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.

فصل‌نامه ارزش آفرینی در مدیریت کسب وکار
https://www.jvcbm.ir
دوره ۴، شماره ۱، بهار ۱۴۰۳، صفحات ۳۹ تا ۷۰
eISSN: 2980-8359
علمی پژوهشی (کیفی)

طراحی الگوی پیاده سازی بیمه سایبری با استفاده ازنظریه داده بنیاد

بهزاد اسماعیلی فر [۱]، منوچهر انصاری [۲]

۱- دانشجوی دکترای،گروه مدیریت بازرگانی، پردیس البرز دانشگاه تهران، تهران، ایران
۲- دانشیار،گروه مدیریت بازرگانی، دانشکده مدیریت، دانشگاه تهران، تهران، ایران

تاریخ دریافت: ۱۴۰۲/۰۴/۲۴
تاریخ بازنگری: ۱۴۰۲/۱۰/۲۴
تاریخ پذیرش: ۱۴۰۲/۱۱/۲۴

کلید واژه‌ها:
بیمه سایبری،
دانش سایبری،
ایمنی و امنیت داده‌ها،
بازاریابی بیمه سایبری،
نگرش بیمه‌ای

چکیده

هدف پژوهش حاضر شناسایی عوامل مؤثر بر پیاده‌سازی بیمه سایبری در بین شرکت‌های بیمه در کشور ایران است. پژوهش حاضر از لحاظ هدف، داده بنیاد است و از نوع روش‌های کیفی است. جامعه آماری پژوهش متخصصان و خبرگان در زمینه بیمه سایبری است که با استفاده از روش نمونه‌گیری گلوله‌برفی مشخص شده‌اند. با استفاده از تکنیک مصاحبه، داده‌ها جمع‌آوری شده و سپس با استفاده از نرم‌افزار MAXQDA نسخه ۲۰۲۰ داده‌ها و مقوله‌ها کدگذاری و طبقه‌بندی شده‌اند. پایایی پژوهش با استفاده از ضریب کاپا اندازه‌گیری شده است. در مرحله آخر مدل پژوهشی بر اساس مدل اشتراوس وکوربین استخراج شده است. بر اساس نتایج پژوهش عوامل علی به شاخص‌های دانشی، فنی و شبکه تقسیم شدند. چشم انداز بیمه‌ای با عنوان عامل مداخله‌گر، تجزیه و تحلیل محیط بیرونی و درونی و همچنین بازاریابی و توجه به بازوهای اجرایی به عنوان عوامل بسترساز، رویکرد اکوسیستمی و تدوین استراتژی بیمه‌ای به عنوان راهکار و نهایتاً افزایش سطح دانش شرکت‌های بیمه، ایمنی و امنیت داده‌ها، بهبود خدمات و درآمد شرکت و عدم اطمینان از کارکرد بیمه به عنوان پیامدهای مثبت و منفی بیمه سایبری شناخته شده‌اند.

لطفاً به این مقاله استناد کنید (APA): اسماعیلی فر، بهزاد، انصاری، منوچهر. (۱۴۰۳). طراحی الگوی پیاده سازی بیمه سایبری با استفاده ازنظریه داده بنیاد. *فصلنامه ارزش آفرینی در مدیریت کسب و کار*. (۱)۴. ۳۹-۷۰.

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

ناشر: انجمن مدیریت کسب و کار ایران

نویسنده مسئول: منوچهر انصاری
ایمیل: mansari@ut.ac.ir

مقدمه

با پیدایش اینترنت و شبکه‌های اطلاع رسانی وابسته به آن، نیازمندی مردم برای استفاده از خدمات اینترنتی و خدمات الکترونیکی نیز بیشتر شده (Kshetri et al, 2020) و عصر توزیع اطلاعات را همچون انقلاب صنعتی به وجود آورده و در نهایت جنبه‌های اقتصادی، اجتماعی و فرهنگی انسان را تغییر داده است (Wang et al, 2019). توسعه فناوری اینترنت رفتارها را تغییر داده و تجارب خرید را به طور گسترده‌ای کارآمدتر، شفاف‌تر و آسان‌تر کرده است (Rousta, Aallafjafari & Ahmadi, 2023). با این حال فناوری مبتنی بر اینترنت باعث بی‌ثباتی بازار و افزایش گزینه‌های انتخاب شده است (Arabshahi, Abbaszadehgaretekan, 2022). علاوه بر آن به تدریج با گسترش اینترنت در کسب و کار سازمان‌ها، فضایی به نام سایبر به وجود آمد که باعث رونق فعالیت‌ها و تعاملات شغلی شد (Swiss Re, 2014؛ Chief Risk Officers Forum, 2014). فضای سایبری هر شبکه‌ای را توصیف می‌کند که سیستم‌های فناوری اطلاعات را به هم متصل می‌کند و بر اهمیت شبکه‌ها تاکید زیادی می‌کند (Lioyds, 2015). این شبکه‌ها زندگی بشر را وارد مرحله تازه‌ای کرده‌ند و فضای مجازی با «عنوان زندگی دوم» شناخته شده و بر دسترسی سریع اطلاعات و اشتراک‌گذاری داده‌ها تأکید داشته است (Aghabeigi et al, 2023).

از سوی دیگر گسترش فضاهای مجازی، نگرانی مدیران شرکت‌های اینترنتی را بیشتر کرد. خطرات ناشی از حملات سایبری و مراقبت از داده‌ها و حفظ حریم خصوصی افراد باعث شد تا مدیران خود را مسئول عدم نظارت صحیح بر شرکت بدانند (Uuganbayar et al, 2020). علاوه بر آن پیدایش نرم‌افزارهای مختلف، ریسک سرقت اطلاعات در فضای سایبری، نفوذ به زندگی‌های فردی و گاه سامانه‌های دولتی بیشتر شده و چنین وضعیتی امنیت اطلاعاتی را به خطر انداخت (Kshetri et al, 2020). وابستگی زیاد سازمان‌ها به دارایی‌ها و اطلاعات شبکه‌ای کامپیوتری، ریسک حملات اینترنتی و ضرر حاصل از آن را بالا برده و تبدیل به یک تهدید جدی برای کاربران شده است (Adibi, Daryayi & Zahdi, 2017) با درنظر گرفتن این نکته که این نوع ریسک تنها یکی از انواع ریسک‌های سایبری است (Alizadeh et al,2023).

به منظور پیدا کردن راهی برای کاهش ریسک سایبری بیمه سایبری به وجود آمد (Poorghasab & Hasani, 2017). مدیریت ریسک از طریق بیمه با انتخاب روش‌های مناسب برای برخورد با ریسکهای جدید سعی می‌کند رشد اقتصادی خدمات را بالابرده و سهم بازار خود را افزایش دهند (Mahmoudi & Pourshahabi, 2023). بیمه سایبری پوششی برای خسارات و پیشامدهای ناگوار ناشی از ریسک‌های الکترونیکی فراهم می‌کند (Wanchun et al, 2018)، بیمه نامه‌ای است که از طرف بیمه‌گرها برای هماهنگی انگیزه‌های بازار به منظور بهبود فضای امنیت اینترنتی ارائه می‌شود (Kshetri et al, 2020) و باعث افزایش سرمایه‌گذاری با سطح امنیت بالاتر برای زیر ساخت‌های فناوری اطلاعات خواهد شد (Wanchun et al, 2018).

بیمه اینترنت ابزاری مهم برای امنیت اینترنتی است و شرکت‌های بیمه‌گذار همراستا با پیشرفت در زمینه فضاهای مجازی سعی در تطبیق خود با این پیشرفت‌ها و ایجاد بیمه نامه‌های گوناگون در راستای کاهش، جبران خسارات کاربران و مدیریت آن‌ها نموده‌اند (Soleymani Rouzbahani & Hoseini, 2016).

با این وجود امنیت سایبری تحت تأثیر حملاتِ سایبریِ موفقیت آمیز، کاهش یافته است Internet Security Report, (2018). این افزایش حملات را می‌توان به عوامل متعددی مانند افزایش اتکای کسب و کار و جامعه به سیستم‌های فناوری اطلاعات، رشد سریع دستگاه‌های پایانی متصل به هم[1]، عدم آگاهی امنیتی و بلوغ دنیای جرائم سایبری نسبت داد (Cisco, 2017؛ Homoliak et al, 2019). ریسک به عنوان بخش جدایی ناپذیر از تمامی فعالیت‌های تجاری درنظر گرفته می‌شود که مدیریت آن به عنوان یک وظیفه اصلی بنگاه‌های تجاری شناخته می‌شوند (Mahmoudi & Pourshahabi, 2023).

چنین نگرانی‌هایی مدیران ارشد را به تأمل وا داشت که خطرات امنیت سایبری را از مهم‌ترین چالش‌های شرکت‌ها و سازمان‌های خود بدانند (Uuganbayar, Yautsiukhin, Martinelli & Massacci, 2020). همچنین مطالعات نشان می‌دهد بیمه سایبری در محاسبه ریسک با چالش‌های بیشتری مواجه است؛ زیرا برخی صنایع و خدمات دارای ریسک مشخصی هستند که تا حدی قابل محاسبه است این در حالی است که در حوزه سایبر به دلیل عمر کوتاه آن و سرعت توسعه شناسایی ریسک سخت‌تر خواهد بود (Wanchun et al, 2018). به علاوه عدم درک بیمه فضای مجازی و عدم افشاسازی ضرر و زیان‌های اینترنتی ناشی از ویروس و هکرها به منظور پنهان کردن ضغف شرکت‌ها، باعث بروز پنهان کاری، کاهش داده و آمارهای دقیق برای صنعت بیمه سایبری شده است (Kshetri et al, 2020). با اینکه نتایج پژوهش بینش‌های کلی درباره ترکیب بازار، انگیزه‌های بازیگران، ابهام درباره پوشش بیمه و دستورالعمل‌های مربوط به رویه‌های عمومی حفاظت از داده‌ها و امنیت اطلاعات و شبکه می‌دهد، اما همچنان پژوهش‌های تجربی درباره بیمه سایبری اندک است (Hajizadeh et al, 2023).

در ایران از جمله چالش‌های بیمه سایبری این است که استانداردهای جهانی جدی گرفته نمی‌شود؛ به خصوص در حوزه مالکیت معنوی که تاکنون به رسمیت شناخته نشده است و تلاش بر استفاده رایگان از نسخه‌های مختلف وجود دارد. در این صورت از آن‌جا که ممکن است نسخه دریافتی اصل نباشد امکان هک و نفود افزایش می‌یابد. به طور مثال اگر چه بانک‌ها تلاش می‌کنند از آنتی ویروس استاندارد استفاده کنند اما از آنجا که ویندوزها استاندارد و اصل نیستند امکان حملات و نفوذ سایبری افزایش می‌یابد. ارزیابی ریسک و تعیین خسارت در فضای سایبر با فضای فیزیکی کاملاً متفاوت است زیرا در واقع حق بیمه درصدی از ارزش چیزی است که بیمه می‌شود و بنابراین بیمه دیتا از قواعد خاص خود پیروی می‌کند. همچنین ورود بدافزارها و باج افزارها به عنوان تهدیدات سایبری سیستم‌های رایانه‌ای روبه افزیش است (ISNA, 2022). اطلاعات دقیقی از میزان حملات سایبری و خسارت‌هایی که اینگونه اقدام‌ها بر اقتصاد کشور دارد، دردسترس نیست و البته همان تعداد باعث خسارتهای کلان مالی می‌شود (taadolnewspaper, 2017, 2018). بر اساس گزارش‌های رسمی در ایران، بودجه‌ای برای کسب و کارهای اینترنتی که خسارت دیده‌اند اختصاص نیافته است (tahlilbazaar.com, 2021).

این در حالی است که شرکت‌های بیمه سایر کشورها حتی در منطقه آسیای میانه، کشورهای حوزه خلیج فارس و ... با اجرای طرح‌های نو آورانه همچون بیمه سایبری، به سرعت در حال پیشرفتند. تاکنون در کشور ایران به‌صورت مشخص و جامع، برای ریسک سایبری پوشش خاص و منسجمی ارائه نشده که عمده علل عدم ارائه آن ازسوی شرکت‌های بیمه را

1 interconnected end devices

می‌توان به نبود اطلاعات و دانش فنی در حوزه ارائه طرح، عدم شناخت این سازمان‌ها از این نوع پوشش بیمه‌ای و نیز عدم وجود شفافیت مالی کافی از سوی شرکت‌های متقاضی این گونه بیمه‌نامه‌ها مربوط دانست. این امر سبب شده که رشدی که این بخش در کشورهای پیشرفته ایجاد کرده، متاسفانه در کشور ایران محقق نشود. در این راستا هدف پژوهش، با توجه به این نکته که پژوهش جامعی درباره اجرای بیمه سایبری در ایران نشده است، بررسی عوامل مؤثر بر اجرای موفقیت آمیز بیمه سایبری در ایران و استخراج مدل کیفی با استفاده از نظریه داده بنیاد است. بنابراین پرسش اصلی تحقیق در راستای نظریه داده‌بنیاد خواهد بود: شناسایی عوامل مؤثر بر پیاده سازی بیمه سایبری در ایران چگونه است؟ ضمن اینکه موانع بیمه سایبری به عنوان یک هدف فرعی نیز مورد بررسی قرار گرفته است.

