پژوهشکده بیمه

گزارش موردی ۷۹

آذر و دی ۱۴۰۲

بیمه سایبری: تقویت تاب‌آوری برای تحول دیجیتال

گزارش موردی

دوماهنامه آموزشی، پژوهشی، تحلیلی

پژوهشکده بیمه، سال دوازدهم، شماره ۵، آذر و دی ۱۴۰۲، دوره جدید، شماره مسلسل ۷۹

صاحب امتیاز: پژوهشکده بیمه

مدیر مسئول: دکتر یعقوب محمودیان

سردبیر: دکتر محمد مهدی عسگری

این نشریه به‌موجب نامه شماره ۸۹/۲۲۴۸۲ مورخ ۸۹/۹/۲۸ وزارت فرهنگ و ارشاد اسلامی دارای مجوز نشر به

عنوان دوماهنامه آموزشی، پژوهشی، تحلیلی در زمینه علوم انسانی (مدیریت بیمه) می‌باشد.

مدیر داخلی: دکتر شبنم رفوآ

صفحه آرا و طراح جلد: علی حسین صفری

نشانی نشریه: تهران- سعادت آباد- میدان شهید تهرانی مقدم (کاج) - خیابان سرو غربی- پلاک ۴۳

صندوق پستی: ۴۴۹۹- ۱۹۳۹۵

تلفن: ۲۲۰۸۴۰۸۴

دورنگار: ۲۲۰۹۲۲۶۵

Workingpaper@irc.ac.ir

چاپخانه:دانشگاه امام صادق

کلیه حقوق برای ناشر، محفوظ و استفاده از مطالب با ذکر مأخذ، مجاز است. مسئولیت مقالات چاپ شده بر عهده نویسنده و مترجم است و مطالب آن لزوماً بیانگر دیدگاه‌های پژوهشکده بیمه نیست. گزارش موردی در پذیرش و ویرایش مقالات آزاد است.

شناسنامه عمومی گزارش موردی	
عنوان گزارش	بیمه سایبری: تقویت تاب‌آوری برای تحول دیجیتال
عنوان انگلیسی	Cyber insurance: strengthening resilience for the digital transformation
سال نشر	۲۰۲۲
مترجم	دکتر سمیه میره
ویراستار علمی	دکتر اسماء حمزه
ویراستار ادبی	امید شعبانی
شمارگان	آذر و دی/گزارش موردی شماره ۷۹

پیشگفتار

چشم‌انداز تهدیدات سایبری به سرعت در حال تغییر و تحول است و با افزایش حملات سایبری، آگاهی از ریسک و تقاضا برای بیمه سایبری نیز افزایش یافته است

چشم‌انداز تهدیدات سایبری به سرعت در حال تغییر و 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 حق بیمه سایبری تنها کسری از کل خسارات ناشی از حملات سایبری است. برآوردها نشان می‌دهد که حدود ۹۰ درصد از افراد و سازمان‌ها تحت پوشش قرار نگرفته‌اند. این میزان، اشاره به وجود پتانسیل رشدی بزرگ در بازار بیمه سایبری دارد، اما این کار به سادگی انجام پذیر نبوده و لازم است که این اطمینان حاصل شود که راه حل‌های کافی برای حفاظت از ریسک‌های سایبری وجود دارد تا جامعه بتواند در برابر ریسک سایبری تاب‌آوری داشته باشد و این تلاش مستلزم همکاری بین کسب و کارها، صنعت بیمه و دولت است.

اولین نیاز در توسعه بیمه سایبری، بهبود کیفیت داده‌ها و مدل‌سازی آنها است. به دلیل کمبود داده‌های استاندارد و محدودیت‌های موجود در مدل‌سازی، کمی‌سازی ریسک‌های سایبری دشوار است. ریسک‌های آتی معمولاً بر اساس داده‌های گذشته‌نگر استنباط می‌شوند، اما این رویکرد در محیطی که ریسک‌های سایبری به سرعت در حال تغییر هستند، ارزش کمی دارد. شرکت‌های بیمه نیز باید بر نیروی کار متخصص سایبری سرمایه‌گذاری کنند تا به تقویت مهارت‌های بیم‌سنجی، فنی و حقوقی مورد نیاز برای چرخه‌های بیمه‌گری و مدیریت خسارت کمک شود.

دومین نیاز، بروزرسانی 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.

با توجه به اهمیت چالش‌های سایبری در عصر دیجیتال، این شماره از گزارش موردی به بیمه سایبری: تقویت تاب‌آوری برای تحول دیجیتال اختصاص یافته است. در این گزارش ضمن تبیین چشم‌انداز ریسک سایبری، مدیریت ریسک با بیمه سایبری، پرداختن به ریسک کل و سایر محدودیت‌های بیمه‌پذیری مورد بررسی قرار گرفته است.

در اینجا لازم است از خانم دکتر سمیه میره به عنوان مترجم و خانم دکتر اسماء حمزه به عنوان ویراستار علمی و همچنین از رئیس اداره کتابخانه، اسناد علمی و نشریات و همکاران ایشان سپاسگزاری نمایم.

محمدمهدی عسگری

رئیس پژوهشکده بیمه

فهرست مطالب

خلاصه اجرایی

ریسک‌های سایبری با بی‌ثباتی ژئوپلیتیکی و اقتصادی و با افزایش اتکای جامعه به فناوری‌های دیجیتال، افزایش یافته است.

بی‌ثباتی ژئوپلیتیکی و اقتصادی در دنیای امروز درحال افزایش است. این امر محرک‌های بسیاری دارد که برجسته‌ترین آن‌ها جنگ اوکراین و تنش‌های موجود بین ایالات متحده و چین است. با توجه به سرعت دیجیتالی شدنِ بسیاری از امور زندگی، افزایش حملات سایبری خارج از انتظار نیست. حملات سایبری کشورها با استفاده از حمله به تأسیسات زیرساختی کشورهای دیگر مانند شبکه‌های برق یا نظام‌های ارتباطی کلیدی آن‌ها و غیره، می‌تواند پیامدهای فاجعه‌باری برای سازمان‌ها، اقتصاد کشور و به‌طور وسیع‌تر، در جامعه داشته باشد.

حملات سایبری پیچیده‌تر شده و به‌سرعت درحال افزایش و تکامل است.

تاکنون حمله نظامی فاجعه‌باری رخ نداده است. بااین‌وجود، ریسک سایبری با استفاده از حملات باج‌افزاری و نگرانی‌های کسب‌وکارها و دولت‌ها درخصوص امنیت سایبری، در حال افزایش است. شرکت مک‌آفی (McAfee) خسارات مالی جهانی ناشی از جرایم سایبری در سال ۲۰۲۰ را حدود ۹۴۵ میلیارد دلار تخمین می‌زند. حملات سایبری پیچیده‌تر شده و هکرها اکنون از تکنیک‌های «اخاذی سه‌گانه[1]» استفاده می‌کنند و به‌وسیله باج‌افزارها، امکان ورود مجرمان به نظام را به‌راحتی فراهم می‌کنند. شرکت‌های کوچک و متوسط[2] (SME) به‌علت داشتن سیستم دفاعی ضعیف، سریع‌تر در معرض مجرمان سایبری قرار می‌گیرند، درحالی‌که دیجیتال شدن صنایع بزرگ ازجمله بخش‌های مربوط به خدمات درمانی و زیرساخت‌های حیاتی، آسیب‌پذیری‌ها را در کل زنجیره تأمین افزایش داده است.

تلاش‌های مدیریت ریسک در پاسخ به این امر افزایش یافته و بیمه نقش کلیدی در این زمینه ایفا می‌کند و بازار به‌سرعت در حال رشد است ...

1. Triple extortion
2. Small and medium-sized enterprises

قبل‌از حمله NotPetya در سال ۲۰۱۷، ریسک‌های سایبری اغلب در حوزه افشای اطلاعات و مسئولیت شخص ثالث رخ می‌داد. در شرکت‌های بیمه/اتکایی، گسترش قانون حفظ حریم خصوصی داده‌ها باعث کشیده شدن دعاوی به دادگاه‌ها شده و منجر به طولانی شدن روند برخورد با ریسک سایبری شده است. در دو سال گذشته، خسارت واردشده به شخص اول به‌جای شخص ثالث، بیشتر مورد توجه بوده و به همین منظور، شرکت‌ها، بیمه‌گران و مقامات دولتی تلاش‌های زیادی در مدیریت ریسک‌های سایبری نموده و انجمن‌های صنعتی و بیمه‌گران برای رسیدگی به موضوعات مرتبط با «سایبری خاموش[1]»، با یکدیگر همکاری کرده‌اند. بیمه نقش کلیدی در این زمینه ایفا کرده و نه‌تنها در انتقال ریسک، بلکه در ایجاد انگیزه کاهش ریسک، حمایت از نظارت و پاسخ به ریسک مناسب، مؤثر عمل می‌کند.

... اما بازار در مقایسه با خسارت‌های اقتصادی، کوچک باقی می‌ماند.

اما استفاده از بیمه در پوشش خسارت احتمالی، همچنان با نواقصی همراه بوده و حق بیمه تنها بخشی از کل خسارات ناشی از حملات سایبری را پوشش می‌دهد. اکثر شرکت‌ها، دارای بیمه سایبری نیستند یا از پوشش بیمه‌ای مناسب برخوردار نمی‌باشند. در یک نظرسنجی که اخیراً انجام شده است، تنها ۵۵ درصد از کسب‌وکارها دارای پوشش سایبری بوده و کمتر از یک شرکت از هر پنج شرکت، دارای پوششی بالاتر از میانگین تقاضای باج‌افزارها بوده است. به‌طور تقریبی، کل خسارات ناشی از یک حمله سایبری در شرکت‌های کوچک و متوسط، به‌طور نسبی سه برابر بیشتر از شرکت‌های بزرگ است. علاوه‌بر این، در شرکتی با گردش مالی کمتر از ۵۰ میلیون دلار، هزینه‌های قانونی[2] معمولاً از ۲۰۰۰۰ تا ۱۰۰۰۰۰ دلار تغییر می‌کند.

بیمه‌گران به افزایش خسارات باج‌افزارها رسیدگی کرده
و اکنون باید با رویدادهای فاجعه‌بار مقابله کنند.

افزایش حملات باج‌افزارها، باعث افزایش ضریب خسارت در سال ۲۰۲۰ شد. بیمه‌گران با افزایش قیمت‌ها، بهبود شرایط بیمه‌نامه، معرفی محدودیت‌های فرعی و بیمه مشترک، شفاف‌سازی شرایط و

۱: Silent cyber خسارات احتمالی مرتبط با سایبری در بیمه‌نامه‌های سنتی اموال و مسئولیت که به‌طور خاص برای پوشش ریسک سایبری طراحی نشده‌اند.

2. Forensic costs

ضوابط، و استثناها- یا قیمت‌گذاری صریح - سعی در برخورد با چنین ریسک‌هایی کردند. این اقدامات تاحدی موفقیت آمیز بوده و منجر به کاهش ضریب خسارت در سال ۲۰۲۱ شد.

ریسک‌های سایبری تمام ویژگی‌های بیمه‌پذیر بودن را ندارند که این امر رشد بالقوه بازار را محدود می‌کند.

