Advances in Social Science, Education and Humanities Research, volume 426
3rd International Conference on Vocational Higher Education (ICVHE 2018)

Analysis of Cyber Insurance Potential in Indonesia

Yulial Hikmah[1], Fia Fridayanti Adam[1]

[1] Administration and Business Department, Vocational Education Program, Universitas Indonesia

*Email: yuli.alhikmah47@gmail.com

Abstract. In the digital era, one cannot deny that the virtual world has been vital in all activities. This makes owners of companies vulnerable to cybercriminals in terms of the personal data security of both customers or consumers. This necessitates cyber insurance products designed to protect vulnerable parties. In 2017, some insurance companies in Japan and America had the most revenue for cyber insurance. However, in Indonesia, cyber insurance has not attracted much interest, and only a few studies have been conducted on the topic. Therefore, this paper intends to examine the potential and constraints of cyber insurance development in Indonesia. Based on the SWOT analysis results, the presence of cyber insurance in Indonesia is under Quadrant 4. One of the major strategies that can be used to further the importance of cyber insurance is literacy and education among IT-based companies.

Keywords: *cyber insurance, digital era, SWOT analysis*

1 Introduction

At present, people are increasingly dependent on technology services. The technology that people currently use supports all aspects of the private and the public sectors (Marotta, Martinelli, Nanni, & Orlando, 2017). A place that creates technology must significantly affect human life. The digital economy is born and developed through information and communication technologies, which can also be globalized. With the development of technology, which also occurs as a result of technology itself, one important issue is the theft of customers' or consumers' personal data. While information and communication technologies can be used in the economy and society, they bring several benefits and disadvantages (Hughes, Bohl, Irfan, Margolase, & Solorzano, 2017). Recent years have seen an increasing interest in the world itself, which is regarded as one of the most challenging issues, as it reflects the place where such a problem can be resolved (Marotta et al., 2017). Cyber risks are defined as the changes brought about by electronic losses.

In 2015, a total of 79,790 cybersecurity incidents were reported by 70 organizations in 61 countries, resulting in 2,122 confirmed data breaches. In addition, cyber risks come in many forms, namely, system attacks, digital asset damage, system interruptions, data loss, theft of monetary value, personal data theft, espionage, reputation damage, and extortion (Phadermrod, Crowder, & Wills, 2017). Marsh's (2013) study on cyber risks revealed that 54% of the organizations interviewed had been targeted by cyberattacks in the past three years (17% of respondents were unable to answer questions). Many companies are beginning to consider cybersecurity as a big business risk, as they are looking for methods to ensure the continuity of their financial operations in the event of a cyberattack. A study by the Ponemon Institute revealed an average corporate loss of $9.4 million due to cyber incidents (Marotta et al., 2017).

Another relevant aspect with regard to insurance is that cyber risks can affect insurance companies in two fundamentally different ways. First, insurance companies' heavy dependence on technological infrastructure makes them extremely vulnerable to cyber risks. Second, writing a cyber risk policy seems an attractive business opportunity for insurance companies (cyber risk guarantees). Both aspects need to be considered in risk management and insurance company regulation (Eling & Schnell, 2016). However, research on cyber risks is limited; while many papers can be found in the technology domain, a relatively few studies have been conducted in the business and economic fields. In Indonesia, it is now almost certain that companies' dependence on information technology will be increasingly important and necessary, with support from highly developed e-commerce advancements. Thus, one would expect a correlation between these factors and the need for cyber insurance. Insurance companies that provide cyber insurance services to anticipate cyber threats or cyber risks remain few, owing to the very minimal cyber insurance demand in Indonesia. This strongly contradicts the notion that Indonesia is a country that most often experiences cybercrimes.