مبانی نظری

بیمه سایبری

بررسی ادبیات بیمه سایبری نشان می‌دهد تعاریفی که از این نوع بیمه شده است طیف مختلفی از خدمات را پوشش می‌دهد. بیمه در فضای مجازی یا بیمه سایبری[1]، بیمه نامه‌ای است که از طرف بیمه‌گرها از راه ایجاد انگیزه‌های بازار و با هدف بهبود فضای امنیت اینترنتی ارائه می‌شود. برای نخستین‌بار بیمه سایبری در اواخر ۱۹۷۰ در آمریکا در ارتباط با از بین‌رفتن داده‌هایی که به واسطه دسترسی فیزیکی غیر مجاز به سیستم‌های کامپیوتری در بانکداری الکترونیکی بوجود آمد، ابداع شد (Kshetri et al, 2020). از سوی دیگر همزمان با افزایش نقش اینترنت در بانکداری، نقش بیمه سایبری نیز بیشتر شد. بیمه سایبری بر پوشش خسارات و پیشامدهای منفی ناشی از ریسک‌های الکترونیکی در مقابل خطرات احتمالی همچون (سرقت وجوه نقدی) توجه دارد، می‌تواند زیان‌های ناشی از توقف کسب و کار را بررسی کند (Wanchun et al, 2018) و همچنین انواع رویدادها یا شرایطی که ممکن است سازمان را از رسیدن به اهدافش باز دارد، بررسی می‌کند (Rezakhani & Dadbeh, 2021).

سابقه بیمه سایبری نشان می‌دهد ریسک‌هایی که در قالب یک بیمه (عمومی) یا بیمه نامه‌های مختلف (خاص)، تحت پوشش بیمه سایبری قرار گیرد شامل خطر از دست دادن داده با توجه به تهدیدها و اقدامات خرابکاری، کرم‌ها و ویروس‌ها و به‌روز نبودن نرم‌افزارها (Kshetri et al, 2020)، خسارت بازسازی با توجه به تأمین مالی هزینه‌های بازسازی شامل خرید و نصب دستگاه‌های تخریب شده یا معیوب، به روز رسانی سامانه، خرید و راه اندازی نرم افزارهای امنیتی، پرداخت خسارت به مشتریان و زیان دیدگان ثالث (Friedman, 2017؛ Adibi, Daryayi & Zahdi, 2017) و نهایتاً خسارت به مالکیت فکری که می‌تواند به صورت شخص اول (همچون نقض حق کپی رایت، علائم تجاری، نقض حق اختراع) و شخص ثالث باشد (همچون خسارت ناشی از نشر، پخش، توزیع، اجرا، نمایش و پخش کابلی، رادیویی) (Elsan,,2021). وانچون عقیده دارد پوشش‌های بیمه سایبری شامل مسئولیت محتوای وب، مسئولیت حرفه‌ای، مسئولیت امنیت شبکه‌ای شخص ثالث، زیان دارایی اطلاعات و غیرقابل لمس، زیان ناشی از درآمد الکترونیکی، اخاذی سایبری و تروریسم سایبری است (Wanchun et al, 2018).

1 Cyber Insurance

بررسی واژه سایبر نیز نشان می‌دهد که واژه سایبر[1] به دو مفهوم "واقعیت مجازی" و"شبکه‌های ارتباطی الکترونیکی" اشاره دارد و ریسک‌های ناشی از آن نیز با سایر خطرها و ریسک‌های متداول متفاوت است (Eling & Schnell, 2016)؛ بدین معنا که ریسک سایبری در مقایسه با خطر تروریسم، کاربرد بیشتری دارد و می‌تواند از مجموعه زیادی از داده‌ها در بازار بیمه حمایت کند (Tonn et al, 2019). ریسک سایبری بر ماهیت نامشهود و در نتیجه مشکلات در ارزیابی زیان‌ها تأکید می‌کند و شبکه‌ها با ارتباط نزدیکی که با فضای مجازی دارند اغلب مترادف با اینترنت استفاده می‌شود (Eling & Schnell, 2016).

سبولا و یانگ ریسک‌های سایبری را به عنوان "ریسک‌های عملیاتی در برابر دارایی‌های اطلاعات و فناوری" تعریف می‌کند که بر محرمانگی، در دسترس بودن، یا یکپارچگی اطلاعات یا سیستم‌های اطلاعاتی تأثیر می‌گذارد (Cebula & Young, 2010). به طور مشابه، انجمن ملی کمیسیون بیمه سرقت هویت، افشای اطلاعات حساس و وقفه در تجارت را به عنوان نمونه‌هایی از خطر سایبری فهرست می‌کند (National Association of Insurance Commissioners, 2013) . سایر پژوهشگران، فقط یک نوع خاص از خطرات سایبری مانند نقض داده‌ها را بررسی می‌کنند (Böhme & Kataria, 2016). برخی همچون (Mukhopadhyay et al, 2013) انگیزه مهاجم را مورد بررسی قرار می‌دهند و فقط بر روی رویدادهای مخرب تمرکز کرده‌اند. در یک طبقه‌بندی دیگر، ریسک‌های سایبری[2] را می‌توان بر اساس فعالیت (به عنوان مثال، مجرمانه و غیر مجرمانه)، نوع حمله (به عنوان مثال، بدافزار، حمله خودی، هرزنامه، انکار سرویس توزیع شده)، و منبع (به عنوان مثال، تروریست‌ها، مجرمان، دولت) تقسیم کرد. در این نوع نگرش به ریسک، حملات عمدتاً به هدف خرابکارها بستگی دارد. این‌گونه فعالیت‌ها توسط اثرات شبکه (به عنوان مثال، کرم‌ها) تقویت می‌شوند. در نهایت، با توجه به پیامدهی حمله سایبری و با در نظر گرفتن هدف مهاجمان[3] (به عنوان مثال، جاسوسی، خرابکاری، اخاذی و بهره‌برداری از اطلاعات)، حمله ممکن است در دسترس بودن خدمات فناوری اطلاعات، یکپارچگی و محرمانه بودن داده‌ها را به خطر اندازد و باعث زیان مالی، آسیب به شهرت و وقفه در تجارت و حتی آسیب به انسان شود (Eling & Schnell, 2016).

این‌گونه حملاتِ سایبری خطری جدی برای خدمات‌دهی شرکت‌ها هستند و عاملی برای توجه بیشتر به بیمه سایبری بوده‌اند. به عنوان مثال در فوریه سال ۲۰۰۰ یک سری حملات هماهنگ[4] بر علیه شرکتهای آمریکایی همچون یاهو[5]، ای‌بی[6]، بای[7]، سی‌ان‌ان[8]، آمازون[9] و دیگر شرکت‌ها انجام شد.[10] علاوه بر این حملات، مجرمان اینترنتی اقدام به بدشکل

[1] Cyber
[2] Cyber Risk
[3] Attackers
[4] Denial - of - service (DOS)
[5] yahoo.com
[6] ebay.com
[7] buy.com
[8] CNN.com
[9] Amazon.com
۱۰- حملات داس، منابع کامپیوتر را برای کاربران غیر قابل استفاده می‌کند. اگر چه ابزارهای اجرا، انگیزه‌ها و اهداف حملات داس ممکن است متنوع باشد اما عموماً شامل تلاش‌های هم جهت از جانب فرد یا افرادی است برای جلوگیری از فعالیت یک سایت به صورت کارا یا از کار انداختن آن به صورت موقت یا نا محدود. این افراد عموماً سایت‌هایی را هدف گذاری می‌کنند که ارئه کننده خدمات به افراد زیادی باشد، نظیر بانک‌ها و ...

کردن سایت‌ها، حملات فیشینگ، دزدی شناسه و ورود غیر مجاز به کامپیوترها نمودند. سه حمله کرمی خطرناک در فاصله سه ماه پیرامون ۹/۱۱ به نام‌های کد رد[1] در جولای ۲۰۰۱، نیمدا[2] در سپتامبر ۲۰۰۱ و کلز[3] در اکتبر ۲۰۰۱ کرم اینترنتی اسلمر[4] نیز در ژانویه ۲۰۰۳ منتشر شد.

علاوه بر آن در ابتدای سال ۲۰۱۱، یک حمله اینترنتی شدید به شرکت سونی صورت گرفت که در ابتدای کار زیانی برابر ۱۰۰ میلیون دلار به حساب‌های مشتریان برآورد شد؛ هرچند شرکت سونی بیان کرد ضرر نهایی به شرکت، بالغ بر ۲۰۰ میلیون دلار خواهد بود. اما چالش قابل توجه در این زمان این بود که شرکت سونی فقط برای خسارت‌های قابل مشاهده همچون خسارت به دارایی‌ها بیمه خریده بود و نه برای اتفاق‌های اینترنتی. چنین اتفاق‌هایی باعث شد تا تقاضا برای محصولات بیمه فضای مجازی افزایش پیدا کند. به‌دنبال حملات سایبری و در نتیجه نیاز به کمتر کردن خسارت، شرکت‌های بیمه شروع به ارائه این خدمات به مشتریان نمودند (Kshetri et al, 2020). در این بین تحقیقاتی هم برای شناخت بیشتر عوامل تهدید اینترنتی نیز انجام گرفت. به عنوان مثال گزارش مرکز ایمنی اینترنت دانشگاه کانبرا، عوامل مؤثر بر تهدیدها و حمله‌های الکترونیکی را شامل ۱. بهره‌برداری از سیستم عامل نادرست پیکربندی شده، ۲. بهره‌برداری از سیستم عامل نادرست پیکربندی شده، ۳. نرم افزارهای اصلاح نشده[5] یا محافظت نشده، ۴. آموزش ناکافی کارکنان، ۵. فرهنگ امنیت سازمانی ضعیف، ۶. نبود فناوری‌های امنیتی، ۷. دسترسی از راه دور و/یا اتصال به سیستم‌های فناوری اطلاعات، ۸. سطوح ناکافی امنیت شبکه‌های کامپیوتری شخص سوم دانسته است (Centre for Internet Safety at the University of Canberra, 2013).

با این حال به‌کارگیری موفق بیمه‌های الکترونیک، بدون توجه به زیرساخت‌هایی مانند حفاظت از حریم خصوصی افراد، تعقیب جرائم رایانه‌ای، ایجاد و تقویت مراجع سنجش اعتبار و سندیت قانونی کردن امضای دیجیتالی، پشتیبانی و وجود افراد متخصص در شرکت‌های بیمه‌ای، طراحی کاربرپسند پروفایل و وبسایت‌های بیمه‌ای، استفاده از شبکه‌های اجتماعی برای پشتیبانی‌ها و اطلاع رسانی امکان پذیر نیست (Kabourati, 2019). با این حال روند بیمه سایبری نشان می‌دهد نهادهای بیمه به گونه‌ای تغییر می‌کنند که به نفع رشد بازار بیمه سایبری خواهد بود و بسیاری از چالش‌های کنونی به احتمال زیاد با راه‌حل‌های فناوری جدید و نوآوری‌های فرآیندی برطرف می‌شوند. از آنجایی که بیشتر سازمان‌ها تحت بیمه یا بیمه نیستند، دولت‌ها باید سیاست‌هایی را برای تشویق پذیرش گسترده بیمه سایبری ارائه کنند، به گونه‌ای که شرکت‌ها را برای خرید تشویق کند (Kshetri et al, 2020). از سوی دیگر تلفات سایبری نیز ممکن است یک اثر توزیعی چند دوره‌ای داشته باشد. همچنین در حالی که ممکن است برخی معیارهای امنیتی فقط یک دفعه هزینه یادگیری را مدنظر قرار دهند، برخی دیگر نیازمند هزینه‌های تعمیر و نگهداری هستند (wang, 2019). در ادامه در پژوهش حاضر از ادبیات پژوهشی بیمه سایبری برای درک بهتر، شناخت و در نهایت طبقه‌بندی بهتر کدهای استخراجی (از مصاحبه) استفاده شده است. در ادامه به روش پژوهش و نحوه گردآوری داده‌ها پرداخته می‌شود.

[1] Code Red.
[2] Nimda
[3] klez.
[4] Slammer
[5] Unpatched

پیشینه پژوهش

(Tsohou et al,2023) در پژوهش خود با عنوان "بیمه نامه سایبری؛ ترکیبی از هنر و روندها و جهت گیری‌های آینده" رشد بازار بیمه نامه سایبری را همراه با ابهام در بعضی از ابعاد آن می‌داند. برای مثال رابطه بین میزان ریسک و پراکندگی جغرافیایی در بحث بیمه نامه سایبری چالش‌هایی را ایجاد می‌نماید. همچنین بسیاری از شرکت‌ها به دلایلی مانند حق بیمه بالا، ابهام در پوشش‌های بیمه نامه و موارد مشابه، تمایلی به خرید بیمه نامه سایبری نشان نمی‌دهند.

(Awiszus et al,2023) در پژوهش خود با عنوان "مدل سازی و قیمت گذاری بیمه نامه سایبری" مروری جامعی می‌کند بر مدلسازی و قیمت گذاری بیمه نامه سایبری که بر پایه توضیحات شفاف و دقیق ریاضی استوار است. نتایج تحقیق بیانگر سه نوع ریسک سایبری است: ریسک خاص، ریسک سیستماتیک و ریسک سیستماتیک سایبری که برای دو مورد اول مدل‌های ریاضی به خوبی جواب می‌دهد ولی برای ریسک سیستماتیک سایبری شرایط پیچیده‌تر هست.

