Scientific Journal of Electronical & Cyber Defence
Vol. 13, No. 1, Spring 2025, Serial No. 49

Analyzing the concept of cyber risk and its security coverage methods

A. Hamzeh *,S. Mireh, Z. Kalhor, H. Fathi Nooran

* Assistant Professor, Insurance Research Institute, Tehran, Iran

Received:2024 /12/26, Revised: 2025/01/21, Accepted: 2025/03/03, Published: 2025/04/21

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.1.3.8

ABSTRACT

Considering the rapid digitization of many aspects of life, the increase in cyber attacks is not unexpected. Some of today's cyber risks do not meet the usual insurable characteristics and cannot be insured. Limited insurability despite growing demand for cyber insurance poses challenges for long-term market growth. In Iran, cyber insurance has not received much attention due to the lack of knowledge and awareness.
In this paper, a formal definition for cyber risk was presented. The types of risks were classified based on the attack scenario. Also, the types of accidents and their insurance coverage areas were examined. In a part of the paper, cyber risk insurability criteria and changes to improve insurability were presented, and also the types of cyber insurance coverage and the consequences of cyber risk in the insurance industry were examined in order to help design cyber insurance policies in the country.

Keywords: Cyber risk, Insurance coverage, Information exchange space. .

* Corresponding Author Email: hamze2006@yahoo.com

«پدافند الکترونیکی و سایبری»
سال سیزدهم، شماره ۱، فصل بهار ۱۴۰۴؛ ص ۴۳-۲۹
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

واکاوی مفهوم ریسک سایبری و روش‌های پوشش امنیت آن

اسماء حمزه[۱]، سمیه میره[۲]، زهرا کلهر[۳]، هانیه فتحی نوران[۴]
۱-استادیار، ۲- استادیار، پژوهشکده بیمه، تهران، ایران،۳-دانشجوی دکتری،۴- دانشجوی دکتری، تهران، ایران

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.1.3.8
(دریافت: ۱۴۰۳/۱۰/۰۶، بازنگری: ۱۴۰۳/۱۱/۰۲، پذیرش: ۱۴۰۳/۱۲/۱۳، انتشار: ۱۴۰۴/۰۲/۰۱)

چکیده

باتوجه‌به سرعت دیجیتالی‌شدن بسیاری از امور زندگی، افزایش حملات سایبری خارج از انتظار نیست. برخی از ریسک‌های سایبری امروزی با ویژگی‌های معمولی بیمه‌پذیر بودن مطابقت ندارند و نمی‌توان آنها را بیمه نمود. بیمه‌پذیری محدود باوجود تقاضای روبه‌رشد بیمه سایبری، چالش‌هایی را برای رشد بازار در بلندمدت ایجاد می‌کند. در ایران بیمه سایبری، به دلیل عدم شناخت و آگاهی لازم، چندان مورد توجه قرار نگرفته است.

در این مقاله یک تعریف استاندارد برای ریسک سایبری بر اساس تعاریف موجود ارائه شد. دسته‌بندی انواع ریسک‌ها بر اساس سناریوی حمله انجام شد. همچنین انواع حادثه و حوزه‌های پوشش بیمه آن مورد بررسی قرار گرفت. در بخشی از مقاله معیارهای بیمه‌پذیری ریسک سایبری و تغییرات برای بهبود بیمه‌پذیری ارائه گردید و همچنین انواع پوشش بیمه سایبری و پیامدهای ریسک سایبری در صنعت بیمه مورد بررسی قرار گرفت تا بتواند برای طراحی بیمه‌نامه‌های سایبری در کشور کمک‌کننده باشد.

کلیدواژه‌ها: ریسک سایبری، پوشش بیمه، فضای تبادل اطلاعات.

۱. مقدمه

امروزه در شروع هزاره سوم میلادی فناوری‌های نوین اطلاعات و ارتباطات به نحوه شگفت‌آوری وارد ساختار زندگی انسان‌ها شده است که تجلی آن فضای تبادل اطلاعات یا فضای سایبر است [۱]. فضای سایبری که به اختصار فتا نامیده می‌شود، فضای تشکیل‌یافته از اتصال زیرساخت‌های فناوری اطلاعات، سامانه‌ها و شبکه‌های ارتباطی است. این فضا اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای، سامانه‌های پردازشی، سامانه‌های ارتباطی- اطلاعاتی و ... را شامل می‌شود. وجه تسمیه این فضا از آن جهت است که امکان ذخیره‌سازی، انتشار و تبادل اطلاعات و داده‌ها را فراهم می‌نماید. به دلیل مزایای متعدد فتا، امروزه استفاده از ابزارهای این حوزه به صورت روزافزونی توسعه می‌یابد و همه شئون جوامع بشری را در سطح خرد و کلان به صورت جدی و اساسی تحت تأثیر قرار داده است. رشد و توسعه فتا و سامانه‌های فعال در این فضا، در کنار همه‌ی مزایایی که داشته باعث ایجاد انواع ریسک‌ها و تهدیدات جدید برای کاربران در تمام سطوح، از شهروندان عادی تا سازمان‌های بزرگ خصوصی و دولتی شده است. در سال‌های اخیر نقض حریم شبکه‌های اطلاعاتی و ارتباطی که بیشتر با نام حملات سایبری شناخته می‌شوند، به‌صورت نمایی در حال افزایش است [۲]. با گسترش روزافزون حملات سایبری، ایجاد امنیت برای فضای سایبری نیز حساس‌تر و مهم‌تر شده است. بنابراین رایانه‌ها، شبکه‌های رایانه‌ای و تمام سامانه‌های رایج با قابلیت اتصال به شبکه اینترنت، همواره در معرض خطر حملات سایبری قرار دارند [۳].

به‌صورت خلاصه، ریسک سایبری، ریسکی است که از اجرای فعالیت‌های فضای سایبری ناشی می‌شود و دارایی‌های اطلاعاتی، منابع فناوری اطلاعات و ارتباطات و دارایی‌های فناورانه را تحت‌تأثیر قرار می‌دهد [۴].

در دنیای کنونی، حفاظت از اطلاعات، از جمله مسائل چالش‌برانگیز نهادهای مختلف در سراسر جهان محسوب می‌شود و هر روزه اخبار متعددی از حملات سایبری منتشر می‌شود. برای مواجهه با این امر، سازمان‌های مختلف همواره بر افزایش امنیت اطلاعات و داده‌ها و پیشگیری از ریسک‌های سایبری تأکید نموده و هزینه‌های گزافی را در این حوزه متحمل می‌شوند [۵].

بر اساس گزارش سنجش ریسک آلیانز[۱]، جرایم سایبری

[1] Allianz Risk Barometer

رایانامه نویسنده مسئول، hamzeh@irc.ac.ir

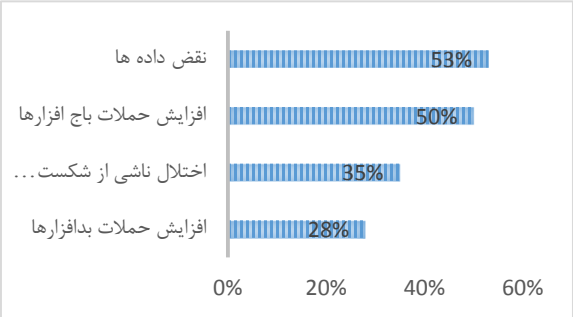
سالانه بیش از هزار میلیارد دلار به اقتصاد جهانی خسارت وارد می‌کنند که تقریباً برابر با یک درصد GDP جهانی است. بنابراین درصورتی‌که راهکارهای مقابله با انواع مختلف ریسک‌ها و حملات سایبری توسط سازمان‌های مرتبط پیش‌بینی و در دستور کار قرار نگیرد، می‌تواند آثار خطرناک و در برخی موارد جبران‌ناپذیری برجای بگذارد. روش‌های مختلفی به‌منظور مدیریت ریسک امنیت سایبری توسط نهادهای مختلف به کار گرفته می‌شود. اگرچه موضوع پوشش بیمه سایبری از دهه ۱۹۷۰ میلادی در دنیا مطرح بوده لیکن در کشورمان تاکنون به‌صورت منسجم و مشخص، پوشش‌های خاص این حوزه برای بهره‌برداری مشتریان ارائه نشده است. به‌عبارت‌دیگر، امروزه بازار بیمه‌های سایبری به‌عنوان یکی از راهکارهای عملیاتی به‌منظور استفاده از مزایای اقتصادی و اجتماعی دنیای دیجیتال در کنار کاهش ریسک استفاده از این فضا، مورد توجه قرار گرفته است.

بررسی‌های جامعی در خصوص مفهوم و تعریف ریسک سایبری صورت‌گرفته است. آل[1] و همکاران علت این بررسی‌های متعدد را نیاز به استانداردسازی و یکسان‌سازی دیدگاه‌های مختلف در مورد ریسک‌های سایبری می‌دانند [۶]. آوِن[2] تسهیل در پیاده‌سازی‌های فنی دستورالعمل‌های ایمنی و امنیت را علت اصلی این بررسی‌های همه‌جانبه عنوان کرده‌اند. به‌هرحال آنچه حائز اهمیت است این مطلب است که درک بهتر ریسک، سنگ بنای فرآیند مدیریت ریسک است [۷]. برخی پژوهش‌ها نیز بر سایر جنبه‌های ریسک سایبری، از جمله انگیزه‌های پیروی از سیاست‌های امنیت سایبری، نحوهٔ گسترش ریسک‌های سایبری توسط کارکنان سازمان‌ها، نحوهٔ تعامل کارکنان با انواع جرائم و ریسک‌های سایبری را بررسی نموده‌اند. علی‌رغم پژوهش‌های صورت‌گرفته، به نظر می‌رسد که هنوز نیاز به توسعه یک تعریف آکادمیک، جامع و پذیرفته شده از ریسک سایبری وجود دارد.

