پژوهشکده بیمه

مطالعه و بررسی مقدماتی تجربیات سایر کشورها در حوزه ریسک‌ها و بیمه‌های سایبری

ارائه‌دهنده:

دکتر اسماء حمزه، عضو هیئت علمی و مدیرگروه پژوهشی فناوری‌های نوین پژوهشکده بیمه


بسم الله الرحمن الرحيم

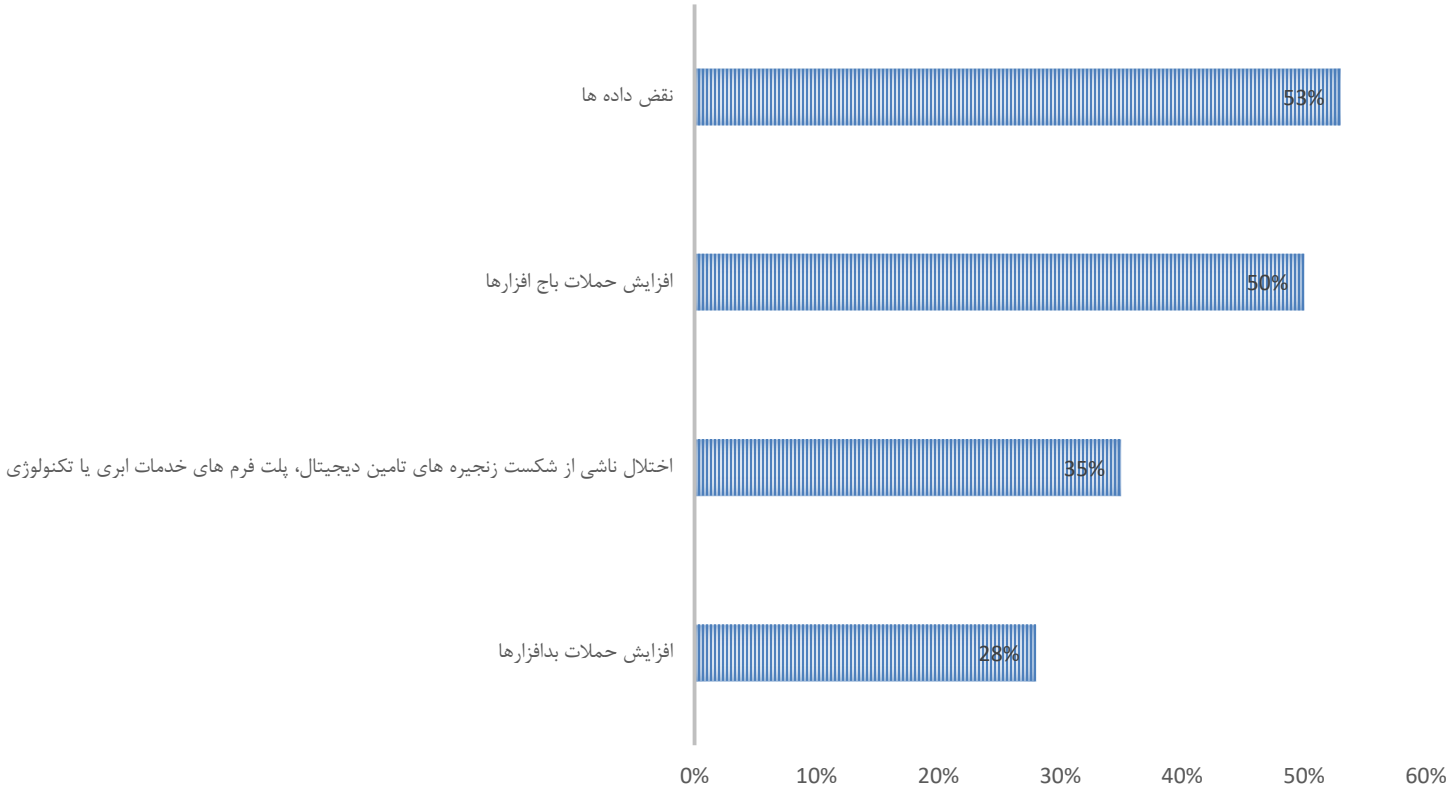
آماری از ریسک سایبری در جهان و ایران

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 به عنوان مهمترین ریسک کسب‌وکارها در سال ۲۰۲۳** معرفی شده است. جرایم سایبری **بیش از یک تریلیون دلار** در سال برای اقتصاد جهانی هزینه دارد.

آماری از ریسک سایبری در جهان و ایران

مهم‌ترین نگرانی شرکت‌ها در خصوص ریسک‌های سایبری



آماری از ریسک سایبری در جهان و ایران

موسسه پونمون که در خصوص استفاده مسئولانه از اطلاعات و شیوه‌های مدیریت حریم خصوصی در کسب‌وکارها و دولت‌ها تحقیق و مطالعه انجام می‌دهد و در این زمینه راهکارهای لازم را بهبود می‌بخشد، هر ساله گزارشی از هزینه درز اطلاعات سایبری و دیجیتالی تحت حمایت شرکت بین‌المللی دستگاه‌های کسب‌وکار (IBM) نیز تهیه و منتشر می‌کند. منطبق بر آخرین گزارش این شرکت با عنوان "گزارش هزینه نقض اطلاعات ۲۰۲۲"، **۸۳ درصد شرکت‌های مورد مطالعه با بیش از یک حادثه نقض اطلاعات در سال مواجه شده‌اند**.

آماری از ریسک سایبری در جهان و ایران

"راهنمای تشخیص هوشمند تهدیدات ایکس-فورس" عنوان گزارش سالانه‌ای است که IBM در مورد تازه‌ترین تهدیدها و روندهای سایبری، مبتنی بر آخرین آمار منتشر می‌کند. بر اساس آخرین گزارش منتشر شده موسسه مذکور در سال ۲۰۲۳ سهم حملات سایبری به تفکیک صنایع مختلف به شرح جدول ذیل بوده است:

آماری از ریسک سایبری در جهان و ایران

سهم حملات سایبری به تفکیک صنایع

صنعت	۲۰۲۲	۲۰۲۱	۲۰۲۰	۲۰۱۹	۲۰۱۸
تولید	۲۴.۸	۲۳.۲	۱۷.۷	۸	۱۰
مالی و بیمه	۱۸.۹	۲۲.۴	۲۳	۱۷	۱۹
خدمات حرفه‌ای، تجاری و مصرف کننده	۱۴.۶	۱۲.۷	۸.۷	۱۰	۱۲
انرژی	۱۰.۷	۸.۲	۱۱.۱	۶	۶
خرده‌فروشی و عمده-فروشی	۸.۷	۷.۳	۱۰.۲	۱۶	۱۱
آموزش	۷.۳	۲.۸	۴	۸	۶
بهداشت و درمان	۵.۸	۵.۱	۶.۶	۳	۶
دولت	۴.۸	۲.۸	۷.۹	۸	۸
حمل و نقل	۳.۹	۴	۵.۱	۱۳	۱۳
رسانه و مخابرات	۰.۵	۲.۵	۵.۷	۱۰	۸

آماری از ریسک سایبری در جهان و ایران

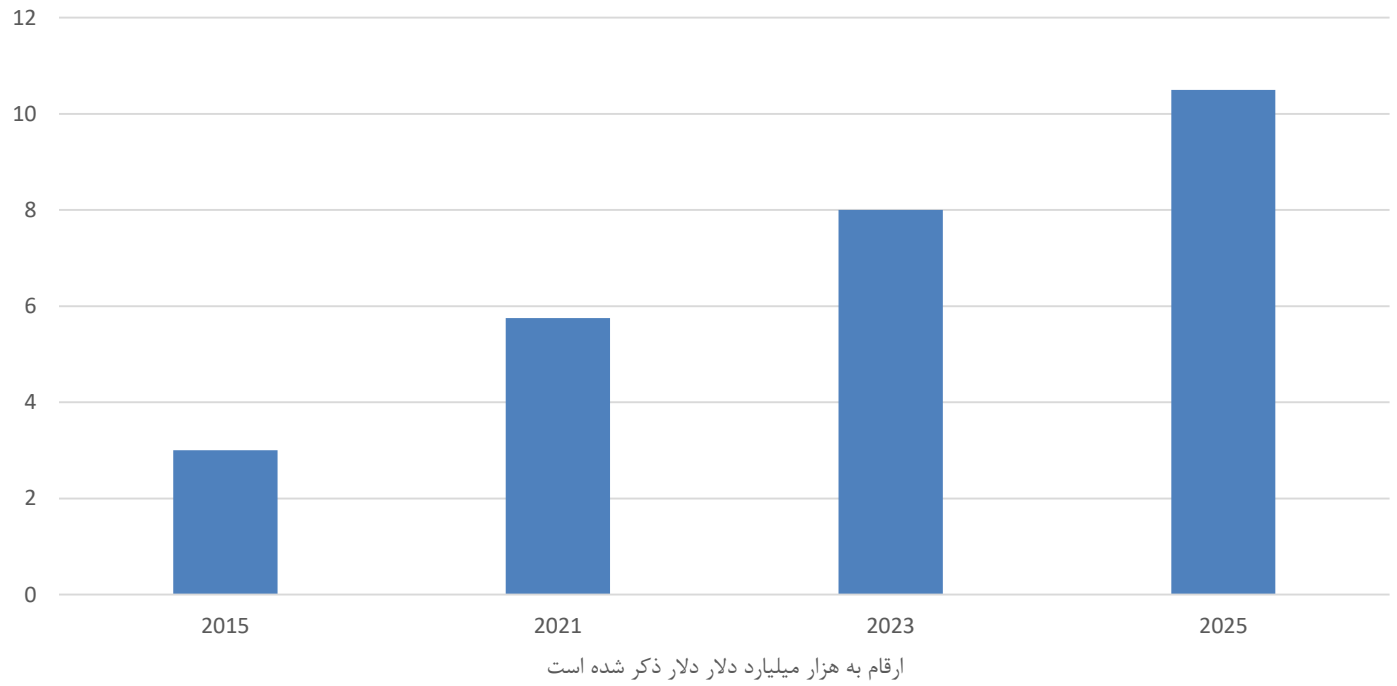
طبق داده‌های این گزارش، بخش تولید برای دومین سال متوالی بیشترین حمله را نسبت به سایر صنایع دیگر تجربه کرده است. قبل از سال ۲۰۲۱ **بخش مالی و بیمه**، پنج سال متوالی رکورددار بیشترین حملات سایبری بوده است.

آماری از ریسک سایبری در جهان و ایران

شرکت سایبرسکوریتی ونچرز گزارش‌های سالانه و فصلی در مورد موضوعاتی چون هزینه‌های جرایم سایبری، اندازه بازار امنیت سایبری و پیش‌بینی هزینه‌ها و به طور کلی تحقیقات و تجزیه‌وتحلیل‌هایی در مورد بازار جهانی امنیت سایبری منتشر می‌کند. طبق آخرین گزارش این شرکت در مورد جرایم سایبری هزینه سالانه جهانی جرایم سایبری **در سال ۲۰۲۳ به ۸ تریلیون دلار در سال** رسیده است. هزینه‌های جرایم سایبری شامل آسیب و تخریب داده‌ها، پول‌های دزدیده شده، بهره‌وری از دست رفته، 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.**

آماری از ریسک سایبری در جهان و ایران

پیش‌بینی هزینه‌های جرایم سایبری



ارقام به هزار میلیارد دلار دلار ذکر شده است

آماری از ریسک سایبری در جهان و ایران

در کنفرانس سایبر در سال ۲۰۲۱ در چتم هاوس، لندی کامرون، مدیر اجرایی مرکز امنیت ملی سایبری بریتانیا، بیان کرده است که حملات باج‌افزارها مهمترین و فوری‌ترین تهدید برای همه کشورها هستند. پیش‌بینی می‌شود هزینه خسارات باج افزارها از ۳۲۵ میلیون دلار در سال ۲۰۱۵ به ۲۶۵ میلیارد دلار در سال ۲۰۳۱ برسد.

آماری از ریسک سایبری در جهان و ایران

علاوه‌براین موارد، همزمان با رشد روزافزون استفاده از سیستم‌های خدمات مالی غیرمتمرکز، جرایم مرتبط با رمز ارزها نیز رشد پیدا کرده است. سایبرسکوریتی ونچرز پیش‌بینی کرده است که این جرایم **۳۰ میلیارد دلار در سال ۲۰۲۵** برای جهان هزینه خواهد داشت. این رقم تقریبا دو برابر هزینه‌ای است که این جرایم در سال ۲۰۲۱ (تقریبا ۱۷.۵ میلیارد دلار) داشته است.

آماری از ریسک سایبری در جهان و ایران

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

آماری از ریسک سایبری در جهان و ایران

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 اجرایی شدن طرح رمز دوم یکبار مصرف در سال ۱۳۹۸ و گسترش آگاهی بخشی پلیس فتا، از میزان شیب صعودی آمار مرتبط با کلاهبرداری از طریق دسترسی غیرمجاز به حساب 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.

آماری از ریسک سایبری در جهان و ایران

وفق اظهارنظر کارشناسان مربوطه، حملات فیشینگ یا مهندسی اجتماعی که سهم حدود ۵۷ درصدی از حملات سایبری در جهان را دارد، در کشورمان سهم حدود ۶۵ الی ۷۰ درصدی را به خود اختصاص داده است. همچنین هزینه حملات در ایران، دو برابر عربستان و چهار برابر امارات برآورد می‌گردد. در شرایط کنونی، دفع حملات DOS به آسانی صورت می‌گیرد، لیکن حملات DDOS همچنان وجود دارد. لازم به ذکر است که با شکل‌گیری شرکت‌های فعال در حوزه امنیت سایبری و خدمات ارائه شده توسط آن‌ها، وضعیت آمادگی جهت مقابله با حملات و مدیریت ریسک مذکور نسبت به دهه قبل بهتر شده است.

آماری از ریسک سایبری در جهان و ایران

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:

آماری از ریسک سایبری در جهان و ایران

- 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؛

آماری از ریسک سایبری در جهان و ایران

- فقدان تعاملات مؤثر با مراکز و آزمایشگاه‌های بین‌المللی در خصوص ویروس‌ها، تروجان‌ها، باج‌افزارها و ... و در نتیجه عدم دریافت بازخوردهای به‌هنگام؛
- فراگیر بودن استفاده از ابزارهای VPN؛
- ناترازی درآمد-هزینه بنگاه‌ها و به صرفه نبودن سرمایه‌گذاری در ظرفیت‌های امنیت سایبری؛
- اطاله زمانی در پروسه‌های آزمایشگاهی؛
- دور زدن الزامات قانونی توسط پیمانکاران.

تعریف ریسک سایبری

- **سایبر** مخفف واژه سایبرنتیک واژه‌ای است برگرفته از لغت یونانی kybernetes به معنای حاکمیت و یا حکومت. عموما واژه "سایبر" به اختصار به جای واژه "فضای سایبری" به کار می‌رود.

- نخستین کسی که واژه‌ی فضای سایبری را به کار برد ویلیام گیبسون نویسنده‌ی داستان‌های علمی-تخیلی در کتاب نورومنسر بود.

- **فضای سایبری**، دامنه‌ای جهانی، درون محیط اطلاعاتی که در بردارنده شبکه به هم متصل زیرساختاری سیستم اطلاعاتی است که خود شامل اینترنت، شبکه‌های ارتباط راه دور، سیستم‌های رایانه‌ای و کنترل‌گرها و پردازشگرهای آن است.

- این فضا محیطی است مجازی و غیرملموس که در فضای شبکه‌های مختلف که از طریق اینترنت به هم وصل می‌شوند، وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد، ملت، فرهنگ‌ها،کشورها، به صورت ملموس و فیزیکی مانند نوشته، تصویر، صوت و اسناد در یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل استفاده و در دسترس استفاده‌کنندگان و کاربران می‌باشد.

