_i stands for an unobserved variable. The survey design simply asks the respondent to answer only yes or no, therefore, $Ans_i = 0$ if the answer is no, and $Ans_i = 1$ if the answer is yes. When $Ans_i = 1$, This indicates that the Willingness to Pay (WTP) is higher than the bid amount (b_i), and the probability is expressed as follows:

$$\begin{aligned} \Pr(Ans_i = 1|z_i) &= \Pr(WTP_i > b_i) \\ &= \Pr(z_i\beta + u_i > b_i) \\ &= \Pr(u_i > b_i - z_i\beta) \end{aligned} \quad \text{Eq. (4.6)}$$

To elaborate further on the standard cumulative normal $\phi(x)$, the traditional probit estimation model only incorporates an additional predictor b_i. When $u_i \sim N(0, \sigma_2)$, and $v_i \sim N(0,1)$, then the formula is:

$$\Pr(Ans_i = 1|z_i) = \Pr\left(v_i > \frac{b_i - \acute{z}_i\beta}{\sigma}\right)$$

$$= 1 - \phi(\frac{b_i - \acute{z}_i\beta}{\sigma})$$

$$\Pr(Ans_i = 1|z_i) = \phi(\acute{z}_i\frac{\beta}{\sigma} - b_i\frac{1}{\sigma}) \quad \text{Eq. (4.7)}$$

As previously pointed out by Kristrom (1997), and further noted by Haab and McConnell (1997), The Contingent Valuation Method was originally devised for estimating WTP for public goods, which means the values obtained cannot be negative. However, the current estimation procedure presents the problem that willingness to pay can be estimated as zero or negative in the case of any public investment project or policy. Therefore, the Contingent Valuation study divides respondents into those with the Willingness to Pay of zero and those with a willingness to pay greater than zero.

To address this problem, it is necessary to distinguish between those who refuse to pay and those who intend to pay. In other words, the former's willingness to pay should be explicitly treated as 0, and the latter's willingness to pay should be sought only from those respondents. This procedure can be used to create an econometric model that better reflects respondents' choices. It also has the advantage of separating non-payers and can be called a spike model, where all willingness to pay zero is specially treated (Kristrom, 1997).

3.3.2 Contingent Valuation Format

The Double Bounded Dichotomous Choice (DBDC) contingent valuation method offers a novel approach to enhance the statistical efficiency of conventional surveys used to estimate the value individuals assign to specific goods or services. In contrast to traditional surveys that involve a single yes/no question about willingness to pay, this method introduces a second question that depends on the response to the first question. If respondents answer affirmatively to the initial query, they are then asked if they would be willing to pay a higher amount. Conversely, if they answer negatively, they are asked if they would be willing to pay a lower amount. This two-step process enables more precise estimation of values and enhances statistical efficiency (Hanemann et al., 1991).

The One and One Half Bound (OOHB) approach is designed to mitigate potential response bias on the follow-up bid in multiple-bound Contingent Valuation Method (CVM) questions while preserving much of the efficiency gains associated with the multiple-bound approach. An examination of survey data revealed that the OOHB estimates displayed greater consistency concerning the follow-up data compared to the Double Bound Dichotomous Choice estimates, demonstrating higher efficiency as well. Consequently, the OOHB approach presents itself as a valuable alternative to the DBDC approach in CVM surveys (Signorello, 2018).

However, Carson & Hanemann (2005) explain the meaning of WTP without an explanatory variable from CV formats such as an open-ended question, a bidding game, or a payment card. Among these formats, Double Bounded Dichotomous Choice can solve starting point bias (Huh et al., 2015) and reduce the variance of the mean WTP. In the Double Bounded Dichotomous Choice (DBDC) format, respondents are presented with an initial bid (Bid^1) and asked whether they would accept (yes) or reject (no) it. If they respond positively (yes), a higher bid (Bid^h) is then offered, which is twice the value of the initial bid. Conversely, if they respond negatively (no), a lower bid (Bid^l) is presented, which is half the value of the initial bid (Ko et al., 2020). The WTP from DBDC consists of four possible answers: a yes-yes answer shows that WTP will be greater than the upper bid (Bid^h) but less than infinity; a yes-no answer shows that WTP will be greater than the initial bid (Bid^1) but less than the upper bid (Bid^h); a no-yes answer shows that WTP will be greater than the lower bid (Bid^l) but less than the initial bid (Bid^1); and a no-no answer shows that WTP will be greater than zero but less than the lower bid (Bid^l) (Zainudin et al., 2016).

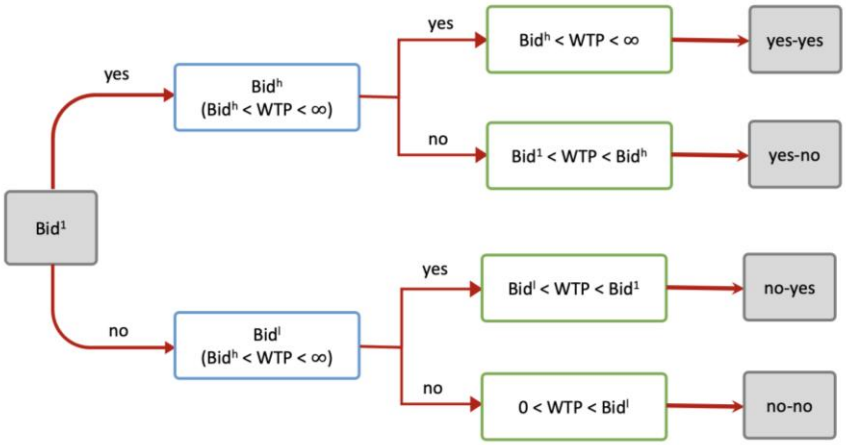


Figure 1. The probability of a Double Bounded Dichotomous Choice Answer, inspire from (Zainudin et al., 2016).

While both the DBDC and OOHDC approaches have their merits, the DBDC method tends to offer greater statistical efficiency, reduced starting point biases, improved validity, and alignment with economic theory Hanemann et al. (1991); Carson & Hanemann (2005). However, the choice between the two ultimately depends on the specific research context and objectives, as well as the trade-offs between efficiency and practical considerations such as respondent burden and survey costs. This research investigates the issue of initial point bias in relation to the characteristics of cyber insurance, specifically the unavailability of market prices and the potential for self-report bias arising from repeated questioning.

In the Spike model's DBDC format, a confirmation bid has been added in the third round for respondents who answer twice with no-no. The two

possible confirmation bids divide the respondents into two groups: the no-no-no group and the no-no-yes group. The value of WTP for the no-no-no group is absolute zero, while the WTP for the no-no-yes group is between zero and a lower bid (Bid^l) (Ko et al., 2020).

3.3.3 Basic components of a CV survey

A critical component of a contingent valuation strategy is the design of a survey questionnaire. It is essential to design a questionnaire that generates information to help respondents to understand the context of the hypnotical market. The questionnaire must provide sufficient information to assist respondents in making informed decisions but not so much that they are distracted by needless technical details (Zainudin et al., 2016).

The Contingent Valuation Method is adopted as an evaluation method, and the target population is determined, a questionnaire setting up a virtual market is created. The two steps of Contingent Valuation survey design are create a hypothetical market by providing responders with comprehensive information of the market, and bids design (Rahmatian, 2005). The basic components to be included in the Contingent Valuation survey questionnaire are Key expression, Hypothetical Market, the Contingent Valuation questions, Behavioral Question, and Items for Statistical Classification.

The Contingent Valuation Method is a way to find out what people want in terms of money by directly asking a random sample of people what they would pay for a clearly defined non-market goods. However, it is important to note that the Willingness to Pay (WTP) obtained through the Contingent Valuation questionnaire is derived from a hypothetical market setting. This virtual market consists of three key components: conditional products, methods of payment, and strategies to encourage individuals to be willing to pay. The design of the Contingent Valuation virtual market aims to create a sense of realism and plausibility for respondents, enhancing their engagement and ensuring meaningful responses. Questionnaires and bids for shows should be made so that people can state their preferences clearly and give answers that are consistent and easy to understand (Sajise et al., 2021).

This study utilizes the Contingent Valuation Method to establish a hypothetical market. Therefore, it simplifies the inclusion of certain cyber insurance features, such as maximum coverage and deductibility, as lead to the need of technical details (Zainudin et al., 2016). Unlike the Choice Experiment survey, which requires clear product features that influence the decision to pay (Jedidi & Zhang, 2002), this study focuses on a simplified approach. Additionally, the study assumes that cyber insurance is a relatively new concept in the Thai market and may not be widely known.

3.3.4 Estimate Optimal Bid value for Dichotomous Choice

The methodology for obtaining bids in this study draws upon a combination of methods, including focus group discussions, pretests, and consultation with expert workshops, as described in (Song et al., 2019). However, for this particular study, we have adopted a bid design that simulates market prices, similar to the approach used in the study on flood insurance by Paopid et al. (2020).

the Office of the Insurance Commission in Thailand [1] revealed that in 2019, nine non-life insurance companies were prepared to offer Cyber Insurance, aligning with the enactment of the Cybersecurity Law and Data Privacy law during the same year. In this study, Insure-AMPM shown the average cost of Cyber Insurance for one year of coverage ranged from THB 45,428 (USD 1,468) to THB 406,368 (USD 13,128). However, it is important to note that these figures are specific to the responses received from SMEs in Thailand.

The research findings indicate that the cost of cyber insurance coverage can vary significantly, ranging from THB 20,150 (USD 650) per year to THB 372,000 (USD 120,000) per year (Ozawa, 2021). Based on a global

[1] The Office of the Insurance Commission (OIC) Thailand is under the supervision of the Thai Minister of Finance, The Office of the Insurance Commission (OIC) is responsible for regulating the Thai insurance market.

survey of 43 insurance providers, it has been found that cyber insurance costs for low-risk firms can range from THB 20,150 (USD 650) to THB 73,067 (USD 2,357) per year. These prices were determined considering a liability limit of THB 31,000,000 (USD 1,000,000), a deductible of THB 310,000 (USD 10,000), and business revenue of THB 31,000,000 (USD 1,000,000). Additionally, in 2020, the average annual cost of cyber insurance in the United States was recorded at THB 45,198 (USD 1,485) (Chen, 2021).

Hence, this study provides a comprehensive table that presents the minimum and maximum average Cyber Insurance Premiums for both the global market and the Thai market.

Table 5**.** Global and Thai average cyber insurance premiums in USD

	Global Market	**Thai Market**
Minimum Average Cost	650	1,468
Maximum Average Cost	2,357	13,128

Source: Author

The optimal bid design for determining individual Willingness to Pay through the Contingent Valuation Method in the double-bound dichotomous choice format involves dividing the bids into two prices: the Initial bid and the Follow-up bid. Both of these bids can further be divided into a higher and a lower bid. To arrive at the appropriate bid, it

is recommended to set the initial bid equal to the median Willingness to Pay, and then present a follow-up bid on both sides of the median Willingness to Pay. This bid design helps to obtain more accurate and meaningful responses from respondents, facilitating a better estimation of their actual Willingness to Pay (Song et al., 2019).

Study of Song et al. (2019) the initial bid was divided into five groups, and each bid design double price for upper bid, and half price for lower bid. We revers at those numbers and found that this study used quartile to divide the values of the initial value. However, we eliminated the minimum, and maximum initial bid as it often bias when the bid amount is too high or too low (Boyle et al., 2019), then we use three initial bid for this study.

Cyber Insurance is an optional value goods usually do not have a specific price because they are new in the market, and need time to write policy that satisfies both buyer and seller before reveal the acceptable premium and coverage. Therefore, the good under evaluation in this study the price for them is not well formed. Therefore, we simulate the bid amounts correspondence with percentile regarding study of (Song et al., 2019), and we formed the first bid and a second bid for the Double Bound Dichotomous Choice as shown in Table 6.

Table 6**.** Estimation of the first bid and the follow up bid in USD.

The first bid	**The Follow-up Bid**	
(Bid1)	*Lower Bid (Bid^{l})*	*Upper Bid (Bid^{h})*
4,400	2,200	8,800
7,300	3,650	14,600
10,000	5,000	20,000

Source: Author
Note: US dollar equivalent as of March 2022 (USD 1 THB31) (Bank of Thailand; www.bot.or.th).

3.3.5 A Double Bound Dichotomous Choice

The Contingent Valuation Method is a widely adopted and extensively used survey technique aimed at assessing individuals' Willingness to Pay for specific goods or services (Huh et al., 2015). Existing research on Willingness to Pay for many forms of Insurance exists. It has been used to determine the cost of insurance premiums.

There are four possible outcomes from respondent $I = 1 \ldots N$ in a sample set, respondent answer yes follows by a no (yes-no), answer no follow by a yes (no-yes), both answers are yes (yes-yes), both answers are no (no-no).