هدف این پژوهش، ارائه یک تعریف استاندارد از ریسک سایبری و احصاء انواع آن، بررسی بیمه‌پذیری ریسک‌های سایبری و بررسی انواع پوشش‌های بیمه‌های سایبری و پیامدهای ریسک سایبری برای صنعت بیمه است. بدین منظور، در بخش دوم مبانی نظری بیان می‌شود. در بخش سوم به مروری بر پیشینه تحقیق پرداخته می‌شود و بخش چهارم به روش تحقیق اختصاص دارد. نتایج تحقیق در بخش پنجم بیان می‌شود و در نهایت بخش ششم نتیجه‌گیری است.

۲. مبانی نظری

شرکت بیمه‌ای آلیانز هرساله با نظرسنجی از مشتریان و کارگزاران خود در سراسر جهان و سازمان‌های تجاری صنعتی و متخصصان و مدیران ارشد و کارشناسان خسارت و سایر متخصصان مدیریت ریسک، گزارشی تحت عنوان سنجش ریسک آلیانز منتشر می‌کند و ریسک‌های مهم کسب‌وکار را شناسایی و گزارش می‌کند. در دوازدهمین نسخه منتشر شده این گزارش در سال ۲۰۲۲، حوادث سایبری به‌عنوان مهم‌ترین ریسک کسب‌وکارها در سال ۲۰۲۳ معرفی شده است. جرایم سایبری بیش از یک تریلیون دلار در سال برای اقتصاد جهانی هزینه دارد. همچنین در بین ریسک‌های سایبری، نقض داده مهم‌ترین نگرانی شرکت‌ها عنوان شده است [۸]. در شکل ۱، مهم‌ترین نگرانی شرکت‌ها در خصوص ریسک‌های سایبری نمایش‌داده‌شده است.



شکل (۱): مهم‌ترین نگرانی شرکت‌ها در خصوص ریسک‌های سایبری [۸].

شرکت سایبرسکوریتی ونچرز[3] گزارش‌های سالانه و فصلی در مورد موضوعاتی چون هزینه‌های جرایم سایبری، اندازه بازار امنیت سایبری و پیش‌بینی هزینه‌ها و به‌طورکلی تحقیقات و تجزیه‌وتحلیل‌هایی در مورد بازار جهانی امنیت سایبری منتشر می‌کند. طبق آخرین گزارش این شرکت در مورد جرایم سایبری که در سال ۲۰۲۲ منتشر شده است، پیش‌بینی شده است که هزینه سالانه جهانی جرایم سایبری در سال ۲۰۲۳ به ۸ تریلیون دلار در سال خواهد رسید. هزینه‌های جرایم سایبری شامل آسیب و تخریب داده‌ها، پول‌های دزدیده شده، بهره‌وری ازدست‌رفته، سرقت مالکیت معنوی، سرقت اطلاعات شخصی و مالی، اختلاس، کلاهبرداری، وقفه در کسب‌وکار پس از حمله، هزینه‌های تحقیقات قانونی، بازیابی و حذف داده‌ها و سیستم‌های هک شده و آسیب به اعتبار سازمان است. همچنین پیش‌بینی شده است که هزینه آسیب‌های جرایم سایبری از سه تریلیون دلار در سال ۲۰۱۵ به ۱۰٫۵ تریلیون (هزار میلیارد) دلار در سال ۲۰۲۵ افزایش یابد [۹].

جمع‌آوری آمار مربوط به خسارات و حملات سایبری در ایران بر عهده سازمان فناوری اطلاعات ایران و مرکز مدیریت راهبردی افتای ریاست‌جمهوری می‌باشد. ولی تاکنون آمار رسمی و دقیق

[1] Ale
[2] Aven
[3] Cybersecurity Ventures

در این حوزه منتشر نشده است. لیکن بر اساس آمار غیررسمی، در سال ۱۴۰۱، تعداد ۸۳۲۱ حمله سایبری دفع شده وجود داشته است. همچنین در سال ماقبل آن، رشد ۱۴ درصدی در میزان جرایم سایبری حادث شده است. کلاهبرداری‌های اینترنتی، برداشت‌های اینترنتی، هتک حیثیت، نشر اکاذیب، دسترسی غیرمجاز به داده و مزاحمت‌های اینترنتی از مهم‌ترین جرائم سایبری در سال ۱۴۰۱ بوده است. کلاهبرداری اینترنتی که عمدتاً به حوزه سایبر-الکترونیک مربوط می‌شود، از جمله ارسال لینک‌های آلوده از طریق پیامک و پیام‌رسان‌ها، نسبت به سال ۱۴۰۰، افزایش حدود ۳۷ درصدی داشته و برداشت‌های اینترنتی در صدر جرایم سایبری سال ۱۴۰۱ قرار گرفته است. لازم به ذکر است که بعد از اجرایی‌شدن طرح رمز دوم یکبار مصرف در سال ۱۳۹۸ و گسترش آگاهی‌بخشی پلیس فتا، از میزان شیب صعودی آمار مرتبط با کلاهبرداری از طریق دسترسی غیرمجاز به‌حساب مالی افراد کاسته شده است. همچنین از منظر تمرکز جغرافیایی استان‌های تهران، اصفهان، مازندران و خراسان رضوی استان‌هایی هستند که به ترتیب، بیشترین حجم کلاهبرداری‌های اینترنتی را در کشور به خود اختصاص داده‌اند.

علاوه بر موارد فوق‌الذکر، برخی چالش‌های مختص کشورمان وجود دارد که ریسک‌های مرتبط با امنیت سایبری را بیشتر از سایر کشورها متأثر نموده و موجب افزایش پیچیدگی‌های مدیریت این موضوع شده است. از جمله این موارد می‌توان به موانع ذیل اشاره نمود:

-تضییقات تحریمی و برخی محدودیت‌های داخلی؛

-تنش‌های سیاسی حول مسائل نظامی، امنیتی و هسته‌ای؛

-بهره‌برداری از انواع مختلف ابزارهای جاسوسی توسط دشمنان؛

-مهندسی اجتماعی ناشی از عدم آگاهی عمومی از طریق انواع مختلف ابزارهای تبلیغی یا دریافت کلیکی؛

-وجود حجم قابل‌توجهی از دیتابیس‌های ارزشمند روی نسخه‌های کرک شده؛

-استفاده از ابزارهای فاقد پچ و پشتیبانی مؤثر، اعم از سخت‌افزاری و نرم‌افزاری؛

-قدیمی شدن بسیاری از تجهیزات مورد استفاده در سازمان‌ها؛

-فقدان تعاملات مؤثر با مراکز و آزمایشگاه‌های بین‌المللی در خصوص ویروس‌ها، تروجان‌ها، باج‌افزارها و... و در نتیجه عدم دریافت بازخوردهای به هنگام؛

-فراگیر بودن استفاده از ابزارهای VPN؛

-ناترازی درآمد-هزینه بنگاه‌ها و به‌صرفه نبودن سرمایه‌گذاری در ظرفیت‌های امنیت سایبری؛

-اطاله زمانی در پروسه‌های آزمایشگاهی؛

-دورزدن الزامات قانونی توسط پیمانکاران.

حوادث سایبری ابعاد مختلفی از پیامدها را شامل می‌شود که لزوماً امکان جبران همه آن‌ها فراهم نیست. بنابراین در راستای کاهش خسارات مرتبط با حملات سایبری بخشی از هزینه‌های قابل‌جبران می‌تواند ذیل انواع مختلف پوشش‌های بیمه‌ای مورد بحث‌وبررسی قرار گیرد. خسارت به اموال و دارایی‌های مشهود و نامشهود، وقفه در کسب‌وکار، سرقت، و همچنین اشکال مختلف مسئولیت در قبال مشتریان، کارکنان، سهامداران و... از جمله این موارد می‌باشد. انواع مختلف پوشش‌های بیمه‌ای مذکور با نظر داشت طبقه‌بندی انجمن CRO را می‌توان در قالب جدول ذیل جمع‌بندی نمود:

جدول (۱): انواع حادثه و حوزه‌های پوشش بیمه‌ای آن.

گروه‌بندی انواع حوادث	حوزه‌های پوشش
وقفه در کسب‌وکار[1]/ وقفه در عملیات[2]	پرداخت سود ازدست‌رفته ناشی از وقفه در تولید که ناشی از آسیب‌های فیزیکی نیست.
وقفه در کسب‌وکار مشروط (CBI[3]) برای خسارات غیرفیزیکی	پرداخت سود ازدست‌رفته ناشی از وقفه در عملکرد اشخاص ثالث مرتبط مانند تأمین‌کنندگان، شرکا، مشتریان به‌جز خسارات مربوط به آسیب‌های فیزیکی
خسارات داده‌ها و نرم‌افزارها	هزینه‌های بازسازی و جایگزینی و بازگردانی و تولید مجدد داده یا نرم‌افزاری که از بین رفته، خراب یا دزدیده شده و یا رمزنگاری شده است.
سرقت مالی یا کلاهبرداری[4]	زیان‌های مالی خالص ناشی از فعالیت‌های مخرب داخلی یا خارجی سایبری که باهدف کلاهبرداری، سرقت پول یا سایر دارایی‌های مالی؛ مانند سهام انجام شده باشد. این مورد خسارات مالی به شرکت بیمه شده و خسارات مالی متوجه اشخاص ثالث مرتبط با شرکت، در نتیجه تخلف ثابت شده شرکت تحت پوشش، را تأمین می‌کند.
باج‌گیری و اخاذی سایبری[5]	هزینه‌های کارشناسی رسیدگی به باج‌گیری یا پرداخت باج در یک حادثه باج‌گیری به طور مثال

[1] Business interruption
[2] Interruption of operations
[3] Contingent business interruption
[4] Financial theft or fraud
[5] Cyber ransom and extortion