2. Literature Review

2.1 Cyberattacks

Various types of cyberattacks have been identified by international literature (Samejima, Shimizu, Akiyoshi, & Komoda, 2016):

a. A disturbing attack between two communications. Every message from source A to source B is attacked before they reach their destination. This attack consists of unauthorized access to sensitive information or allows for information changes before the message reaches its target.
b. Brute force attacks. These consist of repeated attempts to gain access to protected information such as keywords. If the correct keyword is found, then the information can be accessed.
c. Distributed denial of service (DDoS). This attack fills the victim's server with commands, thus disabling its operations.
d. Malware. This is a generic term describing a type of malicious software used by an attacker to compromise data confidentiality, availability, and integrity. The most common types of malware are viruses, worms, trojans, spyware, ransomware, adware, and scareware/rogueware.
e. Phishing. This method aims to steal personal information from a user by masquerading as a trusted source, such as a website.
f. Social engineering. This is a general term for techniques used to gain unauthorized access to information through human interaction.

2.2 Cyber insurance

Cyber insurance products have several provisions to indemnify parties exposed to cyber risks:

a. Problems with devices or virus-infected hardware or attacks or DDoS
b. Losses to third parties caused by virus-infected mails, downloaded documents, or links clicked on websites.

These products do not provide compensation (damages) to the insured if the loss was self-inflicted or if access to the website was not secure (Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukhan, 2013; Eling & Schnell, 2016).

2.3 SWOT analysis

SWOT analysis is a method for evaluating and positioning environmental resources within a region in the form of strengths, weaknesses, opportunities, and threats (De Smidt & Botzen, 2018). Strengths and weaknesses are internal (controlled) factors that respectively support and hamper organizations to achieve their missions. Meanwhile, opportunities and threats are external (uncontrollable) factors that empower employees in pursuit of their mission or sacrifice them for it, respectively. By identifying the factors in these four areas, organizations can be more engaged in decision-making, planning, and strategy development (as stated in Fig. 1) [11].

2.4 Importance-performance analysis

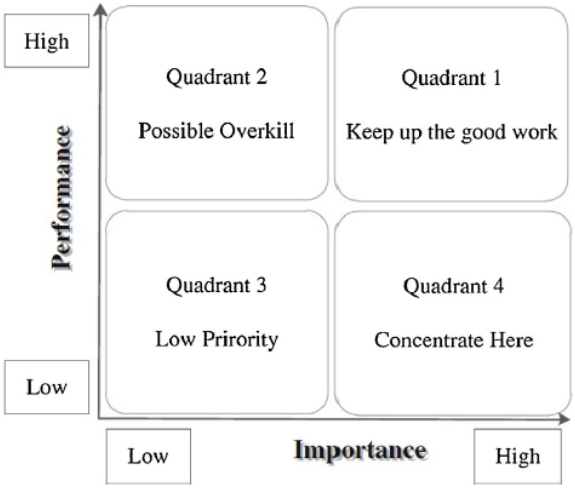


Fig. 1 Importance-performance analysis (IPA) matrix (Hosseini & Bideh, 2013).

The figure 1 displays the following:

a. Quadrant 1 attributes are very important for customers, and the company provides a high level of performance. Thus, the attributes in this quadrant are seen as the company's main strengths and opportunities to achieve or sustain competitive advantage.
b. Quadrant 2 attributes, while unimportant to the customer, are provided by the company at a high level. In this case, companies should look for incoming resources for attributes in the inner quadrant.
c. Quadrant 3 contains attributes with low purpose and serves as a minor factor. Therefore, this quadrant does not show many priorities for improvement.
d. Quadrant 4 attributes are very important for the customer, but the firm's performance level is quite low. These attributes are deemed major weaknesses requiring immediate attention.

3. Methodology

3.1 Type of research

This type of research is descriptive. The descriptive method involves fact-finding and making the right interpretation. Descriptive studies focus on social problems as well as procedures applicable in certain communities and situations, including relationships, activities, attitudes, views, and ongoing processes as well as the effects of a phenomenon.

