

**گزارش راهبردی**

**ضرورت ایجاد صنعت بیمه­سایبری درکشور و چهارچوب‌های توسعه آن**

**(بیمه سایبری رکن مهم پشتیبان امنیت سایبری)**



|  |
| --- |
| **عنوان گزارش:** ضرورت ایجاد صنعت بیمه سایبری در کشور و چهارچوب‌های توسعه آن (بیمه سایبری رکن مهم پشتیبان امنیت سایبری)  **کلمات کلیدی:** بیمه سایبری، ریسک سایبری، تهدیدات و آسیب‌پذیری‌ها، اشتغال دانش­بنیان، صنعت امنیت |
| **تهيه­کنندگان:** سپهر اسکندری، محمد حسام تدین |
| **واحد پژوهشی:** پژوهشکد**ه** امنیت ارتباطات و فناوری اطلاعات  **تأیید و ارزیابی نهایی:** کارگروه تدوین و ارزیابی گزارش‌های راهبردی |
| **ویراستاری و تنظیم:** فریده شهیدی  **تاریخ نشر:** فروردین 1404 |

حقوق معنوی این اثر متعلق به پژوهشگاه ارتباطات و فناوری اطلاعات است و استفاده از آن با ذکر مأخذ بلامانع است.

خلاصه مدیریتی

**الف - یافته­های کلیدی**

* بیمه سایبری در برخی کشورها دارای سابقه‌ای بالغ بر سی و پنج سال است و علی‌رغم بیست سال تلاش علمی و ترویجی جهت آغاز این صنعت در کشور، متأسفانه هنوز هیچ محصولی در این حوزه عرضه نشده است. غیرفعال بودن بیمه سایبری در کشور، عملاً برآورد خسارات ناشی از حملات سایبری که در سال‌های اخیر شدت یافته است را غیرممکن یا پنهان کرده است.
* مجمع جهانی اقتصاد پیش‌بینی می‌کند که خسارات مالی جهانی ناشی از جرایم سایبری در سال 2024 به 14.57 تریلیون دلار و در سال 2027 به 23.82 تریلیون دلار خواهد رسید. این حجم بالای خسارت مالی، انگیزه‌ای مهم برای توسعه صنعت بیمه سایبری در آینده به‌منظور فراهم‌آوری امکان انتقال ریسک شرکت‌ها به شرکت‌های بیمه‌گر است.
* پیش­بینی می­شود ظرف 5 سال آینده حجم خرید بیمه­سایبری توسط شرکت­ها و سازمان­ها در دنیا به رقم 50 میلیارد دلار برسد.
* عوامل سیاسی مؤثر بر توسعه بیمه سایبری در ایران، ترکیبی از فرصت‌ها و تهدیدات را به همراه دارد. وجود تحریم‌ها، استفاده از ظرفیت شرکت‌های بیمه‌گر بین‌المللی را غیرممکن کرده است. بااین­حال، بهره‌گیری از ابتکارات حمایتی دولت و افزایش آگاهی عمومی می‌تواند محیطی مساعد برای رشد صنعت بیمه سایبری داخلی فراهم آورد.
* برای شکل‌گیری صنعت بیمه سایبری، این صنعت با چالش‌های مهمی همچون فقدان اطلاعات، پیچیدگی در ارزیابی ریسک، نیاز به توسعه و استانداردسازی محصولات بیمه‌ای، ضعف در دانش و آگاهی از مدیریت ریسک در حوزه سایبری، عدم شناخت پیامدهای اقتصادی و اجتماعی حملات سایبری بر کسب‌وکارها، و همچنین ضعف در قوانین و مقررات ضروری روبه‌رو است.
* اقتصادی شدن امنیت، راه‌حل نهایی برای شکل‌گیری زیست‌بوم امنیت و اعتماد در فضای سایبر و توسعه صنعت بیمه است. درصورتی‌که حاکمیت مجازات‌های بازدارنده مانند جرایم اقتصادی بسیار سنگین را برای صاحبان دارایی‌های سایبری و سکوهای دیجیتال ناامن که موجب نقض حریم خصوصی شهروندان یا قطع خدمات تعهد شده شوند، تعیین کند، انتقال ریسک از طرف آن‌ها به شرکت‌های بیمه‌گر آغاز خواهد شد. شرکت‌های بیمه‌گر برای پذیرش ریسک، شرایط مطلوب امنیتی را از سوی سکوها و سامانه‌ها خواستار خواهند شد. به‌تبع آن، این شرکت‌ها به سمت امن‌سازی کیفی و عمیق مطابق با استانداردها حرکت خواهند کرد. این چرخه موجب بهبود امنیت سازمان‌ها و دارایی‌های سایبری در کشور خواهد شد و در بلندمدت، هزینه‌های آن‌ها را به واسطه ارتقای سطح امنیت و کاهش خسارات ناشی از حملات سایبری، کاهش می‌دهد. تا زمانی که این چرخه به‌درستی تعریف نشود، نه امنیت مناسبی در فضای سایبری کشور ایجاد خواهد شد و نه صنعت بیمه سایبری شکل خواهد گرفت.

**ب-خلاصه**

با توجه به‌سرعت دیجیتالی‌شدن بسیاری از امور زندگی، حملات سایبری به طور غیرقابل‌وصفی افزایش‌یافته است. امروزه، حملات سایبری با هدف قراردادن تأسیسات زیرساختی مانند شبکه‌های برق، سامانه‌های بانکی، سامانه‌های درمانی و سیستم‌های ارتباطی می‌تواند پیامدهای فاجعه‌باری برای سازمان‌ها، اقتصاد کشور و به طور وسیع‌تر جامعه به همراه داشته باشد. ریسک سایبری، به‌ویژه در قالب حملات باج‌افزاری، و نگرانی‌های فزاینده کسب‌وکارها و دولت‌ها در خصوص امنیت سایبری، به‌سرعت در حال افزایش است. شرکت مک‌آفی[[1]](#footnote-1) خسارات مالی جهانی ناشی از جرایم سایبری در سال 2020 را حدود 945 میلیارد دلار تخمین زده است. این در حالی است که مجمع جهانی اقتصاد[[2]](#footnote-2)، به نقل از استاتیستا[[3]](#footnote-3)، پیش‌بینی می‌کند که این میزان در سال 2024 به 14.57 تریلیون دلار و در سال 2027 به 23.82 تریلیون دلار برسد. حملات سایبری به‌تدریج پیچیده‌تر شده و هکرها اکنون از تکنیک‌های اخاذی ترکیبی استفاده می‌کنند. شرکت‌های کوچک و متوسط به دلیل داشتن سیستم‌های دفاعی ضعیف‌تر، اهداف آسان‌تری برای مجرمان سایبری هستند. از سوی دیگر، دیجیتالی‌شدن صنایع بزرگ، به‌ویژه در بخش‌های مربوط به زیرساخت‌های حیاتی نظیر حوزه‌های بانکی، انرژی و خدمات سلامت، آسیب‌پذیری‌ها را در کل زنجیره تأمین افزایش داده است.

پیش از حمله NotPetya در سال 2017، ریسک‌های سایبری عمدتاً معطوف به حوزه افشای اطلاعات و مسئولیت شخص ثالث بود، اما پس از آن، حوزه ریسک‌های مرتبط با خود کسب‌وکار (شخص اول) گسترش یافت. گسترش قانون حفظ حریم خصوصی داده‌ها و کشیده شدن دعاوی به دادگاه‌ها نیز منجر به طولانی شدن روند تسویه خسارت برای شرکت‌های بیمه مستقیم و اتکایی شده است. در دو سال اخیر، خسارت واردشده به شخص اول، به‌جای شخص ثالث، بیشتر مورد توجه قرار گرفته است. به همین منظور، شرکت‌ها، بیمه‌گران و مقامات دولتی تلاش‌های زیادی در زمینه مدیریت ریسک‌های سایبری انجام داده‌اند و انجمن‌های صنعتی و بیمه‌گران برای رسیدگی به موضوعات مرتبط با ریسک سایبری همکاری کرده‌اند. بیمه نقش کلیدی در این زمینه ایفا کرده و نه تنها در انتقال ریسک، بلکه در ایجاد انگیزه برای کاهش ریسک، حمایت از نظارت و پاسخ مناسب به ریسک، مؤثر عمل می‌کند.

اکثر شرکت‌ها، بیمه سایبری ندارند یا از پوشش بیمه‌ای مناسب برخوردار نیستند. در یک نظرسنجی که اخیراً انجام شده است، مشخص شد که تنها 55 درصد از کسب‌وکارها دارای پوشش سایبری بوده و کمتر از یک شرکت از هر پنج شرکت، دارای پوششی بالاتر از میانگین تقاضای باج‌افزارها هستند. به‌طور تقریبی، کل خسارات ناشی از یک حمله سایبری در شرکت‌های کوچک و متوسط، به‌طور نسبی سه برابر بیشتر از شرکت‌های بزرگ است. علاوه بر این، در شرکتی با گردش مالی کمتر از 50 میلیون دلار، هزینه‌های جرم‌یابی معمولاً از 20 هزار تا 100 هزار دلار متغیر است.

افزایش حملات باج‌افزاری، باعث افزایش ضریب خسارت در سال 2020 شد. بیمه‌گران با افزایش قیمت‌ها، بهبود شرایط بیمه‌نامه، معرفی حد غرامت‌های فرعی و بیمه مشترک، شفاف‌سازی شرایط و ضوابط و استثنائات، تلاش کردند تا با چنین ریسک‌هایی برخورد کنند. این اقدامات تا حدودی موفقیت‌آمیز بوده و منجر به کاهش ضریب خسارت در سال 2021 شد.

برای رفع محدودیت‌های حوزه بیمه سایبری، افزایش دانش سایبری، استفاده از داده‌های استاندارد، مدل‌سازی بهتر، ثبات بیشتر در بیمه‌نامه‌های سایبری و منابع جدید سرمایه‌گذاری، ضروری است. به همین ترتیب، باید زمینه را برای ایجاد فرصت‌های مشارکت عمومی - خصوصی فراهم کرد. این اقدامات می‌تواند به کاهش مواجهه کلی با ریسک، بهبود درک ریسک و تاب‌آوری جامعه در برابر حملات با پیامدهای مخرب و همچنین بهبود ریسک سیستمی کمک کند. حملات سایبری، ماهیت انسانی و شبکه‌ای دارند و به طور مداوم در حال تکامل هستند که این امر نیازمند یک واکنش هماهنگ است. افزایش تاب‌آوری در این زمینه نیز مستلزم همکاری نزدیک بین شرکت‌ها، بیمه‌گران و دولت‌ها است.

فهرست مطالب

1. [مقدمه 1](#_Toc191902132)
2. [روش انجام کار 3](#_Toc191902133)
3. [بحث‌وبررسی تفضیلی 4](#_Toc191902134)

[1-3 تحلیل محیط خارج با استفاده از مدل PESTEL 4](#_Toc191902135)

[1-1-3- عوامل سیاسی 4](#_Toc191902136)

[2-1-3- عوامل اقتصادی 5](#_Toc191902137)

[3-1-3- عوامل فرهنگی - اجتماعی 6](#_Toc191902138)

[4-1-3- عوامل تکنولوژیک 7](#_Toc191902139)

[5-1-3- عوامل جهانی و محیطی 8](#_Toc191902140)

[6-1-3- عوامل قانونی 9](#_Toc191902141)

[2-3- تحلیل جذابیت صنعت با استفاده از مدل PORTER 10](#_Toc191902142)

[1-2-3- محصولات / خدمات جایگزین 11](#_Toc191902143)

[2-2-3- ورود رقبای جدید 12](#_Toc191902144)

[3-2-3- رقابت بین رقبای موجود 12](#_Toc191902145)

[4-2-3- قدرت چانه‌زنی خریداران 13](#_Toc191902146)

[5-2-3- قدرت چانه‌زنی تأمین‌کنندگان 13](#_Toc191902147)

[6-2-3- جمع‌بندی..... 14](#_Toc191902148)

[3-3- نتیجه‌گیری تحلیل عوامل خارجی 14](#_Toc191902149)

[4-3- نتیجه­گیری عوامل تحلیل داخلی 16](#_Toc191902150)

[5-3- مأموریت و چشم‌انداز توسعه بیمه سایبری در کشور 16](#_Toc191902151)

[6-3- فعالیت‌های کسب‌وکاری مطلوب، فاکتورهای کلیدی موفقیت، نقشه قابلیت‌ها و مدل کسب‌وکار 17](#_Toc191902152)

[7-3- نقشه قابلیت­ها 19](#_Toc191902153)

[8-3- مدل کسب‌وکار بیمه سایبری 19](#_Toc191902154)

1. [نتیجه‌گیری 21](#_Toc191902155)

[1-4- راهبردهای تحقق چشم‌انداز و توسعه حوزه‌های کسب‌وکار متناسب با مسیر استراتژیک 21](#_Toc191902156)