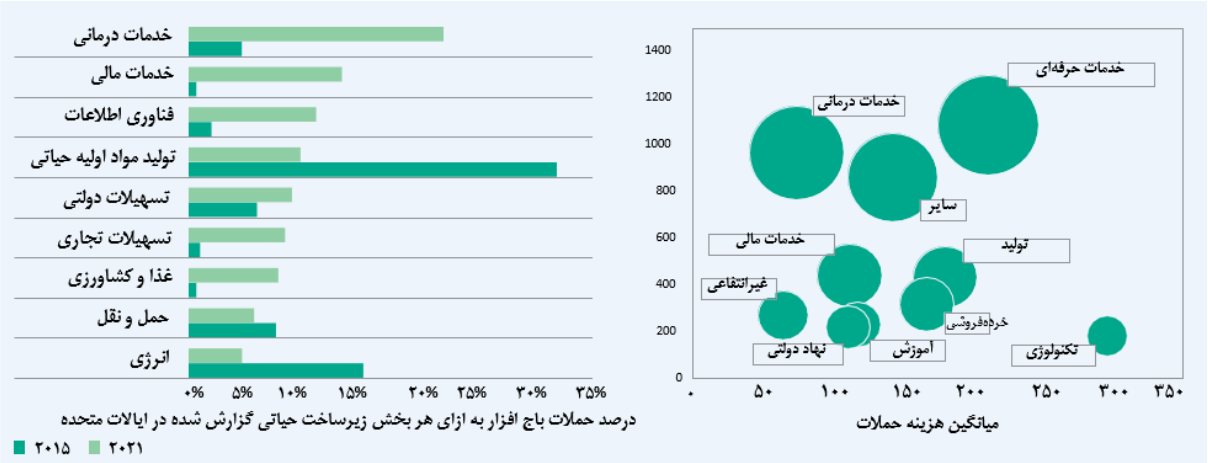
برخی از ریسک‌های سایبری امروزی با ویژگی‌های معمولی بیمه‌پذیر بودن مطابقت ندارند و نمی‌توان آن‌ها را بیمه نمود. در بسیاری از حملات سایبری، اطلاعاتی به سرقت می‌رود که قابل برآورد نبوده و حتی مدل مشخص و معینی به‌منظور برآورد و بیمه نمودن آن‌ها وجود ندارد. بنابراین، تعیین میزان کمّیِ این نوع ریسک‌ها بسیار دشوار می‌باشد. بیمه‌پذیری محدود با وجود تقاضای روبه‌رشد بیمه سایبری، چالش‌هایی را برای رشد بازار در بلندمدت ایجاد می‌کند. برای رفع این محدودیت‌ها، افزایش دانش سایبری، استفاده از داده‌های استاندارد، مدل‌سازی بهتر، ثبات بیشتر در بیمه‌نامه‌های سایبری و منابع جدید سرمایه‌گذاری، مورد نیاز است. به همین ترتیب، باید زمینه را برای ایجاد فرصت‌های مشارکت عمومی- خصوصی فراهم نمود. این اقدامات می‌تواند به کاهش مواجهه کلی با ریسک، بهبود درک ریسک و تاب‌آوری جامعه در برابر حملات با پیامدهای مخرب و بالقوه نظامی کمک کند. حملات سایبری، ماهیت انسانی و شبکه‌ای داشته و به‌طور مداوم در حال تکامل بوده و نیاز به یک واکنش هماهنگ دارند. افزایش تاب‌آوری در این زمینه نیز مستلزم همکاری بین شرکت‌ها، بیمه‌گران و دولت‌ها است.

نکات کلیدی

افزایش استفاده از فضای دیجیتال ناشی از بیماری کووید- ۱۹، آسیب‌پذیری‌های سایبری جدیدی را ایجاد کرده است.

حملات باج‌افزاری گزارش‌شده و شدت آن‌ها در سال‌های اخیر افزایش یافته، به‌صورتی که برآورد میزان خسارات جهانی حملات سایبری در سال ۲۰۲۰ حدود ۹۴۵ میلیارد دلار عنوان شده است. انواع حملات سایبری و هدف‌های مورد نظر آن‌ها نیز دائماً درحال تکامل می‌باشند. مجرمان سایبری

اغلب شرکت‌های کوچک و متوسط به‌ویژه در بخش خدمات درمانی، حرفه‌ای و خدمات مالی را مورد حمله قرار داده‌اند. دیجیتالی شدن صنایع، ازجمله بخش خدمات درمانی و زیرساخت‌های حیاتی، آسیب‌پذیری سایبری را در کل زنجیره تأمین افزایش داده است.



منبع: (چپ)

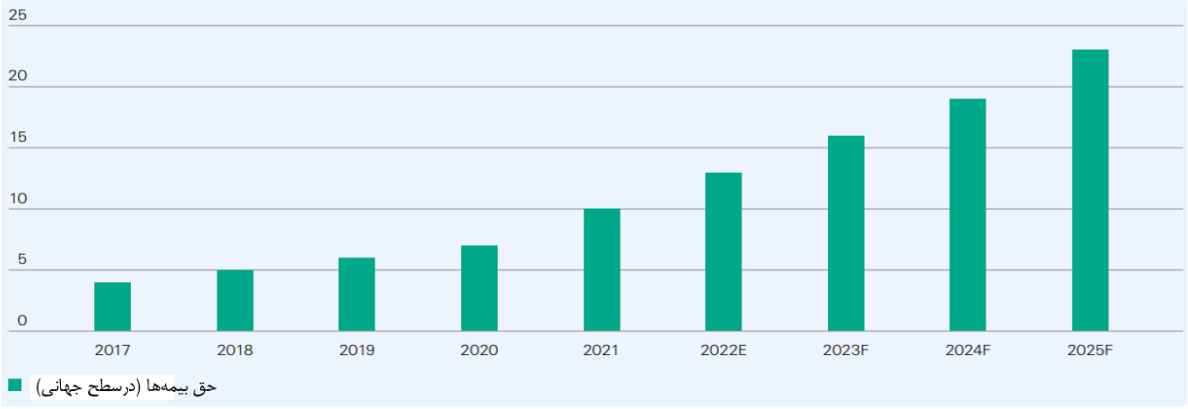
DHS NCCIC/ICS-CERT Year in Review, Department of Homeland Security, 2015; Internet Crime Complaint Center Federal Bureau of Investigation, Swiss Re Institute estimates;

(راست)

Cyber claims study report, NetDiligence, 2021; Swiss Re Institute estimates

همچنین، بازار بیمه سایبری به‌سرعت در حال رشد بوده است.

تلاش‌های مدیریت ریسک و حق بیمه‌های بیمه سایبری در پاسخ به افزایش حملات، به حدود ۱۰ میلیارد دلار در سطح جهانی در سال ۲۰۲۱ گسترش یافته‌اند. ریسک‌های سایبری در اصل حول محور افشای اطلاعات و مسئولیت شخص ثالث متمرکز شده‌اند، اما حملات باج‌افزاری، آسیب‌ها را به کسب‌وکار اصلی و مسئولیت شخص اول تغییر داده است. انتظار داریم که حق بیمه تا سال ۲۰۲۵ به ۲۳ میلیارد دلار افزایش یابد، اما بااین‌وجود، بازار نسبت به ریسکی که به‌سرعت درحال تکامل است، کوچک باقی می‌ماند.



توجه: E = برآوردها، F= پیش‌بینی‌ها. برآوردها/پیش‌بینی‌های Swiss Re شامل بیمه‌نامه‌های سایبری مستقل و پکیجی می‌باشد.

منبع: موسسه Swiss Re

سودآوری بیمه سایبری با افزایش سرسام‌آور حملات باج‌افزاری کمتر شده و با انجام اقداماتی در بیمه‌نامه‌ها تثبیت شده است.

ضریب خسارت بیمه‌نامه‌های سایبری مستقل ایالات متحده در سال ۲۰۲۰ افزایش یافت. در سال ۲۰۲۱ در نتیجهٔ افزایش قیمت‌ها، استانداردهای سخت‌گیرانه‌تر بیمه‌نامه‌ها مانند الزامات احراز هویت چندعاملی، و شرایط و ضوابط سخت‌گیرانه‌تر ازجمله بیمه‌نامه مسئولیت محدود و بیمه‌نامه مشترک، ضریب خسارت بهبود یافته است؛ اما همچنان به‌دلیل خسارت‌های زیان‌بار احتمالی نظامی مقدار بالایی داشت.

منبع: National Association of Insurance Commissioners, S&P Global, Swiss Re Institute calculations

ریسک کل تنوع‌ناپذیر[1] و ماهیت ریسک سایبری که به‌سرعت در حال تغییر است، منجر به افزایش عدم اطمینان و دعوت به راه‌حل‌های جدید در این حوزه می‌شود.

این راه‌حل‌ها شامل تلاش‌های هماهنگ صنعت برای استانداردسازی داده‌ها و زبان بیمه‌نامه‌ها است. افزایش ظرفیت مدل‌سازی بهبودیافته (هم سناریومحور و هم مبتنی بر تجزیه‌وتحلیل داده) و ارتقاء مهارت‌های سایبری، به رفع کاستی‌های کمی در این زمینه کمک می‌کند. در مجموع، این امر به کاهش عدم اطمینان منجر شده، پایه‌ای را برای جذب منابع جدید سرمایه ایجاد می‌کند و درنتیجه بازار اوراق بهادار مرتبط با بیمه سایبری[2] (ILS) را فعال می‌نماید.

بررسی معیارهای بیمه‌پذیری بیمه سایبری

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
معیارهای بیم‌سنجی	فراوانی و شدت ریسک باید به‌طور معقولی قابل اندازه‌گیری باشد.	ریسک سایبری درحال تحول بوده و داده‌های کمی ثبت شده‌اند. قربانیان حملات سایبری، دولت‌ها، شرکت‌های امنیتی و غیره ممکن است از پرداختن به جزئیات به‌منظور اهداف امنیتی خودداری کنند. به‌عمد، ماهیت حملات به‌طور مداوم درحال تغییر است تا از تجزیه‌وتحلیل و کاهش آن فرار کنند. مدل‌های سایبری در مراحل ابتدایی خود باقی مانده و توسعه نمی‌یابند.	خلق نوآوری به‌منظور ایجاد پایگاه داده جمعی (تلفیقی)، بهبود استانداردسازی برای مدل‌سازی و تجزیه‌وتحلیل، و تعریف شفاف مواردی که جزء یک حمله سایبری هستند (توصیه ۱).
	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 قبلاً توضیح داده شد، می‌تواند کمک کند.

1 Undiversifiable aggregation risk
2 Insurance linked securities

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
	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[1] (خسارت‌هایی غیر از خسارات فجایع یا مواجهه‌های بزرگ) جدا کنید.
	متوسط مقدار خسارت در هر رخداد قابل پیش‌بینی باشد و تعداد زیادی از رخدادهای خسارت مشابه در سال اتفاق بیفتد.	اساس بازار بیمه سایبری به‌خوبی تثبیت شده است.	افزایش نرخ جذب بیمه در بخش‌ها و اندازه شرکت‌ها؛ جداسازی ریسک‌های فاجعه‌آمیز از خسارت‌های فرسایشی.
	کمبود اطلاعات نامتقارن[2] در این حوزه (به‌عنوان مثال، کژمنشی یا مخاطرات اخلاقی[3]، کژگزینی/ انتخاب نامطلوب[4])	تجربه و استانداردهای مربوط به اشتراک‌گذاری و کاهش میزان حملات درحال تکامل است.	بیمه مشترک، استانداردهای کاهش میزان حملات، اشتراک‌گذاری داده‌ها، منابع مدیریت بحران
معیارهای بازار	برای یک بازار بیمه پایدار، حق بیمه باید از نظر پوشش ریسک، کافی باشد.	میزان خسارت واردشده 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 مؤثر است (توصیه ۲).

منبع:

C. Biener, M. Eling, J.H Wirfs, Insurability of Cyber Risk – An Empirical Analysis, University of St. Gallen, 2015; C. Christophe, P. Liedtke, "Insurability, its limits and extensions", Insurance Research and Practice, vol 18 (2), 2002; B. Berliner, Limits of Insurability of Risks, 1985

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

چشم‌انداز ریسک سایبری

حوادث سایبری: شدیدتر و پیچیده‌تر

با استفاده بیشتر از فضای دیجیتال، احتمال رخداد ریسک‌های سایبری نیز افزایش می‌یابد.

پیش‌بینی می‌شود که تغییرات دیجیتالی که در زندگی و پس از همه‌گیری ویروس کرونا تسریع شده است، نحوه عملکرد جامعه را در دهه‌های آینده تغییر دهد: تغییراتی در روش فعالیت‌ها، کسب‌وکار، نحوه مصرف، آموزش فرزندان، مدیریت و منبع انرژی و استفاده از حمایت‌های پزشکی. گسترش فضای دیجیتال، احتمال رخداد ریسک‌های سایبری را نیز افزایش می‌دهد. از سوی دیگر، سرعت تغییرات فناورانه، افزایش آگاهی از ریسک‌های سایبری و اتخاذ شیوه‌های امنیت سایبری به‌منظور حفظ امنیت داده‌ها و اطلاعات، با هم هماهنگ عمل نمی‌کنند. همچنین، به نظر می‌رسد که نظام‌ها و پروتکل‌های امنیتی منسوخ شده، نظام‌های فناوری اطلاعات و چارچوب‌های نظارتی نیز نمی‌توانند هم‌زمان با تغییرات فناورانه به‌روز شوند. همین مسئله باعث می‌شود که هکرها به دنبال سوءاستفاده از آسیب‌پذیری‌های دیجیتال برای منافع مالی، شهرت یا ژئوپلیتیک باشند.

دامنه و فراوانی ریسک‌های سایبری در حال افزایش است. باج‌افزارها ریسک اصلی در کسب‌وکارها محسوب می‌شوند.