تعریف ریسک سایبری

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.

تعریف ریسک سایبری

رویداد سایبری

رویداد سایبری طیف گسترده‌ای از فعالیت‌ها، از جمله رویدادهای بی‌خطر و مخرب را در بر می‌گیرد. رویدادهای سایبری می‌توانند شامل فعالیت‌های معمولی مانند به‌روزرسانی نرم‌افزار، تعمیر و نگهداری سیستم، یا نوسانات ترافیک شبکه و همچنین فعالیت‌های غیرعادی یا مخرب مانند حملات سایبری باشند.

تعریف ریسک سایبری

حملات سایبری

حملات سایبری در واقع زیرمجموعه ای از رویدادهای سایبری می‌باشند و به طور خاص به یک اقدام عمدی و مخرب انجام شده برای تخریب، سرقت، مختل کردن، یا آسیب رساندن به سیستم‌های اطلاعاتی، شبکه‌های رایانه‌ای یا دارایی‌های دیجیتال و همچنین هرگونه تلاش برای افشا، تغییر، غیرفعال کردن، تخریب، سرقت یا دستیابی به دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی تعریف می‌شود. حمله سایبری هر نوع مانور تهاجمی است که سامانه‌های اطلاعات رایانه‌ای، زیرساخت‌ها، شبکه‌های رایانه‌ای یا دستگاه‌های رایانه شخصی را هدف قرار می‌دهد. مهاجم یک شخص یا فرایندی است که سعی در دسترسی به داده‌ها، کارکردها یا سایر مناطق محدود سامانه، بدون مجوز، به طور بالقوه با قصد مخرب دارد.

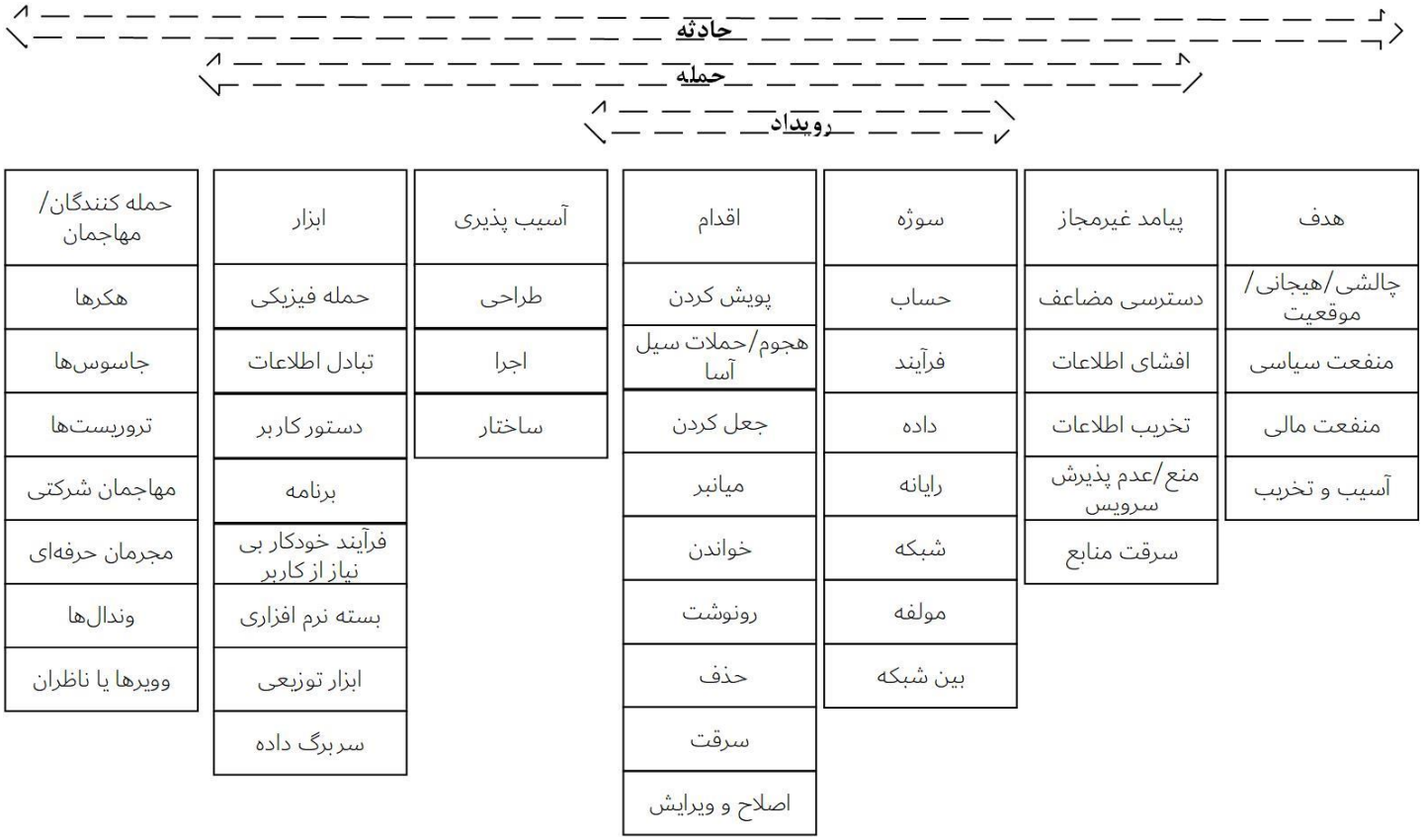
تعریف ریسک سایبری

حادثه سایبری

گروهی از حملات که به دلیل متمایز بودن مهاجمان، اهداف، سایت‌ها و زمان‌بندی از سایر حملات قابل‌تشخیص هستند را حادثه می‌نامند. یک حادثه سه جزء اصلی دارد که شامل مهاجمان/حمله‌کنندگان، حملات و اهداف می‌شود. سازوکار حادثه بیانگر آن است که یک مهاجم یا گروهی از مهاجمان با انجام حملات به اهداف خود می‌رسند. یک حادثه ممکن است از یک حمله منحصربه‌فرد یا چندین حمله تشکیل شده باشد.

تعریف ریسک سایبری

رویداد، حادثه و حملات در ادبیات شبکه و سایبر



تعریف ریسک سایبری

ریسک سایبری

تعریف‌های متعددی از ریسک سایبری ارائه شده است.

در جدول تعاریف ریسک سایبری به طور مختصر آورده شده است:

تعریف ریسک سایبری

نام موسسه	تعریف
انجمن ژنو	هر ریسکی که ناشی از استفاده از فناوری‌های اطلاعاتی و ارتباطی که محرمانه بودن، در دسترس بودن یا یکپارچگی داده‌ها یا سرویس‌ها را به خطر می‌اندازد.
موسسه ملی استانداردها و تکنولوژی	(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 بر یا درون اطلاعات و فناوری. ریسک‌های امنیت سایبری به از دست دادن محرمانگی، یکپارچگی یا در دسترس بودن اطلاعات، داده‌ها یا سیستم‌های اطلاعاتی (یا کنترلی) مربوط می‌شود و منعکس‌کننده اثرات نامطلوب بالقوه بر عملیات سازمانی (مثل ماموریت، عملکرد، تصویر یا شهرت) و دارایی‌ها، افراد، سایر سازمان‌ها و کشور می‌باشد.

تعریف ریسک سایبری

انجمن مدیران ارشد ریسک (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 سوء استفاده از داده‌ها، هرگونه مسئولیت ناشی از استفاده، ذخیره‌سازی و انتقال داده‌ها، در دسترس بودن، یکپارچگی و محرمانه بودن اطلاعات الکترونیکی مربوط به افراد، شرکت‌ها یا دولت‌ها
سازمان بین‌المللی استانداردسازی	خطر ناشی از تهدیدی که از فضای سایبری سوء استفاده می‌کند (فضای سایبری محیط دیجیتال به هم‌پیوسته از شبکه‌ها، سرویس‌ها، سیستم‌ها و فرآیندها است)
موسسه مدیریت ریسک	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.

تعریف ریسک سایبری

بانک تسویه‌حساب‌های بین‌المللی (۲۰۱۹)	ترکیبی از احتمال وقوع یک رویداد در قلمرو دارایی‌های اطلاعاتی یک سازمان، رایانه و منابع ارتباطی و پیامدهای آن رویداد برای یک سازمان.
Eling و Schnell (2016)	ریسک سایبری شامل هرگونه ریسک ناشی از استفاده از فناوری اطلاعات و ارتباطات (ICT) است که محرمانگی، در دسترس بودن 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 به عنوان 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 آنلاین، مانند ذخیره داده‌های شخصی در اینترنت یا انجام تراکنش‌های آنلاین که ممکن است منجر به آسیب مالی، شهرت، اختلال در زندگی یا کسب‌وکار شود را پوشش می‌دهد.

تعریف ریسک سایبری

با توجه به جدول مذکور می‌توان تعریف زیر را به عنوان تعریفی جامع از ریسک سایبری که تمام مولفه‌های 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 بالقوه‌ی ناشی از آن که محرمانگی، در دسترس بودن یا یکپارچگی داده‌ها را به خطر می‌اندازد»

دسته‌بندی انواع حوادث سایبری

در گزارشی از انجمن مدیران ارشد ریسک CRO (۲۰۱۶) حوادث سایبری مطابق جدول زیر تقسیم‌بندی شده‌اند:

گروه حادثه	نوع حادثه	شرح
اشکال در عملکرد سیستم/ مسئله	عملکرد بد سیستم شخص اول	سیستم خود فرد یا یک شرکت، خطاهای سیستمی پیوسته ایجاد می‌کند یا به‌طور کامل متوقف می‌شود. در این حالت سیستم از کار می‌افتد.
	تحت تاثیر بد افزار قرارگرفتن سیستم شخص اول	کنترل‌های داخلی (انسانی یا سیستمی) یا کاربران، یک بدافزار را در پشته‌های خود و یا یک رفتار غیرعادی را در سیستم‌ها و نرم-افزارهای نصب شده شناسایی می‌کنند. نفوذ محتمل (یا مشکوک) است.
	نقص ارتباطات شبکه	سیستم شخص یا شرکت دیگر قادر به تبادل اطلاعات از طریق اینترنت یا سایر شبکه‌های دیجیتال نمی‌باشد یا اتصال به اندازه‌ای کند است که غیر قابل استفاده می‌شود.
	اختلال غیرعمدی در سیستم شخص ثالث	به‌طور معمول، یک هکر کنترل (بخشی از) سیستم رایانه یا شبکه شرکت را به دست می‌آورد و از این طریق، اقدام به فعالیت‌های غیرقانونی علیه شخص ثالث می‌کند. این عملیات، به‌عنوان مثال ذیل شکلی از حملات DoS با استفاده از تعداد زیادی رایانه‌های تحت کنترل (شبکه‌ای از بات‌ها) یا با ارسال پنهانی یک بدافزار یا اطلاعات غلط صورت می‌گیرد.
	اختلال زیرساخت دیجیتال خارجی	شرکت یا شخص حین فعالیت‌ها و کسب‌وکار خود در بستر دیجیتال به دلیل از کارافتادن زیرساخت دیجیتال بیرونی همچون فضای ابری و یا پردازش‌گر/محل ذخیره داده، از کار باز می‌ایستد و یا دچار مشکل می‌شود.

دسته‌بندی انواع حوادث سایبری

محرمانگی داده	سرقت داده‌های شخص اول	فرد یا شرکت داده‌های اختصاصی خود (داده‌های مالی، اسناد محرمانه تجاری و غیره) را خارج از محدوده داده‌ای خود می‌یابد، برای مثال، شخص یا شرکت از این حقیقت که داده به فروش رسیده، مبادله شده و یا در فضای وب تاریک افشا شده و یا اینکه داده به صورت آزاد در دسترس عموم قرار گیرد، آگاه است.
	سرقت داده‌های شخص ثالث	شخص یا شرکت، داده‌های شخص ثالث را که ذخیره‌سازی یا پردازش کرده (به طور معمول، PCI،PHI،PII) خارج از محدوده داده‌ای خود شناسایی می‌کند، به عنوان مثال، شخص یا شرکت متوجه سرقت، تعویض و یا افشای داده‌های شخص ثالث مثلا در فضای وب تاریک یا افشای آن به صورت عمومی می‌شود.

دسته‌بندی انواع حوادث سایبری

یکپارچگی داده/ دسترسی پذیری	حذف داده‌های شخص اول	شخص یا شرکت، متوجه حذف داده خود از راه‌حل ذخیره‌ای خود یا اپلیکیشن‌های خود می‌شود.
	رمزگذاری داده‌های شخص اول	شخص یا شرکت متوجه رمزگذاری شدن داده خود توسط شخص ثالث می‌شود و تنها در صورت رمزگشایی (اغلب به دنبال باج دادن به همان شخص ثالث) قابل دسترس خواهد بود.
	خرابی داده‌های شخص اول	فرد یا شرکت متوجه خراب شدن (تغییر) داده‌های خود می‌شود. در صورتی که تغییرات جزیی و نادر باشد، کشف این مسئله بسیار دشوار بوده و زمان زیادی طول می‌کشد که موضوع شناسایی شود. سایر خرابی-ها در صورتی‌که چشمگیر و آشکار باشند، به راحتی قابل تشخیص خواهند بود.
	حذف داده‌های شخص ثالث	شخص یا شرکت، متوجه حذف داده‌های شخص ثالث از راه‌حل ذخیره‌ای خود یا اپلیکیشن‌های خود که پیش از این ذخیره یا پردازش کرده (به‌طور معمول، PCI،PHI،PII) می‌شود.
	رمزگذاری داده‌های شخص ثالث	شخص یا شرکت متوجه رمزگذاری شدن داده‌های شخص ثالث که پیش از این ذخیره یا پردازش کرده (غالبا داده‌های مربوط به ، PCI،PHI،PII) توسط شخصی با سوء نیت می‌شود و تنها در صورت رمزگشایی (اغلب به دنبال باج دادن به همان شخص) قابل دسترس خواهد بود.
	خرابی داده‌های شخص ثالث	فرد یا شرکت متوجه خراب شدن (تغییر) داده‌های شخص ثالث که پیش ذخیره یا پردازش کرده است (به‌طور معمول داده‌های مربوط به PCI،PHI،PII) می‌شود. در صورتی که تغییرات جزیی و نادر باشد، کشف این مسئله بسیار دشوار بوده و زمان زیادی طول می‌کشد که موضوع شناسایی شود. سایر خرابی‌ها در صورتی‌که چشمگیر و آشکار باشند، به راحتی قابل تشخیص خواهند بود.

دسته‌بندی انواع حوادث سایبری

فعالیت مخرب	سوء استفاده از سیستم	آزار و اذیت سایبری، قلدری سایبری. یک هکر یا شخصی با سوء نیت، از یک سیستم دیجیتالی همچون شبکه اجتماعی برای انتشار یا پخش پیام‌های اهانت آمیز (بهتان و افترا) و شرم‌آور درباره فرد قربانی و مورد حمله سوء استفاده می-نماید.
	ارتباطات مخرب هدفمند	به‌طور معمول، شامل تلاش‌های فیشینگ یا کلاهبرداری مدیرعامل یا انواع پیشنهادات پیچیده‌تر برای درخواست اطلاعات (محرمانه) با اهداف مخرب می‌شود.
	کلاهبرداری سایبری/ سرقت سایبری	یک هکر با نفوذ به سیستم یا سوء استفاده از اطلاعات اعتباری فرد مورد نظر، تراکنش‌های غیرقانونی ارزشی مانند (انتقال وجه) را آغاز می‌کند.