[2-4- برنامه اقدام عملیاتی 21](#_Toc191902157)

1. [توصیه محوری (بیمه سایبری به مثابه پلتفرم) 23](#_Toc191902158)
2. [مراجع 27](#_Toc191902159)
3. [ضمیمه (مصادیقی از حملات سایبری) 28](#_Toc191902160)

فهرست جداول

[جدول 1- فرصت­ها و تهدیدها 15](#_Toc191893894)

[جدول 2- قوت­ها و ضعف­ها 16](#_Toc191893895)

[جدول 3- فاکتورهای کلیدی موفقیت 18](#_Toc191893896)

[جدول 4- اقدامات کلیدی 22](#_Toc191893897)

[جدول 5- بازیگران اصلی اکوسیستم بیمه سایبری شناسایی 24](#_Toc191893898)

فهرست شکل­ها

[شکل 1- فازهای اصلی روش کار 3](#_Toc191893918)

[شکل 2- گام­های اصلی 3](#_Toc191893919)

[شکل 3-چهارچوب عوامل محیطی 4](#_Toc191893920)

[شکل 4- چهارچوب پنج نیروی رقابتی پورتر 11](#_Toc191893921)

[شکل 5- چشمانداز و ماموریت بیمه سایبری 17](#_Toc191893922)

[شکل 6- فعالیت کسب و کارهای مطلوب 18](#_Toc191893923)

[شکل 7- نقشه قابلیت­ها 19](#_Toc191893924)

[شکل 8- مدل کسب و کار CANVA 20](#_Toc191893925)

[شکل 9- راهبردهای تحقق چشمانداز 21](#_Toc191893926)

# مقدمه

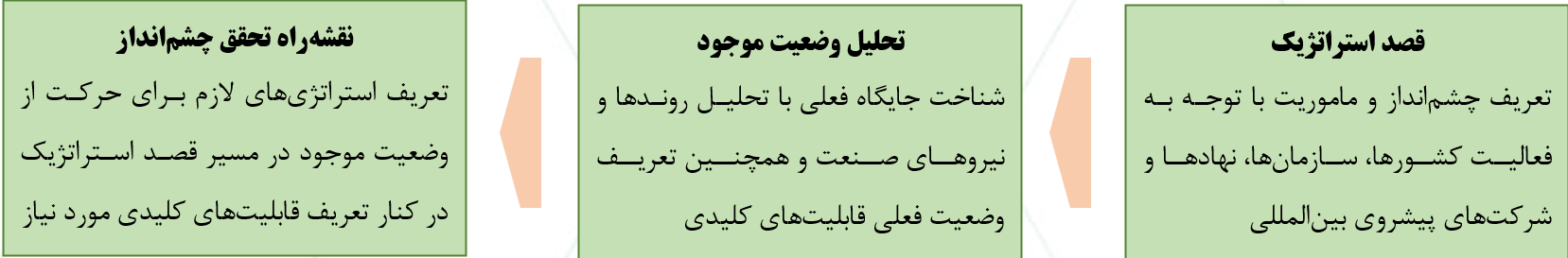
این گزارش بر اساس ضرورت پرداختن به مبحث "بیمه سایبری" که یکی از مهم‌ترین نیازهای حال حاضر در کشور است، و "ضرورت ایجاد صنعت بیمه سایبری در کشور و چارچوب‌های توسعه آن"، تهیه و تدوین شده است. رشته بیمه سایبری به‌واسطة بیمه‌کردن ریسک سایبری، یکی از پیچیده‌ترین و تخصصی‌ترین رشته‌های بیمه‌ای است که شکل مدرن آن کمتر از چهل سال سابقه در سطح جهانی دارد. باتوجه‌به ماهیت پیچیده ریسک سایبری که همواره در حال تحول است و ضرورت توسعه این رشته بیمه‌ای جدید در کشور، حوزه‌های گوناگون در زمینه بیمه سایبری می‌بایست مورد بررسی قرار گیرند. در ادامه، به برخی از چالش‌های پیش‌رو که ضرورت پرداختن به این مهم را تبیین می‌نمایند، اشاره خواهد شد:

* فقدان اطلاعات: بیمه سایبری حوزه نسبتاً جدیدی در دنیا به شمار می‌رود و داده‌های حوادث سایبری و ادعای خسارت بیمه‌شدگان در مقایسه با سایر انواع بیمه محدود است. تحقیقات در زمینه بیمه سایبری از طریق تجزیه‌وتحلیل اطلاعات موجود، ایجاد بانک اطلاعاتی از داده‌ها و ارائه بینشی در مورد فراوانی، شدت و تأثیر مالی حوادث سایبری، می­تواند به پر کردن این شکاف کمک کند. پژوهش در این حوزه برای توسعه مدل‌های دقیق ریسک سایبری و کمک به فرایند بیمه‌گری و پوشش ریسک‌های سایبری، از اهمیت زیادی برخوردار است.
* ارزیابی ریسک پیچیده: ارزیابی ریسک‌های سایبری و تعیین پوشش مناسب، فرایندی پیچیده‌ است. تحقیقات در این حوزه به توسعه روش‌ها، چهارچوب‌ها و ابزارهایی برای ارزیابی ریسک سایبری و تعیین دقیق میزان خسارات احتمالی کمک خواهد کرد.
* نیاز به توسعه و استانداردسازی محصولات بیمه‌ای: توسعه بیمه‌نامه‌ها و استانداردسازی آن‌ها در حوزه امنیت سایبری از الزامات مهم برای پیشرفت صنعت بیمه و کمک به گسترش زیست‌بوم اقتصاد دیجیتال در کشور است. تدوین بهترین شیوه‌ها، دستورالعمل‌ها و استانداردهای صنعت برای پوشش‌های بیمه سایبری، شرایط بیمه‌نامه، شیوه‌های ارزیابی ریسک، مدیریت خسارات و حل اختلاف از مواردی هستند که می‌بایست مورد توجه قرار گیرد. پژوهش در این حوزه به ایجاد یک محیط منسجم و شفاف برای بیمه‌گزاران و بیمه‌گران کمک خواهد کرد.
* آگاهی از مدیریت ریسک در حوزه سایبری: مدیریت ریسک در حوزه سایبری، باتوجه‌به ارزش هنگفت اطلاعات، امروزه یکی از ارکان اصلی تمامی کسب‌وکارها به‌ویژه دررابطه‌با شرکت‌های کوچک و متوسط (SME) است که اغلب با محدودیت‌های منابع مواجه هستند. تحقیقات در حوزه بیمه سایبری، رابطه بین بیمه و استراتژی‌های کاهش ریسک را بررسی کرده و به این موضوع می‌پردازد که چگونه پوشش بیمه می­تواند کسب‌وکارها را تشویق کند تا اقدامات پیشگیرانه امنیت سایبری، مانند اجرای کنترل‌های امنیتی قوی، انجام ارزیابی‌های منظم، و آموزش کارکنان را اتخاذ کنند. نقش بیمه سایبری در ترویج فرهنگ آگاهی از ریسک و تقویت شیوه‌های امنیت سایبری از جمله موارد مهمی است که برای کاهش خسارات ناشی از حملات سایبری باید مورد توجه قرار گیرد.
* بررسی پیامدهای اقتصادی و اجتماعی حملات سایبری بر کسب‌وکارها: حملات سایبری می‌تواند عواقب اقتصادی و اجتماعی شدیدی برای کسب‌وکارها به همراه داشته باشد؛ از جمله نشت داده‌ها و اطلاعات، حملات باج‌افزاری، وقفه در فعالیت­های کسب‌و‌کار و مسئولیت‌های قانونی. ارزیابی تأثیر حوادث سایبری و نحوه حمایت پوشش بیمه‌ای از این حوادث، از جمله موضوعاتی است که برای تحلیل هزینه‌های اقتصادی و اجتماعی ناشی از این حملات، نیازمند بررسی دقیق است.
* ملاحظات قانونی: دولت‌ها و نهادهای نظارتی به طور فزاینده‌ای بر امنیت سایبری و حفاظت از داده‌ها تمرکز کرده­اند. درک نقش بیمه سایبری در انطباق با الزامات قانونی و نظارتی، مانند قوانین اعلان نقض داده و مقررات حفظ حریم خصوصی، برای شرکت‌ها و سیاست­گذاران به طور یکسان از اهمیت بالایی برخوردار است.

به‌طورکلی و با جمع‌بندی موارد فوق‌الذکر می‌توان گفت که دلیل اصلی تدوین این گزارش، نیازی است که به زمینه‌سازی صحیح و کارآمد برای فعال‌سازی و گسترش حوزه بیمه سایبری در کشور وجود دارد، به‌ویژه آن که توسعه اقتصاد دیجیتال، به‌عنوان یکی از سیاست‌های راهبردی، مورد تأکید قرار دارد.

# روش انجام کار

باتوجه‌به نوپا بودن صنعت بیمه سایبری و همچنین ماهیت آن، این گزارش با استفاده از روش Strategic Intent یا نیت استراتژیک، استراتژی توسعه بیمه سایبری در کشور را پیشنهاد می­دهد. روش کار از سه‌فاز اصلی به شرح ذیل تشکیل شده است:

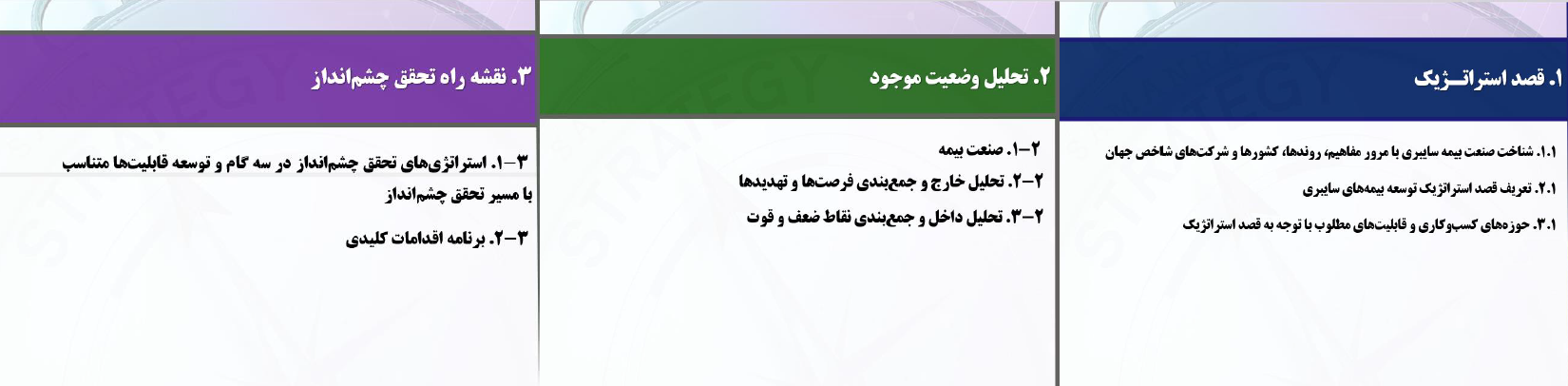
****

شکل 1- فازهای اصلی روش کار

در گام اول، با استفاده از بررسی تجربیات جهانی، شرکت‌های بیمه و کشورهای پیشرو در حوزه بیمه سایبری، حوزه‌های کلیدی کسب‌و‌کار جهت توسعه بیمه سایبری در کشور احصا شده است. همچنین با استفاده از بررسی مفاهیم ارزیابی و مدیریت ریسک سایبری، چهارچوب‌ها، دستورالعمل‌ها و استانداردهای موجود استخراج شده­اند.

در گام دوم، با استفاده از شناخت جایگاه فعلی و تحلیل روندها و نیروهای صنعت، وضعیت فعلی قابلیت‌های کلیدی تبیین شده است. علاوه بر این، فرصت‌ها و تهدیدها و نقاط ضعف و قوت در خصوص توسعه بیمه سایبری مشخص شدند.

در گام آخر، با استفاده از تحلیل شکاف و ترسیم وضعیت موجود نسبت به وضعیت مطلوب، استراتژی‌های توسعه بیمه سایبری در کشور و اقدامات عملیاتی لازم تا افق زمانی 1408 ارائه شده است.



شکل 2- گام­های اصلی

# بحث‌وبررسی تفضیلی

1. تحلیل محیط خارج با استفاده از مدل PESTEL

درگذشته محیط کسب‌وکار محیط ثابتی بود که قدرت پیش‌بینی آن برای مدیران کسب‌وکار فراهم بوده و توانایی کنترل شرایط محیطی نیز وجود داشته ‌است. اما با گذر زمان، این محیط از حالت ثابت گذر کرده و به محیطی پویا تبدیل شده است که علاوه بر تأثیرپذیری، تأثیرگذار نیز است. تحلیل محیطی PESTEL ابزاری است که بسیاری از کسب‌وکارها برای شناسایی محیط پیرامون و تغییرات محیطی از آن استفاده می‌کنند.