دامنه و فراوانی حملات سایبری در حال افزایش است و امروزه باج‌افزارها به‌عنوان ریسک اصلی برای کسب‌وکارها شناخته می‌شوند. در سال ۲۰۲۲، حملات سایبری برای اولین بار، در صدر ریسک‌های عنوان‌شده در گزارش Allianz و پیش‌از ریسک‌های وقفه در کسب‌وکار و فجایع طبیعی قرار گرفت[۱]. شرکت امنیت رایانه‌ای مک‌آفی، مجموع هزینه سالانه جرایم سایبری را در سال ۲۰۲۰، ۹۴۵ میلیارد دلار تخمین زد[۲]، که دوسوم آن را می‌توان به سرقت مالکیت معنوی و جرایم مالی نسبت داد، درحالی‌که هزینه‌های مستقیم[۳] مربوط به چهار نوع از رایج‌ترین حوادث سایبری در ایالات متحده از سال ۲۰۱۶ به‌طور متوسط به ۱۰۰،۰۰۰ دلار در هر حادثه رسیده است[۴]. تنها با نگاهی به باج‌افزار

1. Allianz Risk Barometer 2022, Allianz Global Corporate & Specialty, January 2022.
2. Z. Smith, E. Lostri, The Hidden Costs of Cybercrime, McAfee, December 2020.
۳. هزینه مستقیم شامل هزینه کسب‌وکار ازدست‌رفته، زمان، دستمزدها، پرونده‌ها، تجهیزات، یا خدمات جبرانی برای شخص ثالث نمی‌شود.
4. D. Garcia-Diaz, K. Walsh, Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, Government Accountability Office, June 2022.

NetDiligence می‌توان متوجه شد که ۷۰ درصد از حملات باج‌گیری انجام‌شده از سال ۲۰۱۷، در دو سال گذشته رخ داده‌اند که شدت آن در سال ۲۰۲۱ به بالاترین حد خود رسیده است (میانگین میزان باج ۷۵۰,۰۰۰ دلار آمریکا، بیش از دو برابر رقم سال ۲۰۲۰)[۱]. در یک نظرسنجی از رهبران برتر سایبری جهان که اخیراً انجام شده، ۵۰٪ عنوان کردند که یکی از بزرگ‌ترین نگرانی‌های آن‌ها در حوزه ریسک سایبری، حملات باج‌افزاری است و به دنبال آن حملات مهندسی اجتماعی و فعالیت‌های مخرب داخلی[۲] قرار دارند (جدول ۱ را ببینید)[۳].

حملات باج افزاری پیچیده‌تر می‌شوند.

با پیشرفت فناوری، پیچیدگی حملات باج افزاری به‌طور قابل توجهی افزایش یافته است. درحالی‌که پیشرفت در تجزیه‌وتحلیل هوش مصنوعی (AI) منجر به گسترش قابلیت‌های حمله و دفاع شده است، ظهور رمزارزها باعث شده دریافت و سرقت پول از افراد، راحت‌تر و ردیابی آن‌ها پیچیده‌تر شود[۴]. هکرهای باج‌افزاری اکنون از سه شگرد اخاذی استفاده می‌کنند. آن‌ها داده‌ها و اطلاعات یک شرکت را رمزگذاری کرده و دو بار از آن‌ها باج دریافت می‌کنند- بار اول برای رفع انسداد نظام شرکت و بار دوم برای عدم افشای داده‌ها (اخاذی دوگانه)[۵]. سپس هکرها می‌توانند از داده‌های سرقت‌شده برای استخراج باج سوم از صاحب اصلی آن (اخاذی سه‌گانه)[۶] استفاده کنند. گاهی اوقات هکرها حمله خود را تا زمانی که شرکت پروتکل‌های امنیتی خود را اصلاح نکند، ادامه می‌دهند (اخاذی مجدد)[۷].

---

1. Ransomware 2022 Spotlight Report, NetDiligence, 2022.

۲. مانند کارکنان فعلی یا سابق یک سازمان، پیمانکاران یا شرکای تجاری مورد اعتماد که از دسترسی مجاز خود به دارایی‌های حیاتی سوءاستفاده کرده و بر سازمان تأثیر منفی می‌گذارند.

۳. در این گزارش، رهبران سایبری ارشدترین مدیران بخش خصوصی و دولتی در ۲۰ کشور هستند. مراجعه کنید به:
Global Cybersecurity Outlook ۲۰۲۲, World Economic Forum, January ۲۰۲۲

4. K. Ramachandran, Cybersecurity issues in the AI world – Using AI to address AI-driven cyber attacks, Deloitte, September 2019.

۵. اگر قربانی باج را پرداخت نکند، مهاجم می‌تواند داده‌های قربانی را به‌صورت برخط در وب تاریک افشا کند یا از داده‌های دزدیده‌شده برای سوءاستفاده از آسیب‌پذیری‌ها استفاده کند.

۶. به‌عنوان مثال، این اتفاق در شرکت فنلاندی واستامو در سال ۲۰۲۰ رخ داد، زمانی که هکرها داده‌ها را به سرقت بردند، از شرکت باج گرفتند و همچنین به بیماران ایمیل زدند و تهدید کردند که سوابق سلامت روانی آن‌ها را افشا می‌کنند، مگر اینکه قربانی باج ۲۰۰ یورویی به‌صورت بیت کوین پرداخت کند. مراجعه کنید به: R. Sen, "Opinion: Hacking and data theft are mostly about making a buck not espionage", Houston Chronicle, May ۲۰۲۱.

۷. برای مثال، سه گروه باج‌افزار مجزا موفق شدند بین آگوست تا دسامبر ۲۰۲۰ به سیستم‌های شرکت مهندسی آلمانی ThyssenKrupp نفوذ کنند. مراجعه کنید به: "ThyssenKrupp suffers ransomware attack for the third time", Security Report, ۱February ۲۰۲۱.

خسارت‌های مالی ناشی از افشای اطلاعات افراد، فراتر از ریسک‌های شخص ثالث گسترش یافته و بر کسب‌وکار اصلی نیز تأثیرگذار بوده است.

انواع خسارت‌های مالی مرتبط با این حملات نیز تکامل یافته است. درحالی‌که ریسک‌های سنتی پیشِ روی کسب‌وکارها حول حفاظت از داده‌های شخص ثالث و مسئولیت حفظ حریم خصوصی متمرکز بوده‌اند، در سال‌های اخیر خسارات عمدتاً از ناحیه حملات باج‌افزاری بوده و به سمت کسب‌وکار اصلی بیمه‌شده نیز تغییر جهت داده است. شرکت‌هایی که مورد حمله باج‌افزار قرار گرفته‌اند، به‌علت اختلال در عملیات شرکت با چندین نوع زیان و خسارت به شخص اول مانند باج‌گیری، هزینه‌های قانونی، بازیابی داده‌ها و وقفه در کسب‌وکار (BI) مواجه می‌شوند. این حملات، ممکن است باعث آسیب به نشان تجاری و اعتبار شرکت شده و روابط آن‌ها با مشتریان[۱] و همچنین سرمایه‌گذاری بازار را نیز تضعیف کنند.

جدول ۱: شرح انواع حملات سایبری مخرب منتخب

انواع حملات	تعریف
باج‌افزار	باج‌افزار نوعی حمله نرم‌افزار مخرب ("بدافزار") است که به‌منظور مسدود کردن دسترسی به یک نظام کامپیوتری تا زمان پرداخت باج، طراحی شده است. این حمله به شکل نفوذ به شبکه (سرقت اعتبارنامه[۲] (احراز هویت)، نصب بک دورها (راه مخفی)[۳] و بدافزارها، حرکت جانبی[۴] از طریق شبکه، سرقت اطلاعات محرمانه، درخواست باج) صورت می‌گیرد. هکرها اغلب مدت‌های طولانی را صرف جاسوسی از یک شبکه در معرض ریسک برای برنامه‌ریزی یک حمله و به حداکثر رساندن سود خود می‌کنند.
بدافزار	نرم‌افزار مخربی که رایانه را آلوده می‌کند و به‌طور خاص برای ایجاد اختلال، آسیب یا دسترسی غیرمجاز به یک نظام طراحی شده است.
انکار سرویس توزیع‌شده[۵] (DDoS)	در یک حمله DDoS، هکرها سعی می‌کنند شبکه هدف را از طریق ایجاد ترافیک با استفاده از چندین منبع (از جمله تماس‌های اینترنتی) مسدود نموده و از بین ببرند. هدف اغلب ازکار انداختن کارایی وب، آسیب رساندن به اعتبار و نشان تجاری یا خسارت مالی از طریق غیرقابل دسترس کردن وب‌سایت یا شبکه است.
فیشینگ	حملات فیشینگ زمانی اتفاق می‌افتد که هکرها با ارسال ایمیل از یک منبع به ظاهر قابل اعتماد از منابع

۱. براساس Hiscox's Cyber Readiness Report 2022، ۲۹ درصد از شرکت‌های آمریکایی پس‌از حمله با مشکل بیشتری برای جذب مشتریان جدید مواجه شدند.

2. Credentials

۳. *Backdoor نوعی* از دسترسی به سیستم را فراهم می‌کند که از مکانیزم‌های احراز هویت عادی سازمان عبور می‌کند.

4. Lateral movement

5. Distributed Denial of Service

انواع حملات	تعریف
	آسیب‌پذیر افراد سوءاستفاده می‌کنند. با کلیک بر روی لینک ایمیل‌شده و وارد کردن رمز عبور، قربانی به هکرها اجازه می دهد تا وارد نظام شوند، به اطلاعات شخصی دسترسی داشته باشند و/یا از طرف آن‌ها ایمیل ارسال کنند. اصطلاح "فیشینگ هدفدار (طعمه‌گذاری تک آماج)[1]" به مواردی اشاره دارد که در آن هکرها برای تحقیق در مورد یک هدف مورد نظر، وقت صرف کرده و با پیام شخصی مرتبط، به قربانی نزدیک می‌شوند. این امر به نظر قانونی می‌رسد و شناسایی آن دشوارتر است.
مهندسی اجتماعی	مهندسی اجتماعی روشی است که هکرها برای سوءاستفاده از اعتماد یک فرد به‌منظور به دست آوردن مستقیم پول یا به دست آوردن اطلاعات محرمانه برای انجام جنایت بعدی استفاده می‌کنند. این روش اغلب با استفاده از فریب کارکنان یک شرکت برای انتقال وجوه به یک کلاهبردار از طرف دیگر اجرا می‌شود.

منبع : NetDiligence, Splunk, Swiss Re Institute

مجرمان سایبری در حال تجاری‌سازی خدمات باج‌افزارها هستند.

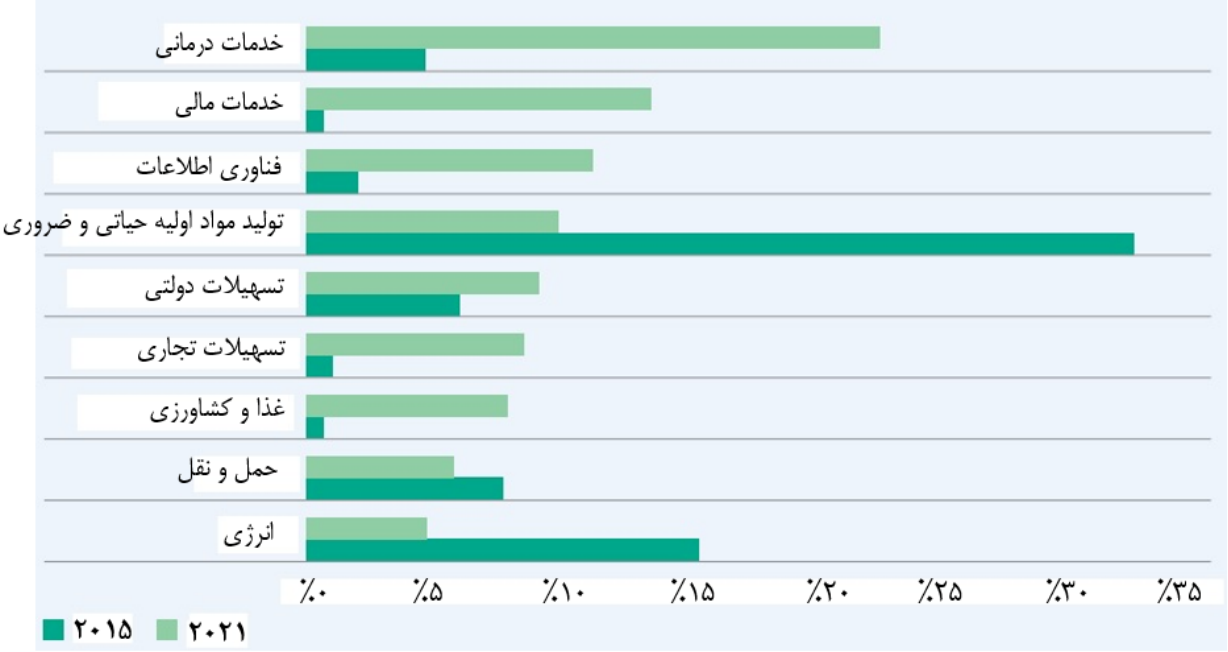
باج‌افزارها به‌عنوان یک سرویس، در حال تبدیل شدن به مدل کسب‌وکار در سازمان‌های مرتبط با جرایم سایبری هستند. درواقع، هکرهای سایبری به دنبال فروش خدمات خود به مقامات دولتی و غیردولتی هستند. آن‌ها عمدتاً دارای انگیزه و منافع مالی بوده و حملات خود را به نمایندگی از سایر افرادی انجام می‌دهند که خود دارای انگیزه و منافع پولی یا ژئوپلیتیکی هستند. به‌عنوان مثال، یک گروه مافیای ایتالیایی از هکرها برای انجام فعالیت‌های مجرمانه خود استفاده می‌کنند[2]. برخی از این گروه‌های سایبری بسیار تکنیکی عمل کرده و از تاکتیک‌های جدید برای حامیان خود استفاده می‌کنند. جنگ در اوکراین خطر اتخاذ تاکتیک‌های سایبری را به‌عنوان یک واکنش جنگی غیرجنبشی علیه متحدان حامی اوکراین و علیه تحریم‌های اقتصادی تشدید کرده است[3].