(Baker et al,2023) در پژوهش خود با عنوان "بیمه و شرکت: بیمه نامه سایبری برای باج افزارها" به این نتیجه رسیده‌اند که بیمه سایبری راه کار خوبی برای بازیابی اطلاعات است ولی در عین حال به دلیل تأمین مالی شرکت‌های آسیب دیده می‌تواند انگیزه هکرها به حملات سایبری را افزایش دهد.

(Rezakhani & Dadbeh, 2021) در پژوهش خود با عنوان "نقش حسابرسی داخلی در مدیریت ریسک جامع شرکت‌های بیمه" به اهمیت مدیریت ریسک جامع پرداخته است. نتایج نشان داده است حسابرسی داخلی بر مدیریت ریسک جامع شرکت‌های بیمه در ایران تأثیر مثبت و معناداری دارد. همچنین، متغیرهای کنترلی حمایت مدیران ارشد، آموزش و فرهنگ سازمانی نیز بر مدیریت ریسک جامع تأثیر معناداری دارند. اما، متغیر فناوری فاقد تأثیر معناداری بر مدیریت ریسک جامع در شرکت‌های بیمه است.

(Naldi & Mazzoccoli, 2021) با عنوان "سرمایه‌گذاری بهینه در امنیت سایبری زیر نظر بیمه سایبری برای شرکت‌های چند شعبه‌ای"، پژوهشگران چارچوبی را تنظیم کرده‌اند که در آن هم حق بیمه و هم تأثیر سرمایه‌گذاری‌های امنیتی را برای یک شرکت مستقل -یعنی شرکتی با یک سایت واحد (بدون شعبه)- در نظر می‌گیرند. در این پژوهش سناریوهای مختلفی از جمله مسئولیت کامل، مسئولیت محدود و مسئولیت محدود با فرانشیز را برای شرکت‌های چند شعبه در نظر گرفته شده است. پژوهشگران از تابع احتمال نقض گوردون و لوب[1] به منظور بررسی میزان آسیب‌پذیری مراکز اصلی و بازتاب اثرات تغییر سرمایه‌گذاری‌های امنیتی در سطح امنیتی واقعی استفاده کرده‌اند. پژوهشگران دریافتند که دانش نامطمئن آن‌ها نسبت به آسیب‌پذیری، با وجود تأثیر بر سرمایه‌گذاری، قابل توجه نیست. نهایتاً پژوهشگران پیشنهاد کرده‌اند مدل‌های مستقل دیگری به عنوان مثال با حذف اثر یک طرفه (تنها از شعبه‌ها به سمت مرکز اصلی و نه برعکس) می‌توانند در نظر گرفته شوند.

بررسی پژوهش‌های داخلی و خارجی نشان می‌دهد که در کشور ایران تنها اشاره‌های جزیی به بیمه‌های سایبری و تأثیرات آن بر ایمنی و امنیت داده‌های شرکت‌ها شده است و مطالعات بر بیمه‌نامه‌های الکترونیک، نقص اطلاعات اینترنتی و اثربخشی نیروی انسانی شرکت‌های بیمه تأکید داشته‌اند و تاکنون مدل یکپارچه‌ای از بیمه سایبری ارائه نشده

[1] Gordon & Loeb

است. از این‌رو ضرورت دارد یک مدل جامعی از عوامل و شرایط فراهم‌کننده بیمه سایبری با توجه به محدودیت‌ها و ظرفیت‌های آن ارائه شود. از این‌رو در پژوهش حاضر سعی بر این است تا به این هدف دست یافت.

(Kshetri et al, 2020) در پژوهش خود با عنوان "تکامل صنعت بیمه سایبری: یک تحلیل نهادی" با اشاره به اینکه بازار بیمه سایبری در مرحله زایش است، به این موضوع پرداخته است که چطور مفاهیم ارائه شده توسط صنعت بیمه سایبری در نهادهای رسمی و غیررسمی بر توسعه این نوع بیمه تأثیر گذاشته است. پژوهشگران دریافتند که بیمه سایبری یک ابزار مهم در حال ظهور برای محافظت از سازمان‌ها در برابر خسارت‌های ناشی از حملات سایبری است.

(Bahsi, Franke & Friberg, 2020) در پژوهش خود با عنوان "بازار بیمه سایبری در نروژ" نویسندگان با اینکه به دنبال تشریح بازار بیمه سایبری در کشور نروژ بوده‌اند. نتایج نشان داده است که طرف‌های عرضه کننده بازار بیمه سایبری در کشور نروژ در ۲ سال اخیر افزایش داشته است. رویه‌های عمومی حفاظت از داده‌ها[1] تا به حال توانسته است تأثیر متوسطی بر بازار داشته باشد و توسط بخش عرضه به عنوان یک عامل "باز شدن بحث[2]" بیمه با مشتریان شناخته شود. دستورالعمل امنیت اطلاعات و شبکه[3] نیز تأثیر کم و یا هیچ تأثیری بر بیمه سایبری نروژ نداشته است. آگاهان بر موضوع اشاره کرده‌اند که کشور نروژ از این لحاظ کمترین بلوغ را در بین چهار بازار شمال اروپا دارد.

(wang, 2019) در پژوهش خود با عنوان "چارچوب یکپارچه برای سرمایه‌گذاری امنیت اطلاعات و بیمه سایبری" به ارائه مدل تحلیلی بهینه‌سازی هزینه‌های امنیت سایبری شرکت و بیمه سایبری بر اساس اثربخشی هزینه‌ها و با هدف کاهش تهدیدهای سایبری، آسیب‌پذیری و اثرات پرداخته‌اند. در سطح کلان، این پژوهش نشان می‌دهد که چگونه مشارکت بخش خصوصی در مقابله با جرائم سایبری می‌تواند ضرر کلی سایبری را کاهش دهد و ارزش اقتصادی ایجاد کند. در سطح خرد نیز اثربخشی هزینه‌های امنیتی یک شرکت در مقابله با تهدیدات سایبری خاص، زمانی که سایر اقدامات امنیتی وابسته به هم اجرا نمی‌شوند را می‌توان کاهش داد.

(Kabourati, 2019) در پژوهش خود با عنوان "شناسایی و اهمیت‌سنجی عوامل مؤثر بر به کارگیری بیمه‌نامه‌های الکترونیک در صنعت بیمه (مطالعه چند شرکت بیمه‌ای)" به دنبال شناسایی و رتبه‌بندی عوامل مؤثر بر به کارگیری بیمه-نامه‌های الکترونیک در صنعت بیمه با مرور ادبیات تحقیق و نظرات خبرگان بوده‌اند. نتایج نشان داد عوامل زمینه‌ای و زیرساختی، فرهنگی و شخصیت و نگرش مشتریان از اهمیت بیشتری نسبت به سایر ابعاد برخوردار هستند. در میان زیرشاخص‌ها نیز؛ تبلیغات، آشنایی و آگاهی دادن جامعه نسبت به کاربرد و فواید خدمات بیمهٔ الکترونیک، زیرساخت-های حقوقی و قانونی، ریسک‌پذیری و وجود امنیت از اهمیت بیشتری نسبت به سایر زیرشاخص‌ها برخوردار بودند.

(Soleymani Rouzbahani & Hoseini, 2016) در پژوهش خود با عنوان "مطالعه جرم و بیمه امنیت در فضای مجازی" با اشاره به رشد سریع تکنولوژی، ورود رایانه و استفاده از اینترنت و تغییرات حاصل از آن در زندگی انسان‌ها، به بیمه اینترنت به عنوان ابزاری برای مقابله با ظهور جرائم مجازی همچون سرقت اطلاعات در دنیای ارتباطات اینترنتی پرداخته است. پژوهشگران به این نتیجه دست یافتند که با ایجاد فضاهای اجتماعی نوظهور در جوامع، ایجاد امنیت در فضاهای اجتماعی جدید از ضروریات است؛ چراکه در این فضاها با وجود سعی سازندگان و ایجاد کنندگان در ایمن

[1] The General Data Protection Regulation (GDPR)
[2] Icebreaker
[3] Network and Information Security (NIS)

سازی آنها و جلوگیری از سوء استفاده‌های احتمالی توسط برخی از کاربران، همچنان راه برای استفاده ناصحیح وجود دارد و این مسئله باعث ایجاد جرائم جدید مانند دزدیده شدن اطلاعات و استفاده از نام‌های جعلی شده است.

روش پژوهش

پژوهش حاضر از لحاظ اینکه با چه هدفی انجام می‌شود، از نوع توسعه‌ای و کاربردی است؛ چرا که نتایج آن می‌تواند در راستای افزایش آگاهی و دانش درباره بیمه سایبری و اقدامات برای کاهش ریسک‌های سایبری مورد استفاده قرار گیرد. بر اساس نحوه گردآوری داده‌ها نیز، پژوهشی توصیفی به شمار می‌رود. روش گردآوری اطلاعات، مصاحبه عمیق با خبرگان است. این پژوهش رویکرد کیفی داشته و از راهبرد پژوهشی نظریه داده بنیاد، به گردآوری و تحلیل داداها پرداخته است (Bahari & Taheri Rouzbahani, 2023). از این رو برای رسیدن به نظریه مراحلی پشت سر گذاشته شده است که شامل کدگذاری باز، محوری و انتخابی بوده و در طول پژوهش به یادداشت برداری، رده‌بندی و نوشتن نظریه پرداخته شده است. بدین منظور از روش نظام‌مند اشتراوس و کوربین بهره گرفته شده است که شیوه‌های منظمی برای تحلیل داده‌ها دارد. جامعه آماری پژوهش شامل ۱۰ نفر از متخصصان صنعت بیمه می‌باشد که اطلاعات آن بشرح جدول زیر می‌باشد. فرآیند مصاحبه با خبرگان تا هنگام شناسایی کامل مؤلفه‌های بیمه سایبری و حصول اشباع نظری ادامه پیدا کرد. شیوه انتخاب نمونه با با بهره‌گیری از روش نمونه‌گیری گلوله‌برفی بوده است؛ بدین صورت که پژوهشگر از طریق یک مصاحبه‌شونده فرد دیگر را انتخاب می‌کند تا بتواند مفاهیم دیگری را کشف کند.

جدول ۱) آمار توصیفی مصاحبه شوندگان (خبرگان پژوهش)

ردیف	جنسیت	سن	وضعیت تحصیلی	پست سازمانی	مدت زمان اشتغال	سابقه شغلی
۱	مرد	۳۴	کارشناسی ارشد	مدیر عامل	۴	۱۵
۲	مرد	۵۳	کارشناسی ارشد	مدیر کل	۵	۲۵
۳	مرد	۵۱	کارشناسی ارشد	مدیر	۵	۲۵
٤	مرد	۵۱	دکتری	مدیر	۵	۲۵
۵	مرد	۴۸	دکتری	مدیر کل	۲	۲۲
٦	زن	۳۵	کارشناسی	مدیر	۴	۱۰
۷	زن	۴۵	کارشناسی ارشد	مدیر	۶	۱۵
۸	مرد	۵۱	کارشناسی	مدیر عامل	۷	۲۱
۹	زن	۴۷	کارشناسی	مدیر	۵	۱۴
۱۰	مرد	۳۷	کارشناسی ارشد	مدیر	۴	۷

بر این اساس ۷۰ درصد مشارکت‌کنندگان آقا و ۳۰ درصد خانم بوده‌اند. بنابراین می‌توان گفت بیشتر مشارکت‌کنندگان آقا بوده‌اند. همچنین ۵۰ درصد مشارکت‌کنندگان دارای مدرک کارشناسی ارشد، ۳۰ درصد دارای مدرک کارشناسی و ۲۰ درصد دارای مدرک دکتری بوده‌اند.

در ادامه پرسشنامه‌ای بر اساس مدل اشتروس و کوربین و با درنظر گرفتن عوامل علی، بسترساز، مداخله‌گر، پیامدها و راهکارهای اجرای بیمه سایبری تدوین شد. بدین منظور پرسشنامه در اختیار خبرگان بیمه سایبری قرار گرفته است و با انجام مصاحبه‌های عمیق سعی در ایجاد ارتباط مؤثر و کسب مفاهیم اولیه و ضروری تحقیق شده است.