دسته‌بندی انواع ریسک‌های سایبری

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

دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی انواع ریسک‌های سایبری براساس نوع حمله و یا حادثه سایبری

- **هک**: منظور هک شدن اطلاعات شخصی توسط هکرها است. هک می‌تواند موجب تضعیف میزان محرمانگی سازمانی یک شرکت شود که خود باعث پایین آمدن اعتبار آن شرکت خواهد بود. چرا که هک ممکن است عملکرد یک شرکت نسبت به امنیت داده‌ها و از دست دادن اطلاعات محرمانه را در معرض قضاوت عموم قرار دهد.
- **حمله عدم سرویس‌دهی**: در حملات عدم سرویس‌دهی از یک کامپیوتر یا ارتباط اینترنتی برای پرکارکردن پهنای باند و منابع سرور و مبدا استفاده می‌شود که در نتیجه آن سرور توان ارائه خدمات نداشته و اصطلاحا مشغول می‌گردد. بنابراین حمله قطع یا اخلال در خدمات، به معنای حمله یک یا چندین شخص از طریق ارسال میزان بسیار زیادی از داده‌های الکترونیکی به سامانه رایانه‌ای به منظور کاستن از ظرفیت آن می‌باشد که در نتیجه افراد مجاز نتوانند برای امور قانونی خود به سامانه دسترسی پیدا کرده و به مبادله اطلاعات بپردازند. در صورتی که پر شدن ظرفیت سامانه ناشی از ناهماهنگی میان ظرفیت آن با حجم اطلاعاتی که معمولا به آن وارد می‌شود، باشد؛ حمله منع سرویس‌دهی، مشمول بیمه نخواهد شد.
- **اخاذی اطلاعاتی**: به طور کلی اخاذی در فضای سایبری هنگامی اتفاق می‌افتد که شخصی از طریق اینترنت دیگری را تهدید به برآورده کردن مطالبات خود می‌کند، مانند دادن مبلغی پول، تحویل کالایی مشخص یا انجام کاری خاص.

دسته‌بندی انواع ریسک‌های سایبری

- **خطای نیروی انسانی**: رویداد سایبری بدون هیچ هدف خرابکارانه از پیش تعیین‌شده (خطای سهوی) مانند کلیک روی لینک‌های ناشناس، نصب نرم‌افزارهای ناشناس، اتصال فلش یا هاردهای آلوده به سیستم‌ها و ...
- **نقص ناشی از نرم‌افزار**: شرکت‌ها اصولا برای به‌کارگیری فعالیت‌های خود از نرم‌افزارهای رایانه‌ای فراوانی استفاده می‌کنند که گاها عدم بازدهی مناسب این برنامه‌های رایانه‌ای ممکن است منجر به ورود خسارت شود.
- **نقض داده**: نقض داده حادثه‌ای است که در اثر آن اطلاعات محرمانه، محافظت شده و سری، به طور پنهانی و بدون مجوز وارسی شده، دزدیده شده و یا مورد استفاده قرار می‌گیرد.
- **فعالیت‌های مخرب**: استفاده نادرست از فناوری با هدف ایجاد اختلال در سیستم‌های خدمات‌رسان یا آسیب رساندن به آن‌ها یا با هدف سود شخصی از طریق انواع بدافزارها (ویروس‌ها، کرم‌ها و تروجان‌ها)
- **حالت عدم فعالیت شبکه/ دان تایم شبکه**: این اصطلاح زمانی به کار می‌رود که سیستمی برای مدت به خصوصی قادر به ارائه خدمات نباشد. ایجاد چنین وضعیتی برای سیستم‌های خدمات‌رسان به سایر مراکز فعال مانند نیروگاه‌ها، بانک‌ها و سایر موسسات مالی موجب اختلال در انجام امور اصلی آن‌ها خواهد شد و بعضا عواقب ناگواری در پی دارد.

دسته‌بندی انواع ریسک‌های سایبری

- **از بین رفتن فیزیکی سیستم**: فعالیت در محیط سایبری نیازمند سیستم فناوری اطلاعات است که از تجهیزات عینی متعددی تشکیل شده است. صدمه به این تجهیزات می‌تواند در اثر هر عامل بیرونی به وقوع بپیوندد؛ از آتش‌سوزی گرفته تا تغییرات دمای اتاق سرور و یا نوسانات الکتریکی.
- **اشکال در عملکرد سیستم:** به عنوان مثال خطایی در سیستم یک شرکت بیمه رخ داده باشد و باعث نفوذ و دخالت شخص ثالث در سیستم شود.
- **از بین رفتن یکپارچگی داده‌ها یا قطع شدن دسترسی به اطلاعات:** دقت، صحت، اعتبار و سازگاری اطلاعات موجود در سیستم بیمه‌گذار آسیب ببیند یا اطلاعات حذف یا دسترسی به آن‌ها قطع شده باشد.

دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی ریسک‌های سایبری بر اساس ملاحظات کسب‌وکارها

- **ریسک امنیتی**: این نوع ریسک، یک خطر امنیتی است که باعث آسیب به یک سازمان می‌شود و می‌تواند به صورت سرقت اطلاعات و داده‌ها، حملات فیشینگ یا بدافزارها باشد. تاثیر یک حمله امنیتی را می‌توان هم از لحاظ مالی و هم از لحاظ تاثیر در شهرت سازمان بررسی کرد.
- **ریسک حریم خصوصی**: این ریسک به خسارات وارد شده به حریم خصوصی مشتریان یا سایر نهادهای طرف قرارداد با سازمان، طبق قرارداد منعقد شده، مربوط می‌شود. قوانین مربوط به حفظ حریم خصوصی و حقوق مصرف‌کننده با توجه به جمع‌اوری، پردازش، ذخیره‌سازی و استفاده از داده‌ها از طریق قوانین خاص هر کشور تعریف می‌شود.
- **ریسک عملیاتی**: این ریسک وابسته به فناوری است. یک سازمان در صورت نیاز به یک فناوری و تکنولوژی خاص در حالی‌که دسترسی به شبکه مختل شده باشد، به دلیل قطع فعالیت‌های تجاری با خسارات مالی روبه‌رو می‌شود. در این صورت با ریسک عملیاتی مواجه شده است.

دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی ریسک‌های سایبری بر اساس سناریوی حمله

ریسک‌های سایبری را می‌توان بر اساس سناریوی حمله نیز دسته‌بندی کرد. سناریوی حمله عبارت است از :

۱- جمع‌آوری اطلاعات

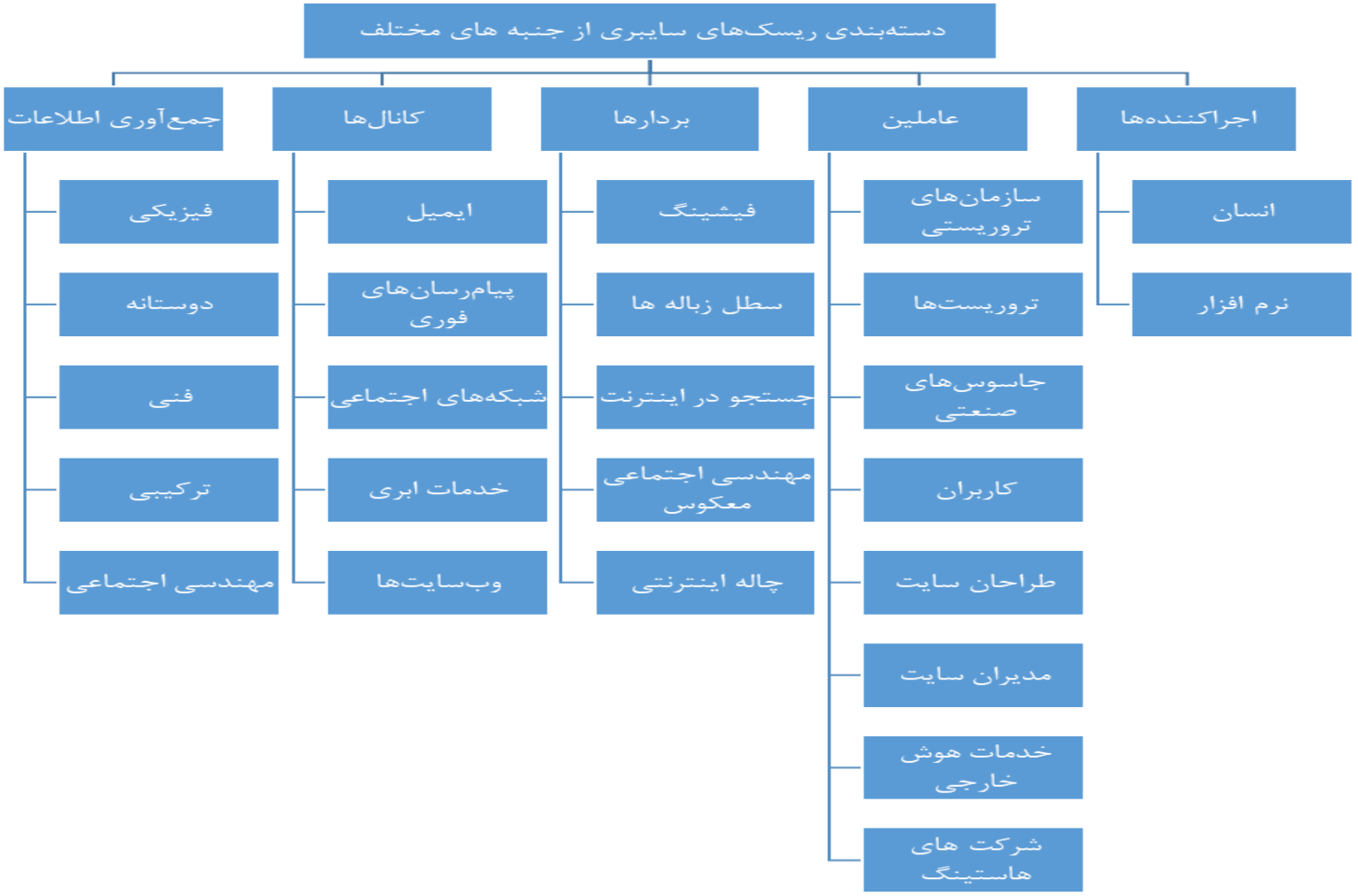
۲- انتخاب کانال مناسب برای پیاده‌سازی حمله

۳- بردارهای حمله

۴- عاملین حمله

۵- پیاده‌سازی و اجرای حمله.

دسته‌بندی انواع ریسک‌های سایبری



دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی از جنبه جمع‌آوری اطلاعات:

جمع‌آوری اطلاعات برای حملات امنیتی روش‌های مختلفی دارد که عبارتند از:

- روش فیزیکی: سهل‌انگاری در امحاء کاغذهای باطله دارای اطلاعات حساس، چاپ و در دسترس قرار گرفتن اطلاعات کاربری و گذرواژه کارکنان، عدم رعایت ملاحظات مربوط به اطلاعات طبقه-بندی شده و بایگانی نامناسب اسناد از جمله نمونه‌هایی هستند که می‌تواند فرد مهاجم به منظور جمع‌آوری اطلاعات قبل از حمله مورد بهره‌برداری قرار دهد.
- روش روابط دوستانه: برقراری ارتباطات دوستانه با قربانی به منظور دریافت اطلاعات حساس یا استفاده از شخص برای نصب نرم‌افزارهای مخرب بر روی سیستم.
- روش فنی: استفاده از اینترنت به منظور جمع‌آوری اطلاعات حساس و مهم قربانی به عنوان مثال استفاده از حساب کاربری شبکه‌های اجتماعی شخص و استخراج اطلاعات مربوط به وی.
- روش ترکیبی: بهره‌گیری از ترکیب روش‌های فوق‌الذکر به‌صورت همزمان.
- روش مهندسی اجتماعی: سوءاستفاده از غفلت قربانی و جلب اعتماد وی به منظور دریافت و جمع‌آوری اطلاعات موردنظر.

دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی از نظر کانال‌های مورد استفاده برای حملات:

مهاجمان برای حملات خود نیاز به کانال‌هایی دارند که بتوانند حمله خود را پیاده‌سازی و اجرا کنند که این نوع کانال‌ها عبارتند از:

- ایمیل به عنوان شایع‌ترین کانال حملات فیشینگ.
- برنامه‌های پیام‌رسان فوری: کانالی برای ارتباط راحت‌تر و قابل اعتمادتر با قربانی و سرقت هویت وی
- شبکه‌های اجتماعی
- خدمات ابری: به اشتراک‌گذاری فایل‌های مخرب در فضای ابری به منظور حمله بعد از دریافت و نصب آن فایل توسط قربانی.
- وب‌سایت‌ها: طراحی سایت و لینک‌های حاوی فایل‌های مخرب و ارسال آن از طریق کانال‌های مختلف به منظور هدایت قربانی به سمت سایت

دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی از جنبه بردارهای حمله:

- فیشینگ: تلاش برای بدست‌آوردن اطلاعات حساس فرد با جلب اعتماد وی
- جستجو در سطل زباله: عمل الک کردن سطل‌های زباله برای بدست آوردن اطلاعات حساس فرد
- گشت‌وگذار در اینترنت: روشی برای مشاهده و بدست آوردن اطلاعات حساس در سایت‌ها
- مهندسی اجتماعی معکوس: جلب اعتماد قربانی به صورتی‌که فرد برای حل مشکلات خود از مهاجم مشورت بگیرد تا مهاجم بتواند فرد را به سمت هدف خود هدایت کند.
- چاله: قرار دادن سایت موردعلاقه قربانی یا لینک مخرب بر سر راه وی توسط مهاجم

دسته‌بندی انواع ریسک‌های سایبری

دسته‌بندی از جنبه عاملین تهدیدها:

هر تهدید یا خطری که در جامعه رخ می‌دهد عامل یا عاملینی دارد که آن را پایه‌گذاری می‌کنند. عاملین تهدیدهای فضای سایبری عبارتند از: سازمان‌های جاسوسی، تروریست‌ها، جاسوس‌های صنعتی، خدمات هوش خارجی، کاربران، طراحان سایت، مدیران سایت‌ها، شرکت‌های هاستینگ و ...

دسته‌بندی از جنبه اجراکننده‌ها:

تهدیدها بعد از جمع‌آوری اطلاعات و انتخاب کانال مناسب نهایتا باید اجرا شوند. در اینجا است که مهاجم باید آن را اجرا کند و به اهداف خود برسد. مهاجم برای اجرای تهدیدهای خود از دو طریق اقدام می‌کند که عبارت است از: انسان یا نرم‌افزار و ربات

با عنایت به مراتب فوق، ملاحظه می‌گردد که ریسک سایبری دامنه وسیعی از ابعاد و موضوعات را شامل می‌شود که متناسب با اهداف مدنظر، می‌توان از هرکدام از دسته‌بندی‌ها یا ترکیبی از آن‌ها جهت طراحی سناریوی مطلوب، بهره‌برداری نمود.

پیامدهای ریسک سایبری در صنعت بیمه

- 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 غیرقابل برگشت باشد.
- هکرها همچنین اطلاعات به دست آمده از بیمه‌گذران را به منظور اهداف مجرمانه مختلف مانند سرقت هویت و به دست آوردن 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.
- با این حال، تأثیر کمتر آشکار اما با اهمیت بیشتر بر شرکت، می‌تواند **از دست دادن اعتماد بیمه‌گذاران** باشد. از آنجایی که تجارت بیمه حول اعتماد می‌چرخد، یک افشای اطلاعات می‌تواند تأثیر بسیار واقعی بر برند و ارزش بازار بیمه‌گران داشته باشد.

پیامدهای ریسک سایبری در صنعت بیمه

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

پیامدهای ریسک سایبری در صنعت بیمه

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

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

پیامدهای ریسک سایبری در صنعت بیمه

به منظور 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.