حوادث سایبری در بخش‌های مختلف

استفاده از فضای دیجیتال، همه بخش‌ها را در معرض تهدیدات سایبری قرار داده است.

1. Spear Phishing
2. How the Mafia Is Pivoting to Cybercrime" vice.com, 22 September 2021.
3. Pathways to Russian Escalation Against NATO from the Ukraine War. Rand Corp, July 2022.

ازآنجایی‌که مجرمان سایبری روش‌های جدیدی را به کار می‌گیرند و حفاظت سازمان‌ها از خود را با مشکل مواجه می‌کنند، قرار گرفتن در معرض حملات سایبری با هر گونه وضعیت اقتصادی، رشد قابل توجهی داشته است. مقایسه حملات باج‌افزاری که بخش‌های زیرساخت حیاتی را در سال‌های ۲۰۱۵ و ۲۰۲۱ هدف قرار داده‌اند، نشان می‌دهد که تعداد حملات ۱۲۰ درصد افزایش یافته است، درحالی‌که توزیع آن‌ها به سمت بخش‌های خدمات درمانی، خدمات مالی و فناوری اطلاعات تغییر کرده است (شکل ۱ را ببینید)[۱]. به همین ترتیب، نهادهای کوچک‌تر بیشتر در معرض تهدیدات سایبری قرار دارند. در نظرسنجی فوق، ۸۸ درصد از پاسخ‌دهندگان، در مورد تاب‌آوری سایبری بنگاه‌های اقتصادی و شرکت‌های کوچک و متوسط[۲] و تهدید مرتبط با زنجیره تأمین، اظهار نگرانی کردند[۳].



منبع:

DHS NCCIC/ICS-CERT Year in Review, Department of Homeland Security, ۲۰۱۵; Internet Crime Complaint Center Federal Bureau of Investigation, Swiss Re Institute estimates

---

۱. در ژوئن ۲۰۲۱، مرکز شکایات جرایم اینترنتی دفتر تحقیقات فدرال (FBI) ردیابی حملات باج افزاری گزارش‌شده را آغاز کرد که در آن قربانی، عضو یکی از بخش‌های زیرساخت حیاتی بود. ما این داده‌ها را با حملات بدافزاری گزارش‌شده به آژانس‌های فدرال در سال ۲۰۱۵ مقایسه کردیم. مراجعه کنید به:

2015 NCCIC/ICS-CERT Year in Review, Homeland Security, 2015 and Internet Crime Report 2021, FBI, 2021.

2. Small & Medium Enterprises (SME)

3. Global Cybersecurity Outlook 2022, World Economic Forum, January 2022.

شرکت‌های کوچک و متوسط در معرض ریسک: هدف حملات سایبری با تاب‌آوری محدود

شرکت‌های کوچک و متوسط بیشتر مورد هدف مجرمان سایبری هستند.

داده‌ها نشان می‌دهد که شرکت‌هایی با گردش مالی کمتر از ۳۰۰ میلیون دلار در ایالات متحده، بریتانیا و کانادا بیشترین تعداد خسارت بیمه‌ای مرتبط با سایبری را بین سال‌های ۲۰۱۶ تا ۲۰۲۰ داشته‌اند (شکل ۲، سمت چپ)[1]. حملات گزارش‌شده بسیاری از بخش‌ها ازجمله خدمات درمانی، خدمات حرفه‌ای و مالی، تولید و خرده‌فروشی را تحت تاثیر قرار داده‌اند (شکل ۲، سمت راست)[2]. استفاده از روش‌های دیجیتال منجر به افزایش حملات سایبری شده است. قبل‌از همه‌گیری کووید-۱۹، شیوه‌نامه‌های امنیت سایبری عمدتاً فقط در داخل شرکت‌ها اجرا می‌شدند، اما پس از افزایش دورکاری، سعی شده به امنیت سایبری همیشه و همه جا توجه شود. درحالی‌که ایمیل‌ها همچنان در معرض خطر حملات فیشینگ قرار دارند، زیست‌بوم کسب‌وکارها نیز با استفاده از ابزارهایی مانند MS Teams[3] و Zoom در حال تغییر است.

شکل ۲: سمت چپ: شرکت‌های متوسط و کوچک: تعداد خسارات مربوط به سایبری و میانگین هزینه خسارت، به ازای گردش مالی شرکت (۲۰۱۶-۲۰۲۰؛ هزاران دلار آمریکا)، راست: شرکت‌های متوسط و کوچک: خسارات مربوط به سایبری و میانگین هزینه‌های خسارت، در هر بخش (۲۰۱۶-۲۰۲۰؛ هزاران دلار آمریکا)

1. Cyber claims study 2021 Report, NetDiligence, 2021.
2. Ibid.
3. Microsoft Teams

میانگین خسارت بیمه‌ای یک حمله سایبری در شرکت‌های متوسط و کوچک، حدودا سه برابر بیشتر از شرکت‌های بزرگ‌تر است.

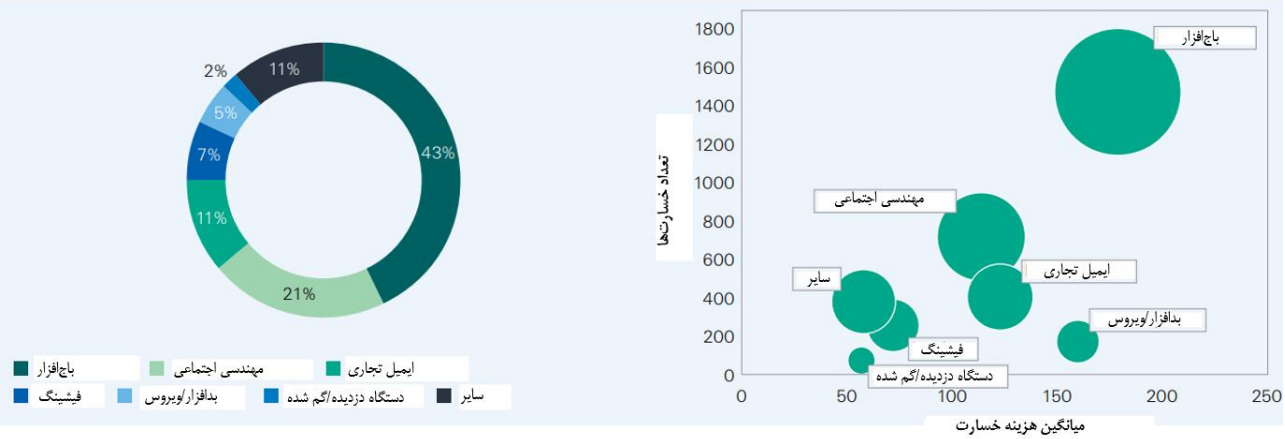
شرکت‌های کوچک‌تر که دارای امنیت سایبری پایین‌تری هستند، بیشتر مورد هدف مجرمان سایبری قرار می‌گیرند و خسارت کمتری می‌بینند[۱]. تجزیه‌وتحلیل داده‌های خسارت از سال ۲۰۱۶ تا ۲۰۲۰ نشان می‌دهد که ۳ مورد از ۴ حمله سایبری موفق در شرکت‌های متوسط و کوچک (شکل ۳، سمت چپ)، از روش‌های باج افزاری، مهندسی اجتماعی و ایمیل‌های تجاری استفاده نموده و به‌طور متوسط هزینه‌ای معادل ۱۵۲،۰۰۰ دلار (شکل ۳، سمت راست)[۲] به شرکت تحمیل کرده‌اند. شرکت‌هایی که به‌تازگی فعالیت برخط/ شیوه‌نامه‌های امنیتی فناوری اطلاعات خود را آغاز کرده، معمولاً دارای شیوه‌نامه‌های آمادگی حمله و واکنش به حادثه ضعیفی هستند و درنتیجه هنگامی که مورد حمله قرار می‌گیرند، تاب‌آوری مالی کمتری دارند. بنابراین، در این‌گونه شرکت‌ها شناسایی و پاسخ به ریسک‌های سایبری زمان بیشتری لازم دارد و در تمام این مدت خسارت واردشده به شخص اول افزایش می‌یابد. طبق ارزیابی صورت‌گرفته، کل خسارات ناشی از یک حمله سایبری در شرکت‌های متوسط و کوچک، به‌طور نسبی سه برابر بیشتر از شرکت‌های بزرگ‌تر است[۳].

---

۱. شرکت‌های بزرگ‌تر با گردش مالی سالانه بالاتر از حد بالای ۲ میلیارد دلاری تعیین‌شده توسط NetDiligence در طبقه‌بندی شرکت‌های متوسط و کوچک استفاده می‌شود.

2. NetDiligence, 2021, op. cit.

۳. با این فرض که شرکت‌های متوسط و کوچک به‌طور متوسط ظرفیت دفاع سایبری کمتری نسبت به شرکت‌های بزرگ‌تر دارند، از گزارش خسارت سایبری NetDiligence در سال ۲۰۲۱ استنباط می‌شود که کل هزینه رسیدگی به یک حمله سایبری - ازجمله هزینه مربوط به حمله و هزینه مدیریت بحران (یعنی مشاوره افشای اطلاعات، خدمات قانونی، اطلاع‌رسانی، نظارت بر اعتبار و روابط عمومی) - به‌عنوان درصدی از درآمد سالانه، حدود ۰٫۳۳٪ در شرکت‌های متوسط و کوچک (متوسط درآمد سالانه ۸۴ میلیون دلار) و حدود ۰٫۱۱٪ در شرکت‌های بزرگ (۱۱ میلیارد دلار) است.