شکل 3-چهارچوب عوامل محیطی

### عوامل سیاسی

**روابط بین‌الملل:** وضعیت ایران از نظر سیاست خارجی و تحریم‌های اعمال شده می‌تواند سرمایه‌گذاری خارجی در بخش بیمه سایبری را تحت‌تأثیر قرار دهد. تحریم‌های اقتصادی اعمال‌شده بر ایران می‌تواند دسترسی به بازارها و فناوری‌های بین‌المللی را محدود کند و بر دردسترس‌بودن محصولات و تخصص بیمه سایبری پیشرفته تأثیر بگذارد. این امر ممکن است شکافی در بازار ایجاد کند، جایی که ارائه‌دهندگان داخلی ممکن است برای ارائه راه‌حل‌های جامع، بدون دسترسی به منابع جهانی، با مشکل مواجه شوند. بااین‌حال، این وضعیت می­تواند فرصتی برای شرکت‌های داخلی برای نوآوری و توسعه محصولات بیمه سایبری متناسب با نیازهای داخلی ایجاد کند. از سوی دیگر، مشارکت با سازمان‌های کشورهای متحد می‌تواند فرصت‌هایی را برای انتقال دانش و اشتراک فناوری فراهم کند و چشم‌انداز بیمه سایبری داخلی را بهبود بخشد.

همچنین، یکی از آثار تحریم بر صنعت بیمه، دشواری در نقل‌وانتقالات ارزی به‌منظور پرداخت حق بیمه به بیمه‌گران طرف قرارداد خارجی یا دریافت خسارت بابت پوشش‌های بیمه‌ای اخذ شده است. ممنوعیت استفاده از خدمات ارتباطی مانند سوئیفت و افزایش ریسک در نقل‌وانتقالات ارزی به دلیل استفاده از شیوه‌های ناامن، از دیگر مشکلات تحریم­ها است. این مسائل باعث می‌شود که فعالیت‌های بیمه سایبری، از جمله واگذاری اتکایی در بیمه سایبری، در حوزه بین‌الملل با چالش­های جدی مواجه شود.

**آگاهی عمومی و آموزش:** کمپین‌های دولتی باهدف افزایش آگاهی عمومی از تهدیدات امنیت سایبری می‌توانند محیط مساعدی را برای توسعه بیمه سایبری ایجاد کنند. با افزایش آگاهی کسب‌وکارها و افراد از خطرات سایبری، تقاضا برای محصولات بیمه سایبری احتمالاً افزایش خواهد یافت. بااین‌حال، اگر دولت نتواند اهمیت امنیت سایبری را به طور مؤثر به جامعه منتقل کند، بازار بیمه سایبری ممکن است توسعه‌نیافته باقی بماند و پتانسیل رشد آن محدود شود.

**مشوق‌های دولتی:** دولت ابتکارات و مشوق‌های مختلفی را باهدف بهبود اقتصاد دیجیتال و چهارچوب­های امنیت سایبری آغاز کرده است. به‌عنوان‌مثال، تلاش برای ترویج تحول دیجیتال در کسب‌وکارها می‌تواند زمینه­ای مساعد برای توسعه و گسترش محصولات بیمه سایبری فراهم کند.

**جمع‌بندی:** عوامل سیاسی مؤثر بر توسعه بیمه سایبری در ایران، ترکیبی از فرصت‌ها و تهدیدها را به همراه دارد. استفاده از ابتکارات حمایتی دولت و افزایش آگاهی عمومی می‌تواند محیطی مساعد برای رشد این صنعت ایجاد کند. بااین‌حال، پیچیدگی‌های نظارتی و چالش­های قانونی برای توسعه و ترویج موفقیت‌آمیز محصولات بیمه سایبری در کشور، نقشی حیاتی و تعیین‌کننده خواهد داشت.

### عوامل اقتصادی

**رشد و ثبات اقتصادی:** نرخ رشد اقتصادی می‌تواند تأثیر قابل­توجهی بر توانایی کسب‌وکارها برای سرمایه‌گذاری در ابزارهای مدیریت ریسک مانند بیمه سایبری داشته باشد. یک محیط اقتصادی باثبات می‌تواند کسب‌وکارها را به تخصیص منابع برای محصولات بیمه تشویق کند، درحالی‌که رکود اقتصادی ممکن است به اتخاذ اقدامات کاهش هزینه منجر شود و در نتیجه تقاضا برای چنین خدماتی کاهش دهد.

**رشد اقتصاد دیجیتال:** گسترش اقتصاد دیجیتال در ایران، با افزایش ضریب نفوذ اینترنت و رشد تعداد کسب‌وکارهای آنلاین، زمینه مناسبی برای بیمه سایبری ایجاد می‌کند. با انتقال بیشتر شرکت‌ها به سیستم‌های دیجیتال، خطرات مرتبط با تهدیدات سایبری افزایش می‌یابد که این امر منجر به افزایش تقاضا برای محصولات بیمه­ای خواهد شد. علاوه بر این، ابتکارات دولتی برای ترویج تحول دیجیتال در بخش‌های مختلف می‌تواند به رشد اقتصاد دیجیتال و در نتیجه افزایش نیاز به بیمه سایبری کمک کند.

**محیط کسب‌وکار:** فضای کلی کسب‌وکار در ایران، از جمله سهولت انجام کسب‌وکار، دسترسی به منابع مالی و چهارچوب نظارتی، می‌تواند تأثیر زیادی بر رشد بخش بیمه داشته باشد. یک محیط حمایتی و پویا، کارآفرینی و سرمایه‌گذاری را تشویق می‌کند و در نتیجه نیاز به راه‌حل‌های مدیریت ریسک، ازجمله بیمه سایبری، را افزایش می­دهد. در مقابل، چالش‌هایی مانند موانع بوروکراتیک، دسترسی محدود به بازارهای بین‌المللی و تحریم‌های اقتصادی می‌تواند مانع رشد کسب‌وکار شده و تقاضا برای بیمه را کاهش دهد.

**قدرت خرید:** قدرت خرید مشاغل و افراد در ایران بر توانایی آن‌ها برای سرمایه‌گذاری یا خرید بیمه سایبری تأثیر می‌گذارد. چالش‌های اقتصادی، مانند تورم و کاهش ارزش پول، ممکن است درآمد را محدود کرده و تمایل به هزینه برای محصولات بیمه را کاهش دهد. درک ظرفیت مالی بازار هدف برای توسعه راه‌حل‌های بیمه سایبری مقرون‌به‌صرفه و قابل‌دسترس، امری حیاتی برای موفقیت در این صنعت است.

**سرمایه‌گذاری در امنیت سایبری:** افزایش سرمایه‌گذاری در اقدامات امنیت سایبری توسط مشاغل می‌تواند منجر به درک بیشتر ریسک‌های موجود شده و در نتیجه احتمال خرید بیمه را افزایش دهد. این سرمایه‌گذاری اغلب تحت‌تأثیر شرایط اقتصادی و تهدید حملات سایبری قرار دارد. نقش دولت در ارتقای ابتکارات امنیت سایبری نیز می‌تواند کسب‌وکارها را به سرمایه‌گذاری بیشتر در امنیت سایبری و بیمه تشویق کند.

**جمع‌بندی:** رشد اقتصاد دیجیتال و افزایش آگاهی از خطرات سایبری می‌تواند تقاضا برای محصولات بیمه را افزایش دهد. بااین‌حال، بی‌ثباتی اقتصادی و قدرت خرید محدود ممکن است چالش‌های مهمی ایجاد کند. درک این پویایی‌های اقتصادی برای توسعه و ترویج مؤثر خدمات بیمه سایبری در ایران حیاتی خواهد بود.

### عوامل فرهنگی - اجتماعی

نگرش فرهنگی نسبت به بیمه: در ایران بدبینی تاریخی نسبت به محصولات بیمه وجود دارد که می‌تواند ناشی از باورهای فرهنگی و مذهبی باشد. بسیاری از افراد و کسب‌وکارها ممکن است بیمه را غیرضروری بدانند یا نگرانی­هایی در مورد مشروعیت آن داشته باشند. این شک‌وتردید می‌تواند مانعی مهم برای پذیرش بیمه سایبری باشد. ارتقای آگاهی از مزایا و ضرورت‌های بیمه سایبری، به‌ویژه در اقتصاد دیجیتال، برای تغییر این ادراکات نگرش‌ها و ارتقای پذیرش آن بسیار مهم است.

**آگاهی از خطرات سایبری:** سطح آگاهی در مورد تهدیدات سایبری در بین مشاغل و مصرف‌کنندگان یک عامل اجتماعی مهم به شمار می­آید. درحالی‌که شناخت روزافزونی از مسائل امنیت سایبری وجود دارد، بسیاری از سازمان‌ها ممکن است خطرات را دست‌کم بگیرند یا معتقد باشند که هدف حملات سایبری نیستند. کمپین‌ها و ابتکارات آموزشی برای افزایش آگاهی در مورد پیامدهای تهدیدات سایبری می‌تواند به افزایش تقاضا برای محصولات بیمه سایبری کمک کند.

**سواد دیجیتال:** میزان سواد دیجیتال در جمعیت بر نحوه درک و مدیریت ریسک‌های سایبری توسط افراد و کسب‌وکارها تأثیر می‌گذارد. سواد دیجیتال بالاتر می‌تواند منجر به درک و اجرای بهتر اقدامات امنیت سایبری شود و در نتیجه احتمال خرید بیمه سایبری را افزایش دهد. در مقابل، سواد دیجیتالی پایین ممکن است مانع از اتخاذ روش‌های مناسب امنیت سایبری و استفاده از محصولات بیمه شود و بر لزوم اجرای برنامه‌های آموزشی هدفمند تأکید می‌کند.

شیوه‌ها و هنجارهای کسب‌وکار: رویه‌های سنتی کسب‌وکار در ایران ممکن است استراتژی‌های مدیریت ریسک، از جمله بیمه، را در اولویت قرار ندهند. بسیاری از شرکت‌ها ممکن است به‌جای استفاده از محصولات بیمه رسمی، برای پشتیبانی در مواقع بحران به‌ شبکه­های غیررسمی تکیه کنند. تغییر هنجارهای کسب‌وکار و ایجاد فرهنگ‌پذیرش شیوه‌های مدیریت ریسک حرفه‌ای برای تقویت تقاضا برای بیمه سایبری ضروری است.

**تأثیر جمعیت‌شناسی جوانان:** ایران دارای جمعیت جوان و آگاه به فناوری است که به طور فزاینده‌ای درگیر فعالیت‌های دیجیتالی هستند. این جمعیت احتمالاً آگاهی بیشتری از خطرات سایبری دارد و از راه‌حل‌های بیمه نوآورانه استقبال بیشتری خواهد کرد. هدف قراردادن مشاغل و کارآفرینان جوان با محصولات بیمه سایبری مناسب می‌تواند استراتژی مؤثری برای جذب این گروه و توسعه بازار بیمه سایبری باشد.

**رسانه‌های اجتماعی و ارتباطات:** نقش رسانه‌های اجتماعی و ارتباطات آنلاین در شکل‌گیری افکار عمومی را نمی‌توان دست‌کم گرفت. پلتفرم‌های رسانه‌های اجتماعی می‌توانند ابزار قدرتمندی برای آموزش مردم در مورد بیمه سایبری و مزایای آن باشند. تعامل با جامعه از طریق کمپین‌های رسانه‌های اجتماعی می‌تواند آگاهی را افزایش دهد و بحث‌ها را در مورد اهمیت حفاظت از دارایی‌های دیجیتال تشویق کند.

**جمع‌بندی:** عوامل اجتماعی نقش بسزایی در توسعه بیمه سایبری در ایران دارند. پرداختن به نگرش‌های فرهنگی، افزایش آگاهی از خطرات سایبری و بهره‌گیری از سواد دیجیتالی جمعیت جوان‌تر برای ایجاد یک محیط حمایتی برای بیمه سایبری ضروری است. ابتکارات آموزشی مناسب و استراتژی‌های بازاریابی هدفمند، برای غلبه بر موانع اجتماعی و ترویج پذیرش راه‌حل‌های بیمه سایبری، امری حیاتی خواهد بود.

### عوامل تکنولوژیک

**زیرساخت دیجیتال:** وضعیت زیرساخت دیجیتال در ایران، از جمله اتصال به اینترنت، مراکز داده و خدمات ابری، برای پذیرش بیمه سایبری حیاتی است. بهبود زیرساخت‌های دیجیتال می‌تواند رشد کسب‌وکارهای آنلاین را تسهیل کرده و تقاضا برای بیمه سایبری را افزایش دهد. بااین‌حال، مسائلی مانند دسترسی به اینترنت، به‌ویژه در مناطق روستایی، ممکن است مانع از رشد اقتصاد دیجیتال شده و بر بازار بیمه سایبری تأثیر منفی بگذارد.