The indicator giving to each respondent answer are $I_i^{yn}\ I_i^{ny}\ I_i^{yy}\ I_i^{nn}$
To set up the indicator function 1(.) for each indicator variable, the value one (1) is given if it is accurate and otherwise is zero (0) so:

$I_i^{yn} = 1$, if respondent I_i answer is yes followed by no

$I_i^{ny} = 1$, if respondent I_i answer is no followed by yes.

I_i^{yy} = 1, if respondent I_i answer both answers is yes.

I_i^{nn} = 1, if respondent I_i answer both answers is no.

Willingness to Pay calculate from a cumulative distribution function (cdf), the loglikelihood function show as below;

$$logL = \sum_{i=1}^{n}\{I_i^{yy} . logP^{yy}\ (Bid^1, Bid^h) + I_i^{yn}. log\ P^{yn}\ (Bid^1, Bid^h) + I_i^{ny}. log\ P^{yn}\ (Bid^1, Bid^l) + I_i^{nn}. log\ P^{nn}\ (Bid^1, Bid^l) \quad \text{Eq. (4.8)}$$

The probability of individual response is $P^{yy}, P^{yn}, P^{ny}, P^{nn}$ then the cumulative distribution performs as follow;

$$P^{yy}(Bid^1, Bid^h) = log[1 - G_c(Bid^h; \theta)]$$
$$P^{yn}(Bid^1, Bid^h) = log[G_c(Bid^h; \theta) - G_c(Bid^1; \theta)]$$
$$P^{ny}(Bid^1, Bid^l) = log[G_c(Bid^1; \theta) - G_c(Bid^l; \theta)]$$
$$P^{nn}(Bid^1, Bid^l) = log[G_c(Bid^l; \theta)] \quad \text{Eq. (4.9)}$$

Denote c is Willingness to Pay, cdf define as $G_c(\cdot; \theta)$, where θ is a vector of parameters, Bid^1 is bid amount. Therefore, a utility-maximizing from respondent i is $Bid^h(Bid^1 < Bid^h)$, where Bid^1 is

the first bid, so in this case the respondent i says yes for the first answer. When the individual i answer no for the initial bid (Bid^1) then offer the lower bid (Bid^l) for the second question $Bid^l(Bid^1 > Bid^l)$.

Yoo & Kwak (2002) derive the logistic cdf, $1 - G_c(\cdot)$ and combine with $\theta = (a, b)$ from previous study (W. M. Hanemann, 1989), and yields:

$G_c(Bid^1; \theta) = [1 + \exp(a - bBid^1)]^{-1}$ ..... Eq. (4.10)

Welfare derives from (4.7) shown as follow:

$\hat{C} = C^* = a/b$ ..... Eq. (4.11)

Where,

$\hat{C}$ is the mean of Willingness to Pay, it can be positive (+) or negative (-) value.

C^* is the median of Willingness to Pay.

So the mean of Willingness to Pay when it greater or equal to zero (≥ 0) formulate as follow:

$\hat{C}^+ = (1/b)\ log[1 + \exp(a)]$ ..... Eq. (4.13)

3.4 Spike Model in Double Bound Dichotomous Choice

In the Contingent Valuation Survey, specifically in the double-bound dichotomous choice format, it is not uncommon to encounter a

significant number of respondents with a zero willingness to pay (Yoo & Kwak, 2002), when it comes to assessing the willingness of people to pay for unfamiliar goods or services, such as cyber insurance, individuals may respond with zero willingness to pay. In such cases, this study uses the Spike model to address this issue, as it can adjust the zero Willingness to Pay responses statistically to better estimate the average Willingness to Pay value. The Spike model assumes that the zero Willingness to Pay responses do not necessarily reflect people's actual preferences but may instead be due to a lack of understanding or knowledge of the good or service being assessed. By adjusting the zero responses statistically, the Spike model can provide a more accurate estimate of the true economic value of the good or service.

The spike model will perform significantly over the conventional model (Yoo & Kwak, 2002). The individual who responses “no” for the initial and the follow up bid are divided in two group, the first group is the one who really unwilling to pay by saying “no” for the first bid, second bid, and confirmed by answer the third time by say “no-no-no”. The second group is the respondent who answer from confirmation answer willingness to Pay induce the set of answer “no-no-yes”, these two groups use to estimate spike model.

The respondent who answers no-no we asked the third round to confirm whether they have zero Willingness to Pay when answered again no for

the third follow-up question. The respondent i who say no-no is I_i^{nn} is classify into two groups,

I_i^{nnn} = 1, if respondent I_i response both answers is no-no-no

I_i^{nny} = 1, if respondent I_i response both answers is no-no-yes

The result show that the spike model performing mean and median Willingness to Pay. The likelihood estimation to get estimates for β and σ can then be used to estimate Willingness to Pay (Yoo & Kwak, 2002). The log-likelihood function for the spike model can be represented as follows:

$$
\begin{aligned}
logL = \sum_{i=1}^{n}\{ & I_i^{yy} \ln\left[1 - G_c\left(\mathrm{Bid}_i^h;\theta\right)\right] \\
& + I_i^{yn} \ln\left[G_c\left(Bid_i^h;\theta\right) - G_c\left(Bid_i^1;\theta\right)\right] \\
& + I_i^{ny} \ln\left[G_c\left(Bid_i;\theta\right) - G_c\left(Bid_i^l;\theta\right)\right] \\
& + I_i^{nny} \ln\left[G_c\left(Bid_i^l;\theta\right) - G_c(0;\theta)\right] \\
& + I_i^{nnn} \ln[G_c(0;\theta)]\}
\end{aligned}
\qquad \text{Eq. (4.14)}
$$

Where;

$$
G_c(Bid;\theta) = \begin{cases} [1+\exp(a - bBid)]^{-1} & \text{If } Bid > 0 \\ [1+\exp(a)]^{-1} & \text{If } Bid = 0 \\ 0 & \text{If } Bid < 0 \end{cases}
$$

Spike model expressed as $[1 + \exp(\alpha+\beta X_i)]^{-1}$ $[1 + \exp(a)]^{-1}$, and the mean Willingness to Pay of respondents can be calculated from equation on study of (Huh et al., 2015), ln[1 + exp(α+ βX_{mean})]/b.

Therefore,

$$\hat{C} = (1/b)\ \ln[1 + \exp(a)] \quad \text{Eq. (4.15)}$$

And

$$C^* = \begin{cases} a/b, & \text{If } [1 + \exp(a)]^{-1} < 0.5 \\ 0 & \text{Otherwise} \end{cases} \quad \text{Eq. (4.16)}$$

The log-likelihood for estimating Spike can be determined using the formula shown below;

$$logL = \sum\big[Ans_{yy} logP_{(yes-yes)} + Ans_{yn} logP_{(yes-no)} + Ans_{ny} logP_{(no-yes)} + Ans_{nnn} logP_{(no-no-no)} + Ans_{nny} logP_{(no-no-yes)}\big] \quad \text{Eq. (4.17)}$$

Spike model expressed as $[1 + \exp(\alpha+\beta X_i)]^{-1}$ and the mean Willingness to Pay of respondents can be calculated from equation on study of (Huh et al., 2015), ln[1 + exp(α+ βX_{mean})]/b.

In this case, the spike model says that they are invalid responders, so they are taken out of the sample and the estimate is made without them. To figure out what percentage of survey participants refused to pay, and subtract the number of resisters from the number of those who refused to pay.

Chapter 4. Experimental design and empirical study

In this chapter, we will discuss the sample design, data collection, and evaluation methods used in this study to assess the monetary value of Willingness to Pay and determine the factors affecting the purchase choices of Cyber Insurance. The Contingent Valuation Method with a Double Bound Dichotomous Choice format will be employed to gather this data. Additionally, this study will utilize the Spike model to handle instances of zero willingness to pay. Subsequently, group and sensitivity testing will be conducted to analyze the relationship between willingness to pay and the key factors influencing the decision to pay.

4.1 Survey Design and Data Collection

To obtain information about the monetary value of cyber insurance in Thailand, the National Cybersecurity Agency of Thailand (NCSA) assist a survey questionnaire to a sample of two hundred organizations across six industries, the sectors covered by this study include public service, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, and public health. The NCSA provide the participant's name list, and requested CEOs to assign the relevant person to fill out the form, and the survey was

conducted between April and the end of June 2022. The survey was completed by one hundred participants using Google Forms.

Table 7. Sample Design.

Subject	Definition
Populations	An organization that employs information technology for its business operations.
Sample Size	200 respondents
Method uses to select the sample	The Cybersecurity Act identifies Critical Information Infrastructure organizations in the following six sectors: substantive public service, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, and public health.
Survey Period	April to June 2022
Survey Method	The Contingent Valuation Method questionnaire was created using the Google Survey platform and officially distributed online by the National Cybersecurity Agency of Thailand.

The dataset includes various socioeconomic and demographic characteristics, such as gender, age, education, job position, industry type, revenue, number of customers and employees, and investment in cybersecurity. Furthermore, the final section of the questionnaire includes variables from previous studies, such as knowledge of cyber insurance, awareness of cyberattacks, experience with purchasing cyber insurance, attitude toward buying cyber insurance, and understanding of legal liability under the Personal Data Privacy Act and the Cybersecurity Act.

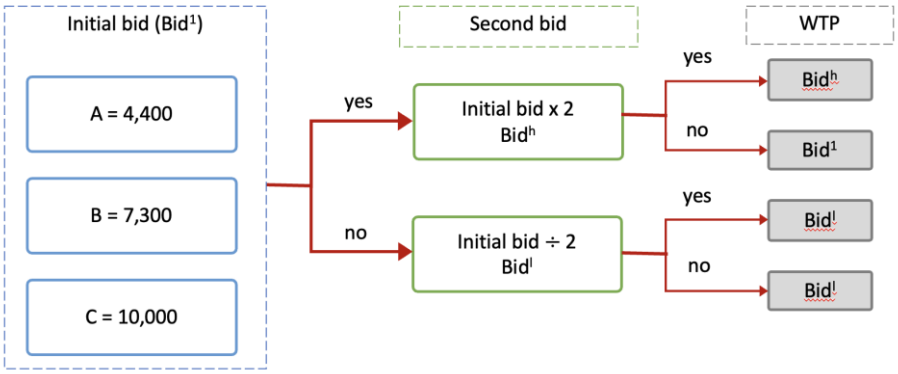
Table 8. List of Variable.

Variable	Label	Definition
sex	Sex	Sex is in two categories;
age	Age	Age (year) in four categories;
pos	Position	Position is in five categories;
edu	Education	Education level is in three categories;
sec	Sector	Industrial sector in seven categories;
rev	Revenue	Revenue in USD in seven categories
emp_no	Employee	Employee number in seven categories
cus_no	Customer	Customer number in five categories
inv	Investment	Cybersecurity Investment in a year in four categories;
cyb	Cyberact	Understanding the Cybersecurity Act in five ordinal scale
pdp	Pdpact	Understanding the Personal Data Privacy Act in five ordinal scale
und	Understci	Cyber Insurance Knowledge in five ordinal scale
awar	Awareness	Risk awareness in five ordinary scale;
exp	ExperienceCI	Cyber Insurance purchasing experienced in two nominal scale;
attr	Attrack	Hack experienced in two nominal scale;

In chapter three of this study, the method of creating bid values was explained, which is derived from Song et al. (2019). Therefore, this study uses three initial bid values derived from three different questionnaire sets: THB 140,000 (USD 4,400), THB 230,000 (USD 7,300), and THB 310,000 (USD 10,000). The second bid amount follows a specific pattern: if the first bid value is THB 140,000 (USD 4,400) and the respondent answers 'yes,' the second bid value increases to THB 280,000 (USD 8,800); if the respondent answers 'no,' the second bid value decreases to THB 70,000 (USD 2,200). Similarly, if the first bid value is THB 230,000 (USD 7,300) and the respondent answers 'yes,' the second bid value increases to THB 460,000 (USD 14,600); if the respondent

answers 'no,' the second bid value decreases to THB 115,000 (USD 3,650). Finally, if the first bid value is THB 310,000 (USD 10,000) and the respondent answers 'yes,' the second bid value increases to THB 620,000 (USD 20,000); if the respondent answers 'no,' the second bid value decreases to THB 155,000 (USD 5,000).

Figure 2. Visualize the pattern of bid design for the Contingent Valuation Method



4.2 Descriptive summary statistics.

The dataset's fundamental characteristics were analyzed using descriptive statistics, such as mean and standard deviation. These statistics help to determine the central tendencies of important variables, the spread of the data around the central measure, and the number of observations for each variable. Furthermore, in addition to identifying outliers and missing values, data dispersion for a variable can affect

inference or hypothesis testing related to that variable (Sajise et al., 2021).