شکل ۳: انواع حملات سایبری که شرکت‌های متوسط و کوچک را تحت تأثیر قرار می‌دهند (٪ سمت چپ)؛ میانگین هزینه حملات سایبری که بر شرکت‌های متوسط و کوچک تأثیر می‌گذارد (هزاران دلار آمریکا، سمت راست)

منبع: Cyber claims study 2021 report, NetDiligence, Swiss Re Institute estimates

... با توجه به هزینه‌های مالی، اداری و حقوقی قابل توجه در شرکت‌های متوسط و کوچک

هزینه مالی، اداری و حقوقی ناشی از یک حمله سایبری در شرکت‌های متوسط و کوچک، به‌طور کلی قابل توجه است. درحالی‌که مبلغ اولیه باج درخواستی در ۷۵٪ موارد به ۲۵،۰۰۰ دلار می‌رسد، هزینه‌های پزشکی قانونی معمولاً از ۲۰،۰۰۰ تا ۱۰۰،۰۰۰ دلار در شرکت‌هایی با گردش مالی کمتر از ۵۰ میلیون دلار[۱]، متغیر است[۲]. اگر اطلاعات مشتریان افشا شود، شرکت باید مطابق با الزامات اطلاع‌رسانی قابل اجرا در حوزه (های) قضایی محل اقامت مشتریان عمل نماید. در این حالت، شرکت علاوه‌بر اینکه متحمل هزینه‌های داخلی می‌شود، تا عملیات خود را مجدداً راه‌اندازی و اجرا نماید و آسیب‌هایی که از حمله متحمل شده است را مدیریت کند (به‌عنوان مثال، بازیابی نظام‌ها و اطلاعات، کمی‌سازی خسارات BI، همکاری با یک شرکت روابط عمومی به‌منظور اطلاع‌رسانی افشا و کاهش اعتبار شرکت)، ممکن است از طرف دادگاه نیز مجبور به جبران مالی مشتریان شود. بیمه‌نامه‌های سایبری معمولاً بیشتر این موارد را پوشش می‌دهند. این بیمه‌نامه‌ها اغلب، خدمات مربوط به مدیریت

---

۱. میزان هزینه بسته به نحوه پاسخ‌گویی بیمه‌شده به یک حمله سایبری، میزان مدرن بودن زیرساخت‌ها قبل‌از حمله و تعداد برنامه‌های کاربردی/سفارشی مختلف که اجرا می‌شوند، متفاوت خواهد بود. برای گردش مالی بین ۵۰ تا ۳۰۰ میلیون دلار، هزینه‌های پزشکی قانونی معمولاً بین ۳۰۰،۰۰۰-۱۰۰،۰۰۰ دلار متغیر است. در گردش مالی بیش از ۳۰۰ میلیون دلار، این مقدار بین ۶۰۰،۰۰۰-۳۰۰،۰۰۰ دلار متغیر است. منبع: بر اساس تجربه Baker Tilly

۲. برآوردشده در دوره ۲۰۲۰-۲۰۱۸. مراجعه کنید به: From Kitchenware to Ransomware – A Short Story, Swiss Re and CyberScout, 2020.

سریع حادثه را نیز پوشش داده و راهنمایی گام‌به‌گام و دسترسی سریع به شبکه‌ای از ارائه‌دهندگان خدمات تخصصی در طول چرخه مدیریت حادثه را به‌منظور تسهیل در خدمت‌رسانی سریع و مؤثر ارائه می‌دهند[۱].

افزایش امنیت سایبری مستلزم زمان و منابع است، اما به تعویق انداختن این فرایند، عملیات شرکت‌های متوسط و کوچک را تهدید می‌کند.

افزایش امنیت سایبری مستلزم زمان و منابع است، اما به تعویق انداختن این فرایند، عملیات شرکت‌های متوسط و کوچک را تهدید می‌کند. برآوردها نشان داده که نیمی از شرکت‌های کوچک در عرض شش ماه پس‌از یک حمله سایبری، نابود شده‌اند[۲]. بهداشت سایبری[۳] و ظرفیت دیجیتال[۴] دو نیروی اصلی در این امر هستند. اول اینکه، دیجیتالی شدن منجر به پیچیده شدن چشم‌انداز ریسک شده و هزینه دستیابی به سطح مطلوب بهداشت سایبری را افزایش می‌دهد. به موازات آن، شرکتی که بهداشت اولیه سایبری پایین‌تری دارد احتمالاً کمتر دیجیتالی شده و درنتیجه رقابت کمتری دارد. بنابراین، میزان تاب‌آوری یک شرکت با ظرفیت دیجیتال کم و راکد توسط دو عامل تهدید می‌شود: ۱) از دست دادن مزیت رقابتی در محیط بازاری که دیجیتالی می‌شود، و ۲) هزینه سرمایه‌گذاری بالاتر برای ایجاد سطح بهینه بهداشت سایبری. هر دو متغیر با کاهش درآمد و افزایش هزینه‌ها بر سودآوری تأثیر می‌گذارند. زمانی که سود به صفر نزدیک شود، یک شرکت متوسط یا کوچک ممکن است در نهایت از بازار خارج شود. یک حمله سایبری نیز می‌تواند این روند را تسریع کند. در این گونه مواقع، بیمه‌گران می‌توانند با افزایش آگاهی از ریسک، ایجاد الزامات برقراری امنیت سایبری و تشویق مستمر بر نظارت/تعدیل ریسک‌ها، به بهبود وضعیت دفاع سایبری در شرکت‌های کوچک‌تر کمک کنند.

---

۱. پوشش‌های شخص اول شامل وقفه در کسب‌وکار و بازیابی داده‌ها و پوشش‌های شخص ثالث شامل هزینه‌های مسئولیت حفظ حریم خصوصی است. علاوه‌بر این، این بیمه‌نامه‌ها اغلب با پوشش هزینه‌های خدمات‌رسانی برای پزشکی قانونی، فناوری اطلاعات، اطلاع رسانی، مدیریت بحران و روابط عمومی همراه هستند.

2. The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses, US Securities and Exchange Commission, 19 October 2015.

۳. Cyber hygiene اقدامات و مراحلی است که کاربران رایانه و سایر دستگاه‌ها برای حفظ سلامت سیستم و بهبود امنیت برخط انجام می‌دهند.

4. Digital capacity

اطلاعات خدمات درمانی: زیست‌بوم‌های دیجیتال در رادار مجرمان سایبری

بخش خدمات درمانی به‌سرعت دیجیتالی می‌شود.

خدمات درمانی همواره در حال تغییر به سمت دیجیتالی شدن هستند. درحالی‌که دستگاه‌های پوشیدنی[1] و اپلیکیشن‌های سلامت و تندرستی[2] به مصرف‌کنندگان این امکان را می‌دهند تا نقش فعالی در مدیریت سلامت خود داشته باشند، دستگاه‌های اینترنت اشیا می‌توانند سلامت بیماران را نظارت کنند و الگوریتم‌های یادگیری ماشینی تشخیص سرطان در مراحل اولیه را ساده‌تر می‌کنند. درنتیجه، بیمه‌گران علاقه زیادی به استفاده از این زیست‌بوم سلامت جدید به‌منظور تشخیص‌های پیشگیرانه، مداخلات زودهنگام و بهترین پوشش متناسب با نیازهای بیمه‌گزاران نشان می‌دهند. به‌عنوان مثال، تجزیه‌وتحلیل داده‌هایی که از طریق دستگاه‌های پوشیدنی جدید امکان‌پذیر است، می‌تواند تشخیص زودهنگام بیماری‌های قلبی عروقی را بهبود بخشد[3].

زیست‌بوم‌های دیجیتال خدمات درمانی، مقادیر بسیار زیادی از داده‌های شخصی را در خود جای می‌دهند.

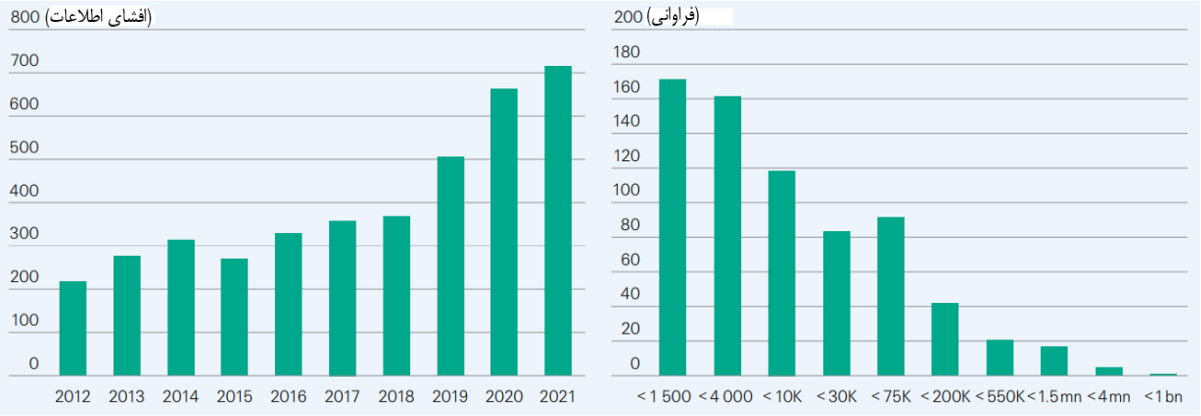
انقلاب خدمات درمانی، در حال ایجاد حجم عظیمی از داده‌های حساس است. در مطالعه‌ای از دانشگاه استنفورد تخمین زده شده که از سال ۲۰۲۰ سالانه بیش از ۲،۳۰۰ اگزابایت داده در بخش خدمات درمانی تولید می‌شود[4] [5]. ماهیت به‌هم‌پیوسته این داده‌ها – متمرکزشده در مراکز خدمات درمانی و غیرمتمرکز در دستگاه‌های خصوصی خارجی یا پایگاه داده‌های بیمه‌گران – احتمال قرار گرفتن زیست‌بوم‌های خدمات درمانی را در معرض حملات سایبری افزایش می‌دهد. حملات افشای اطلاعات به‌دلیل حفظ حریم خصوصی بیمار، برای ذی‌نفعان خدمات درمانی نگران‌کننده هستند؛ علاوه‌بر این، اخلال در ارائه مداوم خدمات درمانی توسط رمزگذاری و باج‌خواهی، نگرانی آن‌ها را تشدید می‌کند. یک نظرسنجی که اخیراً انجام شده و ایالات متحده را نیز در بر دارد، نشان می‌دهد

1. Wearable devices
2. Health & Wellness apps
3. Healthcare Ecosystem – towards an integrated and seamless patient experience, Swiss Re Institute, September 2019.
4. “How Big Data Will Unlock the Potential of Healthcare”, visualcapitalist.com, 26 July 2018
5. For comparison, the data information created every day on the internet in 2012 was estimated to be 1 exabyte. See “What is an exabyte?” techtarget.com.

که از هر چهار حمله سایبری یک مورد در ۲۴ ماه گذشته منجر به افزایش مرگ‌ومیر ناشی از تأخیر در خدمات درمانی شده است[1]. درهم‌تنیدگی هزینه‌های مالی مربوط به دعاوی حقوقی خصوصی افراد و مرگ‌ومیر آن‌ها، موانع را برای بیمه‌گرانی که داده‌های بخش خدمات درمانی را بیمه نموده‌اند، افزایش می‌دهد.

حملات منجر به افشای اطلاعات در این بخش وجود داشته است.

تعداد حملات سایبری که منجر به افشای اطلاعات در بخش خدمات درمانی شده‌اند، همانند سایر بخش‌های کوچک‌تری که داده و اطلاعات بیشتری از مشتریان در خود دارند، در حال رشد بوده است. در ایالات متحده و در سال ۲۰۲۱، رکورد تعداد داده‌های افشاشده که توسط نهادهای خدمات درمانی گزارش شده بود، زده شد (مراجعه کنید به شکل ۴، سمت چپ). مانند شرکت‌های متوسط و کوچک، به‌طور کلی حملات سایبری تأثیر بیشتری بر نهادهای خدمات درمانی کوچک‌تر با ظرفیت‌های سایبری پایین‌تر دارند. در سال گذشته، گزارش ۷۵ درصد از افشای اطلاعات‌ها توسط نهادهایی بوده که در هر حمله، کمتر از ۳۰،۰۰۰ فرد درگیر بوده‌اند. برعکس، افشای اطلاعات طیف وسیعی از افراد، کمیاب‌تر بوده و حملاتی که بیش از ۱/۵ میلیون نفر را تحت تأثیر قرار داده، کمتر از ۱٪ کل را تشکیل می‌دادند (مراجعه کنید به شکل ۴، سمت راست).



شکل ۴: صنعت خدمات درمانی ایالات متحده: تعداد افشای اطلاعات گزارش‌شده (سمت چپ)؛ تعداد افراد درگیر در هر حمله (مقیاس لگاریتمی، سمت راست)

منبع: US Department of Health & Human Services' data breach portal, Swiss Re Institute estimates

1. The Insecurity of Connected Devices in Healthcare 2022, Cynerio and Ponemon Institute, 2022.

زیرساخت‌های حیاتی: ظرفیت بالقوه‌ای برای پیامدهای نظام‌مند

زیرساخت‌های حیاتی، ستون فقرات اقتصاد ملی هستند.