	زمانی که دسترسی به داده‌ها تا زمان پرداخت باج، امکان‌پذیر نباشد.
سرقت مالکیت معنوی[1]	ازدست‌دادن ارزش یک دارایی معنوی که منجر به یک زیان خالص مادی شود.
هزینه‌های واکنش به حادثه	جبران هزینه‌های مدیریت بحران و اقدامات اصلاحی که مستلزم هزینه‌های کارشناسی داخلی یا خارجی است؛ اما شامل هزینه‌های دفاع قانونی و نظارتی نمی‌شود. پوشش شامل موارد زیر است: ۱)تحقیقات IT و تجزیه و تحلیل قانونی به استثنای مواردی که مستقیما به هزینه‌های دفاع قانونی و نظارتی مربوط می‌شوند. ۲) روابط عمومی و هزینه‌های ارتباطات ۳) هزینه‌های اصلاحات به عنوان مثال هزینه‌های حذف یا فعالسازی هجومیه محتوای مخربی که علیه بیمه شده منتشر شده است. ۴) هزینه‌های اطلاع‌رسانی
(جبران) نقض حریم خصوصی[2]	هزینه‌های جبران خسارت پس از نشت داده‌های خصوصی یا حساس از جمله خدمات اعتبارانی به‌جز هزینه‌های واکنش به حادثه
(مسئولیت) امنیت/نقض امنیت شبکه	هزینه‌های جبران خسارت وارده به اشخاص ثالث (شریک، کارپرداز، ارائه‌دهنده، مشتری) از طریق شبکه IT بیمه‌گذار بدون احتساب هزینه‌های واکنش به حادثه. بیمه‌گذار ممکن است دچار آسیب نشده باشد؛ ولی به‌عنوان یک کانال یا مسیر برای دسترسی به شخص ثالث استفاده شده باشد.
خسارت وارد به شهرت[3] **(به‌استثنای حمایت حقوقی)**	جبران سود ازدست‌رفته ناشی از کاهش خریدوفروش یا مشتریان به دلیل ازدست‌رفتن اعتماد آنها نسبت به شرکت
هزینه‌های مقرراتی و دفاع حقوقی (به‌استثنای جریمه)	الف) هزینه‌های مقرراتی[4]: جبران هزینه‌هایی که شرکت یا اشخاص ثالث مرتبط با آن در زمان تحقیقات دولتی یا نظارتی مربوط به یک حمله سایبری متحمل می‌شوند. (خدمات قانونی، فنی یا IT که مستقیماً با تحقیقات مرتبط می‌شود را پوشش می‌دهد به‌استثنای مبلغ جریمه) ب) هزینه‌های دفاع حقوقی[5]: پوشش برای هزینه‌های دفاع از شرکت یا اشخاص ثالث مرتبط که در پی حمله سایبری در دادگاه با پیگرد قانونی مواجه شده‌اند.
جریمه‌ها و مجازات‌های مالی	جبران هزینه‌های جریمه‌ها و مجازات مالی که شرکت محکوم به پرداخت شده است. غرامت شرکت بیمه برای این هزینه‌ها فقط درصورتی‌که قوانین محلی اجازه دهد، پرداخت می‌شود.
(مسئولیت) ارتباطات و رسانه	جبران هزینه‌های خسارات ناشی از سوءاستفاده از رسانه‌های ارتباطی شرکت که منجر به بدنامی، توهین یا افترا به شخص ثالث شود از جمله تحریف صفحات وب، نقض حق نشر یا انحصار و سوءاستفاده از اسرار تجاری
حمایت حقوقی- حق‌الزحمه وکیل	هزینه‌های دعاوی حقوقی که توسط یا علیه بیمه-گذار انجام می‌شود که شامل هزینه‌ها و حق‌الزحمه وکیل در صورت محاکمه می‌شود (به طور مثال در مورد سرقت هویت، هزینه‌های وکیل برای اثبات سوءاستفاده از هویت قربانی)
پوشش کمکی- حمایت روانی	کمک و حمایت روحی به قربانی بعد از حادثه سایبری‌ای که منجر به انتشار اطلاعات مخرب علیه بیمه‌گذار بدون رضایت وی می‌شود.
(مسئولیت) محصولات	هزینه‌های جبران خسارت در صورت معیوب یا مضر بودن محصولات یا عملکرد شرکت بیمه شده ناشی از یک رویداد سایبری به‌استثنای محصولات یا عملکرد فنی (خطاها و رخنه‌های تکنولوژی) و خطاها و رخنه‌های خدمات تخصصی
(مسئولیت) رئیسان و مدیران[6]	هزینه‌های جبران خسارت در صورت اقامه دعوی شخص ثالث علیه رئیسان و مدیران شرکت بیمه شده، از جمله خیانت‌درامانت[7] و ترک وظیفه[8] ناشی یک حادثه سایبری
(مسئولیت) خطاها و رخنه‌های تکنولوژی	جبران هزینه‌های خسارت مربوط به عدم ارائه کافی خدمات و محصولات فنی ناشی از یک رویداد سایبری
(مسئولیت) خطاها و	جبران هزینه‌های خسارت مربوط به عدم ارائه

[1] Intellectual property theft
[2] Breach of Privacy (compensation)
[3] Reputational Damage
[4] Regulatory costs

[5] Legal Defense costs
[6] Directors and officers (D&O) [liability]
[7] breach of trust
[8] breach of duty

رخنه‌های خدمات تخصصی/ (مسئولیت) غرامت حرفه‌ای	کافی خدمات و محصولات حرفه‌ای ناشی از یک رویداد سایبری به‌استثنای خدمات و محصولات فنی (خطاها و رخنه‌های تکنولوژی)
آسیب‌های محیط زیستی	دامنه پوشش[1]: جبران خسارت هزینه‌های پس از نشت محصولات سمی یا محصولات آلوده‌کننده در پی یک رویداد سایبری
آسیب به دارایی‌های فیزیکی	خسارات (شامل وقفه کسب‌وکار و وقفه در کسب-وکار مشروط) مربوط به تخریب اموال فیزیکی شرکت در اثر یک رویداد سایبری در این شرکت
جراحات بدنی و مرگ	جبران هزینه‌های آسیب بدنی یا مرگ از طریق اشتباه یا سهل‌انگاری شرکت یا اشخاص ثالث مرتبط با شرکت (به‌عنوان‌مثال نشت داده‌های حساس که منجر به خودکشی شود)

باتوجه‌به این موارد لزوم مدیریت ریسک سایبری و پوشش آن از طریق بیمه در کشور وجود دارد که هدف از این پژوهش، ارائه یک تعریف برای ریسک سایبری از تعاریف موجود، احصاء انواع ریسک‌ها و بیمه‌پذیری آن‌ها، انواع بیمه‌نامه‌های سایبری و ریسک‌های تحت پوشش آن‌ها است.

۳. مروری بر پیشینه پژوهش

در [۱۰] نویسندگان به بررسی چشم‌انداز بیمه سایبری، مسائل رفتاری در امنیت سایبری و مدل‌های مدیریت ریسک برای بیمه سایبری پرداختند.

در [۱۱] پژوهشگران به بررسی تأثیر قابلیت‌های فناوری اطلاعات سازمان بر توسعه محصولات و خدمات جدید پرداختند. جامعه آماری پژوهش شرکت بیمه سامان بود که با توجه به موضوع تحقیق، ۷۰ نفر از کارکنان این شرکت با استفاده از روش نمونه‌گیری تصادفی ساده جهت پاسخگویی به سوالات پرسشنامه به عنوان نمونه انتخاب شده‌اند. نتایج تحقیق نشان داده است که زیرساخت‌های فناوری اطلاعات، توسعه کسب‌وکار مبتنی بر فناوری اطلاعات و پیشگامی در فناوری اطلاعات تأثیر مثبت و معناداری بر توسعه محصول/ خدمت جدید دارند.

در [۱۲] نویسندگان، انواع مدل‌های جامع تخمین ریسک مانند بازی دوسطحی و تجزیه‌وتحلیل ریسک خصمانه را بررسی کردند. این مدل‌ها برای حمایت از شرکت‌ها در تصمیم‌گیری‌های مدیریت ریسک سایبری، پیاده‌سازی آنها، تعیین سبد بهینه امنیت سایبری یا بهترین تخصیص بودجه برای هزینه‌های کنترل امنیت و محصولات بیمه سایبری، ارائه شده‌اند.

در [۱۳] یک شبکه باور بیزی برای ارزیابی آسیب‌پذیری سایبری و محاسبه ضرر موردانتظار از طریق طراحی یک مدل فرآیندی، پیشنهاد داده‌اند. در این مطالعه شکست امنیتی در یک سازمان به پارامترهای فنی و سازمانی نسبت داده شده است. ساختار پیشنهادی حق‌بیمه‌ای را که یک بیمه‌گر ریسک سایبری می‌تواند برای جبران خسارات سایبری دریافت کند را محاسبه می‌کند.

در [۱۴] با تجزیه‌وتحلیل آماری ۹۹۴ مورد از پرونده‌های خسارات سایبری، کفایت بیمه را برای مدیریت ریسک سایبری بررسی نموده‌اند. بررسی‌های صورت گرفته حاکی از آن است که کمبود داده و عدم تقارن اطلاعاتی شدید موجب بروز ریسک‌های عملیاتی برای شرکت‌های بیمه شده و مانع توسعه پایدار بازار بیمه سایبری شده است.

در [۱۵] فرآیند بررسی ریسک سایبری در شرکت‌ها را بررسی نموده و به دنبال روشی برای منظم کردن برآورد حق‌بیمه سایبری بوده‌اند. طبق بررسی‌های نویسندگان، ارزیابی ریسک‌های سایبری هنوز هم برای شرکت‌های بیمه دشوار است و باید روش‌های مناسب برای آن توسعه یابد. این پژوهش منابع موردنیاز بیمه‌گر در نقشه راه خود برای اجرای ارزیابی ریسک و در نتیجه تعیین قابلیت بیمه‌پذیری شرکت و الزامات رسیدن به چنین شرایطی را معرفی می‌کند. به علاوه شصت‌وسه معیار مهم در ارزیابی ریسک در این پژوهش معرفی شده که وزن‌های آنان به طور یکنواخت توزیع نشده و وزن‌دهی بر اساس ارتباط و اهمیت اعمال می‌شود.