The Contingent Valuation survey provides attributes for estimating individual or aggregate willingness to pay, including bid analysis with upper and lower bounds, mean, median, and average values. This study presents a high-level overview of respondent profiles by summarizing their demographic and socioeconomic characteristics. We estimate the demographic and socioeconomic attributes to understand how they affect individual willingness to pay. A summary of respondent demographic characteristics and socioeconomic attributes can be found in Table 9.

4.2.1 Statistical Explanations

Out of all the participants, 74 percent were male, and 82 percent were aged between 36 and 55-year-old. The majority of respondents (65%) held an undergraduate degree, while the remaining participants had a graduate degree. The participants in this study were all employed in IT-related fields, representing a diverse range of sectors, including public service, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, and public health. About 62% of the respondents were Chief or operational Information Technology officers, while 38% were Chief or operational officers in Cybersecurity.

This survey targets organizational-level data, and therefore, the company's profile is collected, including revenue, number of employees, and number of customers. Out of all the respondents, 50 percent are from large enterprises, while only 22 percent represent small enterprises. Among the respondents from large companies, 46 percent have over a thousand employees, and 11 percent have over two thousand employees. The number of customers also indicates the size of the business, with 60 percent of companies reporting a number of customer from 10,001 to 20,000.

Table 9. Demographic attributes of the sample.

Category	Characteristic	Respondent	Percentage (%)
Total		**100**	**100**
Gender	Female (0)	26	26.00
	Male (1)	74	74.00
Age	25 – 35 years (1)	10	10.00
	36 – 45 years (2)	38	38.00
	46 – 55 years (3)	44	44.00
	Above 55 years (4)	8	8.00
Education	Under graduate (1)	64	64.00
Level	Graduate (2)	36	36.00
Position	Chief Information Officer (1)	29	29.00
	Chief Cyber Security Officer (2)	13	13.00
	Operation Information Officer (3)	33	33.00
	Operation Cyber Security Officer	25	25.00
	(4)	46	46.00
Sector	Substantive public service (1)	10	10.00
	Banking and Finance (2)		
	Information technology and	4	4.00
	telecommunications (3)	13	13.00
	Transportation and logistics (4)	4	4.00
	Energy and public utilities (5)	23	23.00
	Public health (6)	6	6.00
Revenue	Less than 400,000 (1)	11	11.00
	400,000 to 1,900,000 (2)	11	11.00
	1,900,001 to 3,800,000 (3)	5	5.00
	3,800,001 to 6,600,000 (4)	6	6.00
	6,600,001 to 9,400,000 (5)	6	6.00

Category	Characteristic	Respondent	Percentage (%)
	9,400,001 to 18,800,000 (6)	45	45.00
	Over 18,800,001	7	7.00
Number of	Less than 100 (1)	18	18.00
Employee	101 to 500 (2)	11	11.00
	501 to 1,000 (3)	18	18.00
	1,001 to 2,000 (4)	46	46.00
	Over 2,001 (5)	11	11.00
Number of	Less than 1,000 (1)	21	21.00
Customer	1,001 to 5,000 (2)	4	4.00
	5,001 to 10,000 (3)	2	2.00
	10,001 to 20,000 (4)	62	62.00

4.2.2 Bid Distribution

The bid distribution is used to assess the validity of the survey design. It helps visualize the pattern of responses and identify any bias stemming from DBDC survey (Sajise et al., 2021). The distribution of bids in a double-bounded dichotomous contingent valuation (DBDCV) study is crucial for analyzing the respondents' willingness to pay. It visualizes their responses to the series of bid amounts presented in the survey, helping researchers determine the patterns of Willingness to Pay for the goods under consideration.

The bid distribution displays the percentage of 'yes' votes for each bid amount presented in the survey. It is a crucial tool for analyzing the collected data as it can reveal patterns and trends that are not immediately apparent from the raw data. Researchers can use the bid distribution to identify outliers, estimate the distribution of Willingness to Pay values, The data collected from the respondents were analyzed to calculate

summary statistics, such as the mean, median, and standard deviation of Willingness to Pay

The bid distribution can also help assess the validity of the survey design. If the bid distribution indicates a low percentage of 'yes' votes for the lower bid amount and a high percentage of 'yes' votes for the upper bid amount, this may indicate starting point bias or strategic behavior by the respondents. On the other hand, if the bid distribution shows a high percentage of 'yes' votes for the lower bid amount and a low percentage of 'yes' votes for the upper bid amount, it may indicate that the initial bid was too high. Furthermore, some respondents expressed a lack of Willingness to Pay for the specific good or service under consideration, indicating that the stated amount was not within their preferred range for expenditure.

In summary, the bid distribution plays a critical role in analyzing the data obtained through the DBDCV method. It serves as a valuable tool in understanding respondents' willingness to pay for the good or service under study and assists researchers in identifying possible biases in the survey design (Sajise et al., 2021).

The first question in a Contingent Valuation survey determines the number of respondents who agree to a certain bid. Based on the positive responses to the initial bid, the number of respondents who agreed to it can be calculated. The remaining respondents who rejected the initial bid

are excluded from the analysis. The analysis results can be effectively presented in a table format, illustrating the proportion of respondents' responses to the questionnaire. A table 10 is provided below to demonstrate this presentation:

Table 10. The ratio of respondents who answered the Contingent Valuation Method questionnaire.

	First Answer (Answer1)		**Second Answer (Answer2)**	
	Frequency	**Percent (%)**	**Frequency**	**Percentage (%)**
Yes	51	51.00	61	61.00
No	49	49.00	39	39.00
Total	100	100.00	100	100.00

Among the respondents, 51 percent answered 'yes' to the first bid in the Contingent Valuation questionnaire. As the bid amount doubled in the second question, the expected number of 'yes' responses decreased to 39 percent. Conversely, for those who rejected the first bid, the expected 'yes' response rate increased to 61 percent when the bid amount was lower than half of the original price. These findings suggest that the response rate to bid amounts can vary based on the initial bid, highlighting the importance of bid distribution analysis in Contingent Valuation studies.

The findings from the Contingent Valuation questionnaire reveal interesting patterns among the 100 respondents. The responses to the first and second bid are summarized as follows: 24 percent of respondents answered 'yes' to the first bid and 'no' to the second bid. 11 percent of

respondents answered 'no' to the first bid and 'yes' to the second bid. 28 percent of respondents answered 'yes' to both bids. 37 percent of respondents answered 'no' to both bids. These percentages provide valuable insights into the participants' decision-making process when evaluating the two bid options, contributing to a comprehensive understanding of their willingness to pay for the specific good or service.

Table 11. The ratio of four possible answers from the Contingent Valuation questionnaire.

Initial bid Value (THB 1,000)	**Answer**				**Total**	**Percentage (%)**
	yn	**ny**	**yy**	**nn**		
140	4	5	9	9	27	27.00
230	13	0	10	16	39	39.00
310	7	6	9	12	34	34.00
Total	24	11	28	37	100	

The bid distribution is used to assess the validity of the survey design. It helps visualize the pattern of responses and identify any bias stemming from DBDC survey (Sajise et al., 2021). Therefore, the bid distribution Therefore, the bid distribution was analyzed to understand how respondents chose to pay in the initial bids of 140, 230, and 310. The results revealed that 13, 23, and 16 respondents accepted the bid offers, respectively. Next, the number of second bids was determined based on whether the respondents accepted or rejected the first bid. In the double-bound dichotomous choice format, the bidding process was designed to elicit respondents' willingness to pay more accurately. When a respondent accepted the initial bid, the subsequent bid amount was

increased to a higher value, providing a two-step approach to gauge their upper limit of willingness to pay. On the other hand, if the respondent rejected the initial bid, the subsequent bid was decreased by half, allowing for a second opportunity to reveal their lower limit of willingness to pay. This dynamic bidding process aimed to obtain a more precise estimation of the respondents' true willingness to pay for the particular good or service under evaluation. As a result, the table displays the number of respondents who accepted the first bid: 11 respondents accepted a bid of 70, none of the respondents accepted a bid of 115, 13 respondents accepted a bid of 140, 6 respondents accepted a bid of 155, 9 respondents accepted a bid of 280, 10 respondents accepted a bid of 460, and 9 respondents accepted a bid of 620.

Table 11. The distribution of the WTP as stated by respondents.

Bid Value (THB 1,000)	**Distribution**
70	5
115	0
140	13
155	6
230	23
280	9
310	16
460	10
620	9

The adoption of new products and services is often influenced by the price, and cyber insurance is no exception to this trend. Studies conducted by Bodin et al. (2018); Gai et al. (2017); Vakilinia & Sengupta (2019), have investigated the relationship between the price of insurance

and the Willingness to Pay and have identified significant influences. Table 11 presents the findings of these studies, showcasing how the price of insurance affects individuals' WTP, which demonstrates that when the price increases, respondents' Willingness to Pay decreases following the demand law. Specifically, the Willingness to Pay decreases up to 53.85 percent. On the other hand, when the price decreases, the Willingness to Pay for the second offer price increases significantly by 77.08 percent.

Table 12 The percent change when bid amount increase and decrease.

First Answer	Second Answer	Percent (%) Change
Yes (51)	Yes (28)	46.15
	No (24)	53.85
	Yes (11)	77.08
No (49)	No (37)	22.92

4.3 Empirical study

This section presents the analysis of data obtained from 100 respondents who completed a Contingent Valuation survey. The survey used the Double-Bound Dichotomous Choice method, where bid amounts were subjected to logit-probit estimation to determine the probability of acceptance for a given offer.

4.3.1 The Contingent Valuation Method estimation result

In this section use the Contingent Valuation Method to analyze Willingness to Pay without covariates. The log-likelihood function is

utilized to estimate the coefficients for Beta (β) and Sigma (σ), The log-likelihood function, depicted in equation (Eq. 5.1), is a crucial component in estimating the Willingness to Pay. By using this function, can derive valuable insights into respondents' preferences and choices related to the survey questions, leading to accurate estimations of their Willingness to Pay.

$$logL = \sum\left[Ans_{yy} logP_{(yes-yes)} + Ans_{yn} logP_{(yes-no)} + Ans_{ny} logP_{(no-yes)} + Ans_{nn} logP_{(no-no)}\right] \quad \text{Eq. (5.1)}$$

Where $Ans_{yy} = 1$ if the first bid is bid1, bid1 < bid2, and the respondent answer Yes to both questions. $Ans_{yn} = 1$ if the first bid is bid1, bid1 < bid2, In cases where the respondent answers "Yes" to the first question and "No" to the second question, $Ans_{ny} = 1$ if the first bid is bid1, bid1 > bid2, and the respondent say No to the first question and say Yes to the second question, and otherwise is 0; and $Ans_{nn} = 1$ if the first bid is bid1, bid1 > bid2, and the respondent answer No to both questions. Otherwise, it is 0.

In analyzing Contingent Valuation data with Double Bound Dichotomous Choices, the "dcchoice" and "dcspike" packages in R provide valuable tools. These packages offer the capability to examine covariates and assess the impact of various factors, and the outcomes providing insights into decision-making and economic preferences.

The result of Contingent Valuation Method without covariates shows that the utilized 100 observations. The log-likelihood, measuring the model's fit to the data, yields a value of -114.3256. The standard error, at 189.5986, indicates the precision of the estimated coefficients. A Z-value of -7.997, with a negative sign denoting a negative coefficient, tests the significance of the coefficient. The median Willingness to Pay is a robust measure that helps to provide a central tendency of the respondents' valuation result is 152.143. Similarly, the 95% confidence interval for the median Willingness to Pay spans from 89.177 to 204.770, providing a likely range for the true population median.

Table 13: The Contingent Valuation Method estimation result of Willingness to Pay.

Variables	Conventional model
Number of observations	100
Bid	-0.00745
Log-likelihood	-114.3256
Median WTP	152.143
Standard error	0.00093
Z-value	-7.997***
95% conf. interval	89.177 - 204.770

Note: Significant codes: 0 '***' 0.001 '**' 0.01 '*' 0.05
In this study, a currency unit of THB 1000 was utilized, with an exchange rate of USD1 to THB31 as of February 2022.

The mean is affected by extreme values or outliers in the data because it takes into account the value of every observation. If there are extreme values, they can greatly influence the mean and potentially skew the overall picture of the data.

On the other hand, the median is less sensitive to extreme values because it only considers the middle value of the data when arranged in order. The median represents the dividing point that separates the upper half from the lower half of the dataset. Therefore, even if there are outliers, they have less impact on the median.

Therefore, since the median and mean are not close in value, the distribution of Willingness to Pay values might not be symmetric or may be influenced by outliers. In such cases, the median more reliable measure of central tendency as it is less affected by extreme values.