خطری که در بین سیاست‌گذاران و مدیران ارشد اجرایی در سراسر جهان مورد بررسی قرار گرفته، افشای اطلاعات در مقیاس بزرگ است که میزان آسیب‌پذیری زیرساخت‌های حیاتی را در برابر تهدیدات سایبری[۱] برجسته کرده است. اگر حمله سایبری منجر به توقف طولانی‌مدت ارائه خدمات آب پاک، انرژی یا اینترنت شود، عواقب آن بر اقتصاد که گسترده‌تر است، می‌تواند فاجعه‌بار باشد. هنگامی که خط لوله کولونیال[۲] در ایالات متحده در سال ۲۰۲۱ مورد حمله باج افزارها قرار گرفت، این شرکت عملیات تأمین گاز خود را برای شش روز متوالی متوقف کرد که تأثیر زیادی بر مشتریان و مصرف‌کنندگان پایین‌دستی آن داشت (به پیوست ۱ مراجعه کنید)[۳]. آشفتگی‌های ژئوپلیتیکی اخیر، ظرفیت بالقوه حمله گسترده به زیرساخت‌های حیاتی را افزایش می‌دهد. در یک نظرسنجی که اخیراً انجام شده، مهم‌ترین نگرانی رهبران سایبری در حوزه امنیت سایبری شخصی خود، خرابی زیرساخت‌ها به‌دلیل یک حمله سایبری عنوان شده و ۴۲ درصد از آن‌ها به این موضوع اشاره کرده‌اند[۴].

با توجه به اتصالات دیجیتالی بالا، حملات سایبری به زیرساخت‌های حیاتی می‌تواند منجر به خسارات نظامی بزرگی شود.

در طول سال‌ها، زیرساخت‌های حیاتی به فناوری‌های عملیاتی و اطلاعاتی[۵] (OT/IT) وابسته شده‌اند که آن‌ها را در برابر تهدیدات سایبری آسیب‌پذیر می‌کند. از تولید انرژی‌های تجدیدپذیر گرفته تا نظام‌های مدیریت آب و شبکه‌های توزیع انرژی، زیرساخت‌های حیاتی از طریق شبکه‌های نظام کنترل

---

۱. قانون حفاظت از زیرساخت‌های حیاتی ایالات متحده، زیرساخت‌های حیاتی را به‌عنوان سیستم‌ها و دارایی‌های فیزیکی یا مجازی تعریف می‌کند که برای کشور بسیار حیاتی هستند که ناتوانی یا تخریب آن‌ها تأثیر تضعیف‌کننده‌ای بر امنیت، امنیت اقتصادی ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از آن‌ها داشته باشد. مراجعه کنید به:
42 U.S. Code § 5195c – Critical infrastructures protection | U.S. Code | US Law | LII / Legal Information Institute, Cornell Law School, 26 October 2001

2. *Colonial Pipeline*

3. "Cyberattack Forces a Shutdown of a Top US Pipeline", New York Times, 8 May 2021.

4. WEF, January2022, op. cit.

5. Operational and information technologies

صنعتی و نظام‌های فناوری اطلاعات سازمانی تشکیل و عملیاتی می‌شوند. به‌عنوان مثال، سنگاپور مدیریت تأمین آب و میزان کیفیت آن را ازطریق تجزیه‌وتحلیل داده‌ها و به‌وسیله هوش مصنوعی کنترل می‌کند. این داده‌ها اغلب توسط اینترنت اشیا جمع‌آوری می‌شوند. نظارت بر پارامترهای کیفیت و الگوهای مصرف نیز توسط خود آن‌ها انجام می‌پذیرد[1]. علاوه‌بر این، ماهیت به‌هم‌پیوسته زیرساخت‌های حیاتی باعث شده که خرابی یک نظام احتمالاً منجر به خرابی سایر نظام‌ها شود. با دیجیتالی شدن فرایند امور و پذیرش فناوری‌های از راه دور، حملات سایبری فراتر از نظام‌های سنتی IT رفته و به سمت نظام‌های OT که برای مدیریت کل نظام‌های صنعتی استفاده می‌شوند، پیش می‌روند[2]. این موارد همگی راه نفوذ را برای حملات سایبری جدید و مختل کردن زیرساخت‌های حیاتی فراهم می‌کنند.

دارایی‌های زیرساختی قدیمی در برابر حملات سایبری آسیب‌پذیرتر هستند.

دارایی‌های زیرساختی قدیمی معمولاً آسیب‌پذیرتر هستند؛ زیرا بر روی نظام‌های قدیمی محافظت‌نشده اجرا می‌شوند. ازاین‌رو برای اعمال آخرین به‌روزرسانی‌های امنیت سایبری، اجزای نظام باید بُرون‌خط [آفلاین] شوند. زیرساخت‌های حیاتی جدید امروزی را می‌توان با استفاده از جدیدترین فناوری‌ها و به روش‌هایی طراحی کرد که امکان تعمیر و نگهداری و تشخیص سریع افشای اطلاعات را بدون ایجاد اختلال در ارائه خدمات حیاتی فراهم کند (به زیرساخت‌های حیاتی در چین مراجعه کنید: تهدیدها و فرصت‌ها).

1. C. Banerjee, A. Bhaduri, C Saraswat, “Digitalization in Urban Water Governance: Case Study of Bengaluru and Singapore”, Frontiers in Environmental Science, 24 March 2022.
2. Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, US Government Accountability Office, 21 June 2022.

زیرساخت‌های حیاتی در چین: تهدیدها و فرصت‌ها

اقتصاد دیجیتالی در چین در حال رشد است و زیرساخت‌های حیاتی را نیز پوشش می‌دهد.

چین در حال گذار به سمت یک اقتصاد دیجیتال‌محور[۱] است و انتظار می‌رود سهم تولید ناخالص داخلی آن از ۴۰ درصد فعلی تا سال ۲۰۳۰[۲] به ۵۰ درصد برسد[۳]. گسترش دیجیتال در این کشور، بر بسیاری از صنایع سنتی و زیرساخت‌های حیاتی تأثیرگذار بوده و ازطریق سرمایه‌گذاری در «زیرساخت‌های دیجیتال جدید» (مانند فناوری‌های هوش مصنوعی[۴]، ایستگاه‌های پایه 5G) شکل می‌گیرد[۵]. سرمایه‌گذاری در پروژه‌های زیرساختی جدید نیز در برنامه این کشور قرار داشته و انتظار می‌رود طی سال‌های ۲۰۲۰ تا ۲۰۲۵ به ۱۵ تریلیون یوان (۲/۲ تریلیون دلار آمریکا) برسد[۶]. بر اساس مرکز ارزیابی امنیت اطلاعات چین[۷]، در سال ۲۰۲۱ دارایی‌های «زیرساخت جدید» از جمله 5G، اینترنت اشیا، اینترنت صنعتی، هوش مصنوعی و بلاک‌چین هدف حملات سایبری قرار گرفتند[۸] که منجر به افزایش تقاضا برای ایجاد راه‌حل‌های حفاظت از ریسک‌های سایبری در چین شد.

زیرساخت‌های جدید مجهز به آخرین فناوری‌ها در برابر حملات سایبری مقاوم‌تر هستند.

یک پیشرفت مثبت این است که زیرساخت‌های حیاتی مبتنی بر فناوری‌های نوین می‌تواند باعث شود که افراد کمتر در معرض حملات سایبری قرار گیرند. برای مثال، زیرساخت‌های حیاتی دیجیتال، به‌ویژه زیرساخت‌های مرتبط با 5G و AI، می‌توانند در اتخاذ استانداردهای امنیتی ارتقایافته به‌منظور

---

۱. اقتصاد دیجیتال‌محور به طیف گسترده‌ای از فعالیت‌های اقتصادی ازجمله استفاده از اطلاعات و دانش دیجیتالی به‌عنوان عامل اصلی تولید و همچنین شبکه‌های اطلاعاتی مدرن اشاره دارد. مراجعه کنید به :
China’s Digital Economy: Opportunities and Risks, IMF working paper, ۱۷January ۲۰۱۹.

2. China Academy of Information and Communication Technology (CAICT).
3. China spurs digital economy as new driver of growth, Xinhunet, 4 August 2022.
4. “China to build AI-powered 3D printed hydroelectric dam in Tibet”, 3D Printing Industry, 9 May 2022.

۵. براساس تعاریف رسمی، زیرساخت‌های جدیدی که از فناوری‌های نوظهور استفاده می‌کنند، شامل فناوری‌های هوش مصنوعی، ایستگاه‌های پایه 5G، نرم‌افزارهای صنعتی اینترنت اشیا، مراکز پردازش و ذخیره‌سازی داده‌ها، ظرفیت‌های ولتاژ فوق‌العاده (UHV)، راه‌آهن‌های سریع‌السیر بین شهری (HSR) و ایستگاه‌های شارژ برای پشتیبانی شبکه وسایل نقلیه الکتریکی هستند.

6. New Infrastructure Investment Will Reach CNY 15 Trillion Within Five Years, Equal Ocean, 15 Oct. 2020.
7. China Information Security Assessment Center
8. China Cyber Security Assessment and Overview, 30 December 2021.

دفاع در برابر تهدیدات سایبری کمک نمایند. درحالی‌که پیشرفت در نحوه تجزیه‌وتحلیل داده‌ها ابزار مؤثری برای مبارزه با حملات سایبری است، اما ممکن است سطح حملات سایبری را نیز افزایش دهد. مطابق با یک گزارش انجام‌شده، حدود ۷۰ درصد از سازمان‌ها بدون هوش مصنوعی قادر به شناسایی یا پاسخ‌گویی به تهدیدات سایبری نبوده‌اند[1]. به همین ترتیب، همان‌طور که استفاده از فناوری‌های ابری در افزایش تاب‌آوری سازمان مؤثر است، سازگار نبودن امنیت عملیاتی این ابزار با آخرین تهدیدات سایبری، ممکن است منجر به ریسک بیشتر برای سازمان شود.

آسیب‌پذیری‌های زنجیره تأمین

زنجیره‌های تأمین از طریق چندین نقطه ورودی در معرض حملات سایبری قرار دارند.

زنجیره‌های تأمین از چند نقطه ممکن است مورد حمله هکرها قرار گیرند. ماهیت به‌هم‌پیوسته شبکه‌های زنجیره تأمین در سراسر مرزهای دیجیتال و فیزیکی، شرکت‌ها را در برابر شوک‌هایی آسیب‌پذیر می‌کند که می‌تواند در کل نظام منتشر شود. هر چه شبکه به‌صورت دیجیتالی یکپارچه‌تر باشد، انتشار شوک سریع‌تر و اثرات خوشه‌ای کمتری خواهد داشت. حمله سایبری NotPetya در سال ۲۰۱۷، که طی آن هکرها بدافزاری را در نرم‌افزار حسابداری که توسط شرکت‌های اوکراینی برای تهیه گزارش‌های مالیاتی استفاده می‌شد، قرار داده بودند، یکی از نمونه‌های چنین رویدادی است. این حمله سایبری از طریق آلوده شدن نظام‌های چند شرکت و قطع فعالیت آن‌ها، به‌صورت افقی منتشر شد و اثرات سرریز عمودی نیز در زنجیره‌های تأمین و مرزهای متعدد، پس‌از آن صورت گرفت. طبق برآوردها، شرکت‌های پایین‌دستی آسیب‌دیده ۷/۳ میلیارد دلار خسارت متحمل شده‌اند که نسبت به خسارت‌های گزارش‌شده توسط شرکت‌های بالادستی که مستقیماً آسیب دیده‌اند، چهار برابر افزایش داشته است[2]. همان‌طور که دیده می‌شود، خسارت و زیان در میان شرکت‌هایی که مجموعه‌ای از تأمین‌کنندگان متنوع ندارند، بیشتر است و تأمین‌کنندگان آلوده به احتمال زیاد پس‌از حمله از زنجیره تأمین خارج می‌شوند.

1. Reinventing Cybersecurity with Artificial Intelligence, Capgemini Research Institute, 11 July 2019.
2. M. Crosignani, M. Macchiavelli, A.F. Silva, Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains", Federal Reserve Bank of New York, Staff Report No. 937, July 2020 (rev July 2021).

هر چه یک حمله سایبری به سمت بالادست زنجیره تأمین حرکت کند، پیامدهای آن گسترده‌تر می‌شود.

اگر شوک ناشی از حمله سایبری، شرکت‌های بالای زنجیره تأمین را هدف قرار دهد، پیامدهای آن می‌تواند کل شبکه را درگیر نماید. برای مثال، هدف قرار دادن شرکت‌های فعال‌کننده زنجیره تأمین مانند SolarWinds، یکی از این موارد است[۱] [۲]. در سال ۲۰۲۰، هکرها بدافزاری را به نظام نرم‌افزاری این شرکت وارد کردند که طی هفت ماه به ۳۰،۰۰۰ مشتری آسیب رساند. سپس این بازیگر دولت ملی[۳] که مورد حمایت دولت قرار داشت (به ضمیمه ۱ مراجعه کنید)، توانست حمله سایبری خود را به چند سازمان دولتی در ایالات متحده گسترش دهد. این حمله باعث افزایش آگاهی افراد در مورد آسیب‌پذیری سایبری کل زنجیره تأمین از طریق تأمین‌کنندگان بیرونی شد. امروزه این موضوع به‌عنوان یک نگرانی بزرگ باقی مانده است، زیرا آسیب‌پذیری‌های امنیت سایبری می‌توانند توسط عوامل مختلف، ازجمله کسانی که از طرف دولت‌ها کار می‌کنند، مورد سوءاستفاده قرار گیرند. اسکن دقیق تأمین‌کنندگان بیرونی، یک راه برای کاهش ریسک‌های سایبری بالادستی است.