انواع حادثه و حوزه‌های پوشش بیمه‌ای آن

گروه‌بندی انواع حوادث	حوزه های پوشش
وقفه در کسب و کار/ وقفه در عملیات	پرداخت سود از دست رفته ناشی از وقفه در تولید که ناشی از آسیب‌های فیزیکی نیست.
وقفه در کسب و کار مشروط (CBI) برای خسارات غیرفیزیکی	پرداخل سود از دست رفته ناشی از وقفه در عملکرد اشخاص ثالث مرتبط مانند تامین‌کنندگان، شرکا، مشتریان بجز 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	زیان‌های مالی خالص ناشی از فعالیت‌های مخرب داخلی یا خارجی سایبری که با هدف 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 تامین می‌کند.
باج گیری و اخاذی سایبری	هزینه‌های کارشناسی رسیدگی به باج‌گیری یا پرداخت باج در یک حادثه باج‌گیری بطور مثال زمانی‌که دسترسی به داده‌ها تا زمان پرداخت باج، امکان‌پذیر نباشد.

انواع حادثه و حوزه‌های پوشش بیمه‌ای آن

سرقت مالکیت معنوی	از دست دادن 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 هزینه-های ارتباطات ۳) هزینه‌های اصلاحات به عنوان مثال هزینه‌های حذف یا فعالسازی هجوم به محتوای مخربی که علیه بیمه شده منتشر شده است. ۴) هزینه‌های اطلاع‌رسانی
(جبران) نقض حریم خصوصی	هزینه‌های جبران خسارت پس از نشت داده‌های خصوصی یا حساس از جمله خدمات اعتباربانی بجز 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 به عنوان یک کانال یا مسیر برای دسترسی به شخص ثالث استفاده شده باشد.

انواع حادثه و حوزه‌های پوشش بیمه‌ای آن

خسارت وارد به شهرت (به استثنای حمایت حقوقی)	جبران سود از دست رفته ناشی از کاهش خرید و فروش یا مشتریان به دلیل از دست رفتن اعتماد آنها نسبت به شرکت
هزینه‌های مقرراتی و دفاع حقوقی (به استثنای جریمه)	الف) هزینه‌های مقرراتی: جبران هزینه‌هایی که شرکت یا اشخاص ثالث مرتبط با آن در زمان تحقیقات دولتی یا نظارتی مربوط به یک حمله سایبری متحمل می-شوند. (خدمات قانونی، فنی یا IT که مستقیما با تحقیقات مرتبط می‌شود را پوشش می‌دهد به استثنای مبلغ جریمه) ب) هزینه‌های دفاع حقوقی: پوششی 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 در صورتیکه قوانین محلی اجازه دهد، پرداخت می‌شود.
(مسئولیت) ارتباطات و رسانه	جبران هزینه‌های خسارات ناشی از سوء استفاده 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 سوء استفاده از اسرار تجاری
حمایت حقوقی- حق الزحمه وکیل	هزینه‌های دعاوی حقوقی که توسط یا علیه بیمه‌گذار انجام می‌شود که شامل هزینه‌ها و حق‌الزحمه وکیل در صورت محاکمه می‌شود (به طور مثال در مورد سرقت هویت، هزینه‌های وکیل برای اثبات سوء استفاده از هویت قربانی)

انواع حادثه و حوزه‌های پوشش بیمه‌ای آن

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 به استثنای محصولات یا عملکرد فنی (خطاها و رخنه‌های تکنولوژی) و خطاها و رخنه‌های خدمات تخصصی
(مسئولیت) رئیسان و مدیران	هزینه‌های جبران خسارت در صورت اقامه دعوی شخص ثالث علیه رئیسان و مدیران شرکت بیمه شده، از جمله خیانت در امانت و ترک وظیفه ناشی یک حادثه سایبری
(مسئولیت) خطاها و رخنه-های تکنولوژی	جبران هزینه‌های خسارت مربوط به عدم ارائه کافی خدمات و محصولات فنی ناشی از یک رویداد سایبری

انواع حادثه و حوزه‌های پوشش بیمه‌ای آن

(مسئولیت) خطاها و رخنه‌های خدمات تخصصی/ (مسئولیت) غرامت حرفه‌ای	جبران هزینه‌های خسارت مربوط به عدم ارائه کافی خدمات و محصولات حرفه‌ای ناشی از یک رویداد سایبری به استثنای خدمات و محصولات فنی (خطاها و رخنه‌های تکنولوژی)
آسیب‌های محیط زیستی	دامنه پوشش: 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 کسب‌وکار 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 (به عنوان مثال نشت داده‌های حساس که منجر به خودکشی شود)

بررسی معیارهای بیمه‌پذیری ریسک سایبری

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
معیارهای اکچوئری	فراوانی و شدت ریسک باید به طور معقولی قابل اندازه‌گیری 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 به منظور اهداف امنیتی خودداری کنند. به عمد، ماهیت حملات به طور مداوم در حال تغییر است تا از تجزیه و تحلیل و کاهش آن فرار کنند. مدل‌های سایبری در مراحل ابتدایی خود باقی مانده و توسعه نمی‌یابند.	خلق نوآوری به منظور ایجاد پایگاه داده 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 تحت تاثیر قرار دهند.	سایبری اساساً یک ریسک نیروی انسانی است، اما روشن شدن نیت اقدامات جنگ سایبری تحت حمایت دولت و سایر موارد استثنا، مانند اقداماتی که قبلا توضیح داده شد، می‌تواند کمک کند.
	حداکثر خسارت موجود، باید در ظرفیت صنعت قابل مدیریت باشد.	خسارت‌های فاجعه‌آمیز، منجر به تنوع‌پذیر نبودن آنها می‌شود.	ریسک حوادث فاجعه‌آمیز را از پوشش خسارت‌های فرسایشی (خسارت‌هایی غیر از خسارات فجایع یا مواجهه‌های بزرگ) جدا کنید.

بررسی معیارهای بیمه‌پذیری ریسک سایبری

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
معیارهای اکچوئری	متوسط مقدار خسارت در هر رخداد قابل پیش‌بینی باشد و تعداد زیادی از رخدادهای خسارت مشابه در سال اتفاق بیافتد.	اساس بازار بیمه سایبری به خوبی تثبیت شده است.	افزایش نرخ جذب بیمه در بخش‌ها و اندازه شرکت‌ها؛ جداسازی ریسک‌های فاجعه‌آمیز از خسارت‌های فرسایشی.
	کمبود اطلاعات نامتقارن در این حوزه (به عنوان مثال کژمنشی یا مخاطرات اخلاقی، کژگزینی/ انتخاب نامطلوب)	تجربه و استانداردهای مربوط به اشتراک‌گذاری و کاهش میزان حملات در حال تکامل است.	بیمه مشترک، استانداردهای کاهش میزان حملات، اشتراک‌گذاری داده‌ها، منابع مدیریت بحران

بررسی معیارهای بیمه‌پذیری ریسک سایبری

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
معیارهای بازار	برای یک بازار بیمه پایدار، حق بیمه باید از نظر پوشش ریسک، کافی باشد.	میزان خسارت وارد شده و به تبع 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 بیمه کردن کامل ریسک‌های فاجعه بار نیست.	شفافیت در مورد آنچه که منجر به ریسک‌های فاجعه‌آمیز می‌شود، در بالا بردن ظرفیت بیمه‌گر اتکایی موثر است.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

بیمه سایبری **اولین بار 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.
در دهه ۱۹۹۰، با وجود ناشناخته بودن اینترنت، امنیت سایبری در مشاغل مهم به یک عامل تاثیرگذار تبدیل شده و بیمه سایبری به صورت وسیع‌تر در دهه ۱۹۹۰ در کنار بیمه‌نامه‌های مسئولیت ارائه می‌شد.
در طول این مدت، دو تهدید بزرگ، نقض نسخه‌برداری و نشر اطلاعات و سرقت مالکیت معنوی بودند. افراد خبره در صنعت کامپیوتر در آن زمان نگران بودند که رقبا یا مجرمان سایبری نوآوری‌های آنها را به سرقت برده و ادعای مالکیت کنند.
استفاده از رایانه و اینترنت از سال ۱۹۹۸ بسیار گسترش یافت؛ به‌طوری‌که در سال ۲۰۰۰ در آمریکا میزان خسارت‌هایی که بر سایت‌ها و فروشگاه‌های اینترنتی وارد گردید، برابر نیم میلیون دلار اعلام گردیده است.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

افزایش تعداد حملات سایبری و **خسارت‌های احتمالی برای کسب‌وکارهای کوچک و بزرگ**، منجر به نیاز بسیاری از افراد و صاحبان مشاغل به بیمه سایبری شد.

توجه به این نکته ضروری است که ماهیت تهدیدات سایبری به طور مداوم در حال تغییر و تحول است. بنابراین، بیمه‌گران سایبری باید دائماً خود را با شرایط جدید تطبیق دهند، بیمه‌نامه‌های سایبری را تغییر داده و خدمات مختلفی را ارائه کنند تا با تهدیدات نوظهور همگام شوند.

مختصری از تاریخچه بیمه سایبری در شکل صفحه بعد ترسیم شده است:

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

تاریخچه بیمه سایبری

دهه ۱۹۹۰

در ابتدا پوشش‌های بیمه سایبری، در قالب بیمه نامه مسئولیت و در کنار پوشش‌های آن برای شرکت‌های فعال در در بخش‌های فناوری و خدمات حرفه‌ای ارائه شده است.

۲۰۰۵

برخی از اولین محصولات سایبری فقط تعهدات شخص ثالث را پوشش می‌دادند (مانند افشای اطلاعات مشتریان یک کسب‌وکار)؛ اما در اواسط دهه ۲۰۰۰ برخی از پوشش‌های شخص اول مانند خسارات وارده به خود کسب‌وکارها ارائه شد.

۲۰۱۰

افزایش تقاضا برای محصولات بیمه سایبری همزمان با ریسک‌های رو به رشد سایبری که کسب‌وکارها با آن مواجه هستند، منجر به فروش فزاینده بیمه مسئولیت سایبری به عنوان یک محصول مستقل شد.

۲۰۱۶

دنباله‌ای از افشای اطلاعات با هزینه‌های هنگفتی در این دوره رخ داد که نیاز به بیمه سایبری را صرف‌نظر از صنعتی که یک کسب‌وکار در آن فعالیت می‌کند، نشان داد. این امر باعث افزایش تقاضا برای محصولات بیمه سایبری شد.

۲۰۱۸

قانون عمومی حفاظت از اطلاعات(GDPR) به اجرا گذاشته شد و ریسک‌های سایبری در همه مشاغل افزایش یافت.

۲۰۲۰

کووید-۱۹ اکثر سازمان‌ها را مجبور به دورکاری کرد و در نتیجه استفاده از دستگاه‌های تلفن همراه و دسترسی از راه دور به سیستم‌های اصلی کسب و کار، با افزایش بی‌سابقه‌ای همراه بود. مجرمان سایبری این بیماری همه‌گیر را فرصتی برای بهره‌برداری از دستگاه‌های ناامن دانستند. افزایش آگاهی در مورد نیاز به بیمه سایبری مناسب در این دوره احساس شد.

۲۰۲۱

«سایبری خاموش» و موضع بیمه‌گران در این خصوص، بار دیگر بیمه سایبری را مورد توجه قرار داد. سایبری خاموش به قرار گرفتن در معرض احتمالی ریسک سایبری موجود در بیمه‌نامه‌های سنتی اموال و مسئولیت اشاره دارد که ممکن است به طور ضمنی شامل ریسک سایبری یا حذف آن نباشند.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

بیمه سایبری بسیاری از خسارات مربوط به افشای اطلاعات را پوشش می‌دهد. این پوشش‌ها عبارتند از:

- **بازیابی اطلاعات:** این هزینه برای بازیابی یا جایگزینی نرم‌افزار، داده‌های الکترونیکی و سایر برنامه‌هایی که در اثر حمله بدافزارها، حمله هکرها، حمله منع یا محروم‌سازی سرویس (DoS) یا هر شکل دیگری از حمله سایبری، آسیب دیده یا از بین رفته‌اند را پوشش می‌دهد.
- **از دست دادن درآمد و سایر هزینه‌ها ناشی از وقفه در کسب‌وکار:** این پوشش شامل درآمد از دست رفته ناشی از حمله سایبری و همچنین سایر هزینه‌های موردنیاز برای بازیابی اطلاعات پس از پایان یافتن اثر یک ویروس، حمله هکرها و غیره می‌شود.
- **هزینه‌های اطلاع‌رسانی:** این هزینه‌ها، شامل هزینه‌هایی است که جهت اطلاع‌رسانی به اشخاصی که تحت تأثیر افشای اطلاعات قرار گرفته‌اند، پرداخت می‌شود. این نوع پوشش دارای اهمیت زیادی است، زیرا بسیاری از ایالت‌ها قوانینی دارند که کسب‌وکارها را ملزم می‌کند در صورت به خطر افتادن اطلاعات شخصی مشتریان یا کارمندان، آنها را مطلع سازد. بیمه‌نامه‌ها همچنین می‌توانند هزینه‌های مربوط به نظارت بر اعتبار شرکت و همچنین ایجاد یک مرکز تماس برای ارتباط با افراد آسیب‌دیده را پوشش دهند.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

- **اخاذی سایبری:** این نوع پوشش، باج‌های درخواستی از سوی هکری را پوشش می‌دهد که به شبکه یک شرکت نفوذ کرده و تهدید کرده است که آسیب بیشتری به شرکت وارد می‌کند، مانند انتشار داده‌های حساس، آلوده کردن سیستم به ویروس، شروع حمله DoSو غیره.
- **مدیریت بحران:** اکثر بیمه‌نامه‌های سایبری برخی از هزینه‌های مدیریت بحران را نیز پوشش می‌دهند. این نوع پوشش می‌تواند شامل هزینه استخدام یک وکیل، کارشناس امنیت سایبری، حسابدار پزشکی قانونی، یا مدیر روابط عمومی برای ارزیابی وضعیت، تعیین دامنه خسارت، مشخص کردن اطلاعات افراد در معرض ریسک و کمک به کاهش ضرر و زیان برای حفظ اعتبار یک شرکت باشد.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

بسیاری از بیمه‌نامه‌های سایبری برخی از خسارت‌های مربوط به مسئولیت را نیز پوشش می‌دهند. این موارد معمولاً مربوط به تسویه‌حساب‌ها یا خسارات و همچنین هزینه‌های دفاعی است که می‌تواند در محدوده بیمه‌نامه اصلی یا خارج از آن قرار گیرد.

برخی از نمونه مسئولیت‌های تحت پوشش، عبارتند از:

- **مسئولیت رسانه‌های الکترونیکی:** بیمه مسئولیت رسانه‌های الکترونیکی شکایت‌های حقوقی علیه یک شرکت را برای مواردی مانند افترا، توهین، تهمت و غیره بازپرداخت می‌کند. همچنین نقض حق نسخه‌برداری، نقض نام دامنه و تجاوز به حریم خصوصی را پوشش می‌دهد. این خسارت‌ها تنها در صورتی تحت پوشش قرار می‌گیرند که بیمه‌گذار داده‌های الکترونیکی را در اینترنت منتشر کند.
- **مسئولیت حفظ حریم خصوصی:** بیمه مسئولیت حریم خصوصی برای سازمان‌هایی که دارای اطلاعات و حریم خصوصی بالایی هستند، مهم می‌باشد. هر زمان که یک مجرم سایبری اطلاعات حساس مشتریان یا کارمندان را در معرض خطر قرار دهد، کسب‌وکارها را نیز در معرض مسئولیت قرار می‌دهد. این پوشش مسئولیت از کسب‌وکارها در برابر تعهدات ناشی از حمله سایبری یا نقض قانون حریم خصوصی محافظت می‌کند.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

- **مسئولیت امنیت شبکه:** این پوشش، هزینه‌های ناشی از کوتاهی شرکت در مقابل افشای اطلاعات حساس، محافظت از اطلاعات حساس کسب‌وکار، جلوگیری از حمله DoSو معرفی یک ویروس یا بدافزار به سیستم را شامل می‌شود.
- **نقض مقررات و رویه‌های نظارتی:** این پوشش شامل مجازات‌ها و جریمه‌هایی است که توسط سازمان‌های نظارتی و ناشی از نقض مقررات، بر مشاغل اعمال می‌شود. همچنین به پوشش هزینه‌های استخدام وکیل برای کمک به پاسخگویی و نمایندگی روند قانونی کمک می‌کند.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

به طور خلاصه، **پوشش‌های بیمه سایبری** را می‌توان به صورت زیر دسته‌بندی نمود:

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	تامین 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 سوء استفاده از انواع خاصی از مالکیت معنوی آنلاین.
پوشش‌های اضافی	
هزینه‌های مدیریت بحران	هزینه‌های مدیریت بحران ناشی از حمله هکرهای سایبری
هزینه‌های اطلاع رسانی و نظارت	هزینه‌های اطلاع رسانی به مشتریان پس از افشای اطلاعات آنها و نظارت بر جزئیات کارت اعتباری آنها برای جلوگیری از حملات بیشتر.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

پوشش‌های بیمه سایبری را می‌توان هم به صورت **مستقل** و هم به صورت **پکیجی** و در یک بیمه‌نامه بازرگانی چند خطره موجود ارائه کرد.