In conclusion, the Willingness to Pay is presented using a unit of 1000 Thai baht (THB) and converted into USD for convenience. The estimation of Contingent Valuation Method provides that the median Willingness to Pay is estimated at THB 152,143 (USD 4,910).

4.3.2 The estimation result of Willingness to Pay model with covariates

Drawing on the findings of prior research and pertinent studies, we computed the mean Willingness to Pay and investigated the impact of various independent factors present in the dataset. Socio-demographic variables, including gender, age, education, number of employees, number of customers, and income, were among the factors analyzed (Franke (2017); Pooser et al. (2018); Ozawa (2021); Tal Pavel (2020)),

as well as behavioral factors such as cyber-awareness, Cyber Insurance Knowledge, cyber-attack experience, and attitude toward Cyber Insurance, significantly predicted Cyber Insurance adoption (De Smidt & Botzen (2018); Tal Pavel (2020)).

In the second factor analysis, eight variables were added, leading to the following conclusions. Statistics were gathered from one hundred respondents, including percentages, means, medians, and standard deviations. Table 14 provides the means and standard deviations for the following variables: the degree of understanding in cyber insurance, awareness of the benefits of cyber insurance, awareness of risks, experience with purchasing cyber insurance, and understanding of the Cyber Security Act and Personal Data Privacy Act.

Table 14: The basic information regarding the covariates used.

Variable	Mean	Std. dev.
Understanding in Cyber Insurance	3.65	0.96791
Awareness of the benefits of Cyber Insurance	2.19	1.17804
Awareness of the risk	1.94	0.66393
Experience with purchasing Cyber Insurance	0.07	2.05643
Experience with cyber-attacks	1.94	0.66393
Understanding of the Cyber Security Act	4.00	0.77849
Understanding of the Personal Data Privacy Act	3.97	0.74474

Several groups' variations in Willingness to Pay were compared with demographic and socioeconomic characteristics using Z-value testing. The multiple regression analyses use to estimate the association of sociodemographic and parameter with the intention of respondents who decide to say “yes” or “no” for Contingent Valuation survey

questionnaire. We repeating Linear Regression analysis model for this study, Contingent Valuation approach is used then the final models, In this study, non-significant variables related to the choice of purchasing cyber insurance were excluded from the analysis. The following basic econometric model were determined as (Eq. 5.2).

$$WTP_i = \beta_0 + \beta_1 \mathrm{X}_{cio} + \beta_2 \mathrm{X}_{cso} + \beta_3 \mathrm{X}_{oso} + \beta_4 \mathrm{X}_{\mathrm{understci}} + \beta_5 X_{aware} + \beta_6 X_{awrisk} + \beta_7 X_{expci} + \beta_9 X_{cyberact} + \beta_{10} X_{pdpact} + \varepsilon_i \quad \text{Eq. (5.2)}$$

Eight explanatory variables were used to calculate Willingness to Pay, which included three dummy variables representing the positions of a Chief of Information Officer (CIO), a Chief of Security Officer (CSO), and an Operational Security Officer (OSO). Additionally, variables for understanding Cyber Insurance (understci), awareness of the benefits of cyber insurance (aware), awareness of the risks (awrisk), experience with purchasing cyber insurance (expci), understanding of the Cyber Security Act (cyberact), and understanding of the Personal Data Privacy Act (pdpact) were considered.

The Result of the linear regression show that showing the coefficients, standard errors, and Z-values for several predictor variables show in Table 15. The coefficients in the analysis represent the estimated impact of each predictor variable on the outcome variable, while the standard errors indicate the variability of these estimates. The Z-values indicate the statistical significance of each predictor variable, with lower Z-values

indicating stronger evidence of an association between the predictor and outcome variables. Based on the results, there are two variables that are statistically significant in predicting willingness to pay for cyber insurance. These variables include: Chief of Security Officer has a coefficient of 2.10374 and the Z-value of 2.8235 indicates statistical significance at the 0.05 level. This implies that individuals in the position of Chief of Security Officer are more likely to have a higher willingness to pay for cyber insurance compared to those who do not hold this position. Second, understanding of cyber insurance: this variable has a coefficient of 1.18760 and a Z-value of 0.001, indicating that it is significant at the 0.01 level. This indicates that individuals with a better understanding of cyber insurance are more likely to exhibit a higher willingness to pay for it.

Table 15. The result of linear regression analysis.

Covariance	Coefficient	Std. err.	Z-value
Age	0.16632	0.27409	0.6068
Education	0.36819	0.40960	-0.8989
Sector	0.06575	0.09492	0.6927
Chief of Information Officer	0.01856	0.51936	0.0357
Chief of Security Officer	2.10374	0.74507	2.8235*
Operational Security Officer	0.29422	0.54908	0.5359
Understanding in CI	1.18760	0.40738	2.9151**
Awareness	0.02645	0.19519	0.1355
Experience purchasing CI	9.96995	32.2958	0.2839
Experience cyber attack	0.77153	0.47230	1.6335
Understanding of the Cyber Security Act	0.21485	0.62466	0.3439
Understanding of the PDPA Act	-0.30145	0.62916	-0.4791

Significant level: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05

4.3.3 Willingness to Pay: Spike performance

The Spike model is employed to address absolute negative responses in the Contingent Valuation Survey (Kristrom, 1997; Huh et al., 2015). The results reveal that the spike model significantly outperforms the traditional model (Yoo & Kwak, 2002). When respondents answer "no" to both the first and second bids and consistently confirm their decision, the optional product often results in a high likelihood of obtaining Zero Willingness to Pay, leading to uncertainty in the estimation of mean and median Willingness to Pay.

Out of the 100 respondents who participated in the Contingent Valuation Survey, 37 of them responded "no" to both the first and second bids. These 37 respondents were then asked to confirm their decision in a third round. From this confirmation, it was found that 35 respondents had an absolute zero willingness to pay, meaning they were not willing to pay any amount for the product or service. Only 2 respondents changed their response to "yes" in the third round.

Respondents who answer "no" to both the first and second bids are divided into two groups. The first group consists of those who are genuinely unwilling to pay, as they consistently respond with "no" for all three rounds, confirming their decision not to pay. The second group is the respondent who answer from confirmation answer willingness to Pay

induce the set of answer “no-no-yes”, these two groups use to estimate spike model.

The result show that the spike model performing mean and the median of Willingness to pay. The estimates for α and β are obtained using maximum likelihood estimation, which can then be used to estimate Willingness to Pay (Yoo & Kwak, 2002). The log-likelihood function for the spike model is given by:

$$logL = \sum\left[Ans_{yy}logP_{(yes-yes)} + Ans_{yn}logP_{(yes-no)} + Ans_{ny}logP_{(no-yes)} + Ans_{nnn}logP_{(no-no-no)} + Ans_{nny}logP_{(no-no-yes)}\right] \quad \text{Eq. (5.3)}$$

Spike model expressed as $[1 + \exp(+)]^{-1}$ and the mean Willingness to Pay of respondents can be calculated from equation on study of (Huh et al., 2015), ln[1 + exp(+)]/b.

Table 16**.** The estimation result of Spike Model and conventional Model.

Variables	Conventional model	Spike Model
Number of observations	100	100
Bid	-0.00745	-0.00329
Log-likelihood	-114.3256	-145.1004
Median WTP	152.143	207.455
Standard error	0.00093	0.00043
Z-value	-7.997***	-7.575***
95% conf. interval	89.177 - 204.770	87.837 – 323.600

Note: Significant codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05

In this study, a currency unit of THB 1000 was utilized, with an exchange rate of USD1 to THB31 as of February 2022.

The Spike model was employed to analyze Willingness to Pay to deal with zero Willingness to Pay. The analysis was conducted using 100 observations or responses from participants. The model's log-likelihood was -145.1004, and the standard error of the estimated coefficients was 0.00043. The Z-value of -7.575 indicates a significant negative coefficient. The median Willingness to Pay was estimated at 207.455, with a 95% confidence interval spanning from 87.837 to 323.600. The Spike Method estimation indicates that the median Willingness to Pay is estimated to be THB 207.455 (USD 7,280).

4.3.4 Willingness to Pay: Group data analysis

Along with the data analysis conducted for the entire sample, it is important to carry out qualitative analysis for specific subgroups within the sample. The subgroups should be disaggregated based on the stratified or cluster sampling method used in the survey strategy. Performing subgroup analysis allows for identification of differences in preferences and willingness to pay between the subgroups (Sajise et al., 2021).

Table 17. Conventional Model vs Spike model with respect to significant variables.

Variables	Conventional model	Spike model
Number of observations	100	100
Log-likelihood	-111.137	-141.2838
Understand CI		
Median WTP	151.504	204.312
Standard error	0.3995	0.3803
Z-value	2.496*	-2.763**
95% conf. interval	88.755 – 205.950	94.848 – 298.570
Number of observations	100	100
Log-likelihood	-128.4783	-164.1343
CSO		
Median WTP	256.870	287.300
Standard error	0.6773	0.7364
Z-value	2.904**	3.346***
95% conf. interval	170.100 – 353.890	236.240 – 342.380

Note: Significant codes: 0 '***' 0.001 '**' 0.01 '*'
In this study, a currency unit of THB 1000 was utilized, with an exchange rate of USD1 to THB31 as of February 2022.

The Contingent Valuation model and the Spike model were both based on 100 observations or responses from participants. The Conventional model from respondent who understand cyber insurance had a log-likelihood of -111.137, a standard error of 0.3995, and a Z-value of 2.496, indicating statistical significance at the 0.01 level. The estimated median Willingness to Pay was 151.504, with a 95% confidence interval spanning from 88.755 to 205.950, providing likely ranges for the true population value of mean and median of the Willingness to Pay.

The Conventional model from respondent who is Chief of Security Officer (CSO) had a log-likelihood of -128.478, a standard error of 0.6773, and a Z-value of 2.904, indicating statistical significance at the

0.01 level. The estimated median Willingness to Pay was 256.870, with a 95% confidence interval spanning from 170.100 to 353.890, providing likely ranges for the true population mean and median Willingness to Pay values.

The Spike model with respondent who has high understand of cyber insurance exhibited a log-likelihood of -141.2838, indicating its goodness-of-fit to the observed data. The standard error in the Spike model was 0.3803, representing the precision of the estimated coefficients. The Z-value of -2.763 indicated the statistical significance of the coefficient at the 0.01 level. The calculated median Willingness to Pay in the Spike model was found to be 204.312, which signifies the central value within the Willingness to Pay distribution. The 95% confidence interval for the median Willing to Pay spanned from 94.848 to 298.570, offering a likely range for the true population median.

The Spike model from respondent who is Chief of Security Officer (CSO) had a log-likelihood of –164.1343, a standard error of 0.7364, and a Z-value of 3.346, indicating statistical significance at the 0.001 level. The estimated mean Willingness to Pay in the Conventional model of CSO was 303.670, with a 95% confidence interval ranging from 258.630 to 356.070. The estimated median Willingness to Pay was 287.300, with a 95% confidence interval spanning from 236.240 to 342.380, providing likely ranges for the true population mean and median Willingness to Pay values.

In conclusion, this study will use the median of Willingness to Pay because statistically, the mean is affected by extreme values or outliers in the data, which can greatly influence its value. On the other hand, the median is less sensitive to extreme values as it only considers the middle value of the data when arranged in order. The median is a statistical measure that represents the value separating the higher half from the lower half of the Willingness to Pay distribution. It is less affected by outliers, making it a more robust measure for capturing the central tendency of the data, even when extreme values are present.

Upon analyzing the results, the conventional model estimated the median Willingness to Pay without covariate as THB 152,143 (USD 4,910) for respondents in general, THB 256,870 (USD 8,293) for the respondent group of Chief of Security Officer (CSO), and THB 151,504 (USD 4,885) for respondents who understand cyber insurance. On the other hand, the Spike model estimated the median Willingness to Pay without covariate as THB 207,455 (USD 6,694) for respondents in general, THB 204,312 (USD 6,592) for respondents who understand cyber insurance, and THB 287,300 (USD 9,276) for the respondent group of Chief of Security Officer (CSO).

Chapter 5. Discussion, Policy implication, and Conclusion.

This chapter consists of four sections. Firstly, it discusses the result of previous studies and addresses the result from this study. Secondly, it interprets the estimation results of the Contingent Valuation Study and explores the key factors influencing individuals' Willingness to Pay for cyber insurance in Thailand. The third section emphasizes the academic contribution of the study, highlighting its insights and findings. Lastly, this chapter acknowledges the study's limitations and provides recommendations for future research.

5.1 Discussion.

The aim of this study is to explore the Willingness to Pay for cyber insurance in Thailand and analyze the factors influencing individuals' decision-making. The findings of this research will provide answers to two research questions: firstly, the determination of the monetary value individuals are willing to allocate for cyber insurance, and secondly, the identification of the factors that shape their willingness to pay for such coverage.