در [۱۶] ایده ارائه یک نظام بیمه سایبری اجباری برای شرکت‌های در معرض خطر و عموم مردم را بررسی نموده‌اند. ایده آن‌ها این است که با افزایش روزافزون حملات سایبری و نقض داده‌ها، بیمه اجباری سایبری تضمین می‌کند که در صورت افشای ناخواسته اطلاعات شخصی و مالی، قربانیان به درستی غرامت دریافت نموده و همه طرف‌ها در نهایت از یک نظام اجباری بیمه سایبری سود خواهند برد. به علاوه یک نظام اجباری مسئولیت سایبری تضمین می‌کند که استانداردهای پیشرفته و بروز شده امنیت سایبری برای کمک به جلوگیری از نقض داده‌ها و کاهش آسیب‌ها اجرا شود.

در [۱۷] پژوهشگران، پژوهشی را با هدف شناسایی انواع داده‌های کلیدی که توسط متخصصان بیمه سایبری، برای تصمیم‌گیری در فرآیندهای تعهد بیمه و خسارت موردنیاز است، انجام داده‌اند. پردازش حجم انبوهی از داده‌ها برای بررسی صحت ادعاهای مطرح شده خود یکی از چالش‌های موجود است. راه‌حل اصلی این چالش‌ها، طراحی سامانه‌ها و بسترهایی برای جمع‌آوری، تجزیه‌وتحلیل داده‌ها است. نویسندگان در این پژوهش، با هدف طراحی چنین بستری یک نظرسنجی در مقیاس

[1] Coverage scope

بزرگ با متخصصان بیمه سایبری ترتیب داده‌اند و بر اساس تحلیل نظرات این متخصصان، چالش‌های موجود و ورودی‌ها و خروجی‌های کلیدی شناسایی شده است.

در [۱۸] یک بررسی مروری جامع از مدل‌سازی و قیمت‌گذاری بیمه سایبری انجام داده‌اند. آن‌ها خطرات سایبری را به سه گروه: خاص[1]، سیستماتیک و سیستمیک تقسیم‌بندی نموده‌اند. به عقیده آنان، رویکردهای مدل‌سازی بیم‌سنجی کلاسیک برای ریسک‌های سایبری خاص و سیستماتیک، مناسب به نظر می‌رسند و ریسک‌های سایبری سیستمیک نیازمند رویکردهای پیچیده‌تری نظیر مدل‌های شبکه همه‌گیر هستند.

۴. روش تحقیق

این پژوهش به لحاظ طبقه‌بندی بر مبنای هدف، کاربردی است. زیرا نتایج آن می‌تواند راهنمای عمل صنعت بیمه باشد. از نظر چگونگی انجام، این پژوهش از نوع توصیفی با رویکرد تطبیقی خواهد بود و در آن از تلفیقی از چند روش کیفی شامل روش مطالعه اسنادی و روش تحلیل مضمون استفاده می‌شود. زیرا هدف آن واکاوی و شناسایی انواع ریسک‌های این حوزه، شناسایی و احصا پتانسیل‌ها، مطلوب‌ها و سایر موارد مورد نیاز جهت ترسیم نقشه راه این حوزه است. برای تعریف ریسک سایبری از تعاریف ارائه شده مؤسسات مختلف ازجمله، مؤسسه ژنو، سازمان بین‌المللی استانداردسازی، مؤسسه مدیریت ریسک و انجمن ملی ناظران امور بیمه‌ای استفاده شد. از مطالعات کتابخانه‌ای و مرور اسناد، برای ارائه دسته‌بندی انواع ریسک‌های سایبری، معیارهای بیمه‌پذیری و انواع پوشش‌های بیمه‌ای استفاده شد. در ایران بیمه سایبری، به دلیل عدم شناخت و آگاهی لازم، چندان مورد توجه قرار نگرفته است و استفاده از تجربیات بین‌المللی با استفاده از مطالعه کتابخانه‌ای می‌تواند زمینه‌ساز رشد این نوع بیمه در کشور باشد.

۵. نتایج و بحث

سایبر مخفف واژه سایبرنتیک واژه‌ای است برگرفته از لغت یونانی kybernetes به معنای حاکمیت و یا حکومت. عموماً واژه "سایبر" به‌اختصار به‌جای واژه "فضای سایبری" به کار می‌رود. نخستین کسی که واژهٔ فضای سایبری را به کاربرد ویلیام گیبسون نویسندهٔ داستان‌های علمی-تخیلی در کتاب نورومنسر بود. فضای سایبری، دامنه‌ای جهانی، درون محیط اطلاعاتی که دربردارنده شبکه به هم متصل زیر ساختاری سیستم اطلاعاتی است که خود شامل اینترنت، شبکه‌های ارتباط راه دور، سیستم های رایانه‌ای و کنترل‌گرها و پردازشگرهای آن است [۱۹].

امنیت فناوری اطلاعات به هر آن چیزی که اطلاعات را مورد تهدید قرار می‌دهد اطلاق می‌شود. ذیل این مفهوم، امنیت سایبری قرار دارد که به حملاتی که به واحدهای سرویس‌دهنده مانند اپلیکیشن‌ها، نرم‌افزارها، سخت‌افزارها و مراکز اطلاعات می‌پردازد. زیرگروه این بخش هم یک سری تهدیداتی است که مختص شبکه‌ها می‌باشد که به آن امنیت شبکه می‌گویند.

۵-۱- تعریف ریسک سایبری

تعریف‌های متعددی از ریسک سایبری ارائه شده است:

طبقه مطالعات پیشین، ریسک سایبری زیرمجموعه‌ای از ریسک عملیاتی معرفی شده است. در برخی مطالعات، ریسک‌های سایبری را به‌عنوان یک ریسک عملیاتی برای دارایی‌های اطلاعاتی و فناوری که پیامدهایی بر محرمانگی، دردسترس‌بودن و یا یکپارچگی اطلاعات یا سیستم‌های اطلاعاتی دارد، تعریف می‌کنند. در جدول زیر تعاریف ریسک سایبری به طور مختصر آورده شده است:

[1] Idiosyncratic

جدول (۲): تعاریف ریسک سایبری.

نام مؤسسه	تعریف
انجمن ژنو	هر ریسکی که ناشی از استفاده از فناوری‌های اطلاعاتی و ارتباطی که محرمانه بودن، دردسترس‌بودن یا یکپارچگی داده‌ها یا سرویس‌ها را به خطر می‌اندازد.
مؤسسه ملی استانداردها و تکنولوژی[1]	(۲۰۰۲): ریسک‌های مرتبط با فناوری اطلاعات که از تعهد قانونی یا از دست دادن عملیات ناشی می‌شوند که دلایل آن شامل (۱) افشا، تغییر یا تخریب غیرمجاز (با سوء نیست یا سهوی) اطلاعات، (۲) اشتباهات و حذفیات غیر عمدی. (۳) اختلالات فناوری اطلاعات به دلیل بلایای طبیعی یا ساخته دست بشر. (۴) عدم رعایت دقت و اهتمام لازم در اجرا و بهره‌برداری از سیستم فناوری اطلاعات. (۲۰۰۶): ریسک‌های مربوط به منابع سایبری یعنی ریسک‌های مربوط به سیستم یا عناصر سیستمی که در یک فضای سایبری به طور متناوب یا دائمی حضور دارد. تأثیر عدم قطعیت در اطلاعات و فناوری. ریسک‌های امنیت سایبری به ازدست‌دادن محرمانگی، یکپارچگی یا دردسترس‌بودن اطلاعات، داده‌ها یا سیستم‌های اطلاعاتی (کنترلی) مربوط می‌شود و منعکس‌کننده اثرات نامطلوب بالقوه بر عملیات سازمانی (مثل مأموریت، عملکرد، تصویر یا شهرت) و دارایی‌ها، افراد، سایر سازمان‌ها و کشور می‌باشد.
انجمن مدیران ارشد ریسک[2] (CRO)	هرگونه ریسک ناشی از استفاده و انتقال داده‌های الکترونیکی شامل استفاده از ابزارهای فناوری مانند اینترنت و شبکه‌های ارتباط از راه دور، خسارات فیزیکی که ناشی از حملات سایبری باشد، کلاهبرداری با سوءاستفاده از داده‌ها، هرگونه مسئولیت ناشی از استفاده، ذخیره‌سازی و انتقال داده‌ها، دردسترس‌بودن، یکپارچگی و محرمانه بودن اطلاعات الکترونیکی مربوط به افراد، شرکت‌ها یا دولت‌ها
سازمان بین‌المللی استانداردسازی[3]	خطر ناشی از تهدیدی که از فضای سایبری سوءاستفاده می‌کند (فضای سایبری محیط دیجیتال به‌هم‌پیوسته از شبکه‌ها، سرویس‌ها، سیستم‌ها و فرآیندها است)
مؤسسه مدیریت ریسک[4]	ریسک سایبری به معنای هرگونه خطر ضرر مالی، اختلال یا آسیب به اعتبار یک سازمان در اثر شکست سیستم‌های فناوری اطلاعات آن است. چنین خطری می‌تواند به روش‌های زیر تحقق یابد: (۱) نقض عمدی و غیرمجاز امنیت برای دسترسی به سیستم‌های اطلاعاتی به منظور جاسوسی، اخاذی یا بی‌آبرویی. (۲) نقض غیر عمدی یا تصادفی امنیت، که با این وجود ممکن است همچنان یک افشاگری باشد که نیاز به رسیدگی دارد. (۳) ریسک‌های عملیاتی IT ناشی از یکپارچگی ضعیف سیستم یا سایر عوامل.
بانک تسویه‌حساب‌های بین‌المللی[5] (۲۰۱۹)	ترکیبی از احتمال وقوع یک رویداد در قلمرو دارایی‌های اطلاعاتی یک سازمان، رایانه و منابع ارتباطی و پیامدهای آن رویداد برای یک سازمان.