حملات پایین‌دستی زنجیره تأمین، پیامدهای محلی بیشتری دارند.

برعکس، حملات پایین‌دستی زنجیره تأمین، تأثیرات محلی بیشتری دارند. مدل‌های کسب‌وکار امروزی در سراسر زنجیره‌های تأمین به‌صورت دیجیتالی عمل می‌کنند؛ آن‌ها در سراسر مرزهای ملی پیش رفته و از شرکت‌های مختلف با میزان درجات مختلف امنیت سایبری تشکیل شده‌اند. درنتیجه، نقاط ورود چندگانه‌ای برای مجرمان سایبری وجود دارد که عملیات زیرشبکه را تهدید می‌کند، به‌ویژه در مواردی که یک شرکت نمی‌تواند به‌راحتی یکی از تأمین‌کنندگان خود را که تحت حمله سایبری قرار گرفته است، با شرکت دیگر جایگزین نماید[۴]. در یک نظرسنجی که اخیراً انجام شده، ۴۰ درصد از مدیران اجرایی عنوان کردند که زنجیره تأمین سازمان آن‌ها در سال گذشته تحت تأثیر یک حمله

1. “Supply chain attacks show why you should be wary of third-party providers”, csoonline.com, 27 Dec 2021.
۲. شرکت SolarWinds مستقر در آستین، نرم‌افزاری را برای کسب‌وکارها توسعه می‌دهد تا به مدیریت شبکه‌ها، سیستم‌ها و زیرساخت‌های فناوری اطلاعات آن‌ها کمک کند و در ایالات متحده و بسیاری از کشورهای دیگر فعالیت می‌کند.
3. Nation state actor
4. M. Elliott, B. Golub, M. V. Leduc. 2020. “Supply Network Formation and Fragility.” American Economic Review, 12 January 2020 (rev. 18 April 2022).

سایبری قرار گرفته و حدود ۶۰ درصد از آن‌ها، تاب‌آوری سایبری شرکا و تأمین‌کنندگان خود را زیر سؤال بردند[1]. برای اطمینان از تاب‌آوری در برابر حملات سایبری مستقیم و غیرمستقیم، ضروری که شرکت‌ها در هر اندازه‌ای که هستند، به‌طور فعالانه شبکه عرضه خود را بررسی کرده و از تأمین‌کنندگان متنوعی استفاده نمایند.

قوانین حفظ حریم خصوصی داده‌ها: افزایش ریسک‌های بلندمدت برای بیمه‌گران

قوانین حفظ حریم خصوصی داده‌ها با الهام از قانون GDPR اروپا در حال گسترش در سطح جهانی است.

اروپا در ایجاد مقررات حفظ حریم خصوصی داده‌ها پیشرو بوده و بسیاری از مناطق دیگر از آن پیروی می‌کنند. از زمانی که مقررات عمومی حفاظت از داده‌ها[2] (GDPR) در سال ۲۰۱۸ لازم‌الاجرا شد، حداقل ۶۰ کشور قوانین جدیدی را برای حفظ حریم خصوصی داده‌ها وضع کرده‌اند یا در نظر گرفته‌اند که بسیاری از آن‌ها مفاهیم مشابهی با GDPR دارند. در آسیا، سال گذشته شاهد معرفی قوانین جدید حفظ حریم خصوصی در ژاپن، سنگاپور و چین بوده‌ایم. در ایالات متحده، درحالی‌که هنوز قانون فدرال حفظ حریم خصوصی وجود ندارد، کالیفرنیا اولین قانون حفظ حریم خصوصی مبتنی بر ایالت را در سال ۲۰۱۸ معرفی کرد[3]. از آن زمان، کلرادو و ویرجینیا در میان دیگر ایالت‌ها، قوانین مربوط به حریم خصوصی و امنیت داده‌های خود را اجرا کرده‌اند.

قانون حفظ حریم خصوصی داده‌ها، منجر به افزایش دعاوی قضایی، جریمه‌های قانونی و خسارت‌های مالی می‌شود.

قانون حفظ حریم خصوصی داده‌ها، شرکت‌ها و بیمه‌گران را در معرض دعوی قضایی و دادگاهی قرار داده و منجر به خسارات مالی هنگفتی می‌شود. قوانین جدید حفظ حریم خصوصی و امنیت داده‌ها،

1. WEF, January 2022 op. cit.
2. General Data Protection Regulation
3. Referred to as the California Consumer Privacy Act (CCPA).

حقوق بیشتری را برای مصرف‌کنندگان فراهم کرده و حقوقی را که قبلاً وجود داشته است نیز، تقویت می‌کند. به‌عنوان مثال، در ایالت کالیفرنیا میزان خسارت واردشده در قانون پیش‌بینی شده و ارتباطی با میزان زیانی که شخص دیده، ندارد؛ درنتیجه در این ایالت شاهد افزایش میزان خسارت پرداختی هستیم و در اروپا، گزارش افشای اطلاعات، امنیت و/یا حریم خصوصی به قانون‌گذارها و مشتریان، اجباری است[1]. عدم انجام این کار، یا اتخاذ تدابیر امنیتی نادرست، می‌تواند منجر به اخذ جریمه بر اساس GDPR شود (تا ۴ درصد از گردش مالی جهانی یک شرکت یا ۲۰ میلیون یورو، هرکدام بیشتر باشد)[2]. GDPR همچنین عنوان کرده هر شخصی که در نتیجه نقض مقررات، متحمل خسارات مادی و غیرمادی (یعنی ناراحتی عاطفی) شده باشد، حق دریافت خسارت متحمل‌شده را دارد. دعاوی حقوقی در اروپا پس‌از وضع قانون حفظ حریم خصوصی داده‌ها، چه از طریق شکایت‌های فردی یا شکایات گروهی به سبک اتحادیه اروپا، نشان می‌دهد که اکنون مشتریان از این حق خود برای دریافت خسارت هنگام افشای اطلاعات/حریم خصوصی استفاده می‌کنند.

رویه‌های دادرسی طولانی که منجر به دعاوی سنگین شخص ثالث می‌شود، ریسک‌های بلندمدت بیمه‌گران را افزایش می‌دهد.

رویه‌های دادرسی طولانی که منجر به دعاوی سنگین شخص ثالث می‌شود، ریسک‌های بلندمدت بیمه‌گران را افزایش می‌دهد. در ایالات متحده، خسارت‌های بزرگی که به قانون‌گذارها یا مشتریان به دنبال نقض حریم خصوصی و امنیت داده‌ها پرداخت شده، محاسبه شده است (جدول ۲ را ببینید). هزینه‌های حقوقی تحمیلی هنگام دفاع از دعاوی شخص ثالث (بیشتر اوقات به شکل دعوای حقوقی گروهی) بسیار بالا بوده و اغلب به میزان خسارت اضافه می‌شود. درنتیجه، این دعاوی حقوقی بر طولانی شدن اثر خسارت‌های سایبری تأثیر می‌گذارد و اغلب چندین سال طول می‌کشد تا هزینه‌ها پرداخت شود (سال افشای اطلاعات را در مقابل سال تسویه حساب ببینید). در مقابل خسارات شخص اول، که معمولاً میزان مشخصی دارند، ظرف یک سال پس‌از حمله سایبری پرداخت خواهد شد (ریسک‌های کوتاه مدت).

---

۱. در مناطق دیگر، شاهد تعداد فزاینده‌ای از قوانین جدید حفظ حریم خصوصی هستیم که گزارش‌دهی را اجباری می‌کنند.

۲. در سال ۲۰۲۰، شرکت‌های هواپیمایی Marriott و British توسط دفتر کمیسر اطلاعات بریتانیا به‌ترتیب 18/4 میلیون پوند و ۲۰ میلیون پوند جریمه شدند.

جدول ۲: بزرگ‌ترین افشاهای اطلاعات

سازمان‌های که مورد حمله سایبری قرار گرفته‌اند	افراد تحت تاثیر	سال افشای اطلاعات	سال تسویه حساب خسارت	مبلغ (به میلیون دلار)
Deutsche Telekom - T Mobile	۷۶/۶ میلیون	۲۰۲۱	۲۰۲۲	۳۵۰
Morgan Stanley	۱۵ میلیون	۲۰۱۶/۲۰۱۹	۲۰۲۲	۶۰
OPM	۲۲ میلیون	۲۰۱۵	۲۰۲۲	۶۳
Capital One	۱۰۶ میلیون	۲۰۱۹	۲۰۲۱	۱۹۰
Yahoo	۵۰۰ میلیون	۲۰۱۳/۲۰۱۶	۲۰۲۰	۱۱۷/۵
Equifax	۱۶۳ میلیون	۲۰۱۷	۲۰۲۰	۵۷۵
Home Depo	۵۶ میلیون	۲۰۱۴	۲۰۲۰	۲۰۰
Ube	۵۷ میلیون	۲۰۱۶	۲۰۱۸	۱۴۸
Target	۱۱۰ میلیون	۲۰۱۳	۲۰۱۷	۱۸/۵
Anthem	۸۰ میلیون	۲۰۱۴	۲۰۱۵	۱۱۵

منبع: تحقیقات موسسه Swiss Re

خسارت‌های واردشده به شخص ثالث تنها یکی از انواع خسارت‌های مربوط به افشای اطلاعات است.

خسارت‌های واردشده به شخص ثالث تنها یکی از انواع خسارت‌های مربوط به افشای اطلاعات است. علاوه‌بر این مورد، هزینه‌های قانونی، هزینه‌های مدیریت بحران (شخص اول) و جریمه‌های احتمالی نیز می‌تواند وجود داشته باشد. به‌دلیل قوانین نظارتی بین‌المللی و دعاوی بالقوه‌ای که ممکن است توسط طرف‌های متضرر در کشورهای مختلف طرح شود، افشای اطلاعات زمانی پرهزینه‌تر می‌گردد که درگیر حوزه‌های قضایی شود. به‌عنوان مثال، جدول ۳ خسارت‌های ناشی از افشای اطلاعات شرکت Capital One در سال ۲۰۱۹ را نشان می‌دهد که در آن اطلاعات شهروندان ایالات متحده و کانادا در معرض خطر قرار گرفتند. در برخی موارد، جمع همه خسارت‌ها می‌تواند از ارزش کل بیمه سایبری خریداری‌شده توسط بیمه‌گزار فراتر رود.

جدول ۳: نمونه هزینه یک رویداد منجر به افشای اطلاعات

پوشش‌ها	افشای اطلاعات شرکت Capital One	نوع خسارت وارد شده
هزینه‌های مدیریت بحران: 1. هزینه‌های پزشکی قانونی؛ 2. اطلاع‌رسانی، نظارت بر اعتبار و مراکز تماس؛ 3. هزینه‌های مشاوره پس از افشای اطلاعات؛ 4. هزینه‌های روابط عمومی؛ 5. هزینه‌های حقوقی.	۱۰۰ میلیون دلار برآورد شده است	شخص اول
جریمه مقام نظارتی	۸۰ میلیون دلار	شخص ثالث
مسئولیت امنیت شبکه / مسئولیت حفظ حریم خصوصی (دعاوی قضایی در جایی تشکیل می‌شوند که افراد آسیب‌دیده در آن زندگی می‌کنند، بنابراین اگر اطلاعات افراد ساکن در کشورهای مختلف به خطر بیفتد، ممکن است به همان تعداد دعاوی در پی داشته باشد).	آمریکا: ۱۹۰ میلیون دلار کانادا: در دست انجام (در یک شکایت گروهی معادل ۶۳۶ میلیون دلار در ژوئن ۲۰۲۲ تخمین زده شده است).	شخص ثالث
هزینه‌های حقوقی برای دفاع از شکایات قانونی	ده‌ها میلیون دلار تخمین زده شده است.	شخص ثالث
مجموع هزینه‌ها	بیشتر از ۴۰۰ میلیون دلار	

منبع: Capital One, Office of the Comptroller of the Currency, Global Data Review, Insurance Insider

چین یک چارچوب نظارتی حفاظت از داده‌ها با استانداردهایی مشابه GDPR ایجاد کرده است.