**فناوری امنیت سایبری:** دسترسی به و پذیرش فناوری‌های امنیت سایبری پیشرفته (مانند فایروال‌ها، سیستم‌های تشخیص نفوذ، رمزگذاری) مستقیماً بر تقاضای بیمه سایبری تأثیر می‌گذارد. همان‌طور که کسب‌وکارها در این فناوری‌ها سرمایه‌گذاری می‌کنند، ممکن است نیاز به بیمه را برای تکمیل استراتژی‌های مدیریت ریسک خود شناسایی کنند. برعکس، فقدان سرمایه‌گذاری در امنیت سایبری می‌تواند منجر به خطرات و ضررهای بالاتری شود که ممکن است بر ارزش درک شده از بیمه سایبری تأثیر منفی بگذارد.

**نوآوری و تحقیق:** ایران دارای بخش فناوری روبه‌رشدی است که استارت‌آپ‌ها و طرح‌های تحقیقاتی متعددی با تمرکز بر راه‌حل‌های امنیت سایبری دارد. این نوآوری می‌تواند به توسعه محصولات بیمه سایبری متناسب با نیازهای داخلی منجر شود. همکاری بین شرکت‌های بیمه و شرکت‌های فناوری می‌تواند به ایجاد راه‌حل‌های بیمه­ای جامع منجر شود که شامل ارزیابی ریسک و اقدامات امنیت سایبری به طور یکپارچه باشد.

**رعایت مقررات و استانداردها:** ظهور استانداردها و مقررات بین‌المللی امنیت سایبری (مانند GDPR) می‌تواند تأثیر زیادی بر توسعه محصولات بیمه سایبری داشته باشد. ارائه‌دهندگان بیمه باید پیشنهادهای خود را با این استانداردها هماهنگ کنند تا رقابتی و سازگار باقی بمانند. علاوه بر این، مقررات داخلی در خصوص حفاظت از داده‌ها و امنیت سایبری می‌تواند انواع پوشش­ بیمه­ای مورد نیاز در بازار ایران را شکل دهد.

**فناوری‌های نوظهور:** ظهور فناوری‌های نوظهور مانند هوش مصنوعی (AI)، یادگیری ماشینی و اینترنت اشیا (IoT) فرصت‌ها و چالش‌هایی را برای بیمه سایبری ایجاد می‌کند. درحالی‌که این فناوری‌ها می‌توانند اقدامات امنیتی را تقویت کنند، اما همچنین خطرات جدیدی را معرفی می­نمایند که باید از طریق محصولات بیمه مورد توجه قرار گیرند. ارائه‌دهندگان بیمه باید همواره در جریان پیشرفت‌های تکنولوژیکی قرار بگیرند تا پیشنهادهای خود را با خطرات در حال تحول سازگار کنند.

**جمع‌بندی:** عوامل فناورانه در شکل‌دهی چشم‌انداز بیمه سایبری در ایران نقش اساسی دارند. وضعیت زیرساخت دیجیتال، رشد بخش فناوری و آگاهی از خطرات امنیت سایبری نقش اساسی در تعیین پتانسیل بازار خواهد داشت. با بهره­گیری از پیشرفت‌های تکنولوژیکی و پرداختن به ریسک‌های نوظهور، ارائه‌دهندگان بیمه می‌توانند محصولات نوآورانه­ای تولید کنند که نیازهای مشاغل و افراد را در یک محیط دیجیتالی برآورده سازد.

### عوامل جهانی و محیطی

**تأثیر تغییرات آب‌وهوا:** درحالی‌که بیمه سایبری به تهدیدات دیجیتالی می‌پردازد، پیامدهای تغییرات آب‌وهوایی نیز می‌تواند بر زیرساخت دیجیتالی مشاغل تأثیر بگذارد. بلایای طبیعی مانند سیل یا زمین‌لرزه می‌توانند عملیات کسب‌وکارها را مختل کرده و به نوبه خود خطر حوادث سایبری را افزایش دهند، زیرا شرکت‌ها برای بازیابی سیستم‌ها و داده‌ها تلاش می‌کنند. درک اینکه چگونه تغییرات آب‌وهوایی بر دارایی‌های دیجیتال شرکت‌ها تأثیر می‌گذارد، می‌تواند بر انواع پوشش‌های مورد نیاز در بیمه‌نامه‌های سایبری تأثیر بگذارد و محصولات بیمه‌ای را بر اساس این تهدیدات جدید شکل دهد.

**مشوق‌های پایداری:** افزایش تمرکز جهانی بر پایداری و مسئولیت اجتماعی شرکت‌ها می‌تواند سازمان‌ها را به سمت اتخاذ شیوه‌های مدیریت ریسک قوی‌تر، از جمله بیمه سایبری سوق دهد. شرکت‌هایی که پایداری را در اولویت قرار می‌دهند ممکن است به دنبال محصولات بیمه‌ای همسو با اهداف زیست‌محیطی خود باشند. این روند می‌تواند فرصت­هایی را برای ارائه‌دهندگان بیمه ایجاد کند تا محصولات بیمه سایبری سبز را توسعه دهند که هم­زمان خطرات دیجیتال و زیست‌محیطی را پوشش می­دهند.

**انعطاف‌پذیری زیرساخت دیجیتال:** انعطاف‌پذیری زیرساخت‌های دیجیتال در مواجهه با چالش‌های زیست‌محیطی بسیار مهم است. کسب‌وکارهایی که در مناطق مستعد بلایای طبیعی فعالیت می‌کنند باید تأثیر بالقوه این بلایا بر دارایی‌های دیجیتال خود و نیاز به بیمه‌ای که هم تهدیدات سایبری و هم تهدیدات فیزیکی را پوشش دهد، در نظر بگیرند. هنگام طراحی بیمه‌نامه‌های سایبری، بیمه‌گران ممکن است نیاز به ارزیابی ریسک‌های زیست‌محیطی مرتبط با عملیات مشتریان داشته باشند تا پوشش جامع­تری برای آن­ها فراهم کنند.

**محیط نظارتی:** مقررات زیست‌محیطی می‌تواند بر نحوه عملکرد و مدیریت ریسک‌های کسب‌وکارها، از جمله ریسک‌های سایبری، تأثیر بگذارد. شرکت‌هایی که مشمول مقررات سخت‌گیرانه زیست‌محیطی هستند، ممکن است نیاز به رعایت استانداردهای حفاظت از داده‌ها و امنیت سایبری داشته باشند که این امر منجر به افزایش تقاضا برای راه‌حل‌های بیمه جامع می‌شود. بیمه‌گران باید از این مقررات آگاه باشند تا پیشنهادهای خود را مطابق با آن تنظیم کنند و محصولات بیمه‌ای مناسبی ارائه دهند.

**جمع‌بندی:** عوامل محیطی، اگرچه اغلب تحت‌تأثیر ملاحظات مستقیم اقتصادی و فناوری قرار می‌گیرند، نقش بسزایی در توسعه بیمه سایبری در ایران دارند. تأثیر متقابل بین تغییرات آب‌وهوایی، ابتکارات پایداری و انعطاف‌پذیری زیرساخت‌های دیجیتال، چالش‌ها و فرصت‌هایی را برای بیمه‌گران ایجاد می‌کند. با پرداختن به این عوامل محیطی، ارائه‌دهندگان بیمه می‌توانند محصولات جامع و مناسبی ایجاد کنند که نیازهای در حال تحول کسب‌وکارها را در یک محیط پیچیده و پویا برآورده سازد.

### عوامل قانونی

**چهارچوب نظارتی:** به نظر می‌رسد قوانین و مقررات مختلفی دررابطه‌با امنیت سایبری و حفاظت از داده‌ها باید در کشور وضع شود. قانون امنیت سایبری که برای ارتقای امنیت ملی و حفاظت از زیرساخت‌های حیاتی تصویب شده است، زمینه را برای تعهدات قانونی مشاغل در مورد امنیت داده‌ها تا حدودی فراهم می‌کند.رعایت این مقررات برای ارائه‌دهندگان بیمه ضروری است، زیرا آن‌ها باید اطمینان حاصل کنند که محصولاتشان با الزامات قانونی مطابقت دارد و درعین‌حال از مصرف‌کنندگان نیز حمایت می‌کند.

**قوانین حفاظت از داده‌ها:** محیط قانونی پیرامون حفاظت از داده‌ها برای بیمه سایبری بسیار مهم است. قوانین حاکم بر مدیریت، ذخیره‌سازی و پردازش داده‌های شخصی بر خطراتی که مشاغل با آن مواجه هستند و به طور متعاقب بر انواع پوشش‌های مورد نیاز تأثیر می‌گذارد.درک پیامدهای قوانین حفاظت از داده‌ها، از جمله مجازات مربوط به عدم انطباق، می‌تواند به بیمه‌گران کمک کند تا بیمه‌نامه‌‌هایی را طراحی کنند که مسئولیت‌های بالقوه را به طور کامل پوشش دهند و نیازهای قانونی مشاغل را برآورده سازند.

**انطباق بین‌المللی:** برای کسب‌وکارهایی که در حوزه‌های قضایی متعدد فعالیت می‌کنند، رعایت قوانین و استانداردهای بین‌المللی، مانند مقررات عمومی حفاظت از داده‌ها (GDPR) ضروری است. پیمایش این پیچیدگی‌ها می‌تواند بر توسعه و بازاریابی محصولات بیمه سایبری تأثیر بگذارد. ممکن است بیمه‌گران نیاز به ارائه راه‌حل‌های انعطاف‌پذیر داشته باشند که هم الزامات قانونی داخلی و هم بین‌المللی را برآورده کند و جذابیت محصولات خود را برای مشاغل فعال در تجارت جهانی افزایش ‌دهد.

جمع‌بندی: عوامل حقوقی نقش تعیین‌کننده­ای در شکل‌گیری چشم‌انداز بیمه سایبری در ایران دارند. درک چهارچوب نظارتی، قوانین حفاظت از داده‌ها و ملاحظات مسئولیت برای توسعه محصولات بیمه ضروری است. با پیمایش این چالش‌های قانونی و استفاده از فرصت‌ها برای ارائه راه‌حل‌های مناسب، ارائه‌دهندگان بیمه می‌توانند پیشنهادهای خود را بهبود داده و به کسب‌وکارها در یک محیط دیجیتالی پیچیده‌تر خدمت کنند.

1. تحلیل جذابیت صنعت با استفاده از مدل PORTER

چهارچوب پنج نیروی رقابتی پورتر یک ابزار استراتژیک است که برای تجزیه‌وتحلیل محیط رقابتی یک صنعت استفاده می‌شود. مایکل پورتر، استراتژیست معروف دانشگاه هاروارد، در سال ۱۹۸۰ مدلی به نام چهارچوب پنج نیروی رقابتی پورتر را معرفی کرد. این چهارچوب، مدلی بسیار قوی است که به کسب‌وکارها کمک می‌کند تا نقاط ضعف و قوت خود را بهتر بشناسند و بتوانند موقعیت خود را نسبت به رقبای موجود در بازار بررسی کنند. پورتر چهار دهه قبل در کتاب استراتژی رقابتی خود، پنج نیروی رقابتی را مطرح کرده و توضیح داد که حاشیه سود در یک صنعت و به‌تبع آن، جذابیت آن صنعت تابع قدرت و اندازة این پنج نیروست. او معتقد است که تعامل این نیروها و تأثیر آن‌ها بر یکدیگر است که متوسط حاشیة سود در یک صنعت را مشخص می‌کند. برای بازار بیمه سایبری در ایران، این تجزیه‌وتحلیل می‌تواند بینشی در مورد پویایی‌های مؤثر بر ورود به بازار، رقابت و سودآوری ارائه دهد.

شکل 4- چهارچوب پنج نیروی رقابتی پورتر

### محصولات / خدمات جایگزین

محصول جایگزین، محصولی است که ارزش و منافع مشابه محصول فعلی را ارائه می­دهد. به نظر می‌رسد تا به امروز خدمتی مشابه با خدمات و محصولات بیمه سایبری عرضه نشده است؛ حداقل می‌توان اذعان داشت که محصولات مشابه تمامی ارزش‌های "بیمه سایبری" را برای مشتری به ارمغان نمی‌آورند. بااین‌حال، موارد زیر به‌نوعی بر بازار بیمه سایبری تأثیر دارند:

**راه‌حل‌های مدیریت ریسک جایگزین:** کسب‌وکارها ممکن است ریسک‌های سایبری خود را از طریق روش‌های جایگزین مدیریت کنند، مانند سرمایه‌گذاری مستقیم در اقدامات امنیت سایبری به‌جای خرید بیمه. این امر می‌تواند نیاز درک شده به بیمه سایبری را کاهش دهد و به‌عنوان یک مانع برای پذیرش محصولات بیمه سایبری در نظر گرفته شود.