[1] National Institute of Standards and Technology
[2] The CRO(Chief Risk Officers) Forum
[3] International Organization for Standardization (ISO)
[4] Institute of Risk Management (IRM)
[5] Bank of International Settlements

رایانامه نویسنده مسئول، hamzeh@irc.ac.ir

Eling و Schnell (۲۰۱۶)	ریسک سایبری شامل هرگونه ریسک ناشی از استفاده از فناوری اطلاعات و ارتباطات (ICT) است که محرمانگی، دردسترس‌بودن یا یکپارچگی داده‌ها یا خدمات را به خطر می‌اندازد. اختلال فناوری عملیاتی (OT) در نهایت منجر به اختلال در کسب‌وکار، اختلال زیرساختی (بسیار حیاتی) و آسیب فیزیکی به انسان‌ها و دارایی‌ها می‌شود. ریسک سایبری یا ناشی از بلایای طبیعی است یا ناشی از قصور انسانی، جرایم سایبری (مانند اخاذی، کلاهبرداری)، جنگ سایبری یا تروریسم سایبری می‌باشد.
NAIC	ریسک سایبری به‌عنوان ریسک مرتبط با یک رویداد الکترونیکی مخرب که باعث اختلال در کسب‌وکار و ضرر مالی می‌شود، تعریف می‌شود. ریسک سایبری تمام ریسک‌های مربوط به فعالیت برخط، مانند ذخیره داده‌های شخصی در اینترنت یا انجام تراکنش‌های برخط که ممکن است منجر به آسیب مالی، شهرت، اختلال در زندگی یا کسب‌وکار شود را پوشش می‌دهد.

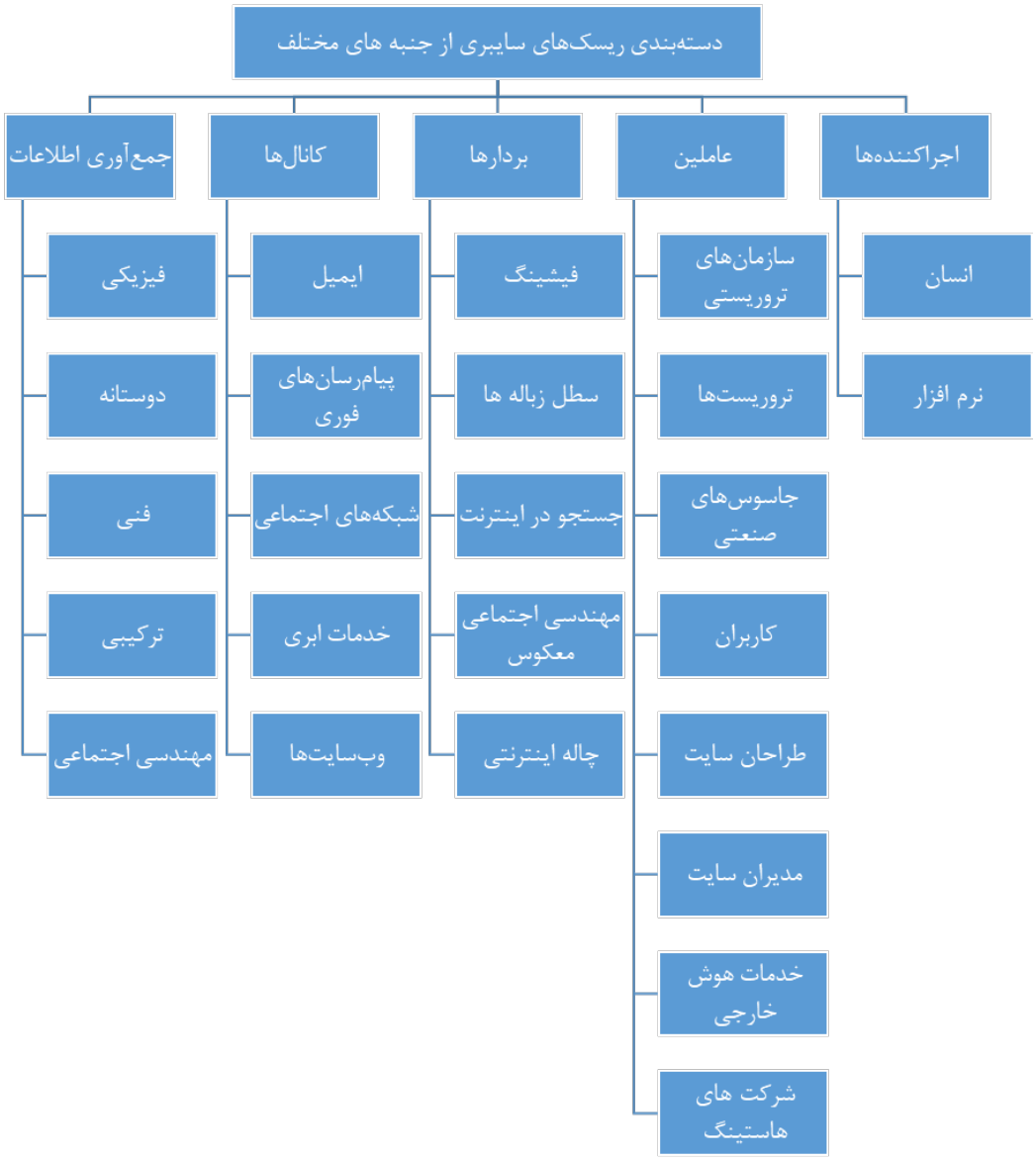
باتوجه‌به جدول مذکور می‌توان تعریف زیر را به‌عنوان تعریفی جامع از ریسک سایبری که تمام مؤلفه‌های مدنظر محققان یادشده را در برمی‌گیرد ارائه نمود:

«خطرات ناشی از استفاده از فناوری‌های اطلاعات و ارتباطات اعم از خطاهای انسانی یا حملات عمدی یا سهوی (چه از طرف عوامل درونِ سازمان چه از طرف عوامل خارج از سازمان) و پیامدهای بالقوهٔ ناشی از آن که محرمانگی، دردسترس‌بودن یا یکپارچگی داده‌ها را به خطر می‌اندازد»

۵-۲- دسته‌بندی انواع ریسک‌های سایبری

به‌منظور دسته‌بندی انواع ریسک‌های سایبری عواملی مختلفی نقش‌آفرینی می‌کند. می‌توان ریسک‌ها را بر اساس نوع حملات و یا حوادث سایبری دسته‌بندی نمود، از طرفی می‌توان ریسک‌ها را بر اساس ابزارهای مورد استفاده حمله‌کنندگان و یا اهداف آن‌ها نیز دسته‌بندی نمود.

دسته‌بندی انواع ریسک‌های سایبری بر اساس نوع حمله یا حوادث سایبری شامل هک، حمله عدم سرویس‌دهی، اخاذی اطلاعاتی، خطای نیروی انسانی، نقص ناشی از نرم‌افزار، نقص داده، فعالیت‌های مخرب، حالت عدم فعالیت شبکه/ دان تایم شبکه، ازبین‌رفتن فیزیکی سیستم، اشکال در عملکرد سیستم، ازبین‌رفتن یکپارچگی داده‌ها یا قطع‌شدن دسترسی به اطلاعات است [۱۹]. علاه‌براین، در [۲۰] به دنبال همه‌گیری کووید-۱۹ و افزایش چشمگیر ریسک سایبری برای کسب‌وکارها، ریسک‌های سایبری را به سه نوع اصلی تقسیم کرد که شامل ریسک امنیتی، ریسک حریم خصوصی و ریسک عملیاتی می‌باشد. ریسک‌های سایبری را می‌توان بر اساس سناریوی حمله نیز دسته‌بندی کرد [۲۱]. سناریوی حمله عبارت است از: ۱- جمع‌آوری اطلاعات ۲- انتخاب کانال مناسب برای پیاده‌سازی حمله ۳- بردارهای حمله ۴- عاملین حمله ۵- پیاده‌سازی و اجرای حمله. نمای کلی این دسته‌بندی در شکل زیر آمده است:



شکل (۲): دسته‌بندی ریسک‌های سایبری بر اساس سناریوی حمله [۲۱].

پوشش‌های بیمه‌ای بستگی به نوع بیمه‌نامه خریداری شده دارد که آن هم باتوجه‌به ماهیت و اندازه کسب‌وکار و میزان ریسک محتمل، ممکن است متفاوت باشد.

۵-۳- معیارهای بیمه‌پذیری ریسک سایبری

قابلیت بیمه‌کردن یک ریسک مشخص معمولاً زمانی از نظر اقتصادی عملی است که معیارهای بیمه‌پذیری برآورده شود. این معیارها شامل موارد زیر است: ریسک‌ها می‌بایست قابل‌سنجش باشند، جامعه به اندازهٔ کافی بزرگ باشد و ریسک‌ها به‌صورت تصادفی اتفاق بیفتد. تعیین موارد تحت پوشش یکی از چالش‌های مهم است. طیف پوشش‌های بیمه سایبری می‌تواند بسیار گسترده باشد که شرکت بیمه بنا بر توان فنی، اطلاعات در دسترس و ریسک احتمالی ممکن است بخش‌هایی را متقبل و از پذیرش بخش‌هایی دیگر امتناع ورزد.

در جدول زیر معیارهای بیمه‌پذیری ریسک سایبری و تغییرات برای بهبود بیمه‌پذیری ارائه شده است.

رایانامه نویسنده مسئول، hamzeh@irc.ac.ir

جدول (۳): بررسی معیارهای بیمه‌پذیری ریسک سایبری [۲۲].