بازار بیمه مستقل سایبری، در پاسخ به معرفی استثناهای بیمه‌ای سایبری در بیمه‌نامه‌های دیگر توسعه یافت و حق‌بیمه صادره مستقیم آن، تقریباً دو برابر بازار سایبری پکیجی شد.

این پوشش‌ها می‌تواند 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.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

بیمه‌نامه‌های مستقل معمولاً توسط شرکت‌های بزرگ‌تر که دارای اطلاعات و منابع مالی مهم و در معرض خطر هستند، خریداری می‌شوند.

بر اساس داده‌ها و اطلاعات مکمل سایبری ثبت شده در NAIC، میانگین حق‌بیمه در بیمه‌نامه‌های صادره مستقل در سال ۲۰۲۱ به ۱۲,۱۶۱ دلار افزایش یافت، در حالی که حق‌بیمه بیمه‌نامه سایبری پکیجی مانند بیمه‌نامه‌های شاخه مالی (بیمه مسئولیت مدیران و مسئولان شرکت‌ها (D&O)) یا حرفه‌ای (تکنولوژی و بیمه مسئولیت اشتباه و خطا (E&O))، افزایش ۴۸۰ دلاری داشته است.

حدود ۲۵۹,۰۰۰ بیمه‌نامه مستقل در پایان سال ۲۰۲۱ در مقایسه با ۵/۳ میلیون بیمه‌نامه پکیجی صادر شده است. نود و چهار درصد از بیمه‌نامه‌های مستقل نیز به جای حادثه-محور، به عنوان خسارت-محور طبقه‌بندی شدند؛ در حالی که این نسبت در بیمه‌نامه‌های پکیجی، حدود ۵۰ درصد حادثه-محور و ۵۰ درصد خسارت-محور بوده است.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

مانند سایر بیمه‌نامه‌ها، بیمه‌نامه سایبری نیز همه چیز را پوشش نمی‌دهد و انواع خاصی از خسارت‌ها را مستثنی می‌کند. چند نمونه از این موارد عبارتند از:

- **خسارت اموال و صدمات بدنی:** بیمه سایبری خسارت و آسیب بدنی یا مالی را پوشش نمی‌دهد. در این موارد باید از بیمه مسئولیت عمومی استفاده کرد.
- **جنگ و تروریسم:** جنگ و تروریسم در محدوده خسارات بیمه‌نامه سایبری قرار نمی‌گیرند.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

- **نقص در خدمات:** بیمه‌گران مسئول حملات ناشی از نقص در ارائه خدمات تاسیسات، مانند قطعی شبکه برق و اینترنت نیستند.
- **عدم صداقت و شفافیت عمدی توسط بیمه‌گذار:** اگر شخصی عمداً به بیمه‌گر اطلاعات نادرست ارائه دهد یا اطلاعات مهم را مخفی نماید، نه تنها مسئول خسارت هستند، بلکه ممکن است با اقدامات قانونی احتمالی از سوی بیمه‌گر مواجه شوند.
- **مسئولیت قراردادی:** هر قرارداد متفاوت است؛ اما بیمه‌گذاران معمولاً برخی از مسئولیت‌های ذکر شده در قرارداد را می‌پذیرند.
- **حملات سایبری انجام شده قبل از تاریخ شروع قرارداد:** بیمه‌نامه سایبری تنها پس از شروع تاریخ قرارداد قابل اعمال است، بنابراین تمام خساراتی که قبل از تاریخ شروع آن رخ داده باشد، پوشش داده نمی‌شود.
- **بازگرداندن سیستم‌های رایانه‌ای به سطح عملکردی بالاتر از قبل از حمله:** یک بیمه‌نامه سایبری مسئولیتی در قبال ارتقاء عملیات یک کسب‌وکار ندارد. فقط مسئول سیستمی است که در زمان حمله در اختیار دارد.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

در ادامه به استثنائاتی که در سایر تحقیقات به آنها اشاره شده است، می‌پردازیم:

- سود بالقوه از دست رفته.
- از دست دادن ارزش معنوی به دلیل سرقت مالکیت معنوی.
- بهینه‌سازی: هزینه بهبود سیستم‌های فناوری داخلی از جمله هرگونه ارتقا نرم‌افزار یا امنیت پس از یک رویداد سایبری.
- بعضی از حملات Dos.
- بعضی از حملاتی که منجر به نشت اطلاعات و یا از بین رفتن اطلاعات محرمانه می‌شود که بعد از کشف جرم مشخص شود منبع داخل سازمانی داشته است.
- اعمال مجرمانه یا متقلبانه یا کلاهبرداری: خسارات ناشی از اعمال مجرمانه یا با هدف تقلب پوشش داده نمی‌شوند.

انواع پوشش بیمه سایبری و استثنائات بیمه سایبری

- عدم تهیه نسخه پشتیبان و هزینه‌های ناشی از آن: بیمه‌گران صریحا اظهار می‌کنند که شرکت‌هایی که از تهیه نسخه پشتیبان برای فایل‌هایشان امتناع می‌کنند، پوششی ارائه نمی‌دهد. به طور مثال بیمه‌ها عموما هزینه‌های وقفه در کسب‌وکار را پرداخت می‌کنند ولی اگر یک شرکت برنامه پشتیبان‌گیری نداشته باشد و نتواند چندین روز بعد از حمله مجددا فعالیت خود را از سر بگیرد، بیمه‌نامه سایبری ممکن است خسارات ناشی از طولانی شدن وقفه را پوشش ندهد.
- خسارات وارده به سیستمی که در مالکیت شرکت نیست یا در راستای اهداف شرکت مورد بهره‌برداری قرار نمی‌گیرد، پوشش داده نمی‌شود.
- تخریب یا ضبط سیستم‌ها توسط دولت.
- بعضی از جریمه‌های دولتی: بعضی از این جرایم نوعی خسارات تنبیهی است و بیمه‌نامه‌های سایبری عموما خسارات تنبیهی را از پوشش خود استثنا می‌کنند.

مهم‌ترین شرکت‌های فعال در حوزه بیمه سایبری

اگرچه شرکت‌های مختلفی درحوزه بیمه سایبری فعالیت می‌کنند، لیکن بر اساس ارزیابی‌های انجام شده بر اساس جنبه‌های مختلف حفاظت سایبری، شهرت و رتبه‌بندی ای ام بست شرکت‌های زیر به عنوان مهمترین ارائه‌دهنده‌های خدمات پوشش بیمه‌ای برای خسارات سایبری قلمداد می‌شوند:

- **ای ام تراست فایننشال:** پوشش‌های بیمه‌ای این شرکت شامل پرداخت باج، مسئولیت رسانه، عدم‌النفع، صدمه به شهرت، هزینه‌های واکنش به حوادث و بازیابی اطلاعات و سیستم است. همچنین پوشش‌ها شامل شخص اول و شخص ثالث می‌باشد.
- **د داکترز کمپانی:** این شرکت بیمه‌نامه مسئولیت سایبری را برای تکمیل بیمه‌نامه مسئولیت پزشکی ارائه می‌دهد.
- **اچ اس بی:** این شرکت بر بیمه‌های تخصصی و پوشش‌های بیمه اتکایی تمرکز دارد. از جمله پوشش‌های بیمه‌ای این شرکت می‌توان به مسئولیت رسانه، اخاذی سایبری، مسئولیت امنیت شبکه، بازیابی هویت و مسئولیت حوادث حریم خصوصی اشاره کرد.

مهم‌ترین شرکت‌های فعال در حوزه بیمه سایبری

- **سایبر پالیسی:** این شرکت به دنبال بیمه‌نامه‌های مقرون به صرفه برای کسب‌وکارهایی با بودجه کم است. البته این شرکت یک ارائه‌دهنده مستقیم خدمات بیمه‌ای نیست، بلکه یک پلت فرم خرید آنلاین بیمه است. بیمه‌نامه‌های موجود در این شرکت توسط شرکت‌های مطرح دنیا ارائه می‌شوند.
- **ترولرز:** پوشش‌های بیمه‌ای برای تمام شرکت‌ها با هر اندازه‌ای، از مشاغل کوچک گرفته تا شرکت‌های بزرگ ارائه می‌دهد. پوشش‌های این شرکت شامل خدمات نظارت بر کارت اعتباری، هزینه‌های شناسایی علت نقض داده‌ها، هزینه‌های دعاوی قانونی و ... می‌باشد.

دلایل اهمیت بیمه سایبری

چند نمونه از دلایل اهمیت بیمه سایبری در سازمان‌ها عبارتند از:

- **جبران خسارت مالی احتمالی:** طبق قوانین محافظت از داده در بسیاری از کشورها، شرکت‌ها و تجارت‌هایی که افشای اطلاعات در آن‌ها رخ می‌دهد و اطلاعات کاربرانش در اختیار افراد غیرمجاز قرار می‌گیرد، ملزم به پرداخت جریمه‌های مالی سنگین هستند.
- **آسیب به اعتبار و شهرت یک سازمان:** در صورت درز و نشر اطلاعات، برند شرکت آسیب دیده که از جمله آنها می‌توان به بی‌اعتمادی مشتریان و یا سقوط ارزش سهام اشاره نمود.
- **خسارات مالی به جا مانده ناشی از توقف کسب‌وکار:** راه‌اندازی عملیات جرم‌شناسی بعد از واقعه و پاسخ به حملات رخ داده، منجر به توقف در کسب‌وکار شده که تاثیر آن‌ها در درآمد سالیانه آن سازمان قابل‌توجه است. تمامی این موارد باید توسط بیمه‌شونده مورد بررسی قرار گیرد و مشخص شود چه سطح پوششی می‌تواند برایش بهترین باشد.

چالش‌های بیمه سایبری

با این حال، علیرغم رشد حجم حق‌بیمه و میزان جذب آن، بازار بیمه مستقل سایبری نسبت به سایر بیمه‌نامه‌ها کوچک است. توسعه ضعیف بازار بیمه سایبری در مقایسه با سایر بیمه‌ها، به دلیل وجود چالش‌هایی است که به چند نمونه از آنها اشاره خواهیم کرد:

- **فقدان تاریخچه غنی:** بیمه‌گرانی که بیمه‌ای غیر از سایبری مانند آتش‌سوزی صادر می‌کنند، می‌توانند از تاریخچه‌ای غنی از این نوع بلایای طبیعی برای تدوین مدل بهینه استفاده کنند؛ اما در زمینه بیمه سایبری که یک حوزه نسبتا جدید است، سابقه تاریخی چندانی وجود ندارد.
- **فقدان داده‌های سایبری کافی به منظور تعیین نرخ بیمه‌نامه:** نه تنها تاریخچه غنی در این حوزه وجود ندارد، بلکه در بسیاری از موارد قانون، سازمان‌ها را ملزم به افشای سرقت‌های سایبری، به جز در موارد افشای اطلاعات مصرف‌کنندگان، نمی‌کند. بنابراین تعداد قابل‌توجهی از حملات سایبری، گزارش نشده و بیمه‌گران را از داده‌های موردنیاز برای اندازه‌گیری تمام خسارات یک حمله سایبری محروم کرده و تعیین نرخ را با مشکل مواجه می‌کنند.

چالش‌های بیمه سایبری

- **آگاهی ضعیف از انواع حملات سایبری:** سازمان‌ها آگاهی کافی در مورد حملات سایبری منحصر به خود را نداشته و در نتیجه، صدور بیمه‌نامه را برای بیمه‌گران بسیار دشوار می‌کند.
- **تعریف نادرست حمله سایبری:** شرکت‌های بیمه همچنان در تلاش هستند تا تعاریف دقیقی از حملات سایبری و تأثیر فناوری‌های جدید مانند اینترنت اشیا بر آنها را ارائه کنند. بدون مشخص کردن نوع تهدیدها و درک چگونگی تأثیر آنها بر بیمه‌گران، بیمه سایبری ممکن است فاقد اثربخشی بوده و سازمان را در معرض آسیب‌های قابل‌توجهی قرار دهند.
- **عدم آگاهی از ریسک‌های موجود:** بسیاری از سازمان‌ها دامنه کامل ریسک‌های سایبری پیش روی خود، نحوه برخورد با آنها و پوشش بیمه‌ای موجود را درک نمی‌کنند. این امر باعث می‌شود که خود را در معرض ریسک ندانسته و در تلاش برای پوشش آنها نباشند.
- **بدون محدودیت جغرافیایی:** مکان‌های جغرافیایی برای پوشش بیمه سایبری بسیار نامشخص‌تر از پوشش‌های بیمه‌نامه سنتی است. برای مهاجمان سایبری که می‌توانند در هر لحظه، بدون توجه به موقعیت مکانی در هر یک از محل‌های سازمان آزادانه عمل کنند، مرزهای جغرافیایی فیزیکی معنایی ندارد.