**خود بیمه‌گری:** جایگزین پررنگ‌تری مانند شرکت‌های کپتیو در دنیای امروز، دغدغه‌ای مهم‌تر برای شرکت‌های بیمه به شمار می‌رود. سازمان‌های بزرگ در دنیا جهت جلوگیری از خروج حق بیمه‌های بسیار زیادی که هر ساله بابت خرید انواع پوشش‌های بیمه‌ای باید بپردازند، تمایل به تأسیس شرکت‌های کپتیو پیدا کرده‌اند. این شرکت‌ها که کارایی مشابه شرکت‌های بیمه را دارند، به‌عنوان صندوقی برای تجمیع ریسک‌های هر سازمان توسط خود آن سازمان ایجاد می‌شوند. بااین‌حال، در ایران دو عامل باعث شده است که شرکت‌های کپتیو به معنای حقیقی وجود نداشته باشند؛ اولین عامل، وجود بیمه مرکزی جمهوری اسلامی ایران به‌عنوان نهاد ناظر و قانون‌گذار است که اشتیاقی به صدور مجوز در این زمینه ندارد و دومین دلیل، وجود نرخ‌های بسیار رقابتی در بازار بیمة سنتی است که سازمان‌ها را از تأسیس چنین شرکت‌هایی منصرف کرده است.

**راه‌حل‌های نوظهور:** راه‌حل‌های جدید انتقال ریسک، مانند اوراق بیمه سایبری، ممکن است به‌عنوان جایگزین برای محصولات سایبری ظاهر شوند و رقابت را تشدید کنند. این اوراق که از ابزار جدید انتقال ریسک به شمار می‌روند، ریسک را به‌جای شرکت بیمه به بازار سرمایه منتقل می‌کنند. این رویکرد می­تواند به کسب­وکارها این امکان را بدهد که از روش­های نوین و انعطاف­پذیرتری برای مدیریت ریسک­های سایبری استفاده کنند و در نتیجه بازار بیمه سایبری تأثیرگذار باشد.

### ورود رقبای جدید

هرچه بازده سرمایة صنعتی از هزینة سرمایة آن بیشتر باشد، جذابیت آن صنعت برای ورود بیشتر خواهد بود. با ورود شرکت‌های تازه به بازار، رقیبان تازه‌ای برای شرکت‌های موجود ایجاد می‌شود که ممکن است قیمت‌ها و حاشیة سود را بسیار رقابتی نماید. در ادامه، عوامل مؤثر بر ورود رقبا را در صنعت بیمه سایبری بررسی می‌کنیم.

**الزامات سرمایه‌ای**: ماهیت بیمه پوشش ریسک است و ارزش ریالی ریسک‌های جمع شده در یک شرکت بیمه بسیار زیاد است. به همین دلیل، شرکت‌های بیمه‌ای که مایل به ورود به رشته‌های بیمه‌ای جدید، مانند بیمه سایبری، هستند، باید سرمایه لازم برای پذیرش این ریسک­ها را تأمین کنند. این الزامات سرمایه‌ای، تضمینی برای توانایی شرکت بیمه در پرداخت تعهدهای خود هستند که باید به‌دقت تأمین گردد. علاوه بر سرمایه، هزینه‌های بالای پرسنل و آموزش آن‌ها نیز وجود دارد که مجموع هزینه‌ها را افزایش می‌دهد.

**صرفه‌جویی مقیاس:** وجود هزینه‌های اولیة بسیار ناشی از الزامات سرمایه‌ای سبب می‌شود تا نقطة سربه‌سر دیرتر حاصل شود. همچنین، شرکت‌های قدیمی‌تر زودتر به سوددهی رسیده‌اند و منابع مالی خود را صرف افزایش سهم بازار خود می‌کنند که این امر رقابت را برای شرکت­های تازه­وارد دشوارتر می­سازد.

**تمایز محصولات:** در بازار بیمة کشور، شرکت‌های قدیمی مانند شرکت بیمه ایران، البرز آسیا و دانا از مزیت شناخت نام تجاری و وفاداری توسط مشتریان برخوردار هستند. اما شرکت‌های جدید باید با صرف هزینه‌های بسیار تبلیغات و برندینگ، اعتبار لازم را برای خود ایجاد کنند تا بتوانند سهمی از بازار رقابتی بیمه سایبری به دست آورند.

### رقابت بین رقبای موجود

**تعداد رقبا:** سطح رقابت در بازار بیمه سایبری در ایران به تعداد بازیگران موجود بستگی دارد. تعداد زیاد رقبا می‌تواند منجر به جنگ قیمت و کاهش سودآوری برای همه بیمه‌گران شود، زیرا رقابت فشرده موجب کاهش حاشیه سود و افزایش فشار بر شرکت­ها برای ارائه قیمت­های رقابتی­تر خواهد شد.

**رشد بازار:** اگر بازار بیمه سایبری به‌سرعت درحال‌رشد باشد، شرکت‌ها ممکن است تمایل بیشتری به سرمایه‌گذاری در بازاریابی و توسعه محصول داشته باشند که این امر منجر به افزایش رقابت می‌شود.

**تمایز:** تمایز در خدمات، مانند ارائه خدمات ارزش افزوده؛ مانند مشاوره ریسک می‌تواند در رقابت اثرگذار باشد.

### قدرت چانه‌زنی خریداران

**آگاهی مشتری:** با افزایش آگاهی از خطرات سایبری، کسب‌وکارها ممکن است در مورد گزینه‌های بیمه خودآگاه‌تر شوند و قدرت چانه‌زنی خود را افزایش دهند. این افزایش آگاهی می‌تواند منجر به تقاضا برای قیمت‌گذاری رقابتی‌تر و پوشش جامع شود، زیرا مشتریان نسبت به نیازهای خود و انتخاب­های موجود در بازار آگاه­تر می­شوند و انتظار خدمات بهتر و مقرون­به­صرفه­تری دارند.

**دردسترس‌بودن گزینه‌های جایگزین:** اگر چندین بیمه‌گر محصولات بیمه سایبری مشابهی را ارائه دهند، خریداران می‌توانند به‌راحتی بیمه‌گر خود را تغییر دهند و قدرت چانه‌زنی خود را افزایش دهند. این رقابت می‌تواند قیمت‌ها را کاهش دهد و باعث بهبود کیفیت خدمات ارائه شده شود، زیرا شرکت­ها مجبور خواهند شد برای حفظ مشتریان خود در خدمات و قیمت­گذاری بهبود ایجاد کنند.

### قدرت چانه‌زنی تأمین‌کنندگان

**تأمین‌کنندگان محدود:** در زمینه بیمه سایبری، تأمین‌کنندگان شامل ارائه‌دهندگان فناوری، کارشناسان امنیت سایبری و تحلیلگران داده می‌شوند. تعداد محدودی از متخصصان واجد شرایط امنیت سایبری در ایران می‌توانند قدرت چانه‌زنی آن‌ها را افزایش دهند. زیرا این متخصصان نقش حیاتی در ارزیابی و مدیریت ریسک­های سایبری دارند و در نتیجه می­توانند به تأمین‌کنندگان خدمات حیاتی تبدیل شوند.

**وابستگی تکنولوژیکی:** بیمه‌گران برای ارزیابی ریسک‌ها و بیمه‌نامه‌ها به فناوری پیشرفته متکی هستند. اگر تعداد کمی از تأمین‌کنندگان فناوری یا خدمات حیاتی وجود داشته باشد، این امر می‌تواند به تأمین‌کنندگان اهرم بیشتری در مذاکرات بدهد. وابستگی بیمه­گران به تأمین‌کنندگان می­تواند رقابت را محدود کرده و قدرت چانه­زنی آن را افزایش دهد.

**دانش تخصصی:** نیاز به دانش تخصصی در امنیت سایبری همچنین می‌تواند به این معنی باشد که تأمین‌کنندگان قدرت چانه‌زنی قابل‌توجهی دارند، به‌ویژه اگر خدمات آن‌ها برای توسعه محصولات بیمه ضروری باشد. تخصص بالا و پیچیدگی خدمات امنیت سایبری می­تواند موجب شود تا این تأمین‌کنندگان به عوامل کلیدی در روند توسعه و ارائه بیمه سایبری تبدیل شوند.

### جمع‌بندی

1. **تهدید ورود رقبای جدید:** درحالی‌که موانعی برای ورود به بازار وجود دارد، مانند الزامات نظارتی و نیاز به دانش تخصصی، بازار بیمه سایبری هنوز به نسبت نوپا است. تازه‌واردها ممکن است فرصت‌هایی پیدا کنند، به‌ویژه اگر بتوانند پیشنهادهای خود را متمایز کنند.
2. **قدرت چانه‌زنی تأمین‌کنندگان:** وجودتعداد محدود متخصصان امنیت سایبری واجد شرایط و اتکا به تأمین‌کنندگان فناوری تخصصی به این تأمین‌کنندگان قدرت چانه‌زنی قابل‌توجهی می‌دهد. تخصص آن­ها برای توسعه محصولات بیمه­ای مؤثر بسیار مهم است.
3. **قدرت چانه‌زنی خریداران:** با افزایش آگاهی کسب و کارها از خطرات سایبری و گزینه­های بیمه­ای خود، قدرت چانه­زنی آن­ها افزایش می­یابد. در دسترس بودن ارائه دهندگان جایگزین به این معنی است که خریداران می­توانند برای شرایط و قیمت‌های بهتر مذاکره کنند.
4. **تهدید محصولات یا خدمات جایگزین:** درحالی‌که جایگزین‌هایی مانند خود بیمه‌گری و سرمایه‌گذاری مستقیم در اقدامات امنیت سایبری وجود دارد، ماهیت منحصربه‌فرد بیمه به‌عنوان ابزار مدیریت ریسک این تهدید را در حد متوسط ​​نگه می‌دارد. بااین‌حال، راه‌حل‌های نوظهور می‌توانند این تهدید را در آینده افزایش دهد،زیرا مشتریان ممکن است به دنبال روش‌های جدید و نوآورانه برای مدیریت ریسک‌های سایبری خود باشند.

**5. رقابت بین رقبای موجود در صنعت:** با افزایش آگاهی از خطرات سایبری، سطح رقابت در حال افزایش است که منجر به ورود بازیگران بیشتری به بازار می شود. این امر ممکن است رقابت را شدیدتر کند. استراتژی­های تمایز می تواند به کاهش شدت رقابت بین شرکت­های موجود کمک کند و آن­ها را قادر سازد که در بازار رقابتی از یکدیگر متمایز شوند.

1. نتیجه‌گیری تحلیل عوامل خارجی

باتوجه‌به بررسی‌های صورت‌گرفته حاصل از مدل PESTEL و Porter، می‌توان محیط پیرامون توسعه بیمه سایبری در ایران را در موارد زیر تحت عنوان فرصت‌ها و تهدیدها جمع‌بندی کرد.

* **فرصت­ها**
  + **افزایش آگاهی از خطرات سایبری:** افزایش آگاهی عمومی و تجاری در مورد اهمیت امنیت سایبری می‌تواند تقاضا برای محصولات بیمه سایبری را افزایش دهد.
  + **محیط نظارتی حمایتی:** مشوق دولت باهدف افزایش امنیت سایبری می‌تواند چهارچوب مطلوبی برای توسعه بیمه سایبری ایجاد کند.
  + **گسترش اقتصاد دیجیتال:** با انتقال کسب‌وکارهای بیشتر به پلتفرم‌های دیجیتال، احتمالاً تقاضا برای محصولات بیمه‌ای که خطرات سایبری را پوشش می‌دهند افزایش می‌یابد.
  + **همکاری با استارتاپ‌های فناوری:** مشارکت با شرکت‌های فناوری می‌تواند نوآوری در محصولات بیمه را تقویت کند و راه‌حل‌های متناسب با نیازهای محلی را فراهم کند.
  + **بازار نوظهور برای پوشش مسئولیت:** با افزایش آگاهی کسب‌وکارها از مسئولیت‌های قانونی خود در مورد نقض داده‌، فرصتی برای ایجاد محصولات پوشش مسئولیت تخصصی وجود دارد.
  + **ابتکارات آموزشی:** برنامه‌هایی باهدف آموزش به کسب‌وکارها در مورد خطرات سایبری و گزینه‌های بیمه می‌تواند پذیرش بیمه سایبری را افزایش دهد.
* **تهدیدها**
  + **بدبینی فرهنگی نسبت به بیمه:** شک‌وتردید تاریخی در مورد محصولات بیمه ممکن است مانع پذیرش و پذیرش در بین مشاغل و مصرف‌کنندگان شود.
  + **تخصص محدود امنیت سایبری:** کمبود متخصصان امنیت سایبری واجد شرایط می‌تواند مانع توسعه محصولات بیمه‌ای مؤثر و افزایش اتکا به تأمین‌کنندگان خارجی شود.
  + **رقابت شدید:** رقابت زیاد در بازار بیمه می‌تواند منجر به جنگ قیمت و کاهش سودآوری بیمه‌گران شود.
  + **چالش‌های نظارتی:** تغییرات مکرر در قوانین و مقررات می‌تواند انطباق را برای بیمه‌گران پیچیده کند و باعث ایجاد عدم اطمینان در بازار شود.
  + **محصولات جایگزین:** دردسترس‌بودن راه‌حل‌های جایگزین مدیریت ریسک، مانند خود بیمه‌گری، می‌تواند تقاضا برای محصولات سنتی بیمه سایبری را کاهش دهد.

