Journal of
Value Creating in Business Management
https://www.jvcbm.ir

Volume 4, Issue 1, Spring 2024, Pages 39 to 70

Research Paper (Qualitative)

eISSN: 2980-8359

Designing a cyber insurance implementation model using foundational data theory

Behzad Esmaeilifar[1], **Manouchehr Ansari**[2]

1- PhD student, Department of Business Administration, Alborz Campus of Tehran University, Tehran, Iran
2- Associate Professor, Department of Business Administration, Faculty of Management, University of Tehran, Tehran, Iran

Receive:
01 April 2023
Revise:
29 May 2023
Accept:
12 August 2023

Keywords:
cyber insurance,
cyber knowledge,
data safety and security,
cyber insurance marketing,
insurance attitude

Abstract
The aim of the current research is to identify the factors affecting the implementation of cyber insurance among insurance companies in Iran. The current research is developmental and applicable in terms of its purpose, and is of qualitative methods .The statistical population of the research is specialists and experts in the field of cyber insurance, who have been identified using the snowball sampling method. Using the interview technique, the data was collected and then the data and categories were coded and classified using the MAXQDA software version 2020. The reliability of the research was measured using the Kappa coefficient. In the last stage, the research model is extracted based on the Strauss and Corbin model. Based on the results of the research, the causal factors were divided into scientific, technical, and network indicators. Insurance perspective with the title of intervening factor, analysis of the external and internal environment as well as marketing and paying attention to the executive arms as foundational factors, ecosystem approach and formulation of insurance strategy as a solution, and finally increasing the level of knowledge of the insurance company, safety and security of data, improvement of services and company income, and uncertainty about the operation of insurance are known as positive and negative consequences of cyber insurance.

Please cite this article as (APA): Esmaeilifar, B., & Ansari, M. (2024). Designing a cyber insurance implementation model using foundational data theory. *Journal of value creating in Business Management*, *4*(1), 39-70.

https://doi.org/10.22034/jvcbm.2024.406060.1135

Publisher: Iranian Business Management Association

Corresponding Author: Manouchehr Ansari

Email: mansari@ut.ac.ir

Journal of
Value Creating in Business Management
https://www.jvcbm.ir
Volume 4, Issue 1, Spring 2024, Pages 39 to 70

Extended Abstract

Introduction

With the emergence of the Internet and related information networks, people's need to use Internet and electronic services has also increased (Kshetri et al, 2020) and has changed the economic, social and cultural aspects of humans (Wang et al. et al., 2019). With the expansion of the Internet in the business of organizations, a space called cyber was created, which boosted business activities and interactions (Swiss Re, 2014; Chief Risk Officers Forum, 2014). On the other hand, the expansion of virtual spaces increased the concern of the managers of Internet companies. The risks caused by cyber-attacks and the care of data and privacy of people caused managers to consider themselves responsible for not properly monitoring the company (Uuganbayar et al, 2020). Furthermore, the emergence of various softwares, the risk of information theft in cyberspace, intrusion into individual lives and sometimes government systems has increased, and such a situation has jeopardized information security (Kshetri et al, 2020). Until now, in Iran, specific and comprehensive coverage for cyber risk has not been provided, and the main reasons for not providing it by insurance companies can be attributed to the lack of information and technical knowledge in the field of providing the plan, the lack of knowledge of these organizations about this type of insurance coverage, and also, lack of sufficient financial transparency on the part of companies applying for such insurance policies. In this regard, the aim of the research, considering the fact that there has not been a comprehensive research on the implementation of cyber insurance in Iran, is to investigate the effective factors on the successful implementation of cyber insurance in Iran and extract a qualitative model using the foundational data theory. Therefore, the main questions of the research will be in line with the data-based theory: How to identify the factors affecting the implementation of cyber insurance in Iran? Besides, the obstacles of cyber insurance as a secondary objective are also examined.

Theoretical framework

Insurance in cyberspace or cyber insurance is an insurance policy that is provided by insurers through creating market incentives and with the aim of improving the internet security environment. For the first time, cyber insurance was invented in the late 1970s in America in connection with the loss of data caused by unauthorized physical access to computer systems in electronic banking (Kshetri et al, 2020). On the other hand, at the same time as the role of the Internet in banking increased, the role of cyber insurance also did so. Cyber insurance focuses on covering losses and negative events caused by electronic risks against possible risks such as "theft of cash", and it can examine losses caused by business interruption (Wanchun et al, 2018), and It also examines the types of events or conditions that may prevent the organization from reaching its goals (Rezakhani & Dadbeh, 2021).