متن مصاحبه با استفاده از نرم افزار MAXQDA نسخه ۲۰۲۰ طبقه‌بندی و کدهای مشابه از نظر ماهیت و معنا در یک طبقه قرار داده شده‌اند. طبقات و کدهای هر مصاحبه با مصاحبه‌های دیگر مقایسه شده تا روابط مشترک بین آن‌ها شناسایی شوند. سپس طبقات مشابه به لحاظ مفهومی در هم ادغام شدند و حول محور مشترکی قرار گرفته‌اند و مقولات وسیع‌تری تشکیل دادند. در مرحله کدگذاری انتخابی یا گزینشی، ساخت پایه‌های نظری زمینه‌ای بر اساس ارتباط مقولات متعدد با مقوله اصلی و مرکزی حاصل می‌شود که در این مرحله با تمرکز بیشتر روی مقولات، ارتباط بین مقولات و زیر مقولات بررسی شده و مقوله اصلی ایجاد شد. در نهایت یک مدل پارادایمی بدست آمده است که حاصل پیوند و ارتباط مقولات فرعی با مقوله اصلی است و بیان‌کننده شرایط علی، بسترساز، مداخله‌گر، راهکارها و پیامدها است. به منظور بررسی اعتبار پژوهش از سه تن از اساتید مدیریت خواسته شد تا نظرات و اظهارات خود را در خصوص کدگذاری‌های صورت گرفته در مرحله کدگذاری باز و کدگذاری محوری بیان نمایند. همچنین با متناسب بودن نمونه سعی شده است از مشارکت‌کننده‌هایی استفاده شود که بهترین دانش را در زمینه موضوع پژوهشی دارا هستند، این امر باعث می‌شود که کارآمدی و اثربخشی اشباع طبقه‌ها همراه با بهینه کردن کیفیت داده‌ها تضمین شود.

پایایی پژوهش

در پژوهش حاضر، در مرحله اول همه مصاحبه‌هایی که از طریق «صدا» و یا «نوشته» توسط مصاحبه‌شوندگان ارائه شده بود، گردآوری و بررسی اولیه آن‌ها انجام شد. در این مرحله با استفاده از فرآیند کدگذاری باز، مفاهیم مرتبط استخراج شد. از این رو در مرحله اول ۱۵۴ کد اولیه اسخراج شد. در مرحله بعد رویه‌هایی که پس از کدگذاری باز انجام می‌شوند تا با برقراری ارتباط بین مقوله‌ها، اطلاعات را با روش‌های جدیدی با یکدیگر پیوند دهند. در واقع این مرحله شامل تعیین الگوهای موجود در داده‌ها می‌باشد و همزمان مقایسه دائمی داده‌ها انجام می‌گیرد. در مرحله سوم از کدگذاری داده‌ها (کدگذاری انتخابی) به عمق داده‌ها پرداخته شد و نظریه‌های اصلی و یا همان اهداف پژوهش ارائه می‌شود.

روش‌ها و ابزار تجزیه و تحلیل داده‌ها در پژوهش حاضر با استناد به روش اشتراوس و کوربین به طور خلاصه در روش داده بنیاد انجام شده است.

یافته‌ها

پس از کدگذاری اولیه، مقوله‌های اولیه مشخص شده‌اند. در جدول ۳ کدهای اولیه، مقوله‌های مرکزی و اصلی و در نهایت نقش‌ها آورده شده است.

جدول ۳- بررسی کدهای اولیه، مقوله مرکزی و مقوله‌های اصلی

ردیف	مقوله‌های اولیه	مقوله مرکزی	مقوله‌های اصلی	نقش
۱	اعتماد سازی	محیطی	عوامل شبکه بیمه سایبری	عوامل علی
۲	فرهنگ			
۳	توجه به نوسانات اقتصادی			
۴	توجیه اقتصادی			
۵	ثبات سیاسی			
۶	تعیین بازیگران مؤثر در بیمه سایبری	اکوسیستم		
۷	ارتباطات			
۸	همکاری			
۹	وجود امنیت بیشتر	حفاظت	عوامل فنی	
۱۰	جرائم رایانه‌ای			
۱۱	حفاظت از حریم خصوصی افراد			
۱۲	تبلیغات	زیر ساخت مناسب		
۱۳	فناوری			
۱۴	استفاده از شبکه‌های اجتماعی			
۱۵	کنفرانس‌ها و نشست‌های تخصصی			
۱۶	آموزش الکترونیک			
۱۷	تدوین مقررات و قوانین			
۱۸	ماهیت شرکت	مدیریت ریسک		
۱۹	شناسایی به موقع خسارت			
۲۰	شناخت دقیق زیان			
۲۱	شرح وظایف سازمان			
۲۲	شرح دقیق خدمات شرکتها			
۲۳	بررسی مزایا و معایب			
۲۴	نظارت بر مدیریت ریسک			
۲۵	ارائه تعریف استاندارد از بیمه سایبری	یکسان سازی تعاریف	عوامل دانشی	
۲۶	استاندارد سازی معنا			
۲۷	شناخت مشتریان	دانش سایبری		
۲۸	فرهنگ سازی			
۲۹	آموزش افراد			
۳۰	شناخت ریسک			
۳۱	آگاهی امنیتی			
۳۲	دانش مدیریت بحران			
۳۳	آگاهی از ریسک سایبری			

۳۴	سیاست‌های سایبری	زیرساخت سایبری	تجزیه و تحلیل محیط درونی	عوامل بستر ساز
۳۵	عوامل انسانی			
۳۶	فناوری اطلاعات			
۳۷	محتوای اطلاعات			
۳۸	شبکه و اتصالات			
۳۹	عوامل نرم افزاری			
۴۰	سخت افزار			
۴۱	توان یا قدرت ابزار			
۴۲	اقدام به موقع	شرایط محیطی		
۴۳	محیط سایبری			
۴۴	آگاهی ریسک بازار			
۴۵	بررسی بازار بیمه			
۴۶	تسلط بر ریسک‌های سایبری			
۴۷	بررسی تهدید سایبری			
۴۸	بهبود وضع اقتصادی			
۴۹	کاهش ریسک	عوامل اجرایی	بازاریابی و توجه بازوهای اجرایی	
۵۰	تسلط بر نرخ گذاری بیمه			
۵۱	طراحی شرایط خصوصی			
۵۲	تدوین قانون و مقررات			
۵۳	محاسبه ریسک			
۵۴	دسته بندی اطلاعات			
۵۵	طراحی شرایط عمومی بیمه نامه			
۵۶	بررسی پیش نیازهای اطلاعاتی			
۵۷	تدوین آیین نامه بیمه سایبری			
۵۸	حمایت از فضای نوآور	معرفی و تسهیل بیمه سایبری		
۵۹	عدم بوروکراسی بیمه‌ای			
۶۰	معرفی ساختار بیمه سایبری			
۶۱	ایجاد انگیزه			
۶۲	رویه‌های امنیت اطلاعات و شبکه			
۶۳	هزینه پژوهش‌های بعد از حادثه	وجود پایگاه داده		
۶۴	واحد تحقیق و توسعه			
۶۵	شناخت ریسک‌های سایبری			
۶۶	هاتجربه سایر کشور			
۶۷	سیاست گذاری	نقش دولت		

۶۸	نظارت دولتی		چشم انداز بیمه‌ای	**عوامل مداخله‌گر**
۶۹	اعتماد بیمه شونده	نگرش بیمه‌ای		
۷۰	آگاهی بیمه گر			
۷۱	خرید آگاهانه بیمه نامه			
۷۲	سابقه شرکت بیمه	عملکرد شرکت بیمه		
۷۳	مسئولیت پذیری شرکت‌های بیمه			
۷۴	تعیین نقش هر بخش	مقررات بیمه‌ای		
۷۵	حقوق کاربر مجازی			
۷۶	شرایط اعلامی بیمه گر			
۷۷	تعریف بیمه نامه			
۷۸	ارائه برنامه بلند مدت و کوتاه مدت	بازاریابی بیمه سایبری	رویکرد اکوسیستمی	**راهکارها**
۷۹	معرفی بیمه نامه			
۸۰	طراحی بیمه نامه فراگیر و جذاب			
۸۱	نقش دولت به عنوان متولی گسترش اقتصاد دیجیتال	رویکرد شبکه‌ای		
۸۲	تشکیل کارگروه فنی			
۸۳	تعیین شفاف مسئولیت سازمان‌ها			
۸۴	تعیین نقش بازیگران درگیر			
۸۵	بهره برداری از مدل‌های استاندارد	مدلسازی بیمه سایبری		
۸۶	رفع نواقص قانونی مرتبط با فضای سایبری			
۸۷	شناسایی و دسته بندی ریسک‌ها			
۸۸	تدوین شرایط عمومی بیمه سایبری			
۸۹	تست‌های نفوذ و امنیتی دوره‌ای	ایمن کردن داده‌ها	تدوین استراتژی بیمه‌ای	
۹۰	داشتن مجوزات امنیتی (افتا)			
۹۱	نگهداری اطلاعات حیاتی بر روی سخت افزارهای مطمئن‌تر			
۹۲	نگهداری نسخه فایل پشتیبان خارج از سرور دیتابیس			
۹۳	داشتن فرآیند نسخه پشتیان بصورت استاندارد و کوتاه مدت			
۹۴	نگهداری بیش از یک نسخه فایل پشتیبان			
۹۵	محدود نمودن پورت‌های دسترسی			
۹۶	انجام اقدامات پیشگیرانه			

۹۷	کنترل دسترسی‌ها			
۹۸	پوشش هزینه‌های حقوقی خسارت	شرح دقیق پوشش‌های بیمه‌ای		
۹۹	پوشش خسارت اطلاعات غیر قابل بازگشت			
۱۰۰	پوشش هزینه مربوط به از دست دادن داده			
۱۰۱	پوشش خسارت وقفه در کسب و کار اینترنتی			
۱۰۲	پوشش هزینه بازگردانی اطلاعات از دست رفته			
۱۰۳	گسترگی خطرات سایبری	محیط غیر قابل پیش بینی	عدم تسلط بر موضوع بیمه سایبری	**موانع بیمه سایبری**
۱۰۴	عدم اطمینان از جبران کامل خسارت			
۱۰۵	احتمال خسارت‌های هنگفت			
۱۰۶	نبود انگیزه	ضعف دانشی		
۱۰۷	عدم تجربه بیمه گران			
۱۰۸	عدم توانایی در شناخت نوع ریسک			
۱۰۹	عدم تخصص و پروتوکل مشخص بیمه گران			
۱۱۰	عدم شناخت از ریسک‌های موجود			
۱۱۱	عدم شناخت و دانش لازم در ارزیابی ریسک			
۱۱۲	عدم آگاهی از ریسک			
۱۱۳	عدم اجرای نمونه پایلوت مشخص	ضعف آماری		
۱۱۴	عدم توجه به استانداردهای جهانی			
۱۱۵	فقدان داده‌های آماری			
۱۱۶	عدم وجود زیرساخت	پروتوکل های دولتی ارتباطات	عدم حمایت دولت	
۱۱۷	ضعف دانش فنی			
۱۱۸	قوانین دست و پا گیر بیمه مرکزی	قوانین دولتی		
۱۱۹	عدم مالکیت معنوی ابزارهای اینترنتی			
۱۲۰	نبود نظارت			
۱۲۱	وجود استثنائات زیاد			
۱۲۲	همسو شدن با تغییرات	درک تغییرات محیطی		
۱۲۳	آمادگی بیشتر			
۱۲۴	کسب تجربه بیشتر		افزایش سطح دانش	

			شرکت‌های بیمه	
۱۲۵	کسب دانش سایبری	افزایش دانش عمومی خطرات سایبری		
۱۲۶	شناخت بیشتر بیمه سایبری			
۱۲۷	شناخت خسارت‌های سایبری			
۱۲۸	رشد بیمه سایبری			
۱۲۹	کاهش ریسک شرکت‌ها	سطح اطمینان شرکتافزایش		
۱۳۰	کاهش ریسک‌های عملیاتی			
۱۳۱	ایمنی دسترسی داده‌ها	حفاظت از داده‌ها	ایمنی و امنیت داده‌ها	
۱۳۲	کاهش سرقت داده‌های هویت			
۱۳۳	پیشگیری از ریسک			
۱۳۴	افزایش میزان محرمانگی داده‌ها			
۱۳۵	جلوگیری از افشای اطلاعات			
۱۳۶	افزایش ایمنی وامنیت شرکت			
۱۳۷	رشد اقتصادی	توجیه اقتصادی	بهبود خدمات و درآمد شرکت	
۱۳۸	به روز شدن زیر ساخت‌ها			
۱۳۹	کاهش هزینه			
۱۴۰	حفاظت از سرمایه ملی			
۱۴۱	افزایش ضریب نفوذ بیمه			
۱۴۲	جبران خسارت سایبری			
۱۴۳	معرفی خدمات برخط	افزایش رضایت مشتری		
۱۴۴	بهبود خدمات برخط			
۱۴۵	بهبود پاسخ گویی به مشتریان			
۱۴۶	کاهش ریسک‌های مشتریان			
۱۴۷	رعایت استانداردهای بیمه‌ای	به روز شدن سطح خدمات		
۱۴۸	استاندارد سازی خدمات			
۱۴۹	عدم اطمینان بیمه گذار	سردرگمی مشتری	عدم اطمینان از کارکرد بیمه	
۱۵۰	عدم توجیه بیمه گذار و مشتری			
۱۵۱	عدم شناخت ریسک سایبری			
۱۵۲	عدم توانایی پوشش خسارت			

پیامدهای بیمه سایبری

۱۵۳	عدم برآورد خسارت سایبری	عدم توانایی برآورد خسارت		
۱۵۴	عدم ارزیابی ریسک			

عوامل علی

بر اساس نتایج پژوهش و جدول شماره ۲، عوامل علی پیاده‌سازی بیمه سایبری در سه مقوله اصلی دانشی، عوامل فنی و عوامل شبکه جای گرفتند. تأکید مصاحبه شوندگان پیرامون تعریف دقیق و شناخت ابعاد مختلف بیمه سایبری باعث تشکیل مقوله‌ای به نام "عوامل دانشی" شده است. همچنین ابعاد فنی و حفاظتی بیمه سایبری که بر تجهیزات و فناوری شرکت‌های بیمه تأکید داشته‌اند به عنوان مقوله "عوامل فنی" شناخته شده‌اند. مؤلفه اصلی دیگر با عنوان "عوامل شبکه" بیمه سایبری شناخته شده است. تأکید مصاحبه شوندگان بر جریانات محیطی تأثیرگذار بر شرکت‌های بیمه دو عامل محیطی و اکوسیستم به عنوان مقوله‌های مرکزی شناخته شده‌اند. با توجه به کدهای استخراج شده به منظور پیاده‌سازی بیمه سایبری، عوامل فرهنگی، نوسانات اقتصادی، توجیه اقتصادی و ثبات سیاسی به عنوان عوامل محیطی مرتبط با شبکه بیمه سایبری در نظر گرفته شده است. همچنین کدهای استخراج شده از مصاحبه شوندگان مفهوم اکوسیستم را به عنوان یکی از عوامل علی بیمه سایبری عنوان کرده‌اند که شامل تعیین بازیگران فعال، ارتباطات و همکاری بین بخش‌های مختلف بیمه بوده است.