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
معیارهای اکچوئری	فراوانی و شدت ریسک باید به طور معقولی قابل‌اندازه‌گیری باشد.	ریسک سایبری در حال تحول بوده و داده‌های کمی ثبت شده‌اند. قربانیان حملات سایبری، دولت‌ها، شرکت‌های امنیتی و غیره ممکن است از پرداختن به جزئیات به‌منظور اهداف امنیتی خودداری کنند. به‌عمد، ماهیت حملات به طور مداوم در حال تغییر است تا از تجزیه‌وتحلیل و کاهش آن فرار کنند. مدل‌های سایبری در مراحل ابتدایی خود باقی‌مانده و توسعه نمی‌یابند.	خلق نوآوری به‌منظور ایجاد پایگاه‌داده جمعی (تلفیقی)، بهبود استانداردسازی برای مدل‌سازی و تجزیه‌وتحلیل، و تعریف شفاف مواردی که جزء یک حمله سایبری هستند.
	خسارت یک رخداد، مستقل از خسارت رخداد دیگر باشد.	حملات هماهنگ می‌تواند باعث خسارات وابسته به هم شود. حملات در مقیاس بزرگ می‌توانند چندین سازمان را تحت‌تأثیر قرار دهند.	سایبری اساساً یک ریسک نیروی انسانی است، اما روشن‌شدن نیت اقدامات جنگ سایبری تحت حمایت دولت و سایر موارد استثنا، مانند اقداماتی که قبلاً توضیح داده شد، می‌تواند کمک کند.
	حداکثر خسارت موجود، باید در ظرفیت صنعت قابل‌مدیریت باشد.	خسارت‌های فاجعه‌آمیز، منجر به تنوع‌پذیر نبودن آنها می‌شود.	ریسک حوادث فاجعه‌آمیز را از پوشش خسارت‌های فرسایشی[1] (خسارت‌هایی غیر از خسارات فجایع یا مواجهه‌های بزرگ) جدا کنید.
	متوسط مقدار خسارت در هر رخداد قابل‌پیش‌بینی باشد و تعداد زیادی از رخدادهای خسارت مشابه در سال اتفاق بی افتد.	اساس بازار بیمه سایبری به‌خوبی تثبیت شده است.	افزایش نرخ جذب بیمه در بخش‌ها و اندازه شرکت‌ها؛ جداسازی ریسک‌های فاجعه‌آمیز از خسارت‌های فرسایشی.
	کمبود اطلاعات نامتقارن[2] در این حوزه (به‌عنوان‌مثال کژ منشی یا مخاطرات اخلاقی[3]، کژگزینی/ انتخاب نامطلوب[4])	تجربه و استانداردهای مربوط به‌اشتراک‌گذاری و کاهش میزان حملات در حال تکامل است.	بیمه مشترک، استانداردهای کاهش میزان حملات، اشتراک‌گذاری داده‌ها، منابع مدیریت بحران
معیارهای بازار	برای یک بازار بیمه پایدار، حق بیمه باید از نظر پوشش ریسک، کافی باشد.	میزان خسارت وارد شده و به‌تبع آن ضریب خسارت در سال‌های اخیر افزایش داشته است.	بهبود مدل‌سازی برای قیمت‌گذاری متناسب با ریسک؛ جداسازی ریسک‌های فاجعه‌آمیز از خسارت‌های فرسایشی.
	ظرفیت کافی صنعت	وجود ظرفیت کافی برای حمایت از رشد قوی در بازار فرسایشی؛ نشان از ظرفیت کافی در بیمه‌کردن کامل ریسک‌های فاجعه‌بار نیست.	شفافیت در مورد آنچه که منجر به ریسک‌های فاجعه‌آمیز می‌شود، در بالابردن ظرفیت بیمه‌گر اتکایی مؤثر است.

[1] Attritional losses
[2] Information Asymmetry
[3] Moral hazard
[4] Adverse selection

۵-۴- انواع پوشش‌های بیمه سایبری

بیمه سایبری اولین‌بار در سال ۱۹۷۰ در ایالات متحده آمریکا مطرح شد. در این کشور، بیمه‌نامه‌ای برای جبران خسارات وارده بر سیستم‌های رایانه‌ای بانک‌ها که ناشی از دسترسی‌های غیرمجاز بوده‌اند، ارائه گردید. به طور خلاصه، پوشش‌های بیمه سایبری را می‌توان به‌صورت زیر دسته‌بندی نمود: [۲۳، ۲۴]

جدول (۴): انواع پوشش بیمه سایبری.

نوع پوشش	توضیحات
خسارت وارد شده به شخص اول	
خسارت ناشی از وقفه در کسب‌وکار	زیان مالی ناشی از نتیجه یک حمله سایبری و وقفه در کار
اخاذی سایبری	مطالبات اخاذی و جلوگیری از تهدیدات آتی
بازیابی اطلاعات و داده‌های الکترونیکی	هزینه‌های بازیابی یا جایگزینی اطلاعات و داده‌های الکترونیکی
خسارت وارد شده به شخص ثالث	
مسئولیت امنیت و حریم خصوصی	آسیب به شهرت ناشی از افشای اطلاعات، مانند افشای اطلاعات شخص ثالث نگهداری شده در سیستم
هزینه‌های حقوقی	تأمین هزینه‌های حقوقی دفاع از دعاوی
مسئولیت نقض مقررات و رویه‌های نظارتی	هزینه‌های قانونی و جریمه‌های ناشی از بررسی و نظارت قانون‌گذار دولتی
مسئولیت رسانه‌های الکترونیکی	هزینه‌های نقض نسخه‌برداری، افترا و سوءاستفاده از انواع خاصی از مالکیت معنوی برخط.
پوشش‌های اضافی	
هزینه‌های مدیریت بحران	هزینه‌های مدیریت بحران ناشی از حمله هکرهای سایبری
هزینه‌های اطلاع‌رسانی و نظارت	هزینه‌های اطلاع‌رسانی به مشتریان پس از افشای اطلاعات آنها و نظارت بر جزئیات کارت اعتباری آنها برای جلوگیری از حملات بیشتر.

پوشش‌های بیمه سایبری را می‌توان هم به‌صورت مستقل و هم به‌صورت بسته‌ای و در یک بیمه‌نامه بازرگانی چند خطر موجود ارائه کرد. بازار بیمه مستقل سایبری، در پاسخ به معرفی استثناهای بیمه‌ای سایبری در بیمه‌نامه‌های دیگر توسعه یافت و حق بیمه صادره مستقیم آن، تقریباً دوبرابر بازار سایبری بسته‌ای شد. این پوشش‌ها می‌توانند شامل موارد زیر باشد: ۱) تمام خسارات ناشی از یک حمله سایبری، ۲) مسئولیت مربوط به افشای اطلاعات؛ و ۳) خسارت‌های مربوط به بازیابی داده‌ها. بیمه‌نامه‌های مستقل معمولاً توسط شرکت‌های بزرگ‌تر که دارای اطلاعات و منابع مالی مهم و در معرض خطر هستند، خریداری می‌شوند.

در سال ۲۰۲۳ عوامل مختلفی در افزایش حملات سایبری دخیل بوده که این عوامل، ضرورت استفاده از بیمه سایبری را دوچندان می‌کنند. طبق رتبه‌بندی جهانی در خصوص حملات سایبری منجر به افشای اطلاعات، ده کشوری که به ترتیب نزولی بیشترین آسیب را از افشای اطلاعات در سه ماهه دوم سال ۲۰۲۳ متحمل شده اند، عبارتند از: ایالات متحده، روسیه، اسپانیا، فرانسه، ترکیه، استرالیا، هند، ایتالیا، بریتانیا و برزیل. علاوه بر این، کشورهایی با بالاترین میزان تراکم حمله افشای اطلاعات که نشان‌دهنده تعداد حساب‌های لورفته به ازای هر ۱۰۰۰ نفر بوده، نیز رتبه‌بندی شده‌اند. این فهرست شامل ایالات متحده، روسیه، اسپانیا، فنلاند، استرالیا، سوئد، فرانسه، سودان جنوبی، ترکیه و دانمارک می‌باشد. این آمارهای هشداردهنده بر نیاز مبرم به افزایش اقدامات امنیت سایبری و تلاش‌های مشترک جهت حفاظت از اطلاعات حساس کاربران در دنیای دیجیتالی، تأکید می‌کند.

۵-۵- پیامدهای ریسک سایبری در صنعت بیمه

همه‌گیری ویروس کرونا، تحول دیجیتال را تسریع کرده است و مؤسسات مالی از جمله صنعت بیمه، اکنون بیشتر به فناوری اطلاعات، راه‌حل‌های دیجیتال و دورکاری برای انجام عملیات روزانه خود و ارائه خدمات به مشتریان متکی هستند. درحالی‌که این امر مزایایی را به همراه داشته است، اتکای فزاینده به فضای دیجیتال خطر حملات سایبری را نیز افزایش داده است.

به‌طورکلی ریسک‌های سایبری به‌عنوان یک ریسک بزرگ جهانی برای بخش مالی و اقتصادی از جمله صنعت بیمه در نظر گرفته می‌شوند. انواع ریسک‌های فناوری اطلاعات و ارتباطات که شرکت‌ها در معرض آن قرار دارند، در سال‌های گذشته تغییری نکرده، بااین‌حال تعداد حملات و میزان تأثیر آن بر واحدهای مالی افزایش‌یافته است. مطالعات اخیر در حوزه کووید-۱۹ و ریسک‌های سایبری در بخش مالی نشان داده که بخش مالی پس از بخش سلامت بیشترین تعداد حملات سایبری مرتبط با کووید-۱۹ را تجربه کرده است. ارائه‌دهنده خدمات پرداخت،

شرکت‌های بیمه و صنعت بانکداری بیشترین آسیب را متحمل شده‌اند.