In this study, we utilize the Contingent Valuation Method and the Spike model to evaluate the value of cyber insurance in a hypothetical market setting. Furthermore, we identify the factors influencing the decision to

purchase cyber insurance coverage. The findings reveal that the Spike model outperforms traditional models, and we use the median Willingness to Pay as a more reliable measure to address the first research question concerning the value of Willingness to Pay. (Hanemann, 1989). Unlike the mean, which can be heavily influenced by extreme values or outliers in the data, so median is an appropriate measure of Net Willingness to pay. The median is less sensitive to such values, and it excluded covariate effects on the conservative side (Nam, 2018) . The median is obtained by arranging the data in order and selecting the middle value, effectively separating the higher half from the lower half and minimizing the influence of outliers. Consequently, the median provides a more robust measure for capturing the central tendency of the Willingness to Pay distribution, even in the presence of outliers.

Furthermore, exploring non-life insurance adds further insights to understanding the Willingness to Pay for cyber insurance and helps overcome some of the limitations in the study. Firstly, these types of insurance share commonalities with cyber insurance in terms of the risk involved. By exploring these related domains, we can gain valuable insights into risk perception, risk management strategies, and consumer behavior that can be applied to the study of cyber insurance. Secondly, non-life insurance sectors, such as auto (Dragos & Dragos, 2017) and natural disaster insurance (Tian & Yao (2015); Paopid et al. (2020), payment extension for cyber insurance (Nam, 2018) have well-

established frameworks and research findings that can serve as a basis for understanding the factors influencing the decision to purchasing insurance. By leveraging this existing knowledge, we can build upon established theories, methodologies, and empirical evidence, providing a more solid foundation for our research on cyber insurance.

Furthermore, studying non-life insurance can offer comparative analysis between different insurance domains. By examining similarities and differences in factors affecting Willingness to Pay. Ultimately, conducting an examination of non-life insurance, particularly auto, floods, and earthquake insurance, allows for a comprehensive exploration of factors influencing insurance decisions, expands the knowledge base, and provides a broader context for understanding the Willingness to Pay for cyber insurance.

However, this study does not discuss the monetary value from previous literature due to differences in insurance types, hypothetical markets, and bit value. Instead, this study provides the monetary value based on a hypothetical market specific to cyber insurance. The findings reveal that among Critical Information Infrastructure Organizations, Spike model provides the median Willingness to Pay for cyber insurance is THB 207,455 (USD 6,694) per year.

In addition, the results relevant to the current study from previous literature have been discussed, including auto and house insurance

(Hansen et al., 2016), earthquake insurance (Tian & Yao, 2015), flood insurance (Paopid et al., 2020), payment extension for cyber insurance (Nam, 2018). The following discussion provides insights into these studies:

Demographic attributes were tested in this study, and the findings aligned with previous research. Nam (2018) found that high incomes and high education were significant covariates. In a previous study conducted by Hansen et al. (2016), age, income, and education level were identified as crucial factors affecting individuals' Willingness to Pay for house and auto insurance. Similarly, Tian & Yao (2015) found that households with higher income showed a greater inclination to purchase earthquake insurance. However, when it comes to cyber insurance, there are notable differences. The demographic factors such as age, education, and industrial sector were found to be insignificant in this context.

The study conducted by Paopid et al. (2020) focused on determining the determinents influencing the Willingness to Pay for floods insurance in, Thailand. Floods insurance serves as a risk management tool to mitigate significant losses caused by floods. The key findings indicated that the flood insurance premium and factors such as house type and prior flood experience influencing on the Willingness to Pay. This study made a comparison between house type as an industrial sector and prior flood experience as prior cyber-attack experience. However, in the domain of

cyber insurance, the industrial sector and prior cyber-attack experience were found to be insignificant in relation to the decision to pay for cyber insurance.

The study conducted by Nam (2018) aimed to determine the Willingness to Pay of cyber insurance for extra payment for blockchain and smart contracts in Korea. The findings revealed that as the additional insurance premium increased, the probability of respondents being willing to pay decreased. The factors influencing consumer decisions to purchase extras in cyber insurance included prior experience in purchasing insurance contracts. However, within the realm of cyber insurance, previous experience in purchasing insurance contracts was found to be insignificant in influencing the adoption rate of cyber insurance.

The study conducted by Hansen et al. (2016) focused on examining the Willingness to Pay for a various type of insurance in Denmark, specifically for car, house, and home insurance. The key findings indicated that awareness of risk is significant factor. The implications of the study highlighted that insurance providers could leverage these findings to design more effective marketing strategies targeting individuals based on significant demographic attributes. Policymakers could also utilize the results to develop policies that incentivize individuals to purchase insurance, such as offering tax incentives.

The study conducted by Tian & Yao (2015) The study focused on investigating preferences for earthquake insurance in rural China and identifying the factors that influenced the Willingness to Pay. The key findings revealed that knowledge of earthquake insurance and personal experience with earthquakes significantly influenced household's willingness to Pay for earthquake insurance. This study also compared knowledge of earthquake insurance with knowledge of cyber insurance and personal experience with earthquakes with experience with cyber-attacks. However, in the domain of cyber insurance, knowledge of cyber insurance was found to be significant, whereas experience with cyber-attacks was not, in relation to the decision to pay for cyber insurance. The implications of the study emphasized the importance of policymakers and insurers developing strategies to increase public knowledge about earthquake insurance and highlighting the significance of earthquake risk mitigation. Furthermore, the study suggested that insurance providers should consider targeted marketing efforts to encourage higher uptake of earthquake insurance among rural households in China.

The study conducted by (Tonn et al., 2019) focuses on cyber insurance in the transportation sector. It found that IT managers play a crucial role in purchasing cyber insurance for transportation infrastructure systems. With the annual increase in cyber incidents and associated costs, prioritizing cyber risk management is vital for IT managers. They should assess and mitigate risks, implement security measures, and

actively seek appropriate cyber insurance coverage. In addition, a larger companies usually employ a chief information officer and other cybersecurity professionals to make strategic decisions, which may inform cyber insurance purchases to minimize catastrophic situations (Meland et al., 2015). The study recommends collaborating with insurers to ensure accurate assessment and pricing of cyber risk, thereby safeguarding the organization against potential damages and disruptions. This study concerns the unique of cyber insurance as it is new and not well known in the market, there for this study investigate the decision making from the personal who understand well in cybersecurity. This study aims to investigate the Willingness to Pay for cyber insurance among IT personnel in operational and professional roles, including IT Operational Officer, Security Operational Officer, Chief Information Officer, and Chief Security Officer. The findings suggest that the Chief Security Officer's role significantly influences the decision-making process regarding the purchase of cyber insurance, reflecting the response from the targeted group of respondents.

The study conducted by Berkman et al. (2018) examines the impact of cybersecurity and data protection laws on organizations. The study uncovers that these regulations have led to the implementation of several measures, such as appointing directors with IT backgrounds, hiring Chief Information Security Officers, forming IT committees of the Board, enhancing security in new systems, and purchasing insurance. The introduction of cybersecurity laws and the emergence of

cyber liability have heightened the legal consequences of security breaches, leading to the expansion of the cyber insurance industry. However, the study explores the influence of cybersecurity and data privacy laws on the decision to purchase cyber insurance. However, the results show that in Thailand, both cybersecurity and personal data protection laws do not significantly impact the decision to pay for cyber insurance.

In conclusion, the key findings from the relevant literature encompass various factors, including knowledge of insurance products, experience in purchasing insurance, risk experience, the position of the IT manager, and the relevant laws. This study identifies two significant factors that influence the decision-making process regarding the purchase of cyber insurance: The Chief Security Officer (CSO) and knowledge of cyber insurance.

Moreover, this study provides insights into the Willingness to Pay from respondents who perceive the value and benefits of cyber insurance. The results indicate that respondents with a higher perceived value of cyber insurance exhibit a Willingness to Pay of THB 204,312 (USD 6,592). Additionally, respondents working in the cybersecurity field, particularly Chief Security Officers, demonstrate a significantly higher Willingness to Pay of THB 287,300 (USD 9,276).

The key findings contribute to the literature by highlighting the importance of the Chief Security Officers and cyber insurance knowledge in the decision-making process for cyber insurance. Furthermore, the study provides empirical evidence of the Willingness to Pay from individuals who recognize the value of cyber insurance, and they might understand in cybersecurity measure.

5.2 Implication.

This section provides policy implications for insurers and policymakers. The study addresses the pertinent issue of enhancing cyber insurance acceptance levels and promoting it as a mechanism for mitigating cybersecurity risks. Additionally, these studies offer suggestions for the government to consider.

5.2.1 Policy Implication

The key findings underscore the need for governments and insurance companies to consider these variables when developing policies and marketing strategies related to cyber insurance. By understanding and addressing the factors that influence consumers' Willingness to pay, these entities can better serve the needs of their customers and promote the adoption of cyber insurance as an important safeguard against cyber threats.

5.2.1.1 Policy Implications of the Government.

Taking into account the monetary value given by CIIs organization, if the government intends to introduce and support cyber insurance as an effective tool to mitigate and transfer cyber risks to insurers, should consider helping cyber insurance premiums affordability, and also focus on influencing the decision-making process of purchasing cyber insurance to increase the adoption rate.

Based on this study, the hypothetical market offers a cyber insurance policy that provides minimum coverage for both first- and third-party losses resulting from cyber-attacks and data breaches. The Willingness to pay figures indicate success or failure of the policy when the government intend to introduce a cybersecurity policy to Critical Information Infrastructure Organization, particularly cyber risk transfers through cyber insurance. Prior study was provide policy implication from Willingness to pay number, Hansen et al. (2016) introduced tax incentives to the Danish government, whereas power purchasing by the government was proposed to the U.S. government by Clinton (2012). Therefore, the Willingness to pay from this study could help the Government to estimate the success or failure of promotion of cyber insurance. If the premium for cyber insurance policies exceeds their monetary value, the government could consider taking the following actions:

- Tax incentive: Utilize the Willingness to pay to develop policies that incentivize individuals to purchase insurance by offering tax incentives. For example, Tax deduction for premium payment for insured, and Tax exemption or reduce Tax rate for insurers.

- Power purchasing of the government: The Government could leverage its strong position in the marketplace by mandating that government contractors and sub-contractors carry cyber-insurance. In addition, acquiring cyber insurance in significant volumes provides an opportunity to obtain more favorable terms, negotiate lower premiums, and shape the market by influencing the development of specialized coverage options.

- Provision of cybersecurity technology: To reduce cyber risk, the government can support the development of innovative cybersecurity technologies and solutions, facilitating the advancement of state-of-the-art cybersecurity tools, techniques, and frameworks. This proactive approach can enable the adoption of more effective risk mitigation strategies and enhance the capability for robust risk assessment, ultimately reducing the likelihood and impact of cyber incidents and potentially resulting in lower insurance premiums.

- Strengthen regulations for cyber insurance adoption: The government can mandate that certain organizations or industries must obtain cyber insurance coverage. This requirement would ensure that businesses adequately protect themselves against cyber risks and promote a more widespread adoption of cyber insurance. By making cyber insurance a mandatory component of risk management, the

government can incentivize organizations to invest in cybersecurity measures and reduce the overall risk landscape.

Turning to the two explanatory variables examined included professionalism in cybersecurity respectively Chief of Security Officer, and knowledge of cyber insurance that have emerged as significant determinants of respondents' Willingness to pay, the Government consideration:

First factor influencing Willingness to Pay for cyber insurance is Knowledge of cyber insurance, it plays a crucial role in enhancing insurance perception as Tian & Yao (2015) mentioned in earthquake insurance study, it is according to risk awareness and preparedness among the individuals. The organization that best understands insurance product they acknowledge that they are required to undergo a thorough assessment of their cybersecurity measures and practices. Insurance providers typically evaluate an organization's security controls, risk management protocols, incident response plans, and overall cybersecurity posture (Chen, 2021). In addition, the assessment process encourages organizations to establish robust cybersecurity risk governance frameworks and adopt best practices for mitigating cyber risks. In order to secure favorable insurance coverage and reasonable premiums, companies need to demonstrate that they have implemented effective cybersecurity measures.

In conclusion, the government could consider taking the following actions to increase the level of understanding of cyber insurance:

- Education program, to make more understanding in cyber insurance benefit, the indirect benefit in increasing cybersecurity posture: cybersecurity governance, cybersecurity practice, awareness of cybersecurity in organization.
- Cooperating with insurers, organizations can achieve this by organizing workshops, seminars, and training sessions in collaboration with insurance organizations. These initiatives aim to increase awareness and understanding of cyber insurance among participants.