بسترها و زمینه‌سازهای بیمه سایبری

بر اساس کدهای استخراج شده مصاحبه‌های پژوهش، دو عامل "تجزیه و تحلیل محیط درونی و بیرونی" و همچنین "بازاریابی و توجه بازوهای اجرایی" به عنوان مؤلفه‌های اصلی بسترساز و زمینه‌ساز شناسایی شده‌اند. در این طبقه‌بندی زیرساخت سایبری و شرایط محیطی به عنوان مقوله‌های مرکزی شناخته شده‌اند. عامل زیر ساخت سایبری به عنوان مقوله مرکزی تجزیه و تحلیل درونی و بیرونی شناخته شده که با زیرکدهای سیاست‌های سایبری، عوامل انسانی، فناوری اطلاعات، محتوای اطلاعات، شبکه و اتصالات، عوامل نرم افزاری، سخت افزار و نهایتاً توان و قدرت ابزار شناخته شده است. کدهای استخراج شده نشان دهنده تأثیرات شرایط محیطی به عنوان مقوله مرکزی و تعیین کننده بستر و زمینه بیمه سایبری بوده است. توجه به تغییرات محیط سایبری، اقدام به موقع، بررسی بازار بیمه سایبری، تسلط بر ریسک‌های سایبری، بررسی تهدیدهای سایبری و بهبود وضع اقتصادی به عنوان مقوله‌های اولیه و تعیین کننده شرایط محیطی بوده‌اند. از سوی دیگر بازاریابی و توجه به بازوهای اجرایی به عنوان مقوله اصلی با دو مقوله مرکزی عوامل اجرایی" و معرفی و تسهیل بیمه سایبری طبقه‌بندی شده است. با توجه به نظرات مصاحبه کنندگان، عوامل اجرایی با کدهای اولیه کاهش ریسک، تسلط بر نرخ‌گذاری بیمه، طراحی شرایط خصوصی، تدوین قانون و مقررات، محاسبه ریسک، دسته‌بندی اطلاعات، طراحی شرایط عمومی بیمه‌نامه، بررسی پیش‌نیازهای اطلاعاتی و تدوین آیین‌نامه بیمه سایبری ارتباط یافته‌اند.

همچنین بررسی کدهای اولیه نشان دهنده ارتباط زیرکدهای اولیه با یکدیگر و مفهوم معرفی و تسهیل بیمه سایبری به عنوان مقوله مرکزی بوده است. حمایت از فضای نوآور، عدم بوروکراسی پیچیده و سنتی بیمه‌ای، ایجاد انگیزه، رویه‌ای امنیت اطلاعات و شبکه به عنوان کدهای اولیه شناسایی شده و زمینه ساز اجرای بیمه سایبری شناخته شده‌اند.

پیامدهای بیمه سایبری

با بررسی کدهای استخراج شده از مصاحبه متخصصان بیمه سایبری، پیامدهای بیمه سایبری در دسته مثبت و منفی قرار گرفته‌اند. سه مقوله اصلی با عنوان "افزایش سطح دانش شرکت‌های بیمه"، "ایمنی و امنیت داده‌ها" و "بهبود خدمات و درآمد شرکت" به عنوان مقوله‌های اصلی و مثبت و "عدم اطمینان از کارکرد بیمه" به عنوان مقوله اصلی و منفی شناسایی شده‌اند.

درک تغییرات محیطی و افزایش دانش عمومی خطرات سایبری به عنوان دو مقوله مرکزی در مؤلفه افزایش سطح دانش شرکت‌های بیمه جای گرفتند. درک بهتر تغییرات محیطی به عنوان مقوله مرکزی با توجه به مقوله‌های اولیه همسو شدن با تغییرات محیطی و آمادگی بیشتر به منظور مقابله با پدیده‌های جدید سایبری شکل گرفته است. با توجه به کدهای اولیه کسب تجربه بیشتر، کسب دانش سایبری، شناخت بیشتر بیمه سایبری، شناخت خسارت‌های سایبری و رشد بیمه سایبری، افزایش دانش عمومی خطرات سایبری به عنوان مقوله مرکزی شناسایی شده و از پیامدهای اجرای بیمه سایبری شناخته شده است. همچنین افزایش سطح اطمینان شرکت و حفاظت از داده‌ها به عنوان دو مقوله مرکزی در زیر مجموعه ایمنی و امنیت داده‌ها (مقوله اصلی) جای گرفته‌اند.

با توجه به بررسی کدهای استخراج شده، مؤلفه‌های اولیه کاهش ریسک شرکت‌ها و کاهش ریسک‌های عملیاتی به سطح اطمینان شرکت را تعیین کرده و از پیامدهای مثبت اجرای بیمه سایبری به حساب می‌آید. کدهای اولیه استخراج شده از مصاحبه کارشناسان بیمه سایبری، شامل ایمن کردن دسترسی داده‌ها، کاهش سرقت داده‌های هویت، پیشگیری از ریسک، افزایش میزان محرمانگی داده‌ها، جلوگیری از افشای اطلاعات و افزایش ایمنی و امنیت شرکت بوده است که به عنوان مقوله مرکزی حفاظت از داده‌ها به عنوان مقوله مرکزی شناسایی شده‌اند. در ادامه با بررسی متن مصاحبه کارشناسان، توجیه اقتصادی، افزایش رضایت مشتری و به روز شدن خدمات به عنوان سه مقوله مرکزی در زیرمجموعه بهبود خدمات و درآمد شرکت (مقوله اصلی) قرار گرفته‌اند. بر اساس نظر کارشناسان و مصاحبه آن‌ها، کدهای اولیه رشد اقتصادی، به روز شدن زیرساخت‌ها، کاهش هزینه، حفاظت از سرمایه ملی، افزایش ضریب نفوذ بیمه و جبران خسارت سایبری در مقوله مرکزی «داشتن توجیه اقتصادی» قرار گرفته و از پیامدهای مثبت اجرای بیمه سایبری بوده‌اند. با توجه به کدهای استخراج شده از پاسخ‌های مصاحبه‌شوندگان، پیامد اجرای بیمه سایبری توجه به مشتری و نیاز آن‌ها بوده است. کدهای اولیه معرفی خدمات برخط، بهبود خدمات برخط، بهبود پاسخ‌گویی به مشتریان و کاهش ریسک‌های مشتریان می‌توانند یک مقوله مرکزی با عنوان رضایت مشتری از اجرای بیمه سایبری تشکیل دهند. کدهای اولیه فایل مصاحبه نشان داده است که رعایت استانداردهای بیمه‌ای و استاندارد سازی خدمات با توجه به نیاز شرکت بیمه و همسو با رقیب-های بیمه‌ای می‌توانند مقوله مرکزی «به روز شدن خدمات بیمه‌ای» به عنوان پیامدهای مثبت اجرای بیمه سایبری را تشکیل دهند.

پیامد منفی اجرای بیمه سایبری با توجه به دیدگاه متخصصان و کارشناسان، در مرحله اول سردرگمی مشتریان و در مرحله دوم عدم توانایی برآورد خسارت (به عنوان مقوله‌های مرکزی) شناسایی شده‌اند. بر اساس کدهای استخراج شده از مصاحبه، پیامدهای منفی بیمه سایبری با مؤلفه‌های اولیه عدم اطمینان بیمه‌گذار و عدم توجیه بیمه‌گذار و مشتری باعث ایجاد مؤلفه مرکزی سردرگمی مشتری شده است. بر اساس نتایج مصاحبه و استخراج کدهای اولیه (عدم شناخت ریسک سایبری، عدم توانایی پوشش خسارت، عدم برآورد خسارت سایبری و عدم ارزیابی ریسک)، مؤلفه «عدم توانایی برآورد خسارت» به عنوان مؤلفه مرکزیِ شناخت ریسک شناخته شده است.

عوامل مداخله‌گر

با بررسی کدهای اولیه و مقوله‌های مرکزی مصاحبه‌های کارشناسان، یک مقوله اصلی با نام "چشم‌انداز بیمه‌ای" به عنوان مقوله اصلی شناسایی شده است. وجود پایگاه داده، نقش دولت، نگرش بیمه‌ای، عملکرد شرکت بیمه‌ای، مقررات بیمه‌ای به عنوان مقوله‌های مرکزی شناخته شده‌اند.

کدهای اولیه استخراج شده نشان می‌دهند که هزینه پژوهش‌های بعد از حادثه، واحد تحقیق و توسعه، شناخت ریسک-های سایبری و تجربه سایر کشورهای در اجرای بیمه سایبری به عنوان عوامل پنهان و مداخله‌گر نقش دارند. از این‌رو و از ترکیب کدهای اولیه وجود پایگاه داده به عنوان مقوله مرکزی شناخته شده است. با بررسی نقش سیاست‌گذاری و نظارت دولتی به عنوان کدهای اولیه در مسیر اجرای بیمه سایبری، نقش دولت به عنوان مقوله مرکزی شناخته شده است. با بررسی کدهای اولیه شناسایی شده (اعتماد بیمه‌شونده، آگاهی بیمه‌گر، خرید آگاهانه بیمه‌نامه) مقوله مرکزی نگرش بیمه‌ای استخراج شده است که به بررسی اعتقاد و میزان آگاهی بیمه‌گر از خرید بیمه سایبری اشاره دارد. همچنین سابقه شرکت بیمه و مسئولیت‌پذیری شرکت‌های بیمه، مقوله مرکزی عملکرد شرکت بیمه شناسایی شد و به عنوان یکی از مؤلفه‌های مداخله‌گر بیمه سایبری از نظر کارشناسان لحاظ شده است. در نهایت با بررسی کدهای اولیه استخراج شده در نرم افزار، مشخص کردن نقش بخش‌های درگیر در بیمه سایبری، حقوق کاربر مجازی، شرایط اعلامی بیمه‌گر و تعریف بیمه‌نامه به عنوان مؤلفه‌های اولیه شناسایی شده که با یکدیگر مؤلفه مرکزی مقررات بیمه‌ای را ایجاد کرده‌اند.