اخیراً گزارش‌های زیادی از شرکت‌های بیمه در خصوص حملات سایبری و بدافزارها منتشر شده است. ناظران بیمه‌ای، ریسک‌های سایبری را به‌عنوان محرک اصلی سایر ریسک‌ها می‌دانند، همان‌طور که مقامات نظارتی اروپا (EIOPA، ESMA و EBA) در گزارش خود در مورد خطرات و آسیب‌پذیری‌های سایبری در بخش مالی تأکید کرده‌اند. برخی از این ریسک‌ها عبارت‌اند از [۲۵]:

- ریسک‌های مرتبط با دیجیتالی‌شدن (برای ۷۳ درصد از ناظران بیمه‌ای)
- ریسک‌های صدور بیمه‌نامه (۱۹ درصد)
- ریسک مرتبط با رقابت اینشورتک‌ها (۸ درصد)

پیامدهای اصلی ریسک‌های سایبری مذکور در صنعت بیمه، وقفه در کسب‌وکار و خسارات مادی برای بیمه‌گران، بیمه‌گذاران و اشخاص ثالث است. علاوه بر پیامدهای مستقیم مالی، حملات سایبری همچنین می‌تواند منجر به مسائل و مشکلات عملیاتی شدید و طولانی‌مدت برای گروه‌های بیمه هدف شود. ریسک آسیب به برند شرکت و ریسک شهرت نیز ممکن است قابل‌توجه یا حتی غیرقابل‌برگشت باشد. هکرها همچنین اطلاعات به‌دست‌آمده از بیمه‌گذاران را به‌منظور اهداف مجرمانه مختلف مانند سرقت هویت و به‌دست‌آوردن منافع مالی مورد استفاده قرار می‌دهند. به بیان دیگر، حملات سایبری شرکت‌های بیمه می‌تواند منجر به خسارات ملموس و قابل‌توجهی مانند پرداخت جریمه به بیمه‌گذاران، هزینه‌های قانونی، دعاوی حقوقی و هزینه‌های نظارت بر تقلب شود. بااین‌حال، تأثیر کمتر آشکار اما بااهمیت بیشتر بر شرکت، می‌تواند ازدست‌دادن اعتماد بیمه‌گذاران باشد. ازآنجایی‌که تجارت بیمه حول اعتماد می‌چرخد، یک افشای اطلاعات می‌تواند تأثیر بسیار واقعی بر برند و ارزش بازار بیمه‌گران داشته باشد.

اگر حملات سایبری مخرب باعث ایجاد وقفه در کسب‌وکار شود، این امر تأثیر مستقیمی بر همه بیمه‌گران دارد. همچنین به‌عنوان یک پیامد مستقیم افزایش حملات ناشی از ریسک‌های فناوری اطلاعات و ارتباطات، ریسک‌های مرتبط با صدور بیمه‌نامه‌ها نیز در حال گسترش هستند.

بسیاری از شرکت‌های بیمه، منابع مادی زیادی را در ابزارها و فرآیندهای امنیتی خود به‌منظور پیشگیری از ریسک‌های سایبری سرمایه‌گذاری کرده‌اند که احساس امنیت کاذبی را برای آنها ایجاد کرده است. باتوجه‌به اینکه هکرها از رمزگذاری و سایر تکنیک‌های پیشرفته استفاده می‌کنند، ابزارهای سنتی مانند فایروال‌ها، نرم‌افزارهای آنتی‌ویروس، سیستم‌های تشخیص نفوذ (IDS) و سیستم‌های پیشگیری از نفوذ (IPS) کمتر و کمتر مؤثر واقع می‌شوند. در نتیجه، بسیاری از بیمه‌گران ممکن است به‌منظور رسیدگی به تهدیدات انطباق محور که به‌راحتی قابل‌شناسایی هستند، منابع محدود خود را به‌اشتباه تخصیص دهند و تهدیدهای بلندمدت پنهانی را که در نهایت می‌توانند بسیار آسیب‌رسان‌تر باشند، نادیده بگیرند.

به‌منظور بررسی دقیق‌تر پیامدهای حملات سایبری بر صنعت بیمه، از مثال‌هایی با استفاده از سناریونویسی بهره می‌بریم [۲۶]:

- مثال ۱:

حمله سایبری: افشای اطلاعات شخصی مشتریان شرکت بیمه

سناریو: مجرمان سایبری، پایگاه‌داده شرکت را هک کرده و اطلاعات شخصی بیش از یک میلیون مشتری را افشا می‌کنند.

مهاجمان و انگیزه: مجرمان سایبری به دنبال اطلاعات قابل‌شناسایی شخصی بودند تا آنها را در بازار سیاه برای اهداف کلاهبرداری و سرقت هویت بفروشند.

تکنیک‌های مورداستفاده: بخشی از شبکه مورداستفاده کارکنان شرکت بیمه توسط مجرمان سایبری مورد نفوذ قرار گرفته و اطلاعات مشتریان به سرقت رفته است.

تأثیر بر کسب‌وکار: این شرکت موظف است به مدت یک سال به مشتریان آسیب‌دیده نظارت رایگان بر امتیاز اعتباری خود را داده و کلیه خسارات ناشی از تخلفات را جبران کند. علاوه‌برآن هزینه‌های ملموس قابل‌توجهی مانند آسیب به نام تجاری و ازدست‌دادن اعتماد مشتریان را باید جبران کند.

- مثال ۲:

حمله سایبری: حمله سایبری با وسعت کم به شرکت‌های بزرگ از طریق ایمیل حاوی بدافزار

سناریو: این حمله کارکنان شرکت را با ایمیل‌های حاوی بدافزار هدف قرار داده و داده‌های محرمانه مانند شماره‌حساب بانکی، شماره کارت ملی، حساب‌های کاربری، رمز عبور و شماره کارت اعتباری را به دست می‌آورد. هکرها از این اطلاعات برای به خطر انداختن چندین سرور، از جمله سرورهایی که توسط کارمندان برای دسترسی از راه دور به سیستم‌های فناوری اطلاعات شرکت استفاده می‌شود، بهره می‌برند.

هدف از ارائه این مثال، بیان این مسئله است که در شرکت بیمه‌های بزرگ، افشای اطلاعات هرچند ناچیز می‌تواند تأثیر معناداری بر شرکت داشته و نیاز به اقدامات اصلاحی سریع داشته باشند.

مهاجمان و انگیزه: مجرمان سایبری به دنبال اطلاعات بانکی افراد بوده‌اند تا برای کسب سود مالی دست به کلاهبرداری بزنند.

تکنیک‌های مورداستفاده: ایمیل‌های حاوی نرم‌افزار مخربی به‌منظور کسب اطلاعات استفاده شده که داده‌های محرمانه افراد را به دست آورد.

تأثیر بر کسب‌وکار: اگرچه این نوع حمله تنها تعداد کمی از کارمندان - و فقط تعداد انگشت‌شماری از مشتریان را تحت‌تأثیر قرار می‌دهد – اما به‌شدت به اعتبار شرکت لطمه می‌زند.

- مثال ۳:

حمله سایبری: حمله به سیستم‌های با امنیت کم در شرکت بیمه

سناریو: مهاجمان از نرم‌افزارهای آسیب‌پذیر نصب شده بر سرورهای شرکت سوءاستفاده کرده و اطلاعات کارت اعتباری پرداخت بیش از ۹۳۰۰۰ مشتری از جمله نام، آدرس و کدهای امنیتی رمزگذاری نشده کارت را به سرقت بردند.

مهاجمان و انگیزه: مجرمان سایبری به دنبال اطلاعات کارت اعتباری پرداخت بوده تا در بازار سیاه بفروشند و کلاهبرداری کنند.

تکنیک‌های مورداستفاده: آسیب‌پذیری‌ها در سیستم‌ها و نرم‌افزارهای این شرکت توسط مجرمان سایبری برای دسترسی به اطلاعات کارت‌های پرداخت مورد سوءاستفاده قرار گرفت.

تأثیر بر کسب‌وکار: این شرکت بلافاصله نرم‌افزارها و موارد آسیب پذیر موجود در فناوری اطلاعات را حذف کرده و مجبور به عذرخواهی رسمی می‌شود. بااین‌حال، این شرکت به دلیل حفظ کدهای امنیتی رمزگذاری نشده - که طبق استاندارد امنیت داده‌های صنعت‌کارت پرداخت (PCI DSS) یک عدم انطباق محسوب می‌شود - و به دلیل گزارش‌نکردن زودهنگام آن به مشتریان خود به‌شدت مورد انتقاد قرار می‌گیرد.

به طور خلاصه پیامدهای ریسک سایبری در صنعت بیمه عبارت‌اند از:

- وقفه در کسب‌وکار و افزایش ریسک نقدینگی؛
- آسیب به برند شرکت و افزایش ریسک اعتبار؛
- ازدست‌دادن اعتماد بیمه‌گذاران؛
- پرداخت جریمه به بیمه‌گذاران و اشخاص ثالث؛
- هزینه‌های قانونی و دعاوی حقوقی به‌منظور پیگیری و شکایت؛
- هزینه افزایش امنیت سیستم و جلوگیری از حمله سایبری در آینده؛
- هزینه بازیابی اطلاعات.

به‌منظور جلوگیری از پیامدهای مخرب مذکور، استفاده از بیمه سایبری پیشنهاد می‌گردد. طبق آمار Statista، انتظار می‌رود بازار بیمه سایبری اروپا بین سال‌های ۲۰۲۰ تا ۲۰۳۰ به طور تصاعدی رشد کند و بین سال‌های ۲۰۲۰ تا ۲۰۲۵ دو برابر شود. در این حالت، بیمه‌گران نقش اساسی ایفا کرده و با این چالش مواجه می‌شوند که چگونه می‌توانند ریسک‌های سایبری را بیمه کرده و از آنها جلوگیری کنند. در نتیجه، صنعت بیمه نه تنها نیاز به مدیریت ریسک سایبری و فناوری اطلاعات در داخل شرکت‌های خود دارند، بلکه باید با تهدیدها و تحولات جدید همگام شوند.

شرکت‌های بیمه، خود یک هدف طبیعی برای حملات سایبری هستند. زیرا دارای تعداد قابل‌توجهی از داده‌های محرمانه بیمه‌گذاران می‌باشند. محصولات بیمه‌ای، بیمه‌نامه‌ها و قیمت‌ها همگی بر اساس داده‌ها هستند و این چیزی است که آنها را بسیار ارزشمند می‌کند. در واقع با استفاده از داده‌ها، یک شرکت بیمه قادر است آنچه را که بیمه‌گذار نیاز دارد، باقیمت مناسب به او ارائه دهد. بیمه‌گذاران نیز اطلاعات خود را به‌منظور استفاده از خدمات بیمه‌ای در اختیار بیمه‌گران قرار می‌دهند. برخلاف سایر بخش‌ها که عمدتاً داده‌های مالی حساس را در اختیار دارند، بیمه‌گران معمولاً مقدار زیادی از اطلاعات حساس شخصی محافظت شده را نیز در اختیار دارند.