Soleymani Rouzbahani & Hoseini (2016) in their research entitled "Study of crime and security insurance in cyberspace" referring to the rapid growth of technology, the introduction of computers and the use of the Internet and the resulting changes in human life, paid attention to Internet insurance as a tool to deal with the emergence of virtual crimes such as information theft in the world of internet communication.

wang (2019) in his research entitled "Integrated framework for information security investment and cyber insurance" presented an analytical model for optimizing company cyber security and cyber insurance costs based on the effectiveness of costs and with the aim of reducing threats Cyber, vulnerability and effects. This research shows how the participation of the private sector in dealing with cybercrimes can reduce the overall cyber loss and create economic value. At the micro level, the effectiveness of a company's security costs in dealing

with specific cyber threats can be reduced when other related security measures are not implemented.

Methodology

In terms of the purpose of this research, it is developmental and applicable. Based on the method of data collection, it is considered a descriptive research. The method of gathering information is an in-depth interview with experts. This research has a qualitative approach and collects and analyzes data from the data-based theory research strategy (Bahari & Taheri Rouzbahani, 2023).

Research Findings

The causal factors of cyber insurance implementation were placed in three main categories of knowledge, technical factors, and network factors. Two factors "internal and external environment analysis" as well as "marketing and the attention of the executive branches" have been identified as the main components of the foundation. Three main categories with the title of "increasing the knowledge level of insurance companies", "data safety and security", and "improving the company's services and income" have been identified as the main and positive categories; and "uncertainty of the functioning of insurance" as the main and negative ones. By examining the primary codes and central categories of experts' interviews, a main category named "insurance perspective" has been identified as the main category. The existence of a database, the role of the government, insurance attitude, insurance company performance, and insurance regulations are known as central categories. The upcoming obstacles are divided into two main categories: "lack of mastery of the subject", and "lack of government support". By examining the extracted codes from the interviews of cyber insurance experts, two main components of "ecosystem approach" and "insurance strategy formulation" were identified as cyber insurance strategies.

Conclusion

The research results were based on the Strauss and Corbin model. 5 indicators influencing the successful implementation of cyber insurance have been identified, which include the causal factors of cyber insurance, the consequences of implementing cyber insurance, the underlying factors of cyber insurance, hidden and interfering factors, and finally the consequences of implementing cyber insurance (both for insurance companies and for insured companies and organizations). Since there is still no specific definition of the motives of cyber insurance and the services it can cover, the trust of different insurance groups is also weak. Therefore, a single and clear definition of insurance coverage and things outside of insurance coverage can restore trust in insurance organizations. Among related researches, Uuganbayar et al, (2020) has emphasized the single definition of the concept of cyber insurance and the precise definition of the type of coverage. The results have shown that cyber insurance can be influenced by the international environment and vice versa. In the meantime, cultural factors and society's insight into this type of insurance, economic fluctuations resulting from currency challenges, the political stability of the country, and the economic status of society are known as environmental factors affecting cyber insurance. Based on the results of the research, the two central components of the external and internal environment should be recognized as factors of cyber insurance platforms. These factors take into account the technical equipment and cyber infrastructural readiness level, and include hardware capability, software factors, tool power or strength, information content, information technology, human factors, and cyber policies. According to the research results, the consequences of cyber insurance can be divided into two positive and negative sections. In this way, increasing the level of knowledge

of insurance companies and increasing the safety and security of data and improving the services and income of the company are recognized as the main and positive components. The experience of dealing with cyber risks, the way of cyber insurance, knowledge of cyber damages, and finally the growth of cyber insurance are factors that can help to increase the understanding and implementation of cyber insurance. This part of the results is also aligned with the research of Wang (2019). The existence of the database, the government and its policies, the insurance attitude, the performance of insurance companies, and insurance regulations as the central and determining components of the insurance landscape (as the main component), have played the role of interventionist in extractive model of the research. According to the results of the research, the lack of mastery over cyber insurance and the lack of government support are known as the two main obstacles to the implementation of cyber insurance. These factors include the lack of mastery of the subject which is related to the unpredictable environment, knowledge weakness, and statistical weakness; and the lack of government support which is related to government communication protocols and cumbersome government laws. This part of the results can be compared with the research of Bahsi, Franke & Friberg (2020) in which the researchers mentioned the support of the public sector in Norway in the two recent years.