موانع بیمه سایبری

موانع پیش‌رو در دو مقوله اصلی "عدم تسلط بر موضوع" و "عدم حمایت دولت" تقسیم‌بندی شده‌اند. محیط غیر قابل پیش بینی، ضعف دانشی و ضعف آماری به عنوان مقوله‌های مرکزی، زیر مجموعه عدم تسلط بر موضوع (مقوله اصلی) قرار گرفته‌اند. توجه به گستردگی خطرات سایبری، عدم اطمینان از جبران کامل خسارت و احتمال خسارت‌های هنگفت به عنوان کدهای اولیه شناسایی شده و مقوله مرکزی محیط غیر قابل پیش‌بینی را ایجاد کرده‌اند. کدهای استخراجی نشان دهنده شناسایی مقوله‌های اولیه نبود انگیزه، عدم تجربه بیمه‌گران، عدم توانایی در شناخت ریسک، عدم تخصص و پروتکل مشخص و عدم شناخت از ریسک‌های موجود، عدم شناخت و دانش لازم در ارزیابی ریسک بوده که در مقوله مرکزی ضعف دانشی دسته‌بندی شده‌اند. نتایج کدهای استخراج شده نشان داد که عدم اجرای نمونه پایلوت مشخص،

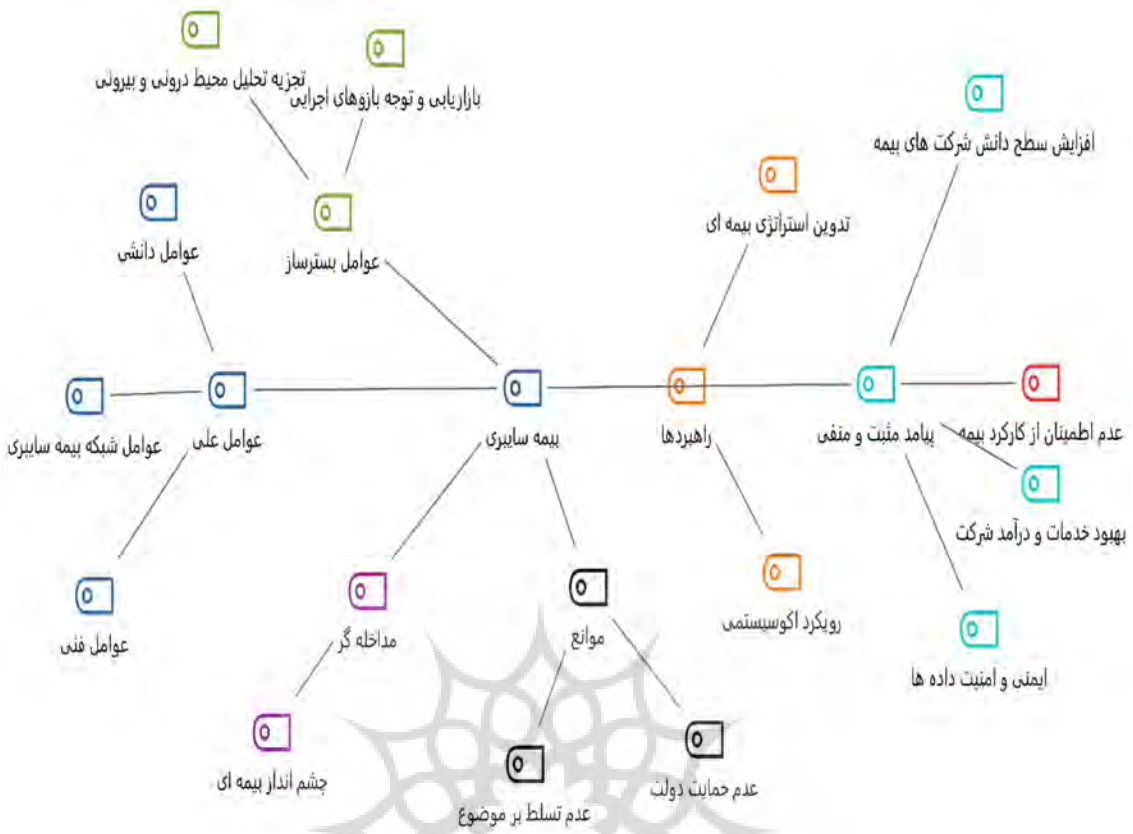
عدم توجه به استانداردهای جهانی و فقدان داده‌های آماری به عنوان مؤلفه‌های اولیه در نظر گرفته شده و ضعف آماری را به عنوان یکی از مقوله‌های مرکزی در ایجاد مانع بیمه سایبری پدید آورده‌اند.

از سوی دیگر پروتکول‌های دولتی ارتباطات، قوانین دولتی به عنوان مقوله‌های مرکزی در زیر مجموعه عدم حمایت دولت (به عنوان مقوله اصلی) قرار گرفتند. بررسی مصاحبه‌های عمیق کارشناسان نشان داد که عدم وجود زیر ساخت مناسب و ضعف دانش فنی به عنوان مؤلفه‌های اولیه پروتکل‌های دولتی ارتباطات را مشخص می‌کنند و مقوله مرکزی را تشکیل می‌دهند.

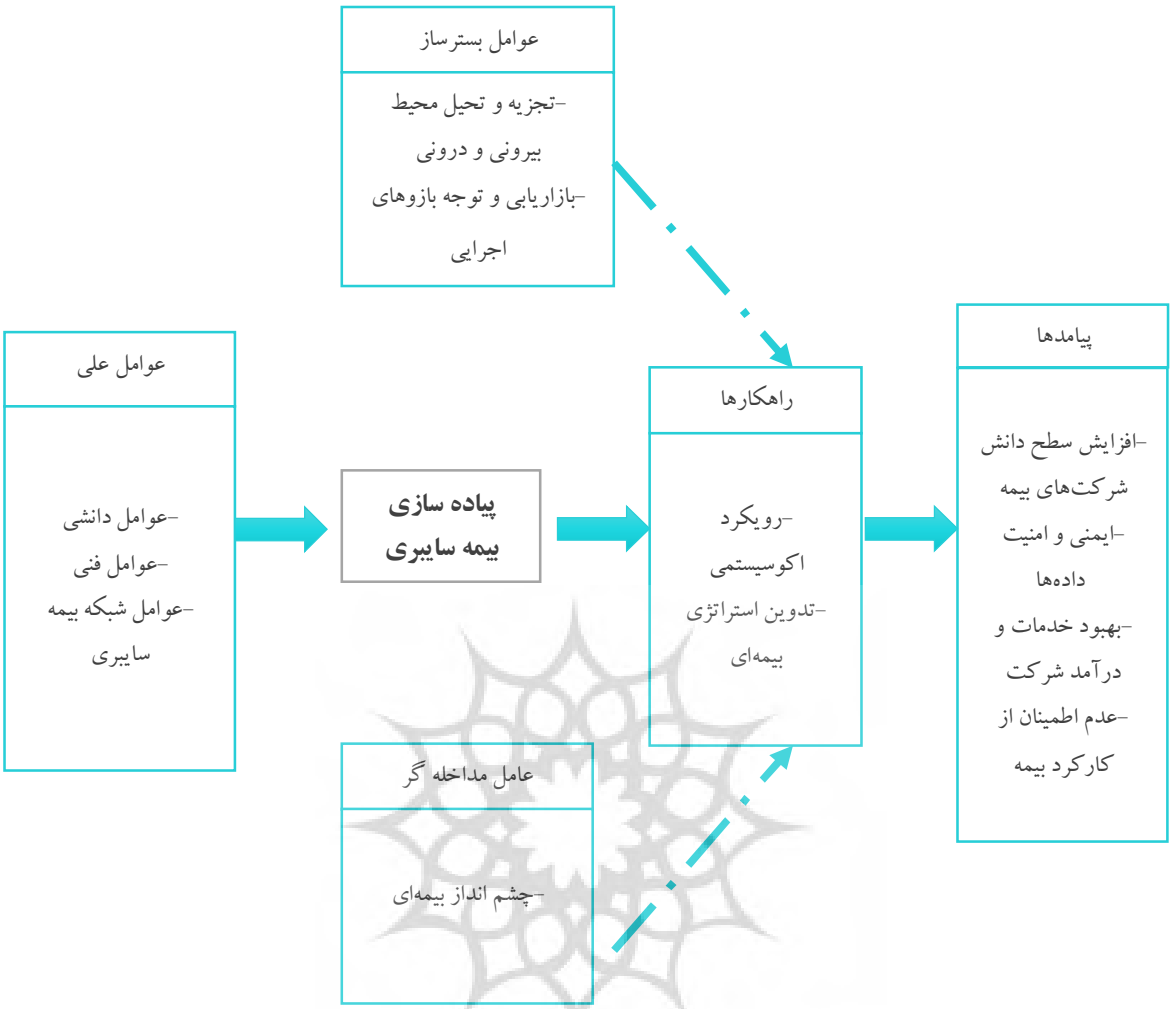
با بررسی مؤلفه‌های اولیه شامل قوانین دست و پاگیر بیمه مرکزی، عدم مالکیت معنوی ابزارهای اینترنتی، نبود نظارت، وجود استثنائات زیاد مقوله مرکزیِ قوانین دولتی شناسایی شده است.

راهبردهای اجرای بیمه سایبری

با بررسی کدهای استخراجی از مصاحبه کارشناسان بیمه سایبری، دو مؤلفه اصلی "رویکرد اکوسیستمی" و "تدوین استراتژی بیمه‌ای" به عنوان راهبردهای بیمه سایبری شناسایی شدند. بازاریابی بیمه سایبری و رویکرد شبکه‌ای و مدلسازی بیمه سایبری به عنوان مؤلفه‌های مرکزی زیر مجموعه رویکرد اکوسیستمی (مؤلفه اصلی) قرار گرفته‌اند. با بررسی کدهای اولیه حاصل از بررسی اولیه مصاحبه، ارائه برنامه مدت و کوتاه مدت، معرفی بیمه‌نامه و طراحی بیمه‌نامه فراگیر و جذاب به عناون کدهای اولیه شناسایی شدند که در دسته «بازاریابی بیمه سایبری» به عنوان مؤلفه مرکزی شناخته شده‌اند. بررسی کدهای اولیه استخراج شده که شامل نقش دولت به عنوان متولی گسترش اقتصاد دیجیتال، تشکیل کارگروه فنی، تعیین شفاف مسئولیت سازمان‌ها و تعیین نقش بازیگران درگیر نشان دهنده مؤلفه‌های اولیه راهبردها هستند. با بررسی این کدها، مؤلفه مرکزی «رویکرد شبکه‌ای» ایجاد شده است. با بررسی اولیه مصاحبه و استخراج کدهای اولیه (بهره‌برداری از مدل-های استاندارد، رفع نواقص قانونی مرتبط با فضای سایبری، شناسایی و دسته‌بندی ریسک‌ها و تدوین شرایط عمومی بیمه سایبری)، مؤلفه مرکزی مدلسازی بیمه سایبری استخراج شده است. ایمن کردن داده‌ها، شرح دقیق پوشش‌های بیمه‌ای به عنوان مقوله‌های مرکزی زیر مجموعه تدوین استراتژی بیمه‌ای (مؤلفه اصلی) قرار گرفتند. در ادامه مؤلفه‌های اولیه، مرکزی، اصلی و ابرکد راهبردهای بیمه سایبری به عنوان خروجی نرم افزار در شکل ۱ و به صورت مدل خروجی پژوهش در شکل ۲ آورده شده است.



شکل ۱) مدل پژوهش، با در نظر گرفتن موانع بیمه سایبری (خروجی نرم افزار)



شکل ۲) الگوی پیاده‌سازی بیمه سایبری بر اساس روش گرندد تئوری (منبع: یافته پژوهش)

بحث و نتیجه‌گیری

پژوهش حاضر بر مقوله محوری پیاده‌سازی بیمه سایبری در سازمان‌های ایران استوار بوده است. نتایج پژوهش بر اساس مدل اشتراوس و کوربین استوار بوده است. از این رو ۵ شاخص تأثیر گذار بر اجرای موفقیت‌آمیز بیمه سایبری شناسایی شده است که شامل عوامل علی بیمه سایبری، پیامدهای اجرای بیمه سایبری، عوامل بسترساز و زمینه‌ای بیمه سایبری، عوامل پنهان و مداخله‌گر و نهایتاً پیامدهای اجرای بیمه سایبری (هم برای شرکت‌های بیمه‌ای و هم برای شرکت‌ها و سازمان‌های بیمه شده) بوده‌اند.

عوامل علی

بر اساس نتایج پژوهش، بیمه سایبری با یک مجموعه از عوامل علی تقویت می‌شود. قبل از اجرای بیمه سایبری نیاز به استاندارد سازی تعاریف و ارائه یک تعریف مشخص از بیمه سایبری وجود دارد. از آن‌جایی که هنوز به طور مشخصی تعریفی از انگیزه‌های بیمه سایبری و خدماتی که می‌تواند پوشش دهد وجود ندارد، اعتماد گروه‌های مختلف بیمه‌ای نیز

کمرنگ است. از این رو، تعریف واحد و مشخص از پوشش بیمه و موارد خارج از پوشش بیمه می‌تواند اعتماد را به سازمان‌های بیمه‌گر بازگرداند. در بین پژوهش‌های مرتبط نیز، (Uuganbayar et al, 2020) بر تعریف واحد از مفهوم بیمه سایبری و تعریف دقیق نوع پوشش، تأکید کرده است. مؤلفه دیگر، میزان آمادگی تجهیزات فنی به منظور حفاظت از داده‌های سازمانی و شخصی شرکت‌ها است که این کار بر عهده شرکت‌های بیمه است. بدین‌ترتیب افزایش زیرساخت‌های فنی و تجهیزات شبکه‌ای به منظور راه اندازی بیمه سایبری و سپس بیمه کردن شرکت‌ها و مدیریت خطر سازمان‌های داوطلب، ورود به بیمه سایبری را شدت می‌بخشد. در پژوهش (Tonn et al, 2019) نیز به اهمیت تجهیزات فنی و آماده‌سازی ابزارهای رسیدن به بیمه سایبری، اشاره کرده است که بعد زیرساختی را عاملی برای ورود به بیمه سایبری می‌داند و بر اهمیت کارکردِ بیمه سایبری بعد از حوادث سایبری تأکید می‌کند. سرمایه‌گذاری در تجهیزات فنیِ بیمه سایبری عاملی برای اثربخشی و بررسی هزینه حوادث سایبری برای مدیران بیمه محسوب می‌شود. با نگاه به پژوهش (Rouzbahani & Hoseini, 2016)، نیز می‌توان دریافت که افزایش توجه به زیرساخت‌های بیمه در ایمن‌سازی فضای مجازی و جلوگیری از جرائم اینترنتی مؤثر است.