3.2 Operational definitions

The operational definitions of this research are as follows:

1. "Potentials" are internal company conditions that refer to the strengths of insurance companies in Indonesia.
2. "Constraints" are internal conditions within the company that indicate weaknesses that may prevent Indonesian insurance companies from running a cyber insurance service.
3. "Opportunities" are external conditions pertaining to prospects that Indonesian insurance companies can take advantage of to help them achieve their business objectives.
4. "Threats" are external conditions that describe factors that can obstruct the business operation of insurance companies in Indonesia.
5. "Strategy" refers to various strategies or policies undertaken by the insurance company to achieve their business objectives using their existing potential and minimizing their constraints.

3.3 Data types and data sources

The types and sources of data used in this study are the following:

1. Primary data. This is data obtained from the first source, either individual or group, which is the object of this research. Primary data is obtained through direct interviews with respondents, which, in this case, are underwriters in an insurance company with cyber insurance products.
2. Secondary data. This refers to readily available data from various studies and references such as journals, articles, and Web sites. These data contain information related to the issues discussed in this study.

3.4 Data collection methods

The data collection methods used in this study are as follows:

1. Interviews. These were conducted by asking questions to respondents or resource persons, namely underwriters of insurance companies. The questions raised are related to the research topic, in this case the potential and constraints of cyber insurance development in Indonesia.
2. Documentation. The collected data consisted of information on cyber insurance growth in some developing countries. In addition, review information or data were sourced from books, journals, and Internet searches on insurance to study their rationales and problem-solving methods.

3.5 Technical analysis

The data analysis technique used in this research is qualitative descriptive analysis. This involves processing qualitative data that has been obtained through a simple representation of facts or characteristics. This study

specifically used SWOT analysis, which is the systematic identification of various factors to formulate a strategy. A company's strategic decision-making process is always related to its development, mission, goals, strategy, and policy. From the SWOT analysis results, one can then see the potentials and constraints of cyber insurance development in Indonesia. These potentials include strengths and opportunities while constraints include weaknesses and threats. The data analysis tools used were the Internal Factor Evaluation (IFE) Matrix, the External Factor Evaluation (EFE) Matrix, the SWOT diagram, and the SWOT matrix.

4. Results and Discussion

A company takes advantage of its internal and external conditions for overall development, and it cannot be separated from the understanding of its internal and external environment. Based on the results of interviews conducted with several cyber insurance actuaries and marketing officers in an insurance company, along with the literature review, the authors identified internal and external factors in the following table:

Internal Factors	External Factors
Strengths	Opportunities
1. Insurance companies with cyber insurance products remain few. 2. Cyber insurance will be purchased by IT companies with middle to upper incomes.	1. Daily activities that use technology will be developed. 2. Many law and IT graduates can be involved in creating cyber insurance products so that it opens employment opportunities.
Weakness	Threats
1. Human resources and quality are still limited. 2. Coverage costs are large; thus, premium value is high. 3. Only a few agents have knowledge of cyber insurance. 4. Cyber insurance is only used by IT-based companies.	1. There are several competitors from the insurance industry abroad. 2. IT-based companies lack an understanding of cyber insurance. 3. There are no specific protection laws.

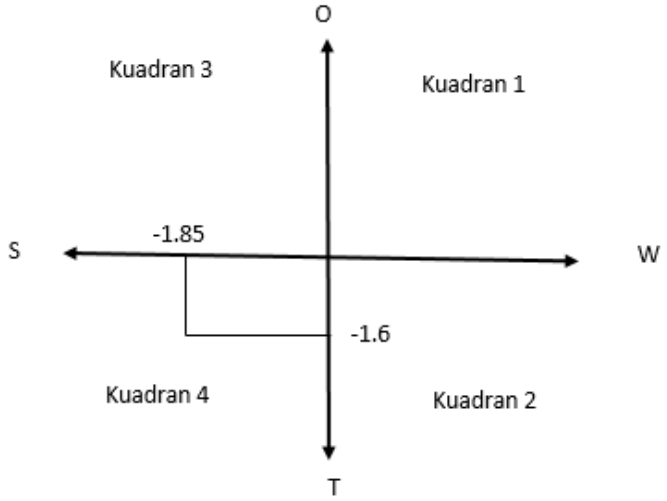
The internal environment (S-W) can be identified using the IFE Matrix approach as in the following table:

Internal Factors	Weight	Rating	Weight × Rating
Strengths			
1. Insurance companies with cyber insurance products remain few.	0.6	1	0.6
2. Cyber insurance will be purchased by IT companies with middle to upper incomes.	0.4	2	0.8
Total Strength Score			1.4
Weaknesses			
1. Human resources and quality are still limited.	0.2	3	0.6
2. Coverage costs are large; thus, premium value is high.	0.4	4	1.6
3. Only a few agents have knowledge of cyber insurance.	0.25	3	0.75
4. Cyber insurance is only used by IT-based companies.	0.15	2	0.3
Total Weakness Score			3.25
Difference (Strength –Weakness)	**−1.85**		

The external environment (O-T) can be identified through the EFE approach as follows:

External Factors	Weight	Rating	Weight × Rating
Opportunities			
1. Daily activities that will use technology will be developed.	0.6	2	1.2
2. Many law and IT graduates can be involved in creating cyber insurance products so that it opens employment opportunities.	0.4	1	0.4
Total Opportunity Score			**1.6**
Threats			
1. There are several competitors from the insurance industry abroad.	0.3	3	0.9
2. IT-based companies lack an understanding of cyber insurance.	0.45	4	1.8
3. There are no specific protection laws.	0.25	2	0.5
Total Threat Score			**3.2**
Difference (Opportunity–Threat)	**−1.6**		

The SWOT diagram was used to show the strategy analysis by looking at a company's opportunities and threats relative to its strengths and weaknesses to get a glimpse of its position among competition. The diagram shows its business position in four quadrants. The results of the comparison between internal analysis (strengths and weaknesses) and external analysis (opportunities and threats) based on the processed data are as follows:



The data analysis results indicate that the existence of cyber insurance in Indonesia is in Quadrant 4, where both internal and external environments have bad weight values. Hence, it can be concluded that cyber insurance in Indonesia requires utmost attention.

5. Conclusion

Based on the SWOT analysis results, we can conclude the following:

1. The potential of insurance companies to have a cyber insurance product remains small, and cyber insurance will be purchased by upper- to middle-class IT companies.

2. Constraints to the existence of cyber insurance continue to be limitations in human resources and quality, high premiums caused by large coverage costs, the insufficient number of agents with cyber insurance knowledge, and cyber insurance being used only by IT companies.
3. After identifying internal and external factors and conducting SWOT analysis, the existence of cyber insurance in Indonesia is found to be in Quadrant 4. Thus, the appropriate strategy is to educate IT-based companies on the importance of cyber insurance.

References

Bendovschi, A. (2015). Cyber-attacks–trends, pattern and security Countermeasures. *Procedia Economics and Finance*, 28, 24–31.

Eling, M., & Schnell W. (2016). What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance*,*17*(5),474–491.

Hosseini, S., & Bideh, A. (2013). A data mining approach for segmentation-based importance- performance analysis (SOM–BPNN–IPA): a new framework for developing customer retention strategies. *Service Business*, *8*(2): 295–312.

Hughes, B., Bohl, D., Irfan, M., Margolase, E., & Solorzano, J. (2017). ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance. *Technological Forecasting and Social Change*, *115*, 117–130.

Marotta, A., Martinelli, F., Nanni, S., & Orlando, A., & Yautsiukhin, A. (2017) Cyber-insurance survey. *Computer Science Review*, 24, 35–61.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not?. *Decision Support System*, 56,11–26.

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329–340.

Phadermrod, B., Crowder, R. M., & Wills, G. B. (2019). Importance-performance analysis based SWOT analysis. *International Journal of Information Management*, *44*, 194–203.

Samejima, M., Shimizu, Y., Akiyoshi, M., & Komoda, N. (2006, August). SWOT analysis support tool for verification of business strategy. In *2006 IEEE International Conference on Computational Cybernetics* (pp. 1–4). IEEE.

De Smidt, G., & Botzen, W. (2018). Perception of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 239–274.