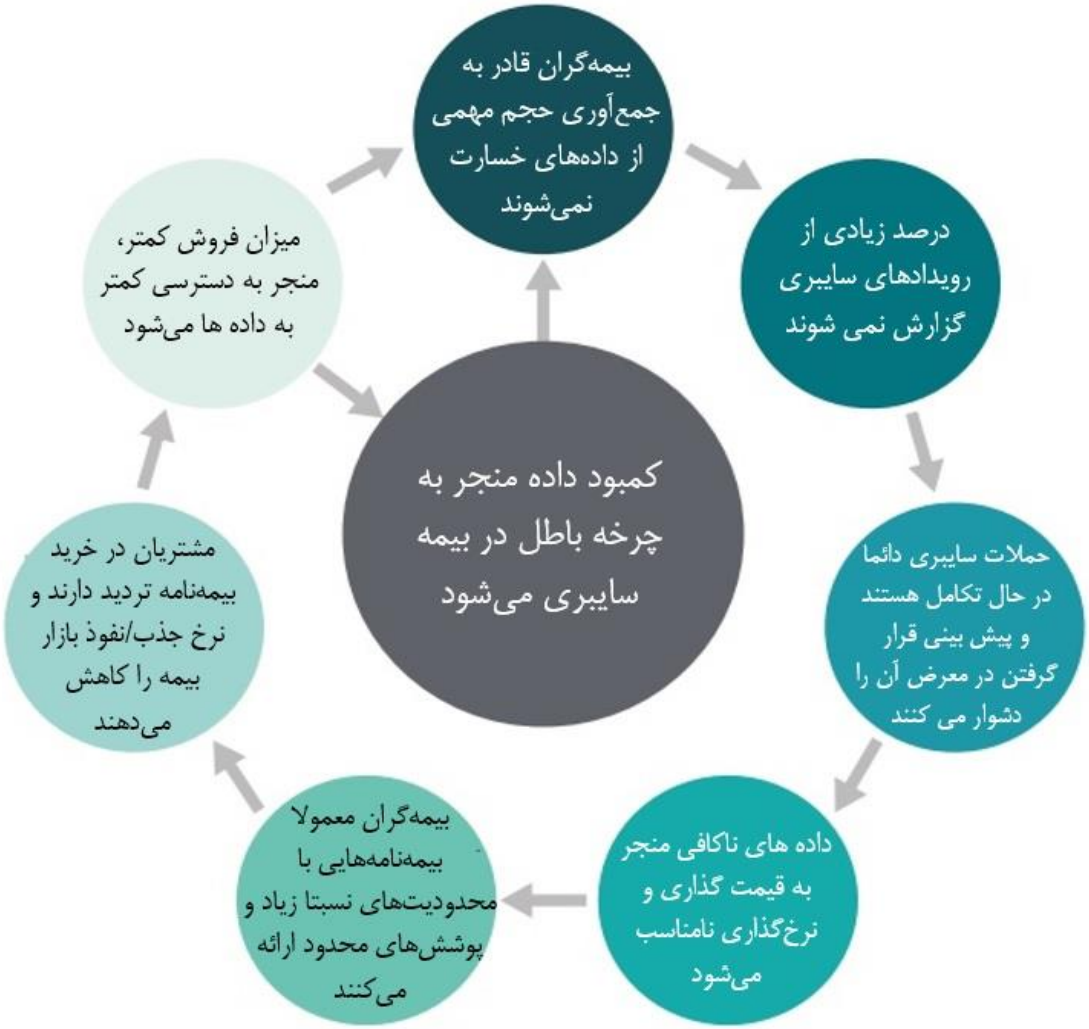
چالش‌های بیمه سایبری

- **پارادوکس/ تناقض اکچوئری:** بیمه سایبری در یک حوزه کلیدی که شرکت Symantec آن را "پارادوکس اکچوئری" می‌نامد، اساساً با سایر بیمه‌ها متفاوت است. به عنوان مثال، اگر اطلاعات یک شرکت افشا شده و این شرکت به سرعت و با شدت با این نوع حمله سایبری مقابله کرده است، آیا این شرکت، از این به بعد آمادگی بیشتری داشته و بنابراین مدیریت ریسک بهتری در آینده خواهد داشت؟ اگر چنین است، آیا بیمه‌گر می‌تواند حق‌بیمه کمتری از اینگونه شرکت‌ها دریافت کند؟
- **هزینه برای پیشگیری یا بیمه:** برای سازمان‌ها این سوال مطرح است که باید برای خرید یک بیمه‌نامه سایبری مناسب سرمایه‌گذاری انجام دهند یا برای فایروال و محافظت در برابر ریسک‌های سایبری هزینه نمایند؟
- **عدم شناخت کافی دو طرف قرارداد:** دو طرف قرارداد از خواسته‌های خود در هنگام صدور، کارشناسی‌های مشترک و نیز پرداخت خسارت مطلع نیستند.

چالش‌های بیمه سایبری

- **عدم رشد بیمه‌های اتکایی در این حوزه:** مانند سایر بخش‌ها، این بخش رشد کافی در بیمه‌های اتکایی مربوطه برای توزیع منطقه‌ای و جهانی ریسک ندارد.
- **عدم آگاهی از تعیین سطح پوشش:** این مسئله هم از سمت بیمه‌گر و از هم سمت بیمه‌گذار چالش بزرگی است. به طور مثال دو باج افزار NotPetyaو Wannacryتعداد زیادی شرکت را در ۱۵۰ کشور مورد حمله قرار داده و خسارتی در حدود ۴ میلیارد دلار تخمین زده شد. اما تعیین دقیق این خسارت‌ها قبل از وقوع حادثه یا بعد از آن حتی کار بسیار پیچیده‌ای است.

دور باطل بیمه سایبری



بررسی تجارب کشورها

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 شده‌اند، عباتند 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 لو رفته 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، تاکید می‌کند. به همین منظور، سعی داریم به بررسی بیمه سایبری در برخی از کشورهای مذکور بپردازیم.

بررسی تجارب کشورها

ایالات متحده آمریکا

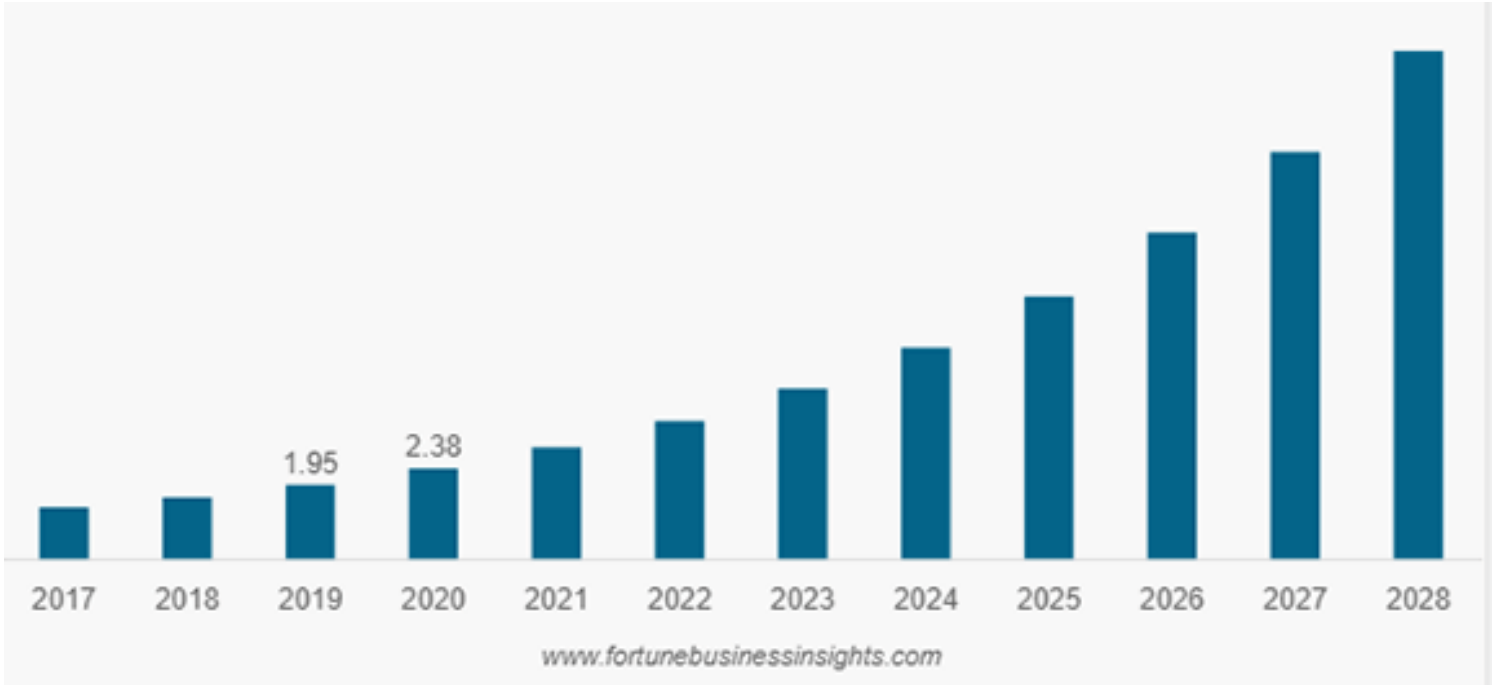
بررسی تجارب کشورها

بزرگترین شرکت‌های بیمه سایبری ایالات متحده، با حق‌بیمه صادره مستقیم (میلیون دلار)

نام شرکت بیمه	حق‌بیمه صادره مستقیم ۲۰۲۱	حق‌بیمه صادره مستقیم ۲۰۲۰	رشد	سهم تجمعی
شرکت Chubb	۴۷۳	۴۰۴	٪ ۱۷	٪ ۱۰
شرکت Fairfax Financial	۴۳۶	۱۰۹	٪ ۳۰۲	٪ ۱۹
شرکت AXA SA	۴۲۱	۲۹۳	٪ ۴۴	٪ ۲۸
شرکت Tokio Marine	۲۵۰	۸۶	٪ ۱۸۹	٪ ۳۳
شرکت AIG	۲۴۱	۲۲۸	٪ ۵	٪ ۳۸
شرکت Travelers	۲۳۲	۲۰۷	٪ ۱۲	٪ ۴۳
شرکت Beazley	۲۰۱	۱۷۸	٪ ۱۳	٪ ۴۷
شرکت CNA (Loews)	۱۸۱	۱۲۰	٪ ۵۲	٪ ۵۰
شرکت Arch Capital	۱۷۱	۱۶	٪ ۹۶۷	٪ ۵۴
شرکت AXIS Capital	۱۵۹	۱۳۴	٪ ۱۹	٪ ۵۷
صنعت بیمه	**٤٨٢٧**	**٢٧٧٤**	**٪ ٧٤**	**٪ ١٠٠**

بررسی تجارب کشورها

میزان حق‌بیمه دریافتی بیمه سایبری آمریکای شمالی از سال ۲۰۱۷ تا ۲۰۲۸ (میلیارد دلار)



بررسی تجارب کشورها

پوشش‌های بیمه سایبری در آمریکا

پس از معرفی چند شرکت برتر بیمه سایبری و بیان مشخصات آنها از جمله پوشش‌های ارائه شده آنها، در ادامه به طور کلی پوشش‌ها و استثنائات بیمه سایبری را در ایالات متحده مورد بررسی قرار می‌دهیم.

پوشش‌های بیمه سایبری در آمریکا عبارتند از:

- هزینه‌های مربوط به افشای اطلاعات (مانند اطلاع‌رسانی به مشتری، هزینه‌های قانونی و دادگاهی، حفاظت از اعتبار سازمان و غیره.)
- اخاذی سایبری (هزینه‌های واکنش به حمله و پرداخت‌های مالی را پوشش می دهد.)
- جرایم سایبری (خسارات مالی را پوشش می‌دهد.)
- وقفه در کسب‌وکار (کسب‌وکار نمی‌تواند طبق معمول فعالیت نماید.)
- بازیابی داده‌ها (هزینه‌های بازیابی، جایگزینی یا بازسازی اطلاعات و نرم‌افزارهای از بین رفته را پوشش می‌دهد.)

بررسی تجارب کشورها

استثنائات پوشش‌های بیمه سایبری در آمریکا

- صدمه و آسیب به اموال؛
- پرونده کیفری؛
- خسارات مربوط به انتقال وجه؛
- حملات قبل از قرارداد؛
- مالکیت معنوی؛
- فعالیت‌های عمدی؛
- خرابی سیستم یا زیرساخت.

بررسی تجارب کشورها

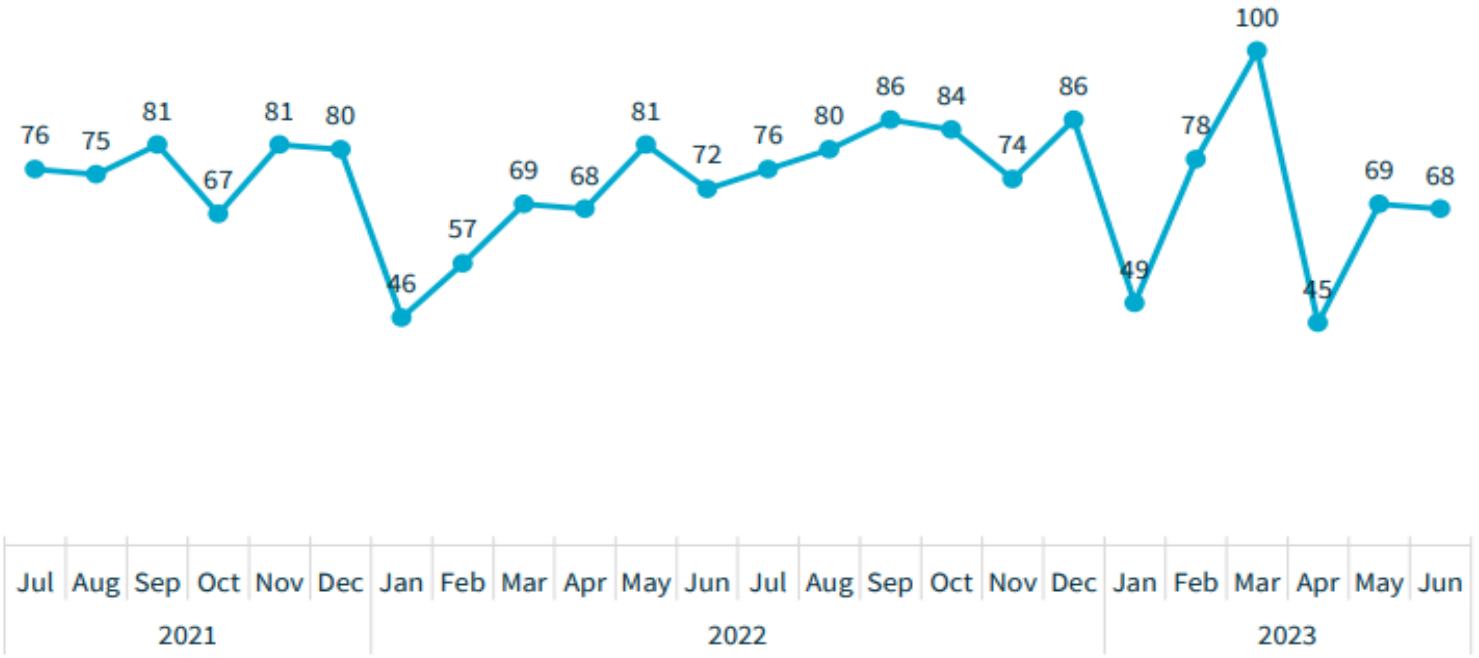
استرالیا

تعداد حملات گزارش شده از سال مالی ۲۰۲۲ الی ۲۰۲۳

دوره	تعداد حملات گزارش شده
جولای تا دسامبر ۲۰۲۲	۴۸۶
ژانویه تا ژوئن ۲۰۲۳	۴۰۹
مجموع	۸۹۵

بررسی تجارب کشورها

تعداد حملات گزارش شده ماهانه از جولای ۲۰۲۱ تا ژوئن ۲۰۲۳



بررسی تجارب کشورها

تعداد استرالیایی‌هایی که تحت تأثیر افشای اطلاعات قرار گرفته‌اند

تعداد استرالیایی هایی که تحت تأثیر قرار گرفته اند	جولای–دسامبر ۲۰۲۲	ژانویه تا ژوئن ۲۰۲۳
۵۰۰۱–۱۰۰۰۰	۱۴	۹
۱۰۰۰۱–۲۵۰۰۰	۹	۵
۲۵۰۰۱–۵۰۰۰۰	۶	۲
۵۰۰۰۱–۱۰۰۰۰۰	۳	۳
۱۰۰۰۰۱–۲۵۰۰۰۰	۲	۱
۲۵۰,۰۰۱–۵۰۰,۰۰۰	۱	۰
۵۰۰,۰۰۱–۱,۰۰۰,۰۰۰	۱	۰
۱,۰۰۰,۰۰۱–۱۰,۰۰۰,۰۰۰	۶	۲
۱۰,۰۰۰,۰۰۱ یا بیشتر	۰	۱
تعداد کل حملاتی که بیش از ۵۰۰۰ نفر را تحت تأثیر قرار داده است	۴۲	۲۳

بررسی تجارب کشورها

بیمه سایبری در استرالیا برای محافظت از کسب‌وکار افراد در برابر هزینه‌های قانونی و هزینه‌های مربوط به جرایم سایبری طراحی شده است. این بیمه‌نامه می‌تواند شامل پوشش‌هایی مانند هزینه‌های قانونی، هزینه‌های اطلاع‌رسانی در صورت افشای اطلاعات، و همچنین از دست دادن سود ناشی از وقفه در کسب‌وکار ناشی از یک رویداد سایبری باشد.
مانند بیمه‌نامه سایبری در سایر کشورها، پوشش‌ها به طور کلی به دو دسته تقسیم می‌شوند: شخص اول و شخص ثالث.