نتایج نشان داده است بیمه سایبری می‌توانند از محیط بین‌الملل نیز تأثیر پذیرفته و بر عکس، بر محیط بین‌الملل تأثیر بگذارد. در این بین عوامل فرهنگی و بینش افراد جامعه به این نوع بیمه، نوسانات اقتصادی حاصل از چالش‌های ارزی، ثبات سیاسی کشور و وضعیت اقتصادی افراد جامعه با عنوان عوامل محیطی تأثیرگذار بر بیمه سایبری شناخته شده‌اند. بدین ترتیب، حملات سایبری که از طریق سیستم‌های اطلاعاتی انجام می‌شود، به طور قابل توجهی متأثر عملکرد اجتماعی، اقتصادی و سیاسی جامعه است. از این‌رو مؤلفه دیگر از عوامل علی در پژوهش حاضر با عنوان عوامل شبکه بیمه سایبری شناسایی شده است که بر اکوسیستم و محیط اجرای بیمه سایبری تأکید داشته است. در کنار این عوامل، فرهنگ برخورد با بیمه سایبری به عنوان یک شیوه جدید ضمانت از داده‌های شخصی و به تبع آن اعتماد گروه‌ها و شرکت‌های مختلف می‌تواند محیطی را به وجود آورد که درکنار محیط سیاسی، اجتماعی و اقتصادی به عنوان یک شبکه مرتبط با هم بر پیاده‌سازی بیمه سایبری تأثیر بگذارد و مفهوم اکوسیستم را با بازیگران مؤثر در بیمه سایبری، به همراه شبکه‌ای از ارتباطات و همکاری را تداعی کند.

عوامل بسترساز

بر اساس نتایج تحقیق، دو مؤلفه مرکزیِ بررسی محیط بیرونی و درونی به عنوان عوامل بسترهای بیمه سایبری شناخته شوند. این عوامل تجهیزات فنی و میزان آمادگی زیرساختی سایبری را مورد توجه قرار می‌دهد و شامل توانایی سخت افزار، عوامل نرم افزاری، توان یا قدرت ابزار، محتوای اطلاعات، فناوری اطلاعات عوامل انسانی و سیاست‌های سایبری هستند. این عوامل با هدف پیاده‌سازی بیمه سایبری، عواملی هستند که در هسته اولیه تصمیم‌گیرندگان بیمه سایبری (شامل بیمه‌گذاران، دولت و یا شرکت‌های بیمه‌ای) قرا می‌گیرند. در عین حال، محیط بیرونی بر شناخت بازارهای رقیب در کشورهای دیگر و شناخت ریسک بازار و توجه به نوع ریسک و نهایتاً تسلط بر ریسک‌های سایبری زمینه سازهای تأکید می‌کند که تجزیه و تحلیل آن‌ها درک بهتری از بیمه سایبری به ما می‌دهد. مؤلفه اصلی دیگر با عنوان بازاریابی بیمه سایبری شناخته می‌شود که از طریق دو مؤلفه مرکزیِ عوامل اجرایی و تسهیل بیمه سایبری، به عنوان عوامل بسترساز بیمه

سایبری شناخته شده‌اند. در این جا، معرفی مزایای بیمه سایبری برای افراد و نهادهای ذینفع از طریق برنامه‌های آگاه‌کننده و ایجاد انگیزه و همچنین حمایت از فضای نوآور توسط شرکت‌های بیمه و اشاعه آن به عنوان عامل بازاریابی بیمه سایبری شناخته شده است. با این حال، مقایسه نتایج با پژوهش (Uuganbayar et al, 2020) نشان می‌دهد متغیرهای بازاریابی بیمه‌ای می‌تواند متفاوت باشد. در واقع توجه به مسائل اصلی و ساده‌سازی تجربه و تحلیلات بیمه سایبری و همچنین رویه‌های بیمه‌ای، درک بیمه، وابستگی متقابل[1]، قابلیت کسر شدن[2]، می‌تواند «مدل رقابتی بازاریابی» را تشکیل دهد. در این راستا، پژوهش (Bahsi, Franke & Friberg, 2020) با توجه به اینکه بازار بیمه سایبری در کشور نروژ را بررسی کرده‌اند، این کشور را از لحاظ بازاریابی بیمه سایبری در مراحل اولیه بلوغ بازار اسکاندیناوی می‌داند و دولت ملی را موظف می‌داند که بهترین درس‌های خارج از کشور را استفاده کند و از نوآوری در کشور حمایت کند تا نقش بیمه سایبری در ترویج جامعه ایمن را ترویج کند. با این حال پژوهش (Naldi & Mazzoccoli, 2021)، عامل توجه و معرفی بیمه سایبری را در گرو توجه به حق بیمه و تأثیر سرمایه‌گذاری‌های امنیتی می‌داند که می‌تواند از طریق اندازه-گیری سناریوهای مختلفی از جمله مسئولیت کامل، مسئولیت محدود و مسئولیت محدود با فرانشیز انجام شود.

پیامدهای بیمه سایبری

با توجه به نتایج پژوهش، پیامدهای بیمه سایبری می‌تواند در دو بخش مثبت و منفی قرار گیرد. بدین ترتیب، افزایش سطح دانشِ شرکت‌های بیمه‌ای و افزایش ایمنی و امنیت داده‌ها و بهبود خدمات و درآمد شرکت به عنوان مؤلفه‌های اصلی و مثبت شناخته شده‌اند. با اجرای بیمه سایبری، ضمن افزایش درک تغییرات محیطی و دانش رقابتی بیمه سایبری در سایر کشورها، شرکت‌های بیمه خود را با تغییرات بهتر تطبیق می‌دهند و با آمادگی بیشتر در مقابل خطرات سایبری و اینترنتی قرار می‌گیرند. به علاوه، تجربه برخورد با خطرات سایبری، نحوه بیمه سایبری، شناخت خسارت‌های سایبری و نهایتاً رشد بیمه سایبری، عواملی هستند که می‌توانند به افزایش درک و اجرای بیمه سایبری کمک می‌کنند. این بخش از نتایج با پژوهش (Wang, 2019) نیز همسو است؛ چراکه دانش برخورد با خطرات سایبری را برای ارزیابی خسارت سایبری شرکت‌ها ضروری می‌داند و گردآوری اطلاعات مهم بیمه به عنوان «گنجینه اطلاعات بیمه» را هموارکننده اشتراک اطلاعات تهدید سایبری[3]، داده حوادث سایبری و دانش مقابله با نفوذ و نشت اطلاعات می‌داند. پیامد مثبت دیگرِ اجرای بیمه سایبری، بهبود خدمات شرکت و افزایش رضایت استفاده کنندگان از بیمه سایبری خواهد بود. توجیه اقتصادی (با توجه به رشد اقتصادی، به روز شدن تجهیزات فناوری، کاهش هزینه‌ها، حفاظت از سرمایه‌های ملی، افزایش ضریب نفوذ بیمه و جبران خسارت سایبری)، افزایش رضایت (با توجه به معرفی خدمات برخط، بهبود خدمات برخط، بهبود پاسخ‌گویی به مشتریان و کاهش ریسک‌های مشتریان) و نهایتاً به روز شدن سطح خدمات از راه رعایت استانداردهای بیمه‌ای و استانداردسازی خدمات، مؤلفه‌های مرکزی استخراج شده از نتایج پژوهش بوده است. در اینجا می‌توان به پژوهش (Kshetri et al, 2020) اشاره کرد که معتقد است بازار بیمه سایبری بعد از مرحله زایش باعث به روز شدن ماهیت خدمات شده و شکل ارائه خدمات را تغییر می‌دهد.

[1] interdependence
[2] deducible
[3] cyber threat intelligence

بر اساس نتایج پژوهش حاضر، مهم‌ترین پیامد منفی اجرای بیمه سایبری عدم اطمینان از کارکرد بیمه سایبری با توجه به سردرگمی مشتری از عملکرد آن در یک سو و عدم توانایی برآورد خسارت توسط شرکت‌های بیمه از سوی دیگر بوده است. شاید بتوان یکی از دلایل عدم اطمینان از بیمه سایبری را جدید بودن آن در ایران دانست و یا آگاهی بخشی در این زمینه به خوبی صورت نگرفته است. از سوی دیگر عدم ارتباط با شرکت‌ها بیمه خارجی به دلیل تحریم‌های بین‌المللی نیز بی تأثیر نبوده است. جدید بودن این مفهوم نیز در سمت شرکت‌های بیمه‌گر نیز بر عدم اطمینان و نبود شاخص‌های معتبر در برآورد خسارت سایبری و ارزیابی ریسک و پوشش بیمه تأثیر خود را گذاشته است.

عوامل مداخله‌گر

با توجه به نتایج پژوهش، وجود پایگاه داده، دولت و سیاست‌های آن، نگرش بیمه‌ای، عملکرد شرکت‌های بیمه و مقررات بیمه به عنوان مؤلفه‌های مرکزی و تعیین کننده چشم انداز بیمه‌ای (به عنوان مؤلفه اصلی)، نقش مداخله‌گر در مدل استخراجی پژوهش داشته‌اند. بدین ترتیب، واحدهای تحقیق و توسعه با بررسی هزینه‌های تحقیق و پژوهش بعد از خسارت و همچنین تجربه سایر کشورها به عنوان منبعی برای ذخیره داده‌های سایبری شناخته می‌شوند. در پژوهش (Naldi & Mazzoccoli, 2021) نیز هزینه‌های تحقیق و بررسی خسارت، عامل مهمی در ایجاد فرمول‌های محاسبه در بیمه سایبری و سرمایه‌گذاری‌های بیمه سایبری بوده است. در ذهن افراد و یا گروه‌هایی که بیمه سایبری را دریافت می‌کنند نیز عنصر اعتماد، آگاهی بیمه‌گر و خرید آگاهانه بیمه زیر مجموعه نگرش بیمه‌ای (از عوامل دیگر مداخله‌گر در اجرای بیمه سایبری) به حساب می‌آید. این بخش از نتایج را می‌توان با پژوهش (Rezakhani & Dadbeh, 2021) مقایسه کرد که در آن متغیرهای حمایت مدیران ارشد، آموزش و فرهنگ سازمانی را بر اعتماد و نگرش بیمه‌ای و نهایتاً مدیریت ریسکِ جامع تأثیرگذار می‌داند. به علاوه، تعیین نقش هر بخش یا قسمت (که تداعی‌گر نقش هر عضو در اکوسیستم است)، حقوق کاربر مجازی، شرایط اعلامی بیمه‌گر و تعریف بیمه‌نامه به منظور شفاف‌سازی جزییات بیمه هر حادثه و نحوه پرداخت بیمه شده به عنوان «مقررات بیمه‌ای» نقش ایفا می‌کنند. در این‌جا می‌توان به پژوهش (Kabourati, 2019) استناد کرد که به اهمیت حقوق کاربر مجازی و آگاهی دادن به جامعه اشاره کرده است.

موانع بیمه سایبری

با توجه به اهمیت موضوع، موانع بیمه سایبری در سؤالات پرسشنامه نیز گنجانده شده بود. بر اساس نتایج پژوهش عامل عدم تسلط بر موضوع بیمه سایبری و عدم حمایت دولت به عنوان دو مانع اصلی اجرای بیمه سایبری شناخته می‌شود. این عوامل شامل عدم تسلط بر موضوع که با محیط غیر قابل پیش‌بینی، ضعف دانشی و ضعف آماری در ارتباط است و عدم حمایت دولت که با پروتکل‌های دولتی ارتباطات و قوانین دولتی دست و پاگیر مرتبط است، بوده‌اند. این بخش از نتایج را می‌توان با پژوهش (Bahsi, Franke & Friberg, 2020) مقایسه کرد که در آن پژوهشگران به حمایت بخش دولتی در کشور نروژ در ۲ سال اخیر اشاره کرده‌اند.

از لحاظ گستردگی خطرات سایبری، عدم اطمینان از جبران کامل خسارت و احتمال خسارت‌های هنگفت، اجرای بیمه سایبری با شک و تردیدهای زیادی رو به‌رو است که تا حدی به دلیل عدم شناخت و آگاهی از نوع خسارت و دانش کافی درباره این حوزه است. این بخش از نتایج غیرهمسو با نتایج با پژوهش (Kabourati, 2019) است؛ چرا که در آن

تبلیغات، آشنایی و آگاهی دادن جامعه نسبت به کاربرد و فوایـد خدمات بیمه سایبری، از اهمیت بیشتری نسبت به سایر زیرشاخص‌ها دارند. همچنین، نبود انگیزه در بین ارائه دهندگان خدمات بیمه‌ای، عدم تجربه بیمه‌گرها، عدم توانایی در شناخت نوع ریسک، عدم شناخت از ریسک‌های موجود، نداشتن دانش لازم در ارزیابی ریسک و عدم آگاهی از ریسک و عدم تخصص و پروتکل مشخص بیمه‌گران باعث کمبود اطلاعات و دانش درباره بیمه سایبری به عنوان یکی از موانع بیمه سایبری بوده است. این بخش از نتایج را می‌توان با پژوهش (Kshetri et al, 2020) مقایسه کرد و البته غیرهمسو دانست؛ چراکه در آن پژوهشگران بیمه سایبری را به واسطه عدم شناخت آن ابزاری انگیزشی می‌داند که در حال زایش و ظهور در بین نهادهای رسمی و غیر رسمی است.