Second factor influencing Willingness to pay for cyber insurance is professionalism in cybersecurity particularly the Chief of Security Officer, it can play a crucial role in the decision to purchase cyber insurance. They are likely to have a deep understanding of the benefits of cyber insurance regarding to their expertise in cyber threats and vulnerabilities. As professionals in the field, they are perceiving cyber risk, and aware of the significant financial losses that can result from a cyber-attack and the importance of having adequate coverage to mitigate these risks. Moreover, they possess extensive knowledge of cybersecurity best practices, enabling them to evaluate and choose the most appropriate cyber insurance policy for their organization.

Given their expertise in the cyber threat landscape and understanding of the benefits of cyber insurance, Chief Security Officer can more readily recognize the value of purchasing cyber insurance. Cybersecurity measures can also help organizations better comprehend and manage cyber risks, making them more appealing candidates for cyber insurance coverage. Therefore, the Chief Security Officer grasp of the benefits of cyber insurance and their ability to manage cyber risks can help organizations protect themselves against the consequences of cyber-attacks. Government should certify the pathway of cybersecurity professional.

In conclusion, the government could consider taking the following actions to promote professionalism in cybersecurity:

- Setting up a national cybersecurity career path can contribute to increasing professionalism in the cybersecurity field.
- Promoting cybersecurity experts who possess a deep understanding of cyber risks and losses enables them to make informed decisions regarding the affective cybersecurity mechanism.
- Encouraging the employment of cybersecurity professionals within organizations can enhance their overall cyber risk management and potentially elevate the perceived value of cyber insurance.

5.2.2.2 Policy Implication of Insurers

The monetary value obtained from this study provides insurers with a fundamental understanding of the Willingness to pay from CIIs organizations. However, relying solely on Willingness to pay is insufficient as it depends on several dimensions within the pricing process. Factors such as cybersecurity maturity, cyber risk assessment information, legal liability fees, prior cyber incidents, history of cyber-attacks, policy limits and deductibles, company size, and industry sector all influence the cyber insurance premium. Hence, when insurers estimate the cyber insurance premium based on their pricing strategy, they can incorporate the Willingness to pay number and subsequently design campaigns to ensure the price is satisfactory to the insured.

On the other hand, if the insurance company sets the premium higher than Willingness to Pay, it may deter customers who are unwilling or unable to pay the higher price, which could limit the adoption rate of cyber insurance overall. Therefore, it's important for insurance companies to strike a balance between affordability and profitability when pricing their cyber insurance policies.

The estimated results assist insurance companies in determining the market size of cyber insurance in Thailand. Estimate market size and set target sectors. For example, according to an OECD Scoreboard, the Thai Office of SMEs Promotion reported approximately three million SMEs.

And cybersecurity Law and Personal Data Protection Law enforce to CIIs organization both in the business and public sector. By using the conservative estimate of median Willingness to Pay excluding covariate effects, the total additional Willingness to Pay of cyber insurance consumers is approximately THB 622 billion (Approx. USD 20 million), indicating the potential benefit to the cyber insurance market. This information also allows insurers to assess the market size and market share of cyber insurance in Thailand. However, it is important to note that these estimates are limited to the domain of cyber insurance premiums so it only provides market size and does not cover net income.

In conclusion, insurers can consider the Willingness to Pay in the following ways:

- Setting up premiums and assessing the gap between the offered price and the Willingness to Pay to determine if the pricing strategy will be attractive to consumers.
- Developing pricing strategies that specifically target potential consumers. For example, Segmentation: Analyze the Willingness to Pay data to identify different segments of potential consumers with varying levels of Willingness to Pay. Group customers with similar Willingness to Pay values together to create distinct segments. Customized Plans: Tailor cyber insurance plans to match the needs and preferences of each segment. For customers with higher Willingness to Pay, offer comprehensive coverage and additional

benefits. For those with lower Willingness to Pay, create more basic and affordable plans

Turning to the two explanatory variables examined included professionalism in cybersecurity respectively Chief of Security Officer, and knowledge of cyber insurance that have emerged as significant determinants of respondents' Willingness to pay, the insurer consideration: collaboration with the government to increase awareness and understanding of cyber insurance, and create network with cybersecurity expert.

5.2.2 Suggestions

To increase the uptake of cyber insurance and enhance market efficiency, standardizing policies is crucial, as recommended by previous literature (Toregas & Zahn, 2014; Talesh, 2018; Granato & Polacek, 2019; Aziz et al., 2020; Abdul Hamid et al., 2022). Standardization helps policyholders understand coverage better and enables insurers to offer comprehensive options, reducing confusion. Collaboratively developed standards involving insurance providers, cybersecurity experts, risk assessors, and legal professionals are vital.

The government can play a leading role by advocating industry-wide guidelines or regulations, establishing standardized language for policies, risk assessment frameworks, and minimum cybersecurity

standards. Insurance companies can participate in industry associations or working groups, sharing information with government agencies to inform standardized language and pricing models.

Moreover, considering cyber insurance's optional availability and budgeting preparation challenges for public organizations, the government should deregulate fiscal budgets for government agencies to allocate resources for purchasing cyber insurance as needed.

5.3 Limitation and further work

The proposed study has the limitations that warrant consideration. Firstly, the scope of the study is confined to the Thai market, and as such, the findings may not be readily applicable to other countries with distinct market conditions. Secondly, the contingent valuation method employed in this research establishes a hypothetical market for the insurance industry, taking into account the aggregate amount of cyber insurance premiums necessary to cover potential losses. However, it does not furnish specific claim payment amounts or deductibility due to the inherent design of the hypothetical market, which was intended to streamline the analysis and minimize the need for further elaboration on terms and conditions.

To address this constraint, further investigation is indispensable to provide more comprehensive insights into the product and features of

cyber insurance. The utilization of a Choice Experiment could be advantageous in supplying more intricate information about the product, as demonstrated in a study on Willingness to Pay for insurance (Dragos & Dragos, 2017). Therefore, by incorporating such methodologies, future research endeavors can enhance the understanding of cyber insurance and its applicability in diverse contexts, paving the way for more nuanced and informed decision-making processes.

Bibliography

Abbas, A., Amjath-Babu, T. S., Kächele, H., & Müller, K. (2015). Non-structural flood risk mitigation under developing country conditions: an analysis on the determinants of willingness to pay for flood insurance in rural Pakistan. *Natural Hazards*, *75*(3), 2119–2135. https://doi.org/10.1007/s11069-014-1415-x

Abdul Hamid, N. H. A., Mat Nor, N. I. @., Hussain, F. M., Raju, R., Naseer, H., & Ahmad, A. (2022). Barriers and enablers to adoption of cyber insurance in developing countries: An exploratory study of Malaysian organizations. *Computers and Security*, *122*, 102893. https://doi.org/10.1016/j.cose.2022.102893

Aizaki, H., Nakatani, T., & Sato, K. (2015). *Stated preference methods using R*. 238.

Alejandro, L. (2012). Introduction to contingent valuation using Stata. *MPRA Paper*, *41018*.

Aziz, B., Suhardi, & Kurnia. (2020). A systematic literature review of cyber insurance challenges. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, 357–363. https://doi.org/10.1109/ICITSI50517.2020.9264966

Bandyopadhyay, T., & Mookerjee, V. (2019). A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, *21*(2), 301–325. https://doi.org/10.1007/s10796-017-9737-3

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Biener, C., Eling, M., & Wirfs, J. H. (2015). *Insurability of Cyber Risk: An Emprical Analysys*.

Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Boyle, K. J., Bishop, R. C., & Welsh, M. P. (2019). *Starting Point Bias in Contingent Valuation Bidding Games*. *61*(2), 188–194.

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63. https://doi.org/10.1080/23738871.2017.1296878

Carson, R. T., & Hanemann, W. M. (2005). Chapter 17 Contingent Valuation. *Handbook of Environmental Economics*, *2*(05), 821–936. https://doi.org/10.1016/S1574-0099(05)02017-6

Chase, A. (2021). *The Evolution of Cyber Risk and the Cyber Insurance Market*. https://scholarcommons.sc.edu/senior_theses/412

Chen, P. (2021). *How Much Does Cyber Insurance Cost? – AdvisorSmith*. https://advisorsmith.com/cyber-liability-insurance/cost/

Clinton, L. (2012). Cyber-Insurance Metrics and Impact on Cyber-Security. *Internet Society Alliance*. https://www.whitehouse.gov/files/documents/cyber/ISA - Cyber-Insurance Metrics and Impact on Cyber-Security.pdf%0Ahttp://cyber.harvard.edu/cybersecurity/Cyber-Insurance_Metrics_and_Impact_on_Cyber-Security

Cybersecurity Act B.E. 2562 (2019). (2019). *136*, 1–24.

D Bailey, L. M. (2014). Mitigating Moral Hazard in Cyber-Risk Insurance. *Journal of Law & Cyber Warfare*, *3*(1), 1–42. https://heinonline.org/HOL/License

De Smidt, G., & Botzen, W. (2018). Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *Geneva Papers on Risk and Insurance: Issues and Practice*, *43*(2), 239–274. https://doi.org/10.1057/s41288-018-0082-7

Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, *527*, 576–589. https://doi.org/10.1016/j.ins.2018.12.051

Dragos, C. M., & Dragos, S. L. (2017). ESTIMATING CONSUMERS' BEHAVIOUR IN MOTOR INSURANCE USING DISCRETE CHOICE MODELS. *E a M: Ekonomie a Management*, *20*(4), 88–102. https://doi.org/10.15240/tul/001/2017-4-007

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

Elnagdy, S. A. (2017). *Cost Reduction Strategy for Cybersecurity Risk Management and Risk Transfer to Insurance in Financial Industry* (Issue January).

Elnagdy, S. A., Qiu, M., & Gai, K. (2016). Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing. *Proceedings - 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016*, 295–300. https://doi.org/10.1109/CSCloud.2016.46

Fahad, S., Wang, J., Hu, G., Wang, H., Yang, X., Shah, A. A., Huong, N. T. L., & Bilal, A. (2018). Empirical analysis of factors influencing farmers crop insurance decisions in Pakistan: Evidence from Khyber Pakhtunkhwa province. *Land Use Policy*, *75*(March), 459–467. https://doi.org/10.1016/j.landusepol.2018.04.016

Forum, C. R. O. (2017). Types of cyber incidents and losses. *Enhancing the Role of Insurance in Cyber Risk Management*, 19–56. https://doi.org/10.1787/9789264282148-4-en

Franke, U. (2017). The cyber insurance market in Sweden. *Computers and Security*, *68*(1), 130–144. https://doi.org/10.1016/j.cose.2017.04.010

Gai, K., Qiu, M., & Hassan, H. (2017). Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing. *Concurrency Computation* , *29*(7), 1–13. https://doi.org/10.1002/cpe.3856

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

GlobalData Thematic Research. (2020). *Cyber Insurance: Timeline*. https://www.verdict.co.uk/cyber-insurance-timeline/

Granato, A., & Polacek, A. (2019a). The growth and challenges of cyber insurance. *Chicago Fed Letter*. https://doi.org/10.21033/CFL-2019-426

Granato, A., & Polacek, A. (2019b). The growth and challenges of cyber insurance. *Chicago Fed Letter*, *426*. https://doi.org/10.21033/cfl-2019-426

Hanemann, M., Loomis, J., & Kanninen, B. (1991). Statistical Efficiency of Double-Bounded Dichotomous Choice Contingent Valuation. *American Journal of Agricultural Economics*, *73*(4), 1255–1263. https://doi.org/10.2307/1242453

Hanemann, W. M. (1989). *Welfare Evaluations in Contingent Valuation Experiments with Discrete Response Data: Reply*.

Hansen, J. V., Jacobsen, R. H., & Lau, M. I. (2016). Willingness to pay for insurance in denmark. *Journal of Risk and Insurance*, *83*(1), 49–76. https://doi.org/10.1111/j.1539-6975.2013.12011.x

Honu, B. (2007). Contingent Valuation Method for General Practitioners: A Cookbook Approach. *Lesotho Social Science Review*, *11*(1–2), 83–96. https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/6218

Horne, R. (n.d.). *Cyber security governance*. Retrieved May 7, 2023, from https://www.pwc.co.uk/issues/cyber-security-services/insights/governing-cyber-security-risk.html

Huh, S. Y., Lee, J., & Shin, J. (2015). The economic value of South Korea's renewable energy policies (RPS, RFS, and RHO): A contingent valuation study. *Renewable and Sustainable Energy Reviews, 50*, 64–72. https://doi.org/10.1016/j.rser.2015.04.107

Hunton Andrews Kurth. (2020). *South Korean Court Imposes Personal Liability on Privacy Officer for Data Breach*. https://www.huntonprivacyblog.com/2020/01/09/south-korean-court-imposes-personal-liability-on-privacy-officer-for-data-breach/

Jagpal, S., & Jedidi, K. (2009). Willingness to pay: Measurement and managerial implications. *Handbook of Pricing Research in Marketing*, 37–60.