جدول 1- فرصت­ها و تهدیدها

|  |  |  |  |
| --- | --- | --- | --- |
| **فرصت‌ها** | | **تهدیدات** | |
| **O1** | **افزایش آگاهی از خطرات سایبری** | **T1** | **بدبینی فرهنگی نسبت به بیمه** |
| **O2** | **محیط نظارتی حمایتی** | **T2** | **تخصص محدود امنیت سایبری** |
| **O3** | **گسترش اقتصاد دیجیتال** | **T3** | **رقابت شدید** |
| **O4** | **همکاری با استارتاپ‌های فناوری** | **T4** | **چالش‌های نظارتی** |
| **O5** | **بازار نوظهور برای پوشش مسئولیت** | **T5** | **محصولات جایگزین** |
| **O6** | **ابتکارات آموزشی** | **T6** | **ماهیت در حال تحول ریسک سایبری** |

1. نتیجه­گیری عوامل تحلیل داخلی

به‌منظور استخراج نقاط ضعف و قوت فضای صنعت بیمه و صنعت فناوری اطلاعات و ارتباطات در راستای توسعه بیمه سایبری در کشور، می‌بایست منابع و قابلیت‌های موجود را بررسی نمود:

جدول 2- قوت­ها و ضعف­ها

|  |  |  |  |
| --- | --- | --- | --- |
| **قوت‌ها** | | **ضعف‌ها** | |
| S1 | بهبود مستمر زیرساخت‌های امنیت اطلاعات | W1 | عدم انباشت مناسب داده‌های تهدیدات |
| S2 | توجه دولت به حوزه امنیت سایبری | W2 | ظرفیت کم اتکایی در خصوص ریسک‌های نوظهور |
| S3 | افزایش سرمایه‌گذاری در زیرساخت‌های امن‌سازی | W3 | کافی‌نبودن اقدامات امنیت سایبری بیمه‌گزاران |
| S4 | افزایش آگاهی از ریسک سایبری در پی انتشار برخی گزارش‌های حملات | W4 | کمبود تخصص امنیت سایبری در صنعت بیمه |
|  | | W5 | عدم وجود بیمه‌نامه استاندارد |
| W6 | عدم وجود راهکارهای ارزیابی ریسک و مدیریت خسارات |
| W7 | عدم توسعه‌بخش جرم‌یابی دیجیتال در کشور |

1. مأموریت و چشم‌انداز توسعه بیمه سایبری در کشور

با عنایت به بررسی تجربیات جهانی و تحلیل صنعت بیمه سایبری مبتنی بر حوزه‌های فعالیت شرکت‌های شاخص بین‌المللی، می‌توان چشم‌انداز توسعه بیمه‌های سایبری در کشور و حوزه‌های اصلی فعالیت در این زمینه را به شرح ذیل خلاصه نمود:

چشم‌انداز

ماموریت

**توانمندسازی سازمان‌ها و کسب‌وکارها برای تاب‌آوری و رشد در اتمسفر دیجیتال**

**افزایش انعطاف‌پذیری در برابر تهدیدات سایبری با ارائه محصولات، خدمات و راهکارهای بیمه سایبری به عنوان ابزار مدیریت ریسک سایبری در کشور**

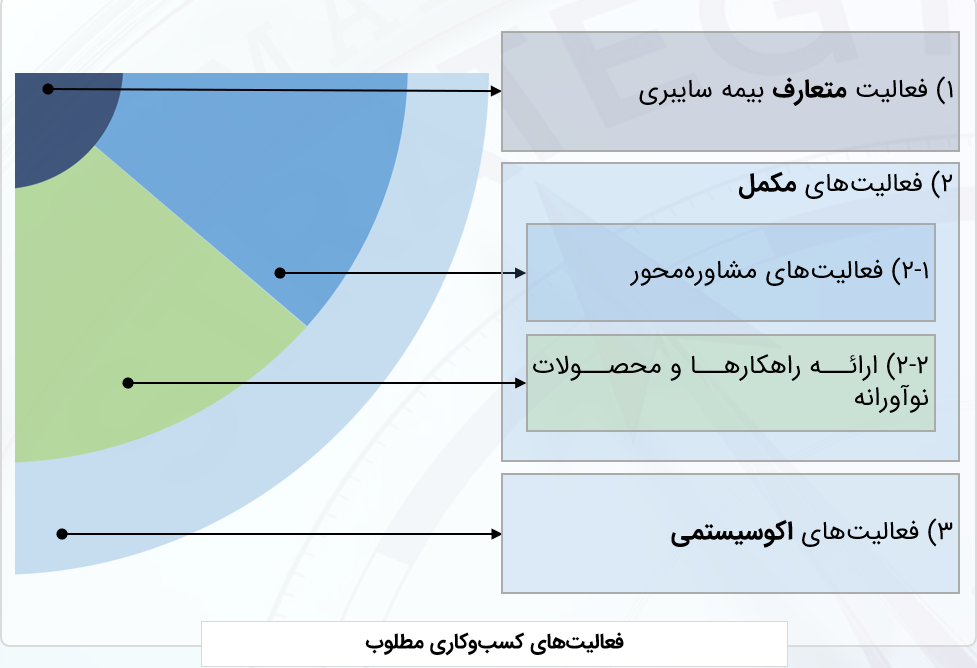
**قصد استراتژیک توسعه بیمه سایبری**

**(Cyber Insurance Strategic Intent)**

شکل 5- چشم­انداز و ماموریت بیمه سایبری

1. فعالیت‌های کسب‌وکاری مطلوب، فاکتورهای کلیدی موفقیت، نقشه قابلیت‌ها و مدل کسب‌وکار

فعالیت‌های متعارف بیمه سایبری شامل ارائه فرم پیشنهاد، ارزیابی ریسک سایبری و تعیین سطح ریسک بیمه‌گزار، تعیین شرایط بیمه‌نامه و میزان پوشش، نرخ‌گذاری ریسک، فرایند الحاقیه در حین بیمه‌نامه و فرایند مدیریت خسارات می‌گردد. از سوی دیگر، شرکت‌های بیمه می‌توانند در فعالیت‌های مکمل نیز نقش ایفا کنند؛ از جمله فعالیت‌های مشاوره محور که به حوزه مشاوره در مدیریت ریسک سایبری و کنترل سطح ریسک بیمه‌گزار، ارزیابی مستمر و به­موقع سامانه‌ها و اقدامات کاهش ریسک می­پردازد. همچنین نوع دیگری از فعالیت مکمل ارائه سامانه‌های پیش هشدار و مدیریت خسارات بر بستر هوش مصنوعی است. فعالیت‌های اکوسیستمی دسته دیگری از حوزه‌های کلیدی کسب‌وکار بیمه سایبری را به خود اختصاص می‌دهد که شامل مشارکت در زنجیره ارزش مدیریت ریسک سایبری به‌عنوان یک بازیگر مؤثر است.



شکل 6- فعالیت کسب و کارهای مطلوب

در راستای هماهنگی با نیت استراتژیک و حوزه‌های مطلوب کسب‌وکار، نیاز است تا قابلیت‌های مورد نیاز جهت اجرای استراتژی‌ها توسعه یابد. باتوجه‌به فاکتورهای کلیدی موفقیت در کسب‌وکار بیمه سایبری، این قابلیت‌ها به شرح ذیل احصا شده‌اند:

جدول 3- فاکتورهای کلیدی موفقیت

| **فاکتورهای کلیدی موفقیت** | |
| --- | --- |
| **عنوان** | **شرح** |
| **ارزیابی جامع ریسک** | ابزارها و روش‌های ارزیابی ریسک مؤثر برای ارزیابی دقیق مواجهه با ریسک سایبری مشتریان ضروری است. این امر شامل درک آسیب‌پذیری‌ها و تهدیدهای خاص صنایع مختلف است. |
| **محصولات بیمه‌ای مناسب** | ارائه راه‌حل‌های بیمه سفارشی‌شده که نیازهای منحصربه‌فرد بخش‌های مختلف، از جمله شرکت‌های کوچک و متوسط ​​ (SMEs)، شرکت‌های بزرگ، و صنایع خاص (مانند صنعت سلامت و مالی) را برآورده می‌کند. |
| **تخصص در بیمه‌گری** | ایجاد تیمی با دانش عمیق در زمینه امنیت سایبری، مدیریت ریسک و روندهای فناوری برای اتخاذ تصمیمات آگاهانه در مورد بیمه‌نامه و تعیین حق بیمه مناسب بسیار مهم است. |
| **ارتباطات و آموزش شفاف** | ارائه اطلاعات شفاف در مورد فرایندهای صدور، استثنائات بیمه‌نامه و ادعای خسارت به ایجاد اعتماد مشتریان کمک می‌کند. ابتکارات آموزشی می‌تواند آگاهی از خطرات سایبری و اهمیت بیمه را افزایش دهد. |
| **فرایند تخصصی مدیریت ادعای خسارت** | یک فرایند مدیریت خسارت کارآمد برای اطمینان از رضایت مشتری حیاتی است. زمان پاسخ سریع و پشتیبانی مؤثر در طول یک بحران می‌تواند به طور قابل‌توجهی وفاداری مشتری را افزایش دهد. |
| **مشارکت با شرکت‌های امنیت سایبری** | همکاری با کارشناسان و شرکت‌های امنیت سایبری می‌تواند ارزش خلق شده محصولات بیمه را افزایش دهد. این مشارکت‌ها می‌توانند منابع و پشتیبانی بیشتری را برای کاهش ریسک در اختیار مشتریان قرار دهند. |
| **رعایت مقررات** | به‌روز ماندن با مقررات محلی و بین‌المللی در مورد حفاظت از داده‌ها و امنیت سایبری برای اطمینان از رعایت و اجتناب از مسائل قانونی ضروری است. |
| **راهکارهای نوآورانه** | استفاده از فناوری‌های پیشرفته، مانند یادگیری ماشینی و هوش مصنوعی، می‌تواند فرایندهای ارزیابی ریسک، صدور و کشف تقلب را بهبود بخشد. |
| **آگاهی و تحقیق در مورد بازار** | تحقیقات مستمر بازار برای درک تهدیدات نوظهور، روندها و نیازهای مشتری به بیمه‌گران کمک می‌کند تا محصولات و استراتژی‌های خود را به طور مؤثر تطبیق دهند. |
| **رویکرد مشتری‌مداری** | قراردادن مشتری در مرکز توسعه محصول و ارائه خدمات تضمین می‌کند که پیشنهادها انتظارات مشتری را برآورده می‌کند و روابط طولانی‌مدت ایجاد می‌کند. |
| **سازگاری با تغییر** | چشم‌انداز سایبری به طور مداوم در حال تغییر است؛ بنابراین، بیمه‌گران باید چابک و آماده باشند تا محصولات و استراتژی‌های خود را برای مقابله با تهدیدات جدید و پویایی بازار تطبیق دهند. |

1. نقشه قابلیت­ها

نقشه قابلیت­ها در دو بخش اصلی و پشتیبان به شرح زیر است:



شکل 7- نقشه قابلیت­ها

1. مدل کسب‌وکار بیمه سایبری

مدل‌ کسب‌وکار به‌عنوان طرحی برای عملکرد موفق تجارت، شناسایی منابع‌ درآمد، مشتری‌ هدف، محصولات و جزئیات‌ تأمین‌ مالی تعریف‌ می‌شود؛ همچنین توضیح‌ می‌دهد که عوامل اصلی یک کسب‌وکار چگونه با هم منطبق می‌شوند.  در این بخش مدل کسب­وکاری بیمه سایبری بر اساس مدل CANVAS ارائه شده است.

در

نیبتن



شکل 8- مدل کسب و کار CANVAS

# نتیجه‌گیری

در این بخش، راهبردهای کلیدی برای تحقق چشم‌انداز و توسعه حوزه‌های کسب‌وکار متناسب با مسیر استراتژیک

تدوین و ارائه شده است. علاوه‌برآن، برنامه اقدامات عملیاتی متناظر با هر راهبرد نیز تدوین شده است تا مسیر اجرایی روشن و امکان‌پذیر باشد. این مجموعه از اقدامات، چهارچوبی کاربردی برای حرکت به‌سوی اهداف تعیین‌شده ارائه می‌دهد.

1. راهبردهای تحقق چشم‌انداز و توسعه حوزه‌های کسب‌وکار متناسب با مسیر استراتژیک

با استفاده از تحلیل‌های ارائه شده، اکنون می‌توان استراتژی‌های تحقق چشم‌انداز را در سه‌گام ارائه نمود. همچنین متناظر با استراتژی‌های مذکور، برنامه اقدام عملیاتی تدوین می‌گردد.