راهبردهای بیمه سایبری

نتایج حاصل از پژوهش و بررسی کدهای استخراج شده از مصاحبه نشان داد که رویکرد اکوسیستمی و تدوین استراتژی بیمه‌ای به عنوان دو رویکرد اصلی (مقوله اصلی) در مدل استخراجی پژوهش شناخته شده‌اند. رویکرد اکوسیستمی بر بازاریابی بیمه سایبری (از راه ارائه برنامه بلند مدت و کوتاه مدت، معرفی بیمه‌نامه و طراحی بیمه نامه فراگیر و جذاب)، رویکرد شبکه‌ای با توجه به تشکیل کارگروه فنی، تعیین شفافیت هر کدام از قسمت‌ها، تعیین نقش بازیگران درگیر و نقش دولت به عنوان متولی گسترش اقتصاد دیجیتال و نهایتاً مدلسازی بیمه سایبری از طریق بهره‌برداری از مدل‌های استاندارد، نقص قانونی مرتبط با فضای سایبری، شناسایی و دسته‌بندی ریسک‌ها و تدوین شرایط عمومی بیمه سایبری به عناون راهبردهای مرکزی و اولیه بیمه سایبری شناخته شده است. از لحاظ بررسی مدل‌ها، پژوهش (Mazzccoli & Naldi, 2021) با استفاده از مدل گوردن و لوئب به دو رویکرد مدیریتی ریسک سایبری (سرمایه‌گذاری در امنیت و بیمه سایبری) اشاره کرده‌اند که می‌تواند در بهینه‌سازی هزینه‌های امنیت استفاده شود. راهبرد دیگر با توجه به ایمن کردن داده‌ها و شرح دقیق پوشش‌های بیمه‌ای مشخص شده است. ایمن کردن داده‌ها با توجه به تست‌های نفوذ و امنیتی دوره‌ای، داشتن مجوزات امنیتی، نگهداری نسخه فایل پشتیبان، داشتن فرآیند نسخه پشتیبان، نگهداری بی از یک نسخه پشتیبان و محدود کردن پورتهای دسترسی، انجام اقدامات پیشگیرانه و کنترل دسترسی‌ها تحقق می‌یابد. همچنین شرح دقیقی از پوشش‌های بیمه‌ای با توجه به پوشش هزینه‌های حقوقی خسارت، پوشش خسارت اطلاعات غیر قابل بازگشت، پوشش هزینه‌های از دست دادن داده‌ها، پوشش خسارت وقفه در کسب و کار اینترنتی و پوشش هزینه بازگردانی اطلاعات از دست رفته راهبرد دیگر اجرای سریع‌تر بیمه سایبری محسوب می‌شود. این بخش از نتایج با نتایج پژوهش (Bahsi, Franke & Friberg, 2020) و (wang, 2019) همسو بوده است چراکه در پژوهش اشاره شده رویه‌های عمومی حفاظت از داده‌ها توانسته است تأثیر متوسطی بر بازار بیمه داشته باشد و توسط بخش عرضه به عنوان یک عامل قابل توجه مشتریان بیمه شناخته شود و ضررهای سایبری را کاهش دهد و ارزش اقتصادی ایجاد کند.

با توجه به نتایج پژوهش به ویژه پیامدهای منفی و موانع اجرای بیمه سایبری که بر اساس نظرات خبرگان استوار شده‌اند می‌توان پیشنهاداتی ارائه داد.

۱. به دلیل عدم تسلط بر موضوع بیمه سایبری و عدم شناخت آن برای سازمان‌های بیمه‌گر و عدم اطمینان کافی در استفاده از این نوع بیمه، پیشنهاد می‌شود در مرحله اول اطلاع رسانی بر اساس مزایای بیمه سایبری در همه کسب و کارهای مبتنی بر اینترنت توسط دولت انجام شود.

۲. به دلیل عدم حمایت دولت پیشنهاد می‌شود شرح دقیق نوع خسارت سایبری و پوشش بیمه توسط سازمان‌های بیمه‌گر

۳. استفاده از درس‌های کشورهای خارجی به منظور شناسایی فرمول‌های تعیین خسارت و ارزیابی ریسک‌های آینده

۴. تهیه فهرستی از کمبودهای فنی و زیرساختی بیمه سایبری در شرکتهای بیمه‌ای به منظور تأمین ضرورت‌های بیمه سایبری

۵. با توجه به تردید محاسبه ضررهای بیمه، استفاده از ابزارهای پیش‌بینی محیط (همچون روش سری زمانی) به منظور کاهش خسارت‌های سایبری و احتمالی

۶. ایجاد پایگاه داده و آمار توسط شرکت‌های بیمه‌ای در جهت ثبت اتفاقات سایبری و استفاده از آن‌ها در تعیین خسارت‌های سایبری

در پژوهش‌های بعدی پیشنهاد می‌شود مدل استخراجی پژوهش با استفاده از مدلسازی ساختاری تفسیری به ارائه یک مدل کمی و قابل اندازه‌گیری با تحلیل عاملی مورد آزمون قرار گیرد. همچنین با استفاده از نظر خبرگان و مصاحبه تخصصی به اولویت‌بندی شاخص‌های استخراج شده پرداخته شود. در نهایت پژوهشگران می‌توانند سازمان‌های متقاضی بیمه سایبری را بر اساس عملکرد و ماهیت طبقه‌بندی کنند و تأثیر بیمه سایبری بر هر کدام را جداگانه بررسی کنند.

از مهم‌ترین محدودیت‌های پژوهش کمبود متخصصان صاحب نظر و با دانش در زمینه بیمه سایبری بوده است که می‌توان گفت عدم شناخت کافی از این حوزه و جدید بودن آن، تأثیر زیادی بر تعداد افراد خبره داشته است. محدودیت دیگر در پژوهش حاضر کمبود مطالعات داخلی در زمینه بیمه سایبری بوده که می‌توان گفت بر محدودیت اول نیز تأثیر داشته است و اظهار نظر درباره این رویکرد بیمه‌ای را با مشکل روبه رو کرده است. همچنین کمبود مطالعات داخلی مقایسه نتایج را با دشوار روبه رو کرده است.

References

Adibi, M., Daryayi, A & zahdi, A. (2017). A review of internet risks and the role of cyber insurane in their management place of publication. Second international conference on management and accounting, 42-61. MANAGECONF02_0257. [In Persian],https://doi.org/10.1002/9781118445112.stat00365.pub2

Aghabeigi Nasrollahabadi, M., garkaz, M., matoofi, A., & khozain, A. (2023). presenting a model for company 's financial strategies with environmental approach and accountability. Journal of value creating in Business Management, 3(3), 108-128, https://doi.org/10.22034/jvcbm.2023.407532.1146.

Alizadeh, S., Nourbakhsh, K., & ghasemi, B. (2023). Identifying the effective dimensions and components on research and development strategies in domestic automobile companies. Journal of value creating in Business Management, 3(3), 293-311, https://doi.org/10.22034/jvcbm.2023.417612.1198.

Arabshahi, M., & Abbaszadehgaretekan, H. (2022). The Impact of Electronic Customer Relationship Management on Marketing Performance with the Analysis of the Mediating Role of Product Innovation and Emphasis on Customer Knowledge. Journal of value creating in Business Management, 3(2), 42-61. https://doi.org/10.22034/jvcbm.2023.396709.1088. [In Persian]

Awiszus, K., Knispel, T., Penner, I. et al. Modeling and pricing cyber insurance. Eur. Actuar. J. 13, 1–53 (2023). https://doi.org/10.1007/s13385-023-00341-9

Bahsi, H., Franke, U., F, E.L. (2020). The cyber-insurance market in Norway. Information & Computer Security. 28 (1): 54-67. DOI 10.1108/ICS-01-2019-0012.

Bahari, B., Taheri Rouzbahani, M. (2023). Designing an electronic human resources management model based on knowledge creation in knowledge-based companies. Journal of value creating in Business Management, 3(1), 106-121. https://doi.org/10.22034/jvcbm.2023.392785.1082. [In Persian]

Baker, T., Shortland, A. Insurance and enterprise: cyber insurance for ransomware. Geneva Pap Risk Insur Issues Pract 48, 275–299 (2023). https://doi.org/10.1057/s41288-022-00281-7

Bohme, R. and Kataria, G. (2006), "Models and measures for correlation in cyber-insurance", The Fifth Workshop on the Economics of Information Security (WEIS 2006). 26-28 June 2006, https://doi.org/10.1002/9781118445112.stat00365.pub2.

Cebula, J. J. and Young, L. R. (2010) 'A taxonomy of operational cyber security risks: technical Note CMU/SEI-2010-TN-028', Software Engineering Institute, Carnegie Mellon University. 10.1184/R1/6571784.v1. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Eling, M., Schnell, W., 2016. What do we know about cyber risk and cyber risk insurance? Journal of risk finance. 17 (5): 474-491, DOI: 10.1108/JRF-09-2016-0122.

Elsan, M. (2021). Electronic commerce law. Samt publication.9th edith. Tehran, ISBN:978-964-530-826-9

Friedman, S. (2017). Deloitte University Press, Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising market. https://www2.deloitte.com/ insights/us/en/industry/financial-services/demystifying-cybersecurity-insurance.html, https://doi.org/10.1016/j.telpol.2020.102007

Ghoodjani, A. (2015). Advanced statistical methods and applications. Jame-e-Negar Publishing House(JPH) .Tehran. [In Persian], https://doi.org/10.22034/jvcbm.2023.383338.1049.

Hajizadeh Majdi, R., Fatahi, S., & Ranjbar, I. (2023). Analyzing the Quantum Leadership's Dimensions, Components and indexes of the Broadcasting Organization in the field of Social Network with Delphi Fuzzi Method. Journal of value creating in Business Management, 2(4), 61-82, https://doi.org/10.22034/jvcbm.2023.383338.1049.

Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martn Ochoa. "insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures." ACM Computing Surveys (CSUR) 52 (2): 1–40, https://doi.org/10.1145/3303771

Kabourati, J. (2019). Identifying and Ranking Factors affecting the Application of the Electronic Insurance in the Insurance Industry: A case Study of selected Insurance Companies. Journal of Insurance Research. 34 (2): 50-69. DOI):10.22056/jir.2019.98422.2156. [In Persian]

Kraemer, H. C. (2014). Kappa coefficient. Wiley StatsRef: Statistics Reference Online, 1-4 .https://doi.org/10.1002/9781118445112.stat00365.pub2

Landis, J.R., Koch, G.G (1997). The Measurement of Observer Agreement for Categorical Data. International Biometric Society. 33 (1): 159-174. https://doi.org/10.2307/2529310

Kshetri, N., (2020). The evolution of cyber-insurance industry and market: An institutional analysis. Telecommunications Policy. 164-196, https://doi.org/10.1016/j.telpol.2020.102007.

Mahmoudi, J., & Pourshahabi, V. (2023). Investigating the effect of financial intelligence value on employees' risk taking with the mediating role of social capital. Journal of value creating in Business Management, 2(4), 25-45. https://doi.org/10.22034/jvcbm.2023.314246.1009. [In Persian]

Mazzccoli, A., Naldi, M. (2021). Optimal Investment in Cyber-Security under Cyber Insurance for a Multi-Branch Firm. Risks. 9 (24): 1-28. https://doi.org/10.3390/risks9010024.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013), "Cyber-risk decision models: to insure IT or not?", Decision Support Systems.56: 11-26, doi: 10.1016/j. dss.2013.04.004.

Poorghasab, A., Hasani, M.A (2017). Cyber insurance, one solution to create security in cyber space. 6th national conference on law and judicial studies. 57- 92. LLSC06_023. [In Persian], https://civilica.com/doc/877233.

Rousta, A., allafjafari, E., & ahmadi, M. (2023). The effect of e-satisfaction and trust on online repurchase intention through the mediation of ease of use and moderation of customers' online experience. Journal of value creating in Business Management, 3(1), 57-81. https://doi.org/10.22034/jvcbm.2023.392081.1081. [In Persian]

Rezakhani, M., Dadbeh, F. (2021). The Role of Internal Audit in Comprehensive Risk Management of Iranian Insurance Companies. Iranian Journal of Insurance Research. 36 (1): 147-172. DOI: 10.22056/JIR.2021.225992.2710. [In Persian]

Soleymani Rouzbahani, F., Hoseini, R. (2016). Study of crime and security insurance in cyberspace. International Conference on Modern Research's in Management, Economic & Accounting. Kualalampur- Malaysia. MRMEA02_203. [In Persian], http://dx.doi.org/10.1145/2857546.2857615.

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

Tsohou, A., Diamantopoulou, V., Gritzalis, S. et al. Cyber insurance: state of the art, trends and future directions. Int. J. Inf. Secur. 22, 737–748 (2023). https://doi.org/10.1007/s10207-023-00660-8

Uuganbayar, G., Yautsiukhin, A., Martinelli, F, (2020). Optimisation of cyber insurance coverage with selection of cost effective security controls. Journal Pre-proof. 101: 139-156. https://doi.org/10.1016/j.cose.2020.102121

Wang, S., (2019). Integrated framework for information security investment and cyber insurance. Pacific-Basin Finance Journal. 57: 122-145. https://doi.org/10.1016/j.pacfin.2019.101173

Wanchun, D., Wenda, T., (2018). An Insurance Theory Based Optimal Cyber-Insurance Contract Against Moral Hazard. Journal Pre-proof. 527: 105-152. https://doi.org/10.1016/j.ins.2018.12.051.