Jason Nurse, R. C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CyberSA49311.2020.9139703

Jedidi, K., & Zhang, Z. J. (2002). Augmenting conjoint analysis to estimate consumer reservation price. *Management Science, 48*(10), 1350–1368. https://doi.org/10.1287/mnsc.48.10.1350.272

Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., & Dobalian, A. (2020). Trends and best practices in health care cybersecurity

insurance policy. *Journal of Healthcare Risk Management : The Journal of the American Society for Healthcare Risk Management*, *40*(2), 10–14. https://doi.org/10.1002/jhrm.21414

Kingdom of Thailand. (2019). *Thailand Personal Data Protection Act, B.E. 2562*, *2019*. *136*, 1–35.

Ko, S., Kim, W., Shin, S. C., & Shin, J. (2020). The economic value of sustainable recycling and waste management policies: The case of a waste management crisis in South Korea. *Waste Management*, *104*, 220–227. https://doi.org/10.1016/j.wasman.2020.01.020

Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review*, *103*(3), 985–1031.

KPMG International. (2018). Cyber Insurance - How Insuretechs Can Unlock The Opportunity. *KPMG Report*. https://assets.kpmg/content/dam/kpmg/za/pdf/2017/12/17383MC-cyber-insurance.pdf

Kristrom, B. (1997). Spike Models in Contingent Valuation. *American Agricultural Economic Association*, 1013–1023.

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy*, *44*(8), 102007. https://doi.org/10.1016/j.telpol.2020.102007

Lyu, K., & Barré, T. J. (2017). Risk aversion in crop insurance program purchase decisions Evidence from maize production areas in China. *China Agricultural Economic Review*, *9*(1), 62–80. https://doi.org/10.1108/CAER-04-2015-0036

Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). *The Evolution of Cyberinsurance*. 1–16. http://arxiv.org/abs/cs/0601020

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Mazzoccoli, A., & Naldi, M. (2020). Robustness of Optimal Investment Decisions in Mixed Insurance/Investment Cyber Risk Management. *Risk Analysis*, *40*(3), 550–564. https://doi.org/10.1111/risa.13416

MDES. (2018). *Thailand Digital Economy and Society Development Plan*. https://doi.org/10.1017/CCOL0521818389.011

Meland, P. H., Tondel, I. A., & Solhaug, B. (2015). Mitigating risk with cyberinsurance. *IEEE Security and Privacy*, *13*(6), 38–43. https://doi.org/10.1109/MSP.2015.137

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, *21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*(1), 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Nam, S. (2018). How much are insurance consumers willing to pay for blockchain and smart contracts? A contingent valuation study.

Sustainability (Switzerland), *10*(11). https://doi.org/10.3390/su10114332

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*(March), 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Noor, U., Anwar, Z., Altmann, J., & Rashid, Z. (2020). *Customer-oriented ranking of cyber threat intelligence service providers*. https://doi.org/10.1016/j.elerap.2020.100976

Ozawa, R. (2021). *Cyber insurance rates rise as cases grow – Paubox*. https://www.paubox.com/blog/cyber-insurance-rates-rise-as-cases-grow/

Pal, R. (2012). *Cyber-Insurance in Internet Security: A Dig into the Information Asymmetry Problem*. http://arxiv.org/abs/1202.0884

Paopid, S., Tang, J., & Leelawat, N. (2020). Willingness to pay for flood insurance: A case study in Phang Khon, Sakon Nakhon Province, Thailand. *IOP Conference Series: Earth and Environmental Science*, *612*(1). https://doi.org/10.1088/1755-1315/612/1/012041

Pooser, D. M., Browne, M. J., & Arkhangelska, O. (2018). Growth in the Perception of Cyber Risk: Evidence from U.S. P&C Insurers. *Geneva Papers on Risk and Insurance: Issues and Practice*, *43*(2), 208–223. https://doi.org/10.1057/s41288-017-0077-9

PwC. (2017). *Cyber Risk – Enlightenment through information risk management*. 5. www.pwc.com.au

Rahmatian, M. (2005). *Contingent Valuation Method*. *November*, 1–9.

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). *Decision support for Cybersecurity risk planning*. https://doi.org/10.1016/j.dss.2011.02.013

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz002

Sajise, A. J., Samson, J. N., Quiao, L., Sibal, J., Raitzer, D. A., & Harder, D. (2021). *Contingent Valuation of Nonmarket Benefits in Project Economic Analysis: A Guide to Good Practice* (Issue December).

Sausalito, C. (2020). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Signorello, G. C. J. C. H. W. M. (2018). One and One Half Bound Dicrotomous Choice. *UC Berkeley*. https://www.youtube.com/watch?v=PCztXEfNJLM

Simoni, M. D., Kutanoglu, E., & Claudel, C. G. (2020). Optimization and analysis of a robot-assisted last mile delivery system. *Transportation Research Part E: Logistics and Transportation Review*, *142*(July), 102049. https://doi.org/10.1016/j.tre.2020.102049

Song, N. Van, Huyen, V. N., Dung, L. T. P., & Thuy, N. T. (2019). Using Double-Bounded Dichotomous-Choice to Estimate Households' Willingness to Pay for Improved Water Quality in Bac Ninh Province of Vietnam. *Journal of Environmental*

Protection, *10*(11), 1407–1418. https://doi.org/10.4236/jep.2019.1011083

Tal Pavel. (2020). The Cyber Insurance Market in Israel. *Computers and Security*, *68*(1), 130–144. https://doi.org/10.1016/j.cose.2017.04.010

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law and Social Inquiry*, *43*(2), 417–440. https://doi.org/10.1111/lsi.12303

ThaiCERT. (2022). *Cyber threats statistics*. https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx

Tian, L., & Yao, P. (2015). Preferences for earthquake insurance in rural China: factors influencing individuals' willingness to pay. *Natural Hazards*, *79*(1), 93–110. https://doi.org/10.1007/s11069-015-1829-0

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, *79*(April), 103–114. https://doi.org/10.1016/j.tranpol.2019.04.019

Toregas, C., & Zahn, N. (2014). Insurance for Cyber Attacks: The Issue of Setting Premiums in Context. *George Washington University*, 20. https://www.seas.gwu.edu/~cspri/s/cyberinsurance_paper_pdf.pdf

Tosh, D. K., Shetty, S., Sengupta, S., Kesan, J. P., & Kamhoua, C. A. (2017). Risk management using cyber-threat information sharing and cyber-insurance. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications*

Engineering, *LNICST*, *212*(May), 154–164. https://doi.org/10.1007/978-3-319-67540-4_14

Uuganbayar, G., Yautsiukhin, A., Martinelli, F., & Massacci, F. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers and Security*, *101*. https://doi.org/10.1016/J.COSE.2020.102121

Visscher, L., Nieuwesteeg, B., & de Waard, B. (2018). The Law and Economics of Cyber Insurance Contracts: A Case Study. In *European Review of Private Law* (Vol. 26, Issue Issue 3). https://doi.org/10.54648/erpl2018027

Wertenbroch, K., & Skiera, B. (2002). Measuring consumers' willingness to pay at the point of purchase. *Journal of Marketing Research*, *39*(2), 228–241. https://doi.org/10.1509/jmkr.39.2.228.19086

Wirth, A. (2017). The economics of cybersecurity get the most out of your CMMS. *Biomedical Instrumentation & Technology*, 52–60.

Wolff, J. (2022a). Breach on the Beach: Origins of Cyberinsurance. *Cyberinsurance Policy*, 27–62. https://doi.org/10.7551/MITPRESS/13665.003.0006

Wolff, J. (2022b). Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks. *Cyberinsurance Policy*. https://doi.org/10.7551/MITPRESS/13665.001.0001

Wolff, J. (2022c). "Insurrection, Rebellion, Revolution, Riot": NotPetya, Property Insurance, and War Exclusions.

Cyberinsurance Policy, 111–150. https://doi.org/10.7551/MITPRESS/13665.003.0010

Woods, D. W., & Moore, T. (2020). Does Insurance Have a Future in Governing Cybersecurity? *IEEE Security and Privacy*, *18*(1), 21–27. https://doi.org/10.1109/MSEC.2019.2935702

World Economic Forum. (2018). The Global Risks Report 2018 13th Edition. In *Annals of Clinical Research* (Vol. 3, Issue 1). https://doi.org/10.1056/nejm196802152780701

Yang, Z., & Lui, J. C. S. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, *74*, 1–17. https://doi.org/10.1016/j.peva.2013.10.003

Yoo, S. H., & Kwak, S. J. (2002). Using a spike model to deal with zero response data from double bounded dichotomous choice contingent valuation surveys. *Applied Economics Letters*, *9*(14), 929–932. https://doi.org/10.1080/13504850210139378

Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, *14*, 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

Zainudin, N., Nordin, N., & Begum, H. (2016). Survey designing for contingent valuation studies. *Proceeding of 2nd International Conference on Economics & Banking 2016, 2016*(November), 1–6. https://www.researchgate.net/profile/Norzalina_Zainudin/publication/303750748_SURVEY_DESIGNING_FOR_CONTINGENT_

VALUATION_STUDIES/links/5acf02f4a6fdcc87840f4223/SURVEY-DESIGNING-FOR-CONTINGENT-VALUATION-STUDIES.pdf%0Ahttp://conference.kuis.edu.my/iceb2016/e

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy*, *42*(5), 409–420. https://doi.org/10.1016/j.telpol.2018.02.004

Zhanna Malekos, Smith; Eugenia, L., & Lewis, J. A. (2020). The Hidden Costs of Cybercrime. In *McAfee* (pp. 1–38). https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Appendix 1: Contingent Valuation Survey Questionnaire

Survey Questionnaire

The Willingness to Pay for cyber insurance. A Contingent Valuation Study.

This survey aims to investigate the acceptance of Cyber Insurance Policies among Critical Information Infrastructure (CII) organizations. Its purpose is to gather general perceptions and opinions on cyber insurance premiums. There are no right or wrong answers to the questions, which will only be used to provide statistics on organizations' opinions on cyber insurance. The responses will be used solely for academic research purposes to analyze the willingness to pay for cyber insurance in Thailand. The responses will be thoroughly protected and will not be shared with any third party.

Part I: Information

This section is providing the overall information about Cyber Insurance. Please read carefully before you answer the question in part II.

Taking into account the enforcement of the Cybersecurity Act B.C. 2562 (2019) and the Data Privacy Act B.C. 2562 (2019).

The Cybersecurity Law, and Data Privacy Law shaping organization to responses to cyber-attack, and data breaches. Therefore, organization have to identify the affective cyber-risk management strategies to prevent and mitigation cyber threat. Risk prevention and mitigation are available in various form, and Cyber Insurance is a new form of Cybersecurity Risk Management Strategy. Cyber Insurance is a cyber-risk transfer mechanism that enables an organization to be accountable for cyber losses caused by cyber-attacks.

1. What is cyber insurance?

Cybersecurity insurance also called "cyber liability insurance" or "cyber insurance", is a contract that an organization can purchase to transfer the financial risks associated with loss from a cyber-attack. In payment for a monthly or yearly fee, the insurance policy transfers some of the risks to the insurer.

2. Why cyber insurance should be considered?

Recently top cyber-attack included Malware, denial-of-service (DoS), fishing, ransomware, SQL injection, DNS Tunneling, and zero-day exploits. Cyber-attack could make the potential

loss such as Financial loss from Business interruption, Data and software loss, and Reputational Damage which is could potentially lead to loss of customers, sales, reduction in profits, and affect the relationship with suppliers, and investors. Moreover, you may have to pay fines, legal liability which is depends on the size of your breach.

Therefore, Cyber Insurance help organization in a better manage cyber risk, and any resulting legal liability from data breaches. Cyber insurance can be critical in assisting an organization in recovering from a data breach, including costs such as business interruption, income loss, equipment damage, legal bills, public relations charges, forensic investigation, and costs connected with legally required notification.

Case I:

In 2011, hackers gained access to Sony's PlayStation Network, revealing the personally identifiable information (PII) of 77 million PlayStation user accounts. The vulnerability stopped PlayStation console users from using the service for 23 days. Sony suffered expenditures of *more than $171 million* as a result of the incident. A portion of this expense may have been covered by a cyber-insurance policy, but Sony's insurance coverage covered only physical property loss, leaving Sony responsible for the entire cost of cyber damages.