شکل 9- راهبردهای تحقق چشم­انداز

1. برنامه اقدام عملیاتی

متناظر با هر استراتژی می‌توان مجموعه‌ای از اقدامات عملیاتی موسوم به Action Plan را تعریف نمود. اقدامات تعریف شده می‌بایست در هر فاز از توسعه بیمه سایبری دارای اولویت لازم بوده و پیش‌زمینه فاز بعدی باشند.

جدول 4- اقدامات کلیدی

| اقدامات کلیدی | گام‌های کلان |
| --- | --- |
| * تحلیل بازار و شناسایی و اولویت‌بندی نیازهای صنایع مختلف از طریق نظرسنجی و مصاحبه. * تحلیل حوادث سایبری رخ‌داده در کشور و طبقه‌بندی آن‌ها از منظر صنعت، فراوانی، شدت، تهدید، آسیب‌پذیری * ایجاد شرایط عمومی بیمه سایبری و تصویب آن در شورای‌عالی بیمه * طراحی ساختار بیمه‌نامه سایبری * طراحی فرم پیشنهاد * طراحی فرایندهای بیمه‌گری سایبری و پرداخت خسارت * تدوین متن بیمه‌نامه، پوشش‌ها، استثنائات و شرایط * تهیه دستورالعمل نرخ‌گذاری * تدوین الگوی ارزیابی ریسک بیمه‌گزار * تهیه بانک اطلاعاتی ریسک سایبری در کشور * ایجاد مدیریت بیمه سایبری در شرکت‌های بیمه * طراحی سازوکار اتکایی ریسک سایبری * آموزش و آگاهی‌رسانی در خصوص ریسک‌های سایبری به بخش‌های مختلف کشور | گام اول  (۱ سال)  **ایجاد حداقل‌های لازم** |
| * ایجاد همکاری‌های هدفمند با شرکت‌های امنیت سایبری در راستای تولید نرم‌افزارهای مشاوره مدیریت ریسک سایبری، ارزیابی ریسک سایبری، مدیریت ادعای خسارت و مانیتورینگ مستمر و سیستم پیش هشدار * ایجاد سیستم‌های تجزیه‌وتحلیل داده * تربیت نیروی متخصص در حوزه جرم‌یابی دیجیتال و مسئولیت در قبال نقض داده و مالکیت معنوی | گام دوم  (۲ سال)  **توسعه راهکارهای نوین** |
| * ایجاد پلتفرم جامع بیمه سایبری جهت مشارکت اکوسیستمی همه ذی‌نفعان زنجیره ارزش انتقال ریسک سایبری * توسعه ظرفیت پذیرش اتکایی * توسعه ابزار نوین انتقال ریسک از جمله اوراق بهادار بیمه سایبری * توسعه صندوق‌های مشارکت دولتی – خصوصی | گام سوم  (۲ سال)  **بلوغ** |

# توصیه محوری (بیمه سایبری به‌مثابه پلتفرم)

با افزایش تهدیدات سایبری و درک بیشتر شرکت‌ها از اهمیت حفاظت از دارایی‌های دیجیتال خود، ایجاد پلتفرم هوشمند بیمه سایبری به‌عنوان یک منبع جامع برای ارزیابی ریسک، صدور بیمه‌نامه بر اساس نیاز و اقتضای کسب‌وکارها، قیمت‌گذاری بر اساس سطح ریسک بیمه‌گزار و شرایط بیمه‌نامه و مدیریت خسارات پیشنهاد می­شود. این پلتفرم بستری جامع را برای تمامی ذی‌نفعان زنجیره ارزش انتقال ریسک سایبری، اعم از ارزیابان ریسک، بیم سنج‌ها (اکچوئران)، بیمه‌گران مستقیم، بیمه‌گران اتکایی، ارزیابان خسارت، مؤسسات حقوقی، شرکت‌های امنیت سایبری، پژوهشکده‌ها، رگولاتور و سایر موارد فراهم می‌آورد. از طریق حضور در این پلتفرم، نه‌تنها برای خود خلق ارزش می­کنند، بلکه به ارائه خدمات بهتر و تخصصی­تر در این حوزه نوین صنعت بیمه گام برمی­دارند.

پلتفرم هوشمند بیمه سایبری یک پلتفرم جامع است که به‌منظور توسعه بیمه‌های سایبری در کشور ایجاد می‌شود. همان‌طور که پیش‌تر ذکر شد، بیمه‌ سایبری در دنیا نیز یک‌رشته جدید بیمه‌ای محسوب می‌گردد و به دلیل ماهیت کمتر شناخته شده ریسک‌های سایبری، تخصصی بودن رشته امنیت سایبری و در نتیجه ارزیابی ریسک و مدیریت خسارات آن، پیامدهای مالی بسیار گسترده در صورت بروز خسارات و عدم آگاهی افراد و کسب‌وکارها از خطرات سایبری، نیازمند تلاشی همگانی جهت توسعه در کشور است؛ تلاشی که همت گروه­های اصلی زیر را می‌طلبد.

* **متخصصین حوزه امنیت سایبری** می‌بایست با ارائه دانش خود در این حوزه به توسعه روش‌های مدیریت ریسک از منظر بیمه، ارائه استانداردهای حوزه ریسک سایبری از جمله NIST، ISO و... توسعه روش‌های ارزیابی خسارت، جرم‌یابی و پاسخ به حادثه بپردازند و مشارکتی فعال در این زمینه با همکاری مشترک شرکت‌های بیمه و دولت داشته باشند. تحلیل وضعیت مشتریان بیمه از منظر پروفایل ریسک، تعیین سطح ریسک سایبری و ارزیابی بلوغ سایبری، بینشی بسیار ضروری برای شرکت‌های بیمه و بیمه‌گزاران در مواجهه با ریسک سایبری است.
* **بازارها و نهادهای مالی** از جمله بانک، بورس و بیمه بستری جهت کمک به انتقال ریسک سایبری هستند. بیمه‌گران مستقیم و اتکایی می‌بایست با طراحی پوشش‌های بیمه‌ای متناسب با نیاز صنایع مختلف و تخصیص ظرفیت برای پذیرش ریسک سایبری، به توسعه بازار بیمه سایبری در کشور کمک نمایند. بازار سرمایه نیز می‌تواند از طریق ارائه مشتقات مالی از جمله اوراق بهادار بیمه‌ای ریسک سایبری (Cyber ILS)، بخشی از ریسک را به بازار سرمایه عرضه کند. در نهایت ارائه سرمایه به‌عنوان پشتوانه پذیرش ریسک، گامی کلیدی در رشد و توسعه بیمه سایبری محسوب می‌شود.
* **دولت** نیز در قدم‌های اولیه شکل‌گیری بازار بیمه سایبری نقشی کلیدی دارد. مطابق با بررسی‌های صورت‌گرفته، دولت می‌تواند از طریق ایجاد صندوق‌ها و برنامه‌های مشارکت دولتی - خصوصی، همچنین ایجاد بستری جهت انباشت داده‌های مرتبط با حملات سایبری در کشور (از منظر فراوانی و شدت به تفکیک صنایع مختلف) که بعضاً محرمانه تلقی می‌گردند، به قیمت‌گذاری عادلانه و تجزیه‌وتحلیل ریسک سایبری کمک نماید.

به‌منظور بررسی ساختار پلتفرم، می‌بایست بازیگران اصلی اکوسیستم بیمه سایبری شناسایی گردیده و نقش هر یک مشخص شود. همچنین باید ارزشی که برای پلتفرم خلق می‌کنند و مزایایی که از کار تعاملی به دست می‌آورند به‌درستی تبیین گردد:

جدول 5- بازیگران اصلی اکوسیستم بیمه سایبری شناسایی

| بازیگر | بخش | خلق ارزش | مزایا |
| --- | --- | --- | --- |
| شرکت‌های امنیت سایبری | **ارزیابی ریسک** | * ارزیابی ریسک و تعیین پروفایل ریسک برای بیمه‌گزاران * استانداردسازی فرایندهای ارزیابی ریسک بر اساس استانداردهای داخلی (پدافند غیرعامل) و خارجی (NIST و ISO) * تهیه گزارش‌های ارزیابی ریسک برای بیمه‌گزاران بزرگ * ارائه توصیه‌ها و پیشنهادهای مرتبط با پروفایل ریسک سایبری هر بیمه‌گزار و کمک به ارتقا و بهبود وضعیت بهداشت سایبری آن‌ها * ارائه زیرساخت‌های لازم (نرم‌افزاری/سخت‌افزاری) جهت امن‌سازی دارایی‌های دیجیتال بیمه‌گزار ارزیابی بلوغ سایبری بیمه‌گزار و میزان انطباق با معیارهای استاندارد بلوغ سایبری | * دسترسی به دیتای جامع از بیمه‌گزاران و استفاده از مزیت کلان‌داده در ارائه نتایج بهتر ارزیابی ریسک * حضور در پلتفرمی جامع و همکاری با متخصصین سایبری دیگر * استفاده از بازاری جدید برای ارائه خدمات |
| **صدور بیمه‌نامه** | * ارائه ریسک پروفایل بیمه‌گزار جهت اعمال در فرایند بیمه‌گری * ارائه تجزیه‌وتحلیل‌های مبتنی بر داده‌های حملات سایبری در صنایع مختلف جهت پیش‌بینی روندها |
| **پس از صدور بیمه‌نامه** | * مانیتورکردن real-time بیمه‌گزار از منظر بررسی وضعیت ایمن بودن سیستم‌ها (ارائه فیدبک به بیمه‌گران) و از منظر بررسی حملات احتمالی (فیدبک به بیمه‌گر و بیمه‌گزار) * ارائه خدمات آموزشی و آگاهی‌بخشی در خصوص ریسک سایبری و نحوه مواجهه با آن |
| **مدیریت خسارات** | * ارائه خدمات جرم‌یابی دیجیتال * ارائه برنامه پاسخ به حادثه * ارائه برنامه تداوم کسب‌وکار |
| **اتکایی** | * بررسی تجمیع ریسک هر شرکت بیمه * بررسی ریسک سیستمی در صنایع مختلف و ارائه گزارش به بیمه‌گران |
| شرکت‌های بیمه | **صدور بیمه‌نامه** | * ارائه پوشش‌های متنوع متناسب با نیاز هر شرکت و هر صنعت در دو بخش شخص اول و شخص ثالث * استفاده از بینش‌های ارائه شده جهت تعدیل شرایط بیمه‌نامه و حق بیمه * استفاده از داده‌های ارائه شده جهت اعمال ابزار هوش مصنوعی | * استفاده از تخصص و خدمات سایر ذی‌نفعان در ارائه پوشش بهتر * مشارکت در بازاری جدید جهت افزایش سودآوری * همکاری نزدیک با ارائه‌دهندگان ظرفیت جهت واگذاری به شرکت‌های اتکایی * خودکارسازی فرایندهای اصلی و پشتیبان بیمه‌گری در این حوزه |
| **پس از صدور بیمه‌نامه** | * ارائه مشوق‌های گوناگون به بیمه‌گزاران دارای وضعیت مناسب ریسک سایبری |
| **مدیریت خسارات** | * ارائه خطوط تلفن 24/7 جهت برقراری ارتباط با زیان‌دیدگان * استفاده از خدمات تخصصی شرکت‌های جرم‌یابی جهت مدیریت خسارات بیمه‌گزاران و افزایش شفافیت و رضایت مشتریان |
| **اتکایی** | * ایجاد کنسرسیومی از بیمه‌گران مستقیم / اتکایی جهت واگذاری اتوماتیک ریسک‌های سایبری متناسب با اشتهای ریسک ارائه شده توسط شرکت‌ها |
| بیمه‌گران اتکایی | **ارزیابی ریسک** | * کمک به ارزیابی ریسک از طریق ارائه بینش‌های موجود در بانک اطلاعاتی | * دسترسی به صندوق بزرگی از ریسک که متنوع‌سازی را برای پرتفوی بیمه‌گران اتکایی به ارمغان می‌آورد. * استفاده از پلتفرم این امکان را برای بیمه‌گران اتکایی به ارمغان می‌آورد که به‌صورت یکپارچه در بازار بیمه سایبری مشارکت داشته باشند. * مدل‌سازی ریسک‌ها با رویکرد مشارکتی از مزایای این پلتفرم برای بیمه‌گران اتکایی است. |
| **صدور بیمه‌نامه** | * کمک به ارائه نرخ و شرایط بیمه‌نامه بر اساس ریسک فاکتورهای بیمه سایبری از جمله درآمد سالانه، صنعت، سوابق خسارت، پوشش مورد نیاز، حد تعهد، وضعیت اقدامات سایبری و... |
| **پس از صدور بیمه‌نامه** | * کمک به محاسبه تجمیع ریسک سایبری * ارائه مدل‌های حوادث فاجعه‌آمیز سایبری |
| **مدیریت خسارات** | * کمک به بیمه‌گر در مدیریت خسارات |
| **اتکایی** | * ارائه ظرفیت جهت پوشش ریسک‌های سایبری * راهبری کنسرسیوم‌های داخلی و مشارکت با سایر بیمه‌گران اتکایی * ایجاد ابزار انتقال ریسک به بازار سرمایه از طریق ILS و CAT Bond |
| ارزیابان خسارت | **مدیریت خسارات** | * ارائه روش‌های نوین جرم‌یابی دیجیتال، با کمک شرکت‌های امنیت سایبری * استفاده از متدهای محاسبه وقفه در کسب‌وکار | * استفاده از افزایش کارایی و شفافیت * دسترسی به مؤسسات امنیت سایبری و جرم‌یابی * ارائه خدمات به بازار جدید |
| بیم سنج­ها و شرکت‌های مشاوره ریسک | **همه بخش‌ها** | * ارائه مدل‌های ارزیابی ریسک مبتنی بر هوش مصنوعی و یادگیری ماشین * مدل‌سازی حوادث سایبری در هر دو زمینه ریسک و خسارت * ارائه روش‌های مبتنی بر داده در محاسبه حق بیمه * طراحی ابزار نوین انتقال ریسک سایبری * ایجاد روش‌های ذخیره‌گیری | * استفاده از داده‌های جمع‌آوری شده * دسترسی به مؤسسات امنیت سایبری * ارائه خدمات به بازار جدید |
| مؤسسات حقوقی | **صدور بیمه‌نامه** | * کمک به ایجاد شرایط و وردینگ بیمه‌نامه از منظر حقوقی * کمک به ایجاد آیین‌نامه‌ها و قوانین مرتبط با ریسک سایبری (از جمله شرایط عمومی) | * استفاده از بازار جدید جهت کسب درآمد * تعامل با سایر ذی‌نفعان جهت توسعه دانش ریسک سایبری در هر دو جنبه بیمه و اقتصاد دیجیتال و مسائل حقوقی مربوطه |
| **مدیریت خسارات** | * کمک به ارزیابی خسارت دررابطه‌با حوادث مرتبط با پوشش‌های مسئولیت |
| نهادهای دولتی و رگولاتور | **ارزیابی ریسک** | * ارائه داده‌های مورد نیاز ارزیابی ریسک دقیق‌تر * تهیه بانک‌های اطلاعاتی از حوادث سایبری | * استفاده از هم‌افزایی دانش و تخصص در تعاملات پلتفرم * کمک به درکی عمیق از روندهای حوزه سایبری و بهبود پایداری سایبری صنایع کشور |
| **صدور بیمه‌نامه** | * تسهیل روند قانون‌گذاری و کمک به توسعه بیمه‌نامه‌های سایبری |
| **اتکایی** | * کمک به ارائه ظرفیت پذیرش ریسک از طریق مشارکت‌های دولتی - خصوصی |
| شرکت‌های فناور بیمه‌ای (اینشورتک) | **همه بخش‌ها** | * شرکت‌های فناور بیمه‌ای در این مدل پلتفرمی به‌عنوان ایجادکنندگان پلتفرم شناخته می‌شوند و وظیفة طراحی و اجرای پلتفرم و پشتیبانی از آن را برعهده دارند | * استفاده از بازار جدید جهت کسب درآمد |

# مراجع

1. A. Tsohou, V. Diamantopoulou, S. Gritzalis, C. Lambrinoudakis, Cyber insurance: state of the art, trends and future directions, 2023.
2. Marsh Commercial, A history of cyber insurance, 2021.
3. Cyber insurance: strengthening resilience for the digital transformation, Swiss Re Institute, November 2022.
4. Allianz Risk Barometer 2022, Allianz Global Corporate & Specialty, January 2022.
5. Z. Smith, E. Lostri, The Hidden Costs of Cybercrime, McAfee, December 2020.
6. Global Cybersecurity Outlook 2022, World Economic Forum, January 2022.
7. Cyber claims study 2021 Report, NetDiligence, 2024.
8. NAIC cyber insurance supplement, 2022.
9. C. Biener, M. Eling, J.H Wirfs, Insurability of Cyber Risk – An Empirical Analysis, University of St. Gallen, 2015.
10. 2023 was a big year for cybercrime – here’s how we can make our systems safer, WEF, 2024.
11. A. Chase, The Evolution of Cyber Risk and the Cyber Insurance Market, 2021.
12. Understanding and Addressing Global Insurance Protection Gaps, The Geneva Association, April 2018.
13. Statista, Estimated Cost of Cybercrime Worldwide 2018-2029, 2024.

# ضمیمه (مصادیقی از حملات سایبری)

| حملات سایبری منتخب در صنایع مختلف | | | |
| --- | --- | --- | --- |
| صنعت | نام حمله | شرح | پیامدها |
| نفت و گاز | **حمله به خط**  **لوله کولونیال** | حمله به خط لوله کولونیال، بزرگ‌ترین حمله سایبری موفق به یک هدف زیرساخت نفتی در تاریخ ایالات متحده بود. خط لوله کولونیال، بزرگ‌ترین سیستم توزیع فراورده‌های نفتی تصفیه شده کشور آمریکا است و حدود 45 درصد از کل سوخت مصرفی در ساحل شرقی را تأمین می‌کند. در 7 می‌2021، حمله باج‌افزاری شرکت را مجبور کرد تا زمانی که باج را پرداخت کند، تمام عملیات را متوقف نماید. این شرکت، هشت روز بعد از حمله، عملیات خود را بازسازی کرد. این تعطیلی باعث ایجاد وحشت، کمبود سوخت، افزایش قیمت و اختلالات اقتصادی گسترده شد. به‌عنوان‌مثال، در جورجیا و کارولینای جنوبی، قیمت بنزین معمولی 8 درصد افزایش یافت. | از نظر ژئوپلیتیکی، این حمله اهمیت نظارت بر امنیت سایبری سیستم‌های انرژی حیاتی کشور را برای ایالات متحده، بالا برد. از نظر مالی، این شرکت 4 / 4 میلیون دلار باج پرداخت کرد (که 3 / 2 میلیون دلار توسط وزارت دادگستری ایالات متحده بازیابی شد. همچنین در این حمله، بخشی از کشور دچار وقفه در کسب‌وکار و افشای اطلاعات شد. |
| سلامت،  انرژی،  چندگانه | **WannaCry** | حمله سایبری باج‌افزاری WannaCry در ماه می‌2017 رخ داد و با رمزگذاری داده‌ها تا زمانی که باج پرداخت شود، نقاط آسیب‌پذیر سیستم عامل ویندوز را هدف قرار داد. برآورد شده که این حمله بیش از 230،000 رایانه را در سراسر جهان آلوده کرده و خسارتی بالغ بر میلیاردها دلار در حوزه عمومی‌و خصوصی ایجاد نموده است. این حمله همچنین خدمات سلامت ملی بریتانیا NHS را به دلیل قدیمی‌بودن سیستم‌های رایانه ای تحت تأثیر قرار داد و منجر به از کار افتادن یا از دسترس خارج کردن تجهیزات و سیستم‌های بهداشتی حیاتی شد. | این حمله، عملکرد خدمات سلامت ملی بریتانیا را به خطر انداخت. وزارت بهداشت و مراقبت‌های اجتماعی تخمین زده که این حمله 92 میلیون پوند برای خدمات سلامت ملی بریتانیا هزینه داشته است که شامل 20 میلیون پوند خسارت به دلیل اختلال در خدمات و 72 میلیون پوند برای هزینه‌های مستقیم فناوری اطلاعات بوده است. |
| حمل‌ونقل،  انرژی،  زنجیره  تأمین | **NotPetya** | در ژوئن 2017 ، نسخه بدافزار NotPetya با سوء استفاده از آسیب‌پذیری‌های مشابه WannaCry در اوکراین شروع به کار کرد و سازمان‌هایی ازجمله دولت، بانک‌ها، شرکت‌های برق دولتی و سیستم‌های کلیدی حمل ونقل عمومی‌(فرودگاه، مترو) و حتی سیستم نظارت بر تشعشعات در چرنوبیل را تحت تأثیر قرار داد. نهادهای آلوده به ویروس شامل شعبه‌های محلی گروه‌های بین المللی مرتبط با شبکه‌های زنجیره تأمین جهانی مانند FedEx یا Maersk بودند. | شبکه زنجیره تأمین در سراسر صنایع و مرزهای متعدد مختل شد. خسارت شرکت‌های پایین‌دستی 3 / 7 میلیارد دلار تخمین زده می‌شود که چهار برابر بیشتر ازخسارت شرکت‌هایی است که به طور مستقیم آسیب دیده اند. |
| غذا | **حمله JBS** | در ماه می‌2021 ، بزرگ‌ترین شرکت فراوری گوشت JBS مستقر در برزیل به دلیل حمله باج‌افزاری مجبور به توقف فعالیتهای خود شد. این شرکت عملیات پرورش گوشت گاو و طیور خود را در چندین مکان در آمریکای شمالی و استرالیا به مدت 3 تا 4 روز متوقف کرد. در نهایت، این حمله با پرداخت 11 میلیون دلار باج به پایان یافت | این حمله کل زنجیره تأمین گوشت را تهدید کرد و مصرف‌کنندگان با ریسک‌های کمبود عرضه و افزایش قیمت گوشت مواجه شدند. |
| آب | **هک سیستم آب**  **تامپا** | در فوریه 2021 ، هک سیستم آب تامپا در فلوریدا رخ داد که در آن هکرها به سیستم کامپیوتری یک مرکز تصفیه آب که15000 نفر را تأمین می‌کرد نفوذ کرده و سعی کردند منبع آب شهر را مسموم کنند | این حمله، نگرانی افراد در مورد کمبود دانش در صنعت امنیت سایبری و مشکلاتی که شهرهای کوچک‌تر در تأمین منابع کارکنان امنیت سایبری و حفظ بهداشت سایبری به‌روز دارند را افزایش داد |
| نفت و گاز | **حمله ARA** | در بحبوحه بحران انرژی قاره‌ای، یک حمله سایبری به ‌هاب‌های پالایش نفت آمستردام - روتردام - آنتورپ (ARA) در فوریه 2022 عملیات پایانی نفتی را مختل کرد. چندین شرکت گزارش دادند که قربانی یک حمله باج‌افزاری شده‌اند که بر سیستم‌های فناوری اطلاعات آن‌ها تأثیر گذاشته و درنتیجه عملیات بنادر (عمدتاً خودکار) را مختل کرده و باعث تغییر مسیر تانکرها شده است. | علاوه بر ریسک اختلال در عرضه انرژی، چنین حملاتی همچنین مانع از اجرای درست قراردادهای تأمین انرژی توسط شرکت‌ها شده و منجر به رخداد مسئولیت‌های قانونی برای آن‌ها می‌شود. |
| زنجیره  تأمین،  چندگانه | **هک**  **SolarWind** | در سال 2020 ، هکرها یک کد مخرب را به سیستم نرم‌افزاری SolarWind وارد کردند. این بدافزار از طریق بروزرسانی‌های معمول سیستم به بیش از 30000 مشتری سرایت کرد و هکرها را قادر ساخت تا به سیستم‌های فناوری اطلاعات هزاران شرکت و سازمان ازجمله سازمان‌های دولتی حساس ایالات متحده نفوذ کنند و از آن‌ها جاسوسی نمایند این حمله سایبری یک افشای اطلاعات پیشرفته در زنجیره تأمین است که در یک دوره 7 ماهه رخ داده است. | این حمله باعث افزایش آگاهی در مورد آسیب‌پذیری سایبری زنجیره‌های تأمین ازطریق تأمین‌کنندگان شخص ثالث شد. |
| آلومینیوم | **Norsk Hydro** | در سال 2019، Norsk Hydro تولیدکننده آلومینیوم مستقر در نروژ در میان بزرگ‌ترین تولیدکنندگان صنعت جهان با کارخانه‌هایی در 40 کشور در معرض یک حمله باج‌افزاری عظیم قرار گرفت که کل سازمان را تحت تأثیر قرار داد. این حمله، نتیجه یک ایمیل آلوده بود که شرکت را مجبور کرد به عملیات دستی خود برگردد تا سیستم‌های کنترل صنعتی خود را بسیار کندتر از زمان عادی مدیریت کند. | سالی که حمله رخ داد، Norsk Hydro هزینه کل حمله سایبری را حدود 650 تا750 میلیون کرون (تقریباً 65 تا 75 میلیون دلار) تخمین زد. |
| شبکه‌های برق | **هک شبکه**  **برق اوکراین** | در دسامبر 2015 ، شبکه برق اوکراین هک شد که منجر به قطع برق بیش از 200000 مصرف کننده در اوکراین برای چند ساعت شد. | حملات سایبری جدید ریسک حوادث ژئوپلیتیکی را افزایش می‌دهند. |



1. McAfee [↑](#footnote-ref-1)
2. World Economic Forum [↑](#footnote-ref-2)
3. Statista [↑](#footnote-ref-3)