۶. نتیجه‌گیری

افزایش اتکا به فناوری‌های دیجیتال منجر به افزایش ریسک‌های امنیت دیجیتال و حریم خصوصی و به‌تبع آن ظهور بازار بیمه سایبری شده است تا از بیمه‌گذاران در برابر این خطرها محافظت کند. کشور جمهوری اسلامی ایران نیز همواره در معرض ریسک های سایبری قرار داشته است. لذا توجه به حوزه بیمه سایبری در

کشور اهمیت بسزایی دارد. لذا به‌منظور طراحی بهینه این بیمه‌نامه در ایران، در این پژوهش، به ارائه یک تعریف برای ریسک سایبری، احصاء انواع ریسک‌ها و بیمه‌پذیری آن‌ها، انواع بیمه‌نامه‌های سایبری و ریسک‌های تحت پوشش آن‌ها پرداخته شد.

باوجود بیمه سایبری و راه‌های جبران خسارت هنگام وقوع جرم، کشورهای خارجی همواره به فکر پیشگیری از این حملات نیز بوده‌اند و همواره سعی در آموزش شهروندان خود دارند. چشم‌انداز ریسک سایبری به‌سرعت در حال تحول است و با افزایش حملات سایبری، آگاهی از ریسک و تقاضا برای بیمه سایبری نیز افزایش‌یافته است. بااین‌حال، بیشتر مشاغل و افراد، بیمه نشده یا به میزان کافی تحت پوشش قرار نگرفته‌اند، و حق بیمه سایبری تنها کسری از کل خسارات ناشی از حملات سایبری است. برآوردها نشان می‌دهد که حدود ۹۰ درصد از افراد و سازمان‌ها تحت پوشش قرار نگرفته‌اند. این میزان، اشاره به وجود پتانسیل رشدی بزرگ در بازار بیمه سایبری دارد، اما این کار به سادگی انجام‌پذیر نبوده و لازم است که این اطمینان حاصل شود که راه‌حل‌های کافی برای حفاظت از ریسک‌های سایبری وجود دارد تا جامعه بتواند در برابر ریسک سایبری تاب‌آوری داشته باشد و این تلاش مستلزم همکاری بین کسب‌وکارها، صنعت بیمه و دولت است. اولین نیاز در توسعه بیمه سایبری، بهبود کیفیت داده‌ها و مدل‌سازی آنها است. به دلیل کمبود داده‌های استاندارد و محدودیت‌های موجود در مدل‌سازی، کمی‌سازی ریسک‌های سایبری دشوار است. ریسک‌های آتی معمولاً بر اساس داده‌های گذشته‌نگر استنباط می‌شوند، اما این رویکرد در محیطی که ریسک‌های سایبری به سرعت در حال تغییر هستند، ارزش کمی دارد. معرفی استانداردهای امنیت سایبری باعث شده که داده‌ها از نظر وسعت و شفافیت بهبود یافته، درک ریسک روشن‌تر شده، و قیمت‌گذاری و مدل‌سازی دقیق‌تری را امکان‌پذیر کند. شرکت‌های بیمه نیز باید بر نیروی کار متخصص سایبری سرمایه‌گذاری کنند تا به تقویت مهارت‌های اکچوئری، فنی و حقوقی موردنیاز برای چرخه‌های بیمه‌گری و مدیریت خسارت کمک شود. با این وجود، درجه بالای عدم اطمینان در مورد خسارت‌های موردانتظار و ماهیت در حال تحول ریسک، بیمه‌پذیری ریسک‌های کل و فاجعه‌آمیز را به چالش می‌کشد. دومین نیاز، بروزرسانی زبان بیمه‌نامه‌ها توسط بیمه‌گران/بیمه‌گران اتکایی، به منظور وضوح بیشتر و سازگاری با شرایط است. جدید بودن نسبی بازار بیمه سایبری و پیچیدگی ریسک باعث شده استانداردسازی کلوزهای استثنا و شرایط و ضوابط عمومی بیمه‌نامه سایبری به راحتی صورت نگیرد. همچنین قرار گرفتن در معرض ریسک‌های سیستمی که به سختی بیمه می‌شوند، مانعی برای افزایش ظرفیت صنعت در ریسک سایبری باقی مانده است. ذینفعان اقداماتی را برای رفع برخی از این مسائل انجام داده‌اند، اما عواملی مانند تشخیص مرتکب و مقصر رویدادهای سایبری همچنان یک مشکل اصلی است. عواملی مانند شفاف‌سازی دامنه پوشش، حمایت از تحلیل و ارزیابی ریسک، تلاش در کاهش ریسک و شفافیت و سازگاری قرارداد می‌توانند منجر به افزایش ظرفیت سایبری در بازار شوند. در نهایت، همچنین نیاز به استفاده از انواع جدیدی از مکانیسم‌های اشتراک ریسک عمومی-خصوصی وجود دارد. همکاری بخش دولتی و خصوصی برای کاهش تهدیدات سایبری در زیرساخت‌های حیاتی، امری کلیدی است. طرح بیمه مشارکت عمومی-خصوصی، که در آن پوشش ریسک‌های سیستمی بین بیمه‌گران و صندوق‌های تحت حمایت دولت(ها) تقسیم می‌شود، یکی از گزینه‌های رفع بخشی از شکاف حفاظت سایبری است. یکی دیگر از این موارد، بهره‌برداری از بازار سرمایه جایگزین، مانند توسعه بازاری اوراق بهادار مرتبط با بیمه سایبری است.

۷. مراجع

[1] Heydari, S., Barzegar, M., & Mohammad Davoudi, A., (2023). "Identifying the factors affecting cyber security culture and awareness using thematic analysis", Electronic and Cyber Defense, vol. 11(1), pp. 67-80. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.1.6.7

[2] Shoushian, K., Rashidi, A. J., & Dehghani, M. (2020). "Modeling of cyber-attacks obfuscation, based on alteration technique of attack", Electronic and Cyber Defense, vol. 8(1), pp. 67-77. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.1.6.6

[3] Dadashtabar Ahmadi, K., & mahmoudbabouei, M. (2022). "The Presentation of an Active Cyber Defense Model for Application in Cyber Deception Technology", Electronic and Cyber Defense, vol. 9(4), pp. 125-140. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1400.9.4.10.3

[4] Deibert, R. J., & Rohozinski, R. (2010). "Risking security: Policies and paradoxes of cyberspace security", International Political Sociology, vol. 4(1), pp. 15-32.

[5] Mohammadzadeh, Azadeh, (2019). "The growing market of cyber insurance", Iran and world insurance news monthly. pp. 11-17. (In Persian).

[6] Ale, B., Burnap, P., & Slater, D. (2015). "On the origin of PCDS–(Probability consequence diagrams)", Safety science, vol. 72, pp. 229-239.

[7] Aven, T. (2014). "What is safety science?", Safety science, 67, pp. 15-20.

[8] Allianz Risk Barometer.2023. Allianz Global Corporate & Specialty.

[9] Ventures, C. (2022). "2022 Official Cybercrime Report", Cybersecurity Ventures.

[10] Roodpashti Rahmanai, Fereydoun, Zandi, Anahita, (2021). "Security Risk Models for Cyber Insurance", Insurance Research Center. (In Persian)

[11] Tadaion, Mehtab, Ahmadian, Yasmin, Jahangirzadeh, Elnaz, Maleki, Hamid, (2021). "Investigating the impact of the organization's information technology capabilities on the development of new products and services (case study: development of cyber insurance as a new product in Saman Insurance Company)", 20 and the 8th Insurance and Development Conference, Tehran, https://civilica.com/doc/1390759 (In Persian)

[12] Sadeghi, Ali, Asghari Eskoui, Mohammad Reza, (2021). "Review of risk estimation models in cyber insurance", 28th Insurance and Development Conference, Tehran, https://civilica.com/doc/1390872 (In Persian)

[13] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). "Cyber-risk decision models: To insure IT or not?", Decision Support Systems, vol. 56, pp. 11-26.

[14] Biener, C., Eling, M., & Wirfs, J. H. (2015). "Insurability of cyber risk: An empirical analysis", The Geneva Papers on Risk and Insurance-Issues and Practice, vol. 40(1), pp. 131-158.

[15] Bartolini, D. N., Benavente-Peces, C., & Ahrens, A. (2017). "Using risk assessments to assess insurability in the context of cyber insurance", In International Conference on E-Business and Telecommunications Springer, Cham, pp. 337-345.

[16] Trang, M. N. (2017). "Compulsory corporate cyber-liability insurance: Outsourcing data privacy regulation to prevent and mitigate data breaches", Minn. JL Sci. & Tech., no. 18, vol. 389.

[17] Nurse, J. R., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). "The data that drives cyber insurance: A study into the underwriting and claims processes", In 2020 International conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, pp. 1-8.

[18] Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2022). "Modeling and Pricing Cyber Insurance--A Survey", arXiv preprint arXiv:2209.07415

[19] Elsan, M., (2016). "Cyber space insurance: basic concepts and operational plan", Insurance Research Center (In Persian)

[20] Burke, D. (2020, April 2). "Coronavirus Impact on Cyber Insurance Coverage", Woodruff Sawyer. https://woodruffsawyer.com/cyber-liability/coronavirus-impact-cyber-insurance/

[21] Pourshikhi, M., Karam Elahi, A. and Moghadisi, M., (2013). "Introduction of security threats in the virtual world", The first specialized conference of electrical and computer engineering. (In Persian).

[22 Swiss Re Institute, (2022). "Cyber insurance: strengthening resilience for the digital transformation".

[23] Moody Kiddell and partnered, (2022). "Cyber Insurance", https://www.mkpgroup.com.au-/insurance/cyber-insurance.

[24] Roso, J., (2020), "The Importance of Cyber Insurance in a Working from Home Economy", https://www.linkedin.com/pulse/importance-cyber-insurance-working-from-home-economy-jonathan-ross

[25] Eiopa, (2021). "Joint Committee Report on risks and vulnerabilities in the EU financial system".

[26] Deloitte, (2022). "Global Cyber Executive Briefing: Insurance", https://www2.deloitte.com-/tw/en/pages/risk/articles/insurance.html