Source:https://www.techtarget.com/searchsecurity/definition/cybersecurity-insurance-cybersecurity-liability-insurance

Case II:

In 2020, a privacy officer for the South Korean travel business Hana Tour Service Inc. was found negligent for failing to prevent a data breach affecting over 465,000 of the agency's clients and 29,000 of its workers. The Court fined the privacy officer 10 million South Korean Won, which is *approximately $8,500*. This is in addition to the corporation being fined separately by the Ministry of Interior and Safety 327,250,000 (*about $280,000*). A portion of this expense may have been covered by a cyber-insurance policy, but if Hana Tour Service Inc. does not have cyber insurance, leaving Hana responsible for the entire cost of cyber damages.

Source: https://www.huntonprivacy.com/

3. What does cyber insurance cover?

Cyber risks typically fall into "first party" risks and "third party" risks. Cyber insurance provide coverage for one or both of these categories.

First party insurance	Third party insurance
First party insurance covers damage your business such as; - Forensic analysis for identifying the attack source. - Public relations services - Notification of clients - Credit monitoring services - Loss of income	Third party insurance covers damages if customer or partner are affect by a cyber-attack on your business such as; - Settlement cost - Media liability - Legal fees

4. What is cyber insurance not covered?
   - Potential future lost profits
   - Loss of value due to theft of your intellectual property
   - The cost to improve technology systems, including any software or security upgrades after a cyber-event.
   - Reputation recovery.

5. Advantage of cyber insurance.

Insurance company will cover almost of total loss you get from cyber-attack from coverage you buy included for company loss and customer loss.

6. Disadvantages of cyber insurance.

Cyber insurance premiums vary depending on the agreement, so no reference package is available in the market. The insurer has to deal with the insurance company to find the premium that they have to pay.

Part I: Investigation Questions

Q1. Are you willing to pay the premium $1400 (xxx USD) for one year to transfer the risk of cyber-attack that causes liability under the Cybersecurity Act B.C. 2564 (2019) and Data Privacy Act B.C. 2564 (2019)?

☐ 1.Willingness to pay

☐ 2. No intent to pay —▶ Go to Q4.

Q2. (Please answer only if you answered 1. willing to pay in Q1.)
You mediate a cyber-attack that causes liability under the Cybersecurity Act B.C. 2564 (2019) and the Data Privacy Act B.C. 2564 (2019).
Are you willing to pay the premium of $2800 (xxx USD x2) for one year to transfer the risk to Cyber Insurance Company?

☐ 1.Willingness to pay

☐ 2. No intent to pay —▶ Go to Q5

YY

Q3. (Please respond only if you answered 1. willing to pay" in Q2.)
You mediate a cyber-attack that causes liability under the Cybersecurity Act B.C. 2564 (2019) and the Data Privacy Act B.C. 2564 (2019).
How much of a premium are you willing to pay each year for it? *Please respond with* ***the maximum*** *amount.*

As you answered that you are willing to pay $2800 (xxx USD x2) in Q2., you must respond with an amount of (xxx USD x2) or more.

Estimate of Cyber Insurance Premium for one year is: $ _ _ _ _ _

N

Q4. (Please answer only if you answered Q1 No intention to pay.)
You mediate has cyber-attack that causes liability under the Cybersecurity Act B.C. 2564 (2019) and Data Privacy Act B.C. 2564 (2019).
Are you willing to pay the premium 700 (XXXX USD ÷2) for one year to transfer the risk to Cyber Insurance Company?

☐ 1.Willingness to pay —▶ Go to part III

☐ 2. No intent to pay

NN

Q5. (Please respond only if you answered Q2. and Q4. No intention to pay.)
Then, you will mediate has cyber-attack that causes liability under the Cybersecurity Act B.C. 2564 (2019) and Data Privacy Act B.C. 2564 (2019).
Are you willing to pay the premium for one year to transfer the risk to Cyber Insurance Company?

☐ 1.Willingness to pay

☐ 2. No intent to pay —▶ Go to part III ⊞6

Q6. (Please respond only if you answered No intent to pay in Q4.)
Then, you mediate has cyber-attack that causes liability under the Cybersecurity Act B.C. 2564 (2019) and Data Privacy Act B.C. 2564 (2019).
How much of a premium are you willing to pay each year for it? *Please respond with* ***the maximum*** *amount.*

In Q4, you answered that you are not willing to pay 700 (XXXX USD ÷2), so you must respond with an amount less than (XX won ÷ 2).

Estimate of Cyber Insurance Premium for one year is: $ _ _ _ _ _

Part III: Classification Questions

1. Gender: ☐ Male ☐ Female

2. Age:
   - ☐ 25 – 35
   - ☐ 36 – 45
   - ☐ 46 – 55
   - ☐ above 55

3. Education:
   - ☐ Under Graduate
   - ☐ Graduate
   - ☐ Other (.....)

4. Occupation:
   - ☐ Chief Information Officer
   - ☐ Chief Cyber Security Officer
   - ☐ Operation Information Officer
   - ☐ Operation Cyber Security Officer
   - ☐ Other (.....)

5. Organization Name: .....

6. Industry:
   - ☐ Substantive public service
   - ☐ Banking and Finance
   - ☐ Information technology and telecommunications
   - ☐ Transportation and logistics
   - ☐ Energy and public utilities
   - ☐ Public health
   - ☐ Other (.....)

7. Organization Revenue/Capital/Fiscal budget year
   - ☐ Annual income not over $400,000
   - ☐ Annual income does not exceed $400,000 - $1,900,000
   - ☐ Annual income not over $1,900,000 - $3,800,000
   - ☐ Annual income not over $3,800,000 - $6,600,000
   - ☐ Annual income not over $6,600,000 - $9,400,000
   - ☐ Annual income does not exceed $9,400,000 - $18,800,000
   - ☐ Annual income not over $18,800,000

8. How much the organization investment in cybersecurity last year?

- ☐ Less than $30000
- ☐ $30001 to $90000
- ☐ $90001 to $180000
- ☐ Over $180000

9. Number of Employee:

- ☐ Less than 100
- ☐ 101 to 500
- ☐ 501 to 1000
- ☐ 1001 to 2000
- ☐ Over 2001

10. Number of Customer (Estimate the number of people who get service/you hold their personal data)

- ☐ Less than 1000
- ☐ 1001 to 5000
- ☐ 5001 to 10000
- ☐ 10001 to 20000
- ☐ Over 20001

[Experiences of Cyber Attack and the loss.]

11. Which use to describe your organization?

- ☐ Have been hacked.
- ☐ Not sure have been hacked.
- ☐ About to be hacked.

12. Do you experience cyber-attack in the last 3 years?

- ☐ Yes, please specify year …… (Go to No.13)
- ☐ No, (Go to No.14)

13. What kind of Cyber-attack you had experienced? (You can answer more than one)

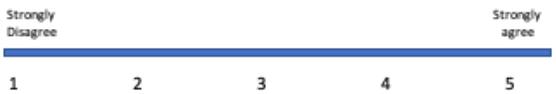
- ☐ Malware
- ☐ Denial-of-service (DoS)
- ☐ Fishing
- ☐ Ransomware
- ☐ SQL injection
- ☐ DNS Tunneling
- ☐ Zero-day exploit
- ☐ Other, please specify……

[Knowledge about law]
14. Do you know your organization's role in the 2019 Cybersecurity Act (B.C. 2562)?

15. Do you know your organization's role in the Data Privacy Act B.C. 2019 (2562)?

[Knowledge about Cyber Insurance]
16. Do you think your organization would benefit from cyber insurance coverage for losses resulting from cyber-attacks?

[Awareness of cyber-attack]
17. Many organizations are not aware of the possibility of cyber-attacks because they have robust cyber threat prevention technology and assume that data breaches only target large organizations with a large customer base. Do you believe that your organization is also not at risk of a cyber-attack?



[Awareness of risk transfer measure]
18. What measure do your organization will use to comply with Cyber-Security Law?

- ☐ Investment in security technology
- ☐ Purchase Cyber Insurance.
- ☐ Sharing Cyber Threat Information.
- ☐ Outsourcing cybersecurity expert

[Experiences of purchasing CI]
19. Do your organization purchase Cyber Insurance before?
☐ Yes, ... (Number of Year)
☐ No

[Attitude]
20. Do you think Cyber Insurance would be help your organization to reduce the risk of legal liability from the Cybersecurity Act B.C. 2564 (2019) and Data Privacy Act B.C. 2562 (2019).

Personal Data (Optional):

Full Name: .....
E-mail: .....

This is the end of survey questionnaire.
Thank you very much

Abstract (Korean)

최근, 일상 업무에서 디지털 기술에 대한 의존도가 높아짐에 따라, 증가하는 사이버 공격 위협에 대한 기업과 기관들의 관심이 높아지고 있다. 사이버 범죄는, 사이버 공격 위협에 취약한 개인과 조직, 인프라 시스템을 표적으로 하여, 잠재적인 혼란을 야기하고, 인명 피해를 초래하기도 한다. 이에 따라 태국 정부는, 디지털 보안에 대한 신뢰를 보장하여 태국의 국가 경쟁력을 강화하고자, 디지털 경제 개발 정책, 사이버 보안 법 및 개인 데이터 보호법 등을 시행하고 있다. 그리고 태국의 시장에서도, 다양한 사이버 보안 방법 중에서, 사이버 공격 위협을 제 3 자에게 이전하는 사이버 보험을 효과적인 대안으로 도입하고자 한다. 하지만, 사이버 보험의 가격 및 적용 범위 등 관련된 고려 사항의 복잡성으로 인해, 태국 시장, 특히, 중요 정보 인프라 (CII, Critical Information Infrastructure) 기관에서의 도입이 쉽지 않다.

본 연구는, 태국의 CII 기관에서 사이버 보험에 대한 의사결정 프로세스 및 지불 의사(willingness to pay)를 분석하여, 관련 의사결정에 대한 혜안을 제공하고자 한다. 이를 위해, 사이버 보험과 같은 비시장 상품의 경제적 가치를 평가하는 조건부 평가 방법(CVM)을 활용하였다. 연구를 통해, CII 기관의 구매 의사 결정과, 사이버 보험에 대한 투자에 영향을 미치는 중요한 요인들을 도출하였다.

사이버 보험은, 다양한 사이버 보안 방법 중에서, 사이버 공격 위협을 제 3 자인 보험사로 이전하여 위험을 완화하는 효과적인 방법으로 시장에 등장하였다. 그리고, 사이버 보험은 사이버 사고로 인한 잠재적인 재정적 손실과 평판 훼손에 직면한 기관에 절실하게 필요한 안전망을 제공한다. 그러나 여러가지 보험의 이점에도 불구하고, 사이버 보험은 태국 시장, 특히 CII 기관에서 활용되는 사례가 생소하다. 이는 사이버 보험의 적절한 가격 및 적용 범위와 관련한 고려사항이 복잡하여, CII 기관 등에서의 채택 결정이 어렵기 때문이다.

포괄적인 분석을 위해 본 연구에서는, 조직이 사이버 보험에 대한 투자를 거부할 수 있는 상황을 효과적으로 해결하는 spike 모델을 통합하였다. 이러한 접근 방식을 통해, 사이버 보험의 잠재적

채택자들의 지불 의사를 보다 정확하게 추정함으로써, 위험 관리 우선 순위를 심도 있게 확인할 수 있었다.

연구 결과에서, 태국의 CII 기관에서 사이버 보험에 대한 지불 의사가 유의미하게 나타났다. Spike 모형에 따르면, 평균 지불 의사는 연간 THB 207,455(USD 6,694)으로 확인된다. 또한 본 연구를 통해, 사이버 보험 관련 의사결정에, 기관 내 주요 구성원, 특히 최고 사이버 보안 책임자의 사이버 보험에 대한 이해와 전문성 수준이 중요함을 확인하였다. 지불 의사 또한 그들의 지식과 전문성으로부터 큰 영향을 받았으며. 각각 연간 THB 287,300(USD 9,267) 및 THB 204,312(USD 6,592)의 금전적 가치가 있었다.

본 연구의 결과는 스파이크 모델에 의해 도출된 지불 의사를 근거로, 정부와 보험사에 중요한 정책적 시사점을 제공한다. 또한, 태국 시장 내에서 사이버 보험에 대한 수요를 촉진하는데 있어, 사이버 보험에 대한 인식 제고의 중요성과, 자격을 갖춘 사이버 보안 전문가의 필요성을 강조하였다. 궁극적으로 본 연구는, 기관들이 사이버 위험을 완화시키는 조치를 통해, 사이버 위협으로부터 조직의 이익을 보호하면서 안전하게 디지털 기술을 도입하여, 태국의 보다 안전하고 탄력적인 디지털 생태계 조성에 기여하는 것을 목표로 한다.

주요어: 사이버 위험 관리, 사이버 보험, 지불 의향, 조건부 평가 방법, 스파이크 모델, 태국.
학 번: 2020-33021