در چین، قانون حفاظت از اطلاعات شخصی[1] (PIPL) در نوامبر ۲۰۲۱ به تصویب رسید. این قانون، یک چارچوب قانونی برای حفاظت از حریم خصوصی داده‌ها مشابه قانون GDPR ترسیم می‌کند؛ با این تفاوت که قوانین بیشتری برای مجازات سازمان‌هایی که باعث افشای اطلاعات شده‌اند، ارائه می‌کند (به‌عنوان مثال، قانون تعلیق کار شرکت‌های متخلف). از زمان اجرایی شدن این قانون، حملات منجر به نقض حریم خصوصی داده‌ها، شرکت‌ها را بیشتر در معرض ریسک‌های تجاری و نظارتی قرار

1. Personal Information Protection Law

داده است. چنین ریسک‌هایی تا حدی می‌توانند تحت پوشش بیمه قرار گیرند و بیمه‌گران چینی انتظار دارند در بخش افشای اطلاعات مشارکت بیشتری داشته باشند.

مدیریت ریسک با بیمه سایبری

مدیریت ریسک سایبری به شرکت‌ها کمک می‌کند تا تعیین کنند که آیا میزان مواجهه با ریسک‌ها را کاهش دهند، آن‌ها را انتقال دهند، اجتناب کنند یا بپذیرند.

مدیریت ریسک فرایند شناسایی، ارزیابی و پاسخ به/کاهش ریسک است[1]. سازمان‌ها باید احتمال و شدت بالقوه حملات سایبری را درک کرده و سطح ریسک قابل قبول خود را تعیین کنند. بر اساس سطح تحمل هر سازمان، آن‌ها می‌توانند از ریسک‌های خاص اجتناب کنند، آن‌ها را بپذیرند، اقداماتی را برای کاهش ریسک انجام دهند و یا ازطریق سازوکارهایی آن را انتقال دهند. در زمینه ریسک‌های سایبری، سازمان‌ها باید آسیب‌پذیری نظام‌های رایانه‌ای و شبکه خود را مدیریت کنند. آن‌ها همچنین باید کارکنان خود را برای شناسایی تهدیدها، رعایت قوانین حفظ حریم خصوصی و هدایت یک محیط ژئوپلیتیک پرریسک آموزش دهند.

تلاش‌های بخش عمومی و خصوصی برای مدیریت ریسک سایبری تشدید شده است.

تلاش‌ها برای مدیریت ریسک‌های ناشی از مسئولیت شخص ثالث، حملات باج‌افزاری و تهدیدات زنجیره تأمین/زیرساخت‌های حیاتی از دهه ۱۹۹۰ ادامه داشته است[2]. از آن زمان، دامنه تهدیدات سایبری به سطوح جدیدی رسیده و آگاهی کلی در این زمینه افزایش یافته است. بخش خصوصی و دولتی با استفاده از تلاش در مدیریت ریسک بیشتر، سرمایه‌گذاری در حوزه امنیت سایبری و رشد بازار بیمه سایبری، به این نوع ریسک‌ها پاسخ داده‌اند.

---

1. Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1, National Institute of Standards and Technology, 6 April 2018.

۲. به‌عنوان مثال، تهدیدات سایبری برای زیرساخت‌های حیاتی در لینک زیر مورد تجزیه‌وتحلیل قرار گرفت:
Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, 1997.

بازار بیمه سایبری به‌سرعت در حال رشد است.

شرکت‌ها سهم بیشتری از ریسک سایبری را نسبت به ریسک‌های اموال و سایر مسئولیت‌ها حفظ می‌کنند. این موضوع، تا حدی نشان‌دهنده نوظهور و نوین بودن نسبی اقتصاد دیجیتال است. در سال ۲۰۲۲، تنها ۱۶/۶ درصد از دارایی‌های دیجیتال و سایر دارایی‌های نامشهود بیمه شده بودند، درحالی‌که این مقدار برای دارایی‌های مشهود به ۵۸ درصد می‌رسد[1]. اما بازار بیمه سایبری در سال ۲۰۲۱ به‌سرعت رشد کرد که ناشی از افزایش باج افزارها و خسارت‌های شخص اول بود، درحالی‌که در همان زمان شاهد افزایش میزان خسارت شخص ثالث نیز بوده‌ایم. انتظار می‌رود که در سال‌های آینده رشد بیمه سایبری افزایش یابد؛ زیرا آگاهی نسبت به ریسک‌های سایبری روزبه‌روز بیشتر می‌شود.

بیمه با انتقال ریسک و ایجاد انگیزه در اقدامات کاهشی ریسک، جزء ارزشمندترین تلاش‌ها در حفظ امنیت سایبری است.

بیمه نقشی کلیدی در بهبود امنیت سایبری شرکت‌ها، فراتر از عملکرد اصلی آن که انتقال ریسک است، ایفا می‌کند. به دنبال افزایش اخیر حملات بدافزارها، صنعت بیمه استانداردهای لازم هنگام صدور بیمه‌نامه سایبری را تشدید کرد که به کاهش موقت دفعات و شدت حملات و میزان خسارت باج افزارها در سال ۲۰۲۲ کمک کرده است[2]. بیمه سایبری علاوه‌بر اینکه موجب ایجاد انگیزه‌های مالی برای بهبود شیوه‌نامه‌های امنیتی و کاهش آسیب‌پذیری‌ها قبل‌از انعقاد بیمه‌نامه می‌شود، به سه دلیل، یک ورودی ارزشمند در فرایند مدیریت ریسک می‌باشد: ۱) قیمت‌گذاری ریسک‌ها، که مبنایی مالی برای چارچوب‌بندی تصمیم‌ها فراهم می‌کند؛ ۲) نظارت[3]، که می‌تواند آسیب‌پذیری‌ها را در طول دوره بیمه‌نامه کاهش دهد[4]؛ و ۳) پرداخت خسارت‌ها و پشتیبانی پاسخ‌ها که تاب‌آوری را بهبود بخشیده و می‌تواند خسارات ناشی از یک حمله سایبری را کاهش دهد.

---

1. 2022 Intangible Assets Financial Statement Impact Comparison Report, Aon/Ponemon, April 2022.
2. 2022 SonicWall Cyber Threat Report, Sonicwall, July 2022.

۳. به‌عنوان مثال، Coalition که یک نماینده عمومی مدیریت سایبری است و Swiss Re را در میان شرکای خود دارد، بر آدرس‌های IP مشتریان نظارت دارد.

۴. به‌عنوان مثال، Coalition بیان می کند که هر ماه ۴/۵ میلیارد آدرس IP را اسکن می کند تا دائماً ریسک‌های سایبری را نظارت کند و آسیب‌پذیری‌ها را قبل‌از تشدید آن‌ها، شناسایی کند.

سایبری: پیشی گرفتن از رشد در سایر بیمه‌ها

اولین پوشش‌های بیمه سایبری مربوط به قرار گرفتن در معرض مسئولیت (مرتبط با افشای اطلاعات) بوده است.

بازار بیمه سایبری با دیجیتالی شدن اقتصاد رشد کرده است. بیمه سایبری در اواسط / اواخر دهه ۱۹۹۰ در ایالات متحده ایجاد شد و از بیمه‌نامه‌های مسئولیت حرفه‌ای مانند E&O شکل گرفت[۱]. این بیمه‌نامه‌ها به شرکت‌های بیمه بابت پرداخت خسارت هنگام نقض حریم خصوصی/امنیتی شخص ثالث که بر مشتریان، کارمندان، سرمایه‌گذاران و/یا شرکای تجاری تأثیرگذار هستند، زیان مالی وارد می‌کنند. پوشش خسارت‌های شخص اول در اواسط دهه ۲۰۰۰ معرفی شد، اما با توجه به قانون حفظ حریم خصوصی داده‌های ایالات متحده، مسئولیت شخص ثالث کاتالیزور اصلی برای نوآوری محصول باقی ماند. در دهه ۲۰۱۰، بازار بیمه سایبری فراتر از ایالات متحده پیش رفته و گسترش یافت. تحولاتی مانند اجرای قانون GDPR در اتحادیه اروپا در سال ۲۰۱۸، افزایش سرمایه‌گذاری در زیرساخت‌های دیجیتال و افزایش آگاهی از تهدیدات سایبری به رشد بازار جهانی بیمه سایبری کمک کرده است[۲].

خسارت‌ها و حق بیمه‌های سایبری در سال‌های اخیر به‌سرعت رشد کرده، اما شکاف حفاظت از اطلاعات همچنان زیاد است.

محرک اصلی رشد بازار بیمه سایبری افزایش دفعات و شدت حملات سایبری بوده که به نوبه خود، آگاهی از ریسک را افزایش داده است. در ایالات متحده که بزرگ‌ترین بازار بیمه سایبری را داشته، حق بیمه‌ها در سال ۲۰۲۱، ۷۴ درصد رشد کرد[۳]. حق بیمه‌های بیمه مستقل سایبری، ۹۲ درصد افزایش یافت که ناشی از افزایش نرخ پس از حملات باج‌افزاری بود که منجر به افزایش ضریب

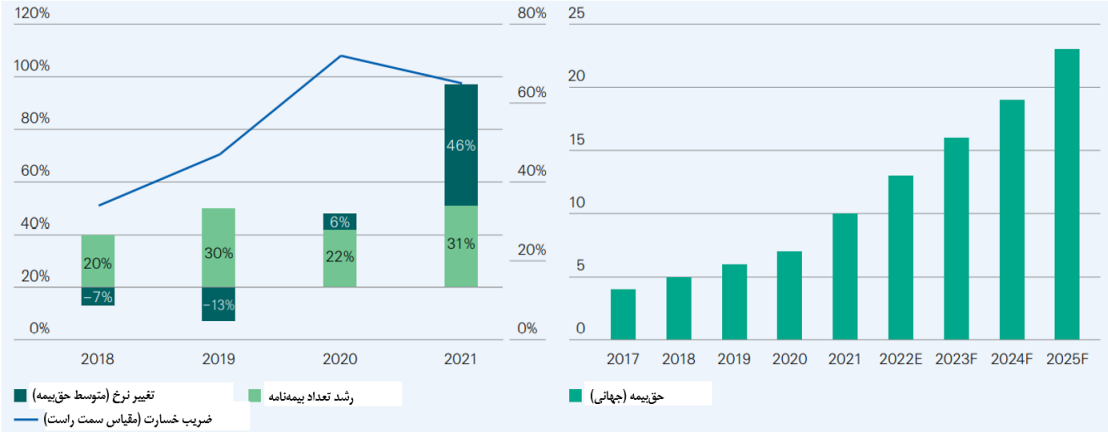
---

۱. اولین بیمه‌نامه مستقل سایبری در سال ۱۹۹۷ صادر شد (مراجعه کنید به: Cyber Claims: A Guide to Calculating Business Interruption, JS Held, 2022) اگرچه نمونه‌هایی از پوشش های وقفه در کسب‌وکار سیستم اطلاعاتی شخص اول در دهه ۱۹۸۰ وجود داشت.

۲. برای خلاصه ای از وضعیت بازار و تحولات تاریخی در آن سال، و اصول مدیریت ریسک مرتبط با آن‌ها، مراجعه کنید به : sigma ۲۰۱۷/۱: Cyber: getting to grips with a complex risk, Swiss Re.

۳. براساس داده‌های ثبت شده در NAIC

خسارت در سال ۲۰۲۰ شد (شکل ۵، سمت چپ را ببینید[۱]). تخمین زده می‌شود که حق بیمه جهانی سایبری در سال ۲۰۲۱ به ۱۰ میلیارد دلار رسیده و رشد سالانه ۲۰ درصدی را تا سال ۲۰۲۵ تجربه کند و درنتیجه کل حق بیمه‌ها به ۲۳ میلیارد دلار افزایش یابد (شکل ۵، سمت راست را ببینید). البته بازار بیمه سایبری ظرفیت رشد قابل‌توجهی فراتر از این پیش‌بینی‌ها دارد. با توجه به تخمین‌های سالانه خسارت سایبری جهانی، ۹۴۵ میلیارد دلار[۲]، تقریباً تمام ریسک‌ها بیمه‌نشده باقی می‌مانند و طبق برآوردی که انجام شده، حدود ۹۰ درصد از ریسک‌ها بیمه نشده‌اند[۳]. براساس تحقیقات اخیر، تنها ۵۵ درصد از کسب‌وکارهای مورد نظرسنجی بیمه شده‌اند و کمتر از یک‌پنجم آن‌ها دارای محدودیت پوشش باج افزاری بالاتر از ۶۰۰،۰۰۰ دلار آمریکا هستند که میانگین خسارت ناشی