این بدان معنی است که یک بیمه‌نامه سایبری می‌تواند حوادث سایبری را پوشش دهد که به کسب و کار افراد (شخص اول) و همچنین مشتریان آنها (شخص ثالث) آسیب می‌رساند.

بررسی تجارب کشورها

پوشش‌های بیمه سایبری در استرالیا

مانند بسیاری از انواع بیمه‌نامه‌ها، پوشش‌های بیمه سایبری می‌تواند بسته به بیمه‌گذار و شرایط آن متفاوت باشد. با این حال، به طور کلی پوشش‌های زیر برای بیمه سایبری وجود دارد:

- افشای اطلاعات، از جمله سرقت یا از دست دادن اطلاعات مشتری؛
- نقض امنیت شبکه؛
- هزینه‌های وقفه در کسب‌وکار- از دست دادن سود و هزینه‌های عملیاتی؛
- تحقیقات قانونی در مورد علت یا دامنه افشای اطلاعات؛
- هزینه‌های بازیابی اطلاعات و آسیب وارد شده به سیستم؛
- اخاذی سایبری؛
- هزینه اطلاع‌رسانی افشای اطلاعات به مشتریان؛

بررسی تجارب کشورها

- هزینه‌های مدیریت بحران (برای محافظت یا کاهش آسیب به شهرت کسب‌وکار در نتیجه یک رویداد سایبری)؛
- خسارات و هزینه‌های قانونی، از جمله جریمه‌های ناشی از ادعای شخص ثالث برای نقض امنیت داده یا شبکه علیه شرکت،
- مسئولیت حفظ حریم خصوصی و امنیت،
- مسئولیت رسانه‌ها.

معمولاً پوشش‌های اضافی برای دریافت حق‌بیمه اضافی وجود دارد:

- مهندسی اجتماعی و تقلب در انتقال وجوه؛
- وقفه احتمالی کسب‌وکار؛
- مسئولیت امنیت داده کارت پرداخت.

بررسی تجارب کشورها

استثنائات بیمه سایبری در استرالیا

مانند پوشش‌ها، استثنائات بیمه‌ای هم در بیمه‌نامه‌های مختلف با هم متفاوت است؛ اما برخی از استثناهای استاندارد در بیمه‌نامه‌های سایبری عبارتند از:

- بهبود سیستم‌های شرکت به موقعیت بهتری نسبت به قبل از حمله سایبری؛
- زیان و خسارت ناشی از عدم خدمت‌رسانی هر یک از تامین‌کنندگان؛
- صدمات بدنی و خسارت مالی.

بررسی تجارب کشورها

حق‌بیمه سایبری در استرالیا

حق‌بیمه سایبری برای هر نوع کسب‌وکاری متفاوت است زیرا عوامل مختلفی که اغلب مختص هر شرکت است، در تعیین آن نقش دارد. برخی از مواردی که ممکن است بر میزان حق‌بیمه تأثیر بگذارد عبارتند از:

- صنعتی که کسب‌وکار در آن فعالیت می‌کند؛
- تعداد کارمندان شرکت؛
- میزان و حساسیت داده‌هایی که ذخیره شده است (مثلاً شرکتی که در سیستم‌های پزشکی خود داده‌ها و اطلاعات بیمار را ذخیره می‌کند، احتمالاً در مقایسه با یک نانوایی محلی با ریسک افشای اطلاعات بیشتری مواجه خواهد شد)؛
- میزان رعایت دستورالعمل‌های امنیت سایبری در شرکت؛
- پوشش‌های اضافه شده به بیمه‌نامه سایبری؛
- شرکت بیمه‌ای که انتخاب می‌شود.

بررسی تجارب کشورها

مثال‌هایی از ادعای خسارت در استرالیا

تحقیقات مرکز امنیت سایبری استرالیا نشان داده است که کسب‌وکارهای کوچک اغلب توسط ایمیل‌های فیشینگ مورد هدف قرار می‌گیرند.

تمام شرکت‌ها در استرالیا باید از قانون اطلاع‌رسانی افشای اطلاعات (NDB) پیروی کنند. این امر باعث می‌شود تا تمام کسب‌وکارها در صورتی که افشای اطلاعات در آنها منجر به سوء استفاده از اطلاعات و داده‌های مشتریان شود، ملزم به ارائه گزارش آن به دولت و مشتریانشان شوند. در ادامه چند نمونه از ادعاهای خسارت هنگام افشای اطلاعات ارائه خواهند شد (Cpa Australia):

مثال ۱: حمله سایبری به یک مؤسسه حقوقی

- گردش مالی مؤسسه: ۱.۸ میلیون دلار
- تعداد کارمند: ۷ نفر
- شرح حمله: در این مؤسسه، شرکت بیمه سایبری CPA از یک نرم‌افزار مبتنی بر ابر شخص ثالث برای نگهداری اطلاعات محرمانه استفاده نمود. این نرم‌افزار توسط یک هویت غیرمجاز هک شده و اطلاعات ۵۰۰۰ مشتری از این نرم‌افزار حذف شد و در نتیجه ارائه خدمات‌رسانی به مشتریان مختل گردید.
- نتیجه: بیمه‌گر مربوطه ضمن استفاده از مشاوران حقوقی فناوری اطلاعات برای بررسی وضعیت موجود، به مشتریان طبق قانون NDB اطلاع‌رسانی نمود. کل خسارت وارد شده به این شرکت ۱۲۴۰۰۰ دلار بود که شامل هزینه‌های وقفه در کسب‌وکار، مشاوران حقوقی و هزینه‌های جانبی می‌شد.

بررسی تجارب کشورها

آلمان

بررسی اجمالی بازار بیمه سایبری آلمان (واحد درصد/ میلیون یورو)

بیمه‌نامه‌های مستقل به میلیون یورو	۲۰۱۶	۲۰۱۷	۲۰۱۸	۲۰۱۹	۲۰۲۰
حق بیمه ناخالص صادرشده	۴۸.۸	۵۹.۹	۱۲۳.۸	۱۷۵.۱	۲۴۰.۰
حق بیمه کسب شده، بدون بیمه اتکایی	۳۰.۷	۳۸.۳	۶۳.۳	۹۰.۱	۹۸.۲
نگهداری	٪۶۲.۹	٪۶۳.۹	٪۵۱.۱	٪۵۱.۵	٪۴۰.۹
نسبت خسارت ناخالص	٪۹.۳	٪۱۱.۰	٪۲۵.۱	٪۴۷.۰	٪۴۲.۱
نسبت خسارت خالص	٪۱۳.۶	٪۱۵.۴	٪۲۰.۱	٪۳۶.۱	٪۴۳.۳

بررسی تجارب کشورها

شرکت‌های بیمه پیشرو از نظر درآمد در حق‌بیمه‌های صادر شده ناخالص در آلمان (میلیون یورو)

نام شرکت	۲۰۱۷	۲۰۱۸	۲۰۱۹	۲۰۲۰	۲۰۲۱
گروه آلیانز	۱۲۶۱۴۹	۱۳۰۵۵۷	۱۴۲۳۶۹	۱۴۰۴۵۵	۱۴۸۵۱۱
گروه مونیخ‌ری	۴۹۱۱۵	۴۹۰۶۴	۵۱۴۵۷	۵۴۸۹۰	۵۹۵۶۷
گروه تالانکس	۳۳۰۶۰	۳۴۸۸۵	۳۹۸۸۵	۴۱۱۰۵	۴۵۵۰۷
گروه آر پلاس وی	۱۵۳۳۸	۱۶۱۳۳	۱۷۳۹۸	۱۸۹۵۲	۱۹۱۸۴
بیمه دبکا	۱۳۱۳۷	۱۳۱۰۳	۱۳۴۸۰	۱۳۹۹۹	۱۵۳۸۶

بررسی تجارب کشورها

بازار بیمه سایبری در آلمان پیچیده و تاحدودی غیر شفاف است. تحلیل‌ها، حق بیمه‌های کم و رشد پراکنده در بازار را نشان می‌دهد که ناشی از عوامل مختلفی در سمت عرضه و تقاضای بازار است. به طور خلاصه، رشد پراکنده بازار تا حدی ریشه در شکست بازار دارد که این موضوع هم به دلیل عدم تقارن اطلاعات در سمت تقاضای بازار است. در ادامه به محدودیت‌ها به عنوان عوامل توضیحی شرایط کنونی بازار به تفکیک موانع در طرف عرضه و تقاضا پرداخته خواهد شد.

بررسی تجارب کشورها

محدودیت‌های رشد بازار بیمه سایبری عمومی در آلمان

محدودیت رشد بازار بیمه سایبری عمومی	
محدودیت‌های سمت عرضه	محدودیت‌های سمت تقاضا
مشکلات اکچوئری: • **کمبود داده‌های تجربی مناسب** • **دشواری محاسبه حق بیمه** • **کمبود متخصصان باتجربه**	عدم تقارن اطلاعات: عدم شفافیت پوشش عدم آگاهی عدم شفافیت و تنوع طرحهای موجود
مسائل مربوط به هزینه-فایده: • **ظرفیت تحمل ریسک/ ریسک نقدینگی**	تجزیه و تحلیل هزینه-فایده: ارزیابی منفی یا اشتباه
	نظارتی-قانونی: پیچیدگی صدور گواهی‌نامه

بررسی تجارب کشورها

پوشش‌های رایج بیمه‌نامه‌های سایبری در آلمان به ترتیب فراوانی

۱	بازیابی اطلاعات
۲	وقفه در کسب‌وکار (عدم‌النفع) سرقت یا از دست رفتن داده‌ها
۳	مسئولیت جریمه‌های قراردادی و مطالبات خسارت‌ها
۴	انتشار یا استفاده غیرمجاز از داده‌ها
۵	تحقیقات کشف جرم حفاظت‌های قانونی آسیب به شهرت

بررسی تجارب کشورها

انگلستان

سه عامل اساسی در بالا بردن **نرخ پذیرش بیمه سایبری در انگلستان**، رشد ریسک‌های سایبری، اعلام مقررات عمومی حفاظت از داده‌ها و افزایش آگاهی در مورد وقایع سایبری می‌باشد.

نفوذ بیمه سایبری در بین مشاغل انگلستان بسته به اندازه کسب‌وکار و نوع فعالیت متفاوت است. ۳۵ درصد از مشاغل بزرگ در انگلستان دارای بیمه سایبری هستند؛ در حالیکه تنها ۱.۲٪ از شرکت‌های خرد و کوچک بیمه سایبری دارند. از میان شرکت‌های متوسط هم حدود ۳۱٪ بیمه سایبری خریداری کرده‌اند که در مجموع حدود ۱۱ درصد از کسب‌وکارها در انگلستان بیمه سایبری دارند. همچنین بیمه‌های سایبری در بین شرکت-های بزرگ خدمات و فناوری مالی که با حجم زیادی از داده‌ها سر و کار دارند، رواج بیشتری دارد. ریسک‌های زنجیره تامین یکی از نگرانی‌های شرکت‌های بزرگ مقیاس است. به همین دلیل بیمه سایبری یکی از الزامات در قراردادهای تامین در صنایع خاصی مانند بازاریابی و تکنولوژی است.

بررسی تجارب کشورها

مطالعات نشان می‌دهند که بازار بیمه سایبری پوشش‌های گسترده‌ای را برای خطرات سایبری ارائه می‌دهد. به عنوان مثال می‌توان به موارد زیر اشاره کرد:

- وقایع مرتبط با حریم خصوصی: در این حوزه، پوشش بیمه‌ای برای هر دو بعد شخص اول مانند هزینه‌های اطلاع‌رسانی به مشتریان، راه‌اندازی مرکز تماس، جمع‌آوری و بررسی علت حادثه و ... و مسئولیت‌های شخص ثالث مانند خسارات نقض حریم خصوصی و یا هزینه‌های قانونی مرتبط، ارائه می‌شود.
- مسئولیت امنیت شبکه: پوشش‌هایی که در این بخش ارائه می‌شود شامل موارد زیر است: ۱) مسئولیت‌های شخص ثالث ناشی از رویدادهای امنیتی خاص که در شبکه فناوری اطلاعات سازمان رخ می‌دهد ۲) مسئولیت‌های شخص ثالث ناشی از حملاتی که از دارایی‌های فناوری اطلاعات سازمان به عنوان بخشی از یک حمله استفاده می‌شود ۳) مسئولیت‌های شخص ثالث ناشی از حملاتی که از دارایی‌های سازمان به عنوان مجرایی برای ارسال کدهای مخرب به شخص ثالث استفاده شده است.

بررسی تجارب کشورها

- آسیب به داده‌ها و نرم‌افزار: در صورت حذف یا خرابی داده‌ها یا نرم‌افزار، بیمه هزینه‌های کارشناسان خارج از سازمان را برای بازسازی داده‌ها و نرم‌افزار متقبل می‌شود.
- جرایم سایبری: شامل پوشش هزینه‌هایی است که ناشی از استفاده از رایانه برای ارتکاب کلاهبرداری یا سرقت پول، اوراق بهادار یا سایر اموال می‌باشد.
- اخاذی سایبری: شامل پوششی برای: ۱) هزینه کارشناسان خارج از سازمان برای رسیدگی به حادثه از جمله مذاکرات مربوط به باج و ۲) پرداخت مبلغ باج است.
- وقفه در کسب‌وکار (عدم النفع): پوششی برای جبران هزینه‌های ناشی از اختلال در شبکه سازمان است که می‌تواند باعث از دست رفتن سود بالقوه یا تحمیل هزینه‌های اضافی به سازمان شود.
- آسیب به دارایی‌های فیزیکی: در حال حاضر تعداد محدودی از شرکت‌های بیمه پوشش سایبری مستقلی برای این دسته از خطرات ارائه می‌دهند.
- آسیب به اعتبار سازمان: این پوشش نیز توسط تعدادی از شرکت‌های بیمه ارائه می‌شود؛ زیرا کشف ارتباط صریح بین رویداد سایبری و هزینه‌های ایجاد شده مانند کاهش مشتریان یا تراکنش‌های سازمان، مشکل است.
- پوشش هزینه‌های قانونی

بررسی تجارب کشورها

- پوشش‌های قبل از حادثه: بیمه سایبری به شرکت‌ها در مدیریت ریسک سایبری و جلوگیری از وقوع حوادث سایبری کمک می‌کند. بیمه‌گران دسترسی به متخصصان سایبری، سیستم-های هوش تهدید، تست‌های آسیب‌پذیری فناوری اطلاعات، آموزش کارکنان و ... را تسهیل می‌کنند .
- پوشش‌های بعد از حادثه: در صورت وقوع حادثه سایبری این پوشش پشتیبانی سریع توسط متخصصان سایبری را ارائه می‌کند. این متخصصان سیستم‌های شرکت را ارزیابی می‌کنند، منبع هرگونه حملات را شناسایی می‌کنند و اقدامات پیشگیرانه برای آینده را ارائه می‌دهند. همچنین راهنمایی‌های لازم در مورد الزامات قانونی و نظارتی و یا مراحل اطلاع‌رسانی به مشتریان را ارائه می‌دهند.

بررسی تجارب کشورها

بسیاری از استثنائات بیمه‌نامه‌های سایبری مانند استثنائات سایر بیمه‌نامه‌ها مانند جنگ و تروریسم است، اما یکسری از استثنائات مختص این بیمه‌نامه‌ها هستند که از آن جمله می‌توان به موارد زیر اشاره کرد:

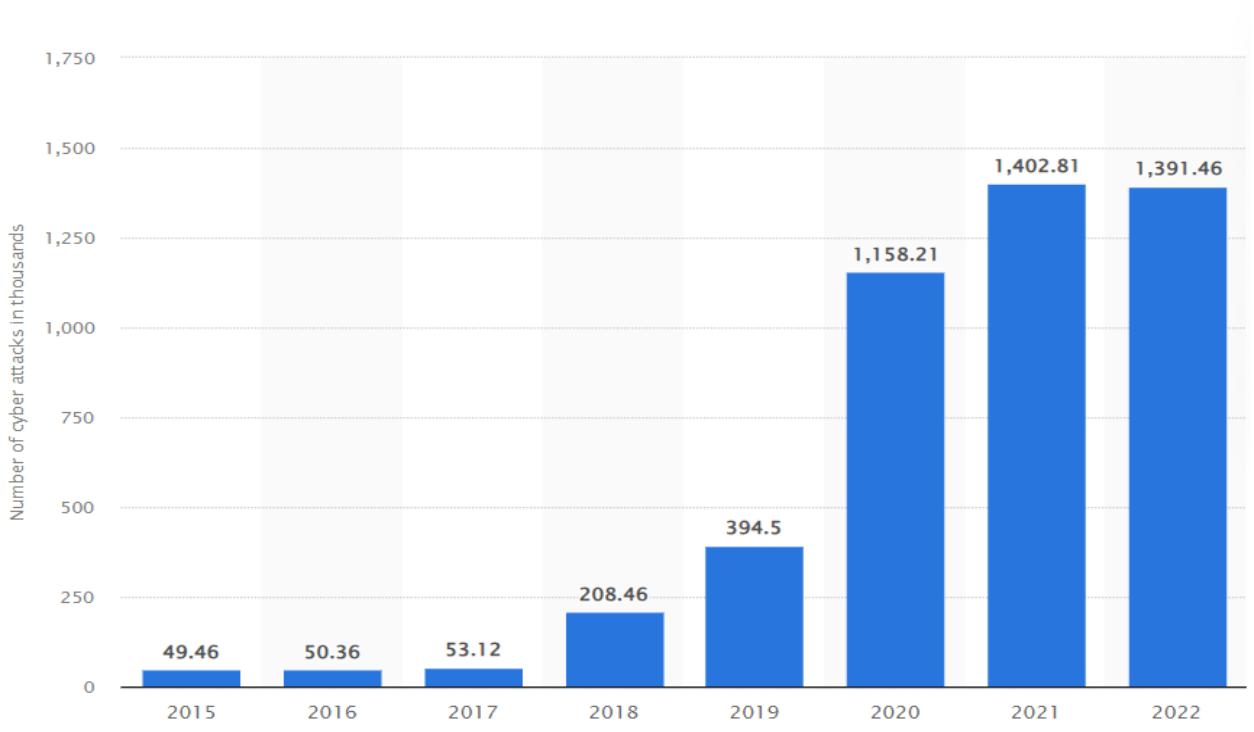
- صلاحیت دادگاه: به این معنی که بیمه‌های سایبری خریداری شده در انگلستان عموما پوششی برای اتحادیه اروپا و بعضی از نقاط دیگر جهان ارائه می‌کنند؛ در اغلب بیمه‌نامه‌ها آمریکای شمالی از محدوده پوشش بیمه‌ها مستثنی می‌شود.
- ادعاهای مطرح شده توسط افراد داخلی شرکت: به عنوان مثال اگر کارمندان داخل شرکت به دلیلی نقض اطلاعات شخصی خود به دنبال خسارت باشند، بیمه سایبری این خسارات را پوشش نخواهد داد.
- صدمات جانی و خسارت به اموال: عموما بیمه‌نامه‌های سایبری این موارد را تحت پوشش قرار نمی‌دهند و باید از بیمه‌نامه‌های دیگر مثل بیمه اموال یا مسئولیت برای پوشش این هزینه‌ها استفاده کرد.
- زیرساخت‌های حیاتی ملی: خسارات ناشی از قطعی زیرساخت‌های ملی مانند آب، برق، گاز، مخابرات و ... مستثنی هستند. این خسارات مانند جنگ و تروریسم دامنه بسیار بزرگی از شرکت‌ها را در بر می‌گیرند و جبران این زیان‌ها خارج از توان بیمه‌گران است.
- جنگ‌های سایبری: خسارات وارده به کسب‌وکارها ناشی از جنگ سایبری که به اقدامات یک کشور یا یک دولت خاص مرتبط باشد، به دلیل دامنه اثر وسیع، جزو استثنائات رایج بین بیمه‌گران است.
- جریمه‌ها و مجازات‌ها: بیمه‌های سایبری جرایم و هزینه‌های کیفری یا حقوقی که کسب‌وکار قانونا موظف به پرداخت آن است را پوشش نمی‌دهد.

البته این استثنائات در بین بیمه‌گران ممکن است متفاوت باشند.

بررسی تجارب کشورها

هند

تعداد حملات سایبری در هند از سال ۲۰۱۵ تا ۲۰۲۲ (به هزار)



بررسی تجارب کشورها

برخی از شرکت‌های ارائه‌دهنده بیمه سایبری

بسیاری از شرکت‌های بیمه در هند بیمه سایبری را با حق‌بیمه معقول ارائه می‌کنند. سرمایه تحت پوشش بیمه سایبری از ۱ میلیون روپیه تا ۱ کرور می‌باشد. برخی از شرکت‌هایی که در هند این بیمه را ارائه می‌دهند عبارتند از:

- HDFC Ergo
- Bajaj Allianz
- SBI General

بررسی تجارب کشورها

یک بیمه‌نامه سایبری معمولاً شامل پوشش‌های زیر است:

- نقض امنیت و نقض حریم خصوصی: یک بیمه‌نامه سایبری معمولا افشای اطلاعات محرمانه تجاری، اطلاعات شخصی، اطلاعات کارکنان یا اطلاعات برون‌سپاری شده توسط طرف بیمه شده به پیمانکاران، پیمانکاران فرعی، فروشندگان یا هر شخص ثالث دیگری را تحت پوشش قرار می‌دهد. بیمه سایبری در هند تمام هزینه‌هایی که طرف بیمه شده به طور قانونی موظف به پرداخت آن می‌شود، از جمله مسئولیت پرداخت هزینه‌ها و هزینه‌های حقوقی پس از نقض حریم خصوصی، را پرداخت می‌کند.
- خسارت سیستم: یک بیمه‌نامه ریسک سایبری هزینه‌های مربوط به بازیابی، تعمیر، یا جایگزینی هر یک از سوابق رایانه‌ای بیمه شده (یا هر سوابق رایانه‌ای دیگری که بیمه شده مسئول آن است) که از بین رفته، آسیب دیده، گم شده، تغییر کرده، تحریف یا پاک شده (و پس از جستجوی دقیق نمی‌توان آن‌ها را پیدا کرد) و در نتیجه مستقیم حملات سایبری بوده که برای اولین بار توسط بیمه شده کشف شده و در اسرع وقت در طول دوره بیمه‌نامه به طور کتبی به شرکت بیمه اعلام شده است، پرداخت می‌کند.

بررسی تجارب کشورها

- هک یا انتقال ویروس کامپیوتری: یک بیمه‌نامه مسئولیت سایبری در هند تمام هزینه‌هایی را که طرف بیمه شده از نظر قانونی موظف به پرداخت آن است پرداخت می‌کند؛ از جمله مسئولیت هزینه‌های شخص مدعی خسارت و هزینه‌های دفاعی و حقوقی ناشی از هرگونه ادعایی که علیه طرف بیمه شده و در اسرع وقت به طور کتبی به شرکت بیمه در طول دوره بیمه‌نامه گزارش شده و به عنوان نتیجه مستقیم هر گونه زیان مالی شخص ثالث بوده که مستقیماً از:
  - حمله ویروسی یا هک کامپیوتری که از سیستم‌های رایانه‌ای دارنده بیمه‌نامه به سایر رایانه‌ها منتشر شده و یا از طریق آنها آلوده شده‌اند، یا
  - حمله ویروسی یا هک کامپیوتری که دسترسی اشخاص ثالثی را که از طرف بیمه شده مجاز به دستیابی به چنین دسترسی هستند، محدود یا مانع از دسترسی به سیستم‌های رایانه‌ای دارنده بیمه‌نامه می‌شود، یا
  - از دست دادن یا سرقت اطلاعات بیمه‌گذار یا اطلاعاتی که بیمه‌گذار مسئول آن است یا ادعا می‌شود مسئول آن بوده است و مستقیماً از حمله ویروسی یا هک کامپیوتری ناشی می‌شوند.

بررسی تجارب کشورها

- مسئولیت چندرسانه‌ای: یک بیمه‌نامه سایبری تمام هزینه‌هایی را که طرف بیمه شده از نظر قانونی موظف به پرداخت آن است پرداخت می‌کند؛ از جمله مسئولیت هزینه‌های شخص مدعی خسارت و هزینه‌های دفاعی و حقوقی ناشی از هرگونه ادعایی که علیه طرف بیمه شده و در اسرع وقت به طور کتبی به شرکت بیمه در طول دوره بیمه‌نامه گزارش شده و به عنوان نتیجه مستقیم از:
  - توهین، تهمت یا افترا؛
  - تجاوز یا مداخله در حق حریم خصوصی، از جمله حقوق کارکنان، یا تصاحب نام‌های تجاری یا موارد مشابه؛
  - سرقت ادبی یا سوء استفاده از ایده‌ها؛
  - نقض قانون کپی رایت، نام دامنه، آرم یا عنوان تجاری، تضعیف یا نقض علامت تجاری، آرم یا برند خدمات

  که مستقیماً از:
    - ایمیل و محتوای اینترنتی تولید شده توسط دارنده بیمه‌نامه؛ یا
    - تبلیغات دارنده بیمه‌نامه؛ یا
    - محتوای دیجیتال شخص ثالث که توسط سیستم‌های رایانه‌ای دارنده بیمه‌نامه دانلود، به اشتراک گذاشته یا توزیع شده است.

بررسی تجارب کشورها

- پوشش اخاذی سایبری: یک بیمه‌نامه سایبری در هند هزینه‌های اخاذی سایبری را به دنبال یک تهدید امنیتی علیه طرف بیمه شده پرداخت می‌کند.
- وقفه در کسب‌وکار: یک بیمه‌نامه سایبری خسارت ناشی از وقفه در کسب‌وکاری که در طول دوره غرامت به عنوان نتیجه مستقیم یک رویداد سایبری در طول دوره بیمه‌نامه ایجاد شده است، پرداخت می‌کند.

بررسی تجارب کشورها

استثنائات بیمه‌نامه سایبری

- عدم امنیت - اگر سازمانی نتواند سیستم‌هایی با امنیت بالا برای حفاظت از داده‌های خود داشته باشد، هزینه حمله سایبری آنها توسط بیمه پوشش داده نمی‌شود.
- خطای انسانی - اگر حمله سایبری به دلیل سهل‌انگاری کارمند یا خطای مستقیم انسانی اتفاق بیفتد، خسارت آن پوشش داده نمی‌شود.
- حملات داخل سازمانی - اگر اختلال داخلی سازمان منجر به یک حمله سایبری شود یا کارمند فعلی یا سابق مسئول افشای اطلاعات باشد، بیمه سایبری مسئولیتی نخواهد داشت.
- ارتقای فناوری نامرتبط- هر پولی که صرف بهبود فناوری‌های موجود می‌شود تا از حملات یا هرگونه هزینه‌ای که مستقیماً با حمله مرتبط نیست، جلوگیری شود، تحت پوشش قرار ندارد.
- آسیب‌پذیری‌های گذشته - حملات یا تهدیدات سایبری که به دلیل آسیب‌پذیری‌های قبلی که ممکن است شرکت از آنها آگاه باشد، ایجاد می‌شود، تحت پوشش قرار ندارند.
- خسارات مضاعف یا تشدید شده – خساراتی که توسط بیمه‌گذار تشدید شده باشد، تحت پوشش قرار ندارند.
- صدمات بدنی / خسارت به اموال.
- مسئولیت ناشی از حملات رخ داده قبل از شروع بیمه‌نامه.
- مسئولیت‌هایی که در قرارداد برای بیمه‌گذار ذکر شده است.
- خسارت غیر قابل شرح از هر نوع.
- جمع‌آوری داده‌ها بدون مجوز.

بررسی تجارب کشورها

حق‌بیمه سایبری

میزان حق‌بیمه سایبری در هند به عوامل زیر بستگی دارد:

- گردش مالی شرکت؛
- میزان قلمرو و حوزه‌های قضایی تحت پوشش؛
- پوشش‌های موردنیاز؛
- تجربه خسارات گذشته شرکت؛
- صنعتی که شرکت به آن تعلق دارد.

بررسی تجارب کشورها

نحوه نرخ‌گذاری بیمه‌نامه سایبری

هنگام محاسبه نرخ بیمه‌نامه موارد متعددی مورد بررسی قرار می‌گیرند که برخی از آنها عبارتند از:

- تجربیات گذشته یک شرکت: آیا قبلاً با افشای اطلاعات مواجه شده است یا خیر. این مورد می‌تواند ریسک‌های احتمالی را تا حدی مشخص کند؛
- صنعتی که شرکت در آن فعالیت می‌کند؛
- نوع داده‌هایی که شرکت با آنها سروکار دارد؛
- میزان امنیت آنلاین آنها؛
- گردش مالی سالانه شرکت: اگر شرکت سود خوبی داشته باشد، می‌تواند بسیاری از زیان‌ها را به تنهایی جبران کند؛
- سیستم‌های مدیریت داده ایجاد شده و گزارش‌های PII و PHI شرکت؛
- سیستم‌های مدیریت داده‌های موجود و معایب آن‌ها؛
- شبکه‌ها و ارتباطات شرکت؛
- شهرت شرکت در بازار و نحوه ارتباط با مشتریان.

Personally Identifiable Information
Protected Health Information

بررسی تجارب کشورها

نحوه ادعای خسارت تحت بیمه سایبری

در کشور هند روند خسارت بیمه سایبری مشابه سایر بیمه‌های عمومی است:

- به محض وقوع خسارت به شرکت بیمه اطلاع داده شود.
- بیمه‌گر یک متخصص سایبری را برای تجزیه‌وتحلیل و تعیین میزان ریسک و خسارت اعزام می‌کند.
- بیمه‌گذار و هم بیمه‌گر در مورد جزئیات حمله سایبری بحث می‌کنند.
- جزئیات حمله و مختصری از راه‌حل‌های ممکن بر اساس شدت حمله به بیمه‌گذار ارائه می‌شود.
- بر اساس انتخاب بیمه‌گذار، بیمه‌گر خسارت را طبق بیمه‌نامه سایبری پرداخت می‌کند.

بررسی تجارب کشورها

فرآیند ادعای خسارت

در اغلب شرکت‌های بیمه هند که بیمه سایبری ارائه می‌کنند، فرآیند خسارت به صورت زیر می‌باشد:

- به محض اطلاع از کلاهبرداری یا حمله سایبری احتمالی، به پلیس امنیت سایبری اطلاع داده شود.
- در اسرع وقت به شرکت بیمه اطلاع داده شود.
- در هنگام ثبت خسارت از فرمت کتبی استفاده شود.
- ادعای خسارت ظرف ۹۰ روز ارسال شود.
- مدارک ادعای خسارت به شرکت ارائه گردد.
- ادعای خسارت توسط بازپرس معرفی شده از طرف شرکت بیمه تأیید شود.
- پس از تأیید مدارک، اگر خسارت نیز تایید شد، پرداخت خواهد شد.
- در صورتی که ادعای خسارت قابل قبول نباشد، رد شده و به بیمه‌گذار اطلاع داده خواهد شد.
- در موردی که مدعی خسارت احساس کند که رای صادره مورد رضایت او نبوده، می‌تواند درخواست بررسی مجدد نماید.

بررسی تجارب کشورها

با وجود 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 به سرعت در حال تحول است و با افزایش حملات سایبری، آگاهی از ریسک و تقاضا برای بیمه سایبری نیز افزایش یافته است. با این حال، بیشتر مشاغل و افراد، بیمه نشده یا به میزان کافی تحت پوشش قرار نگرفته‌اند، و حق‌بیمه 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.

بررسی تجارب کشورها

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.

بررسی تجارب کشورها

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.

بررسی تجارب کشورها

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.

با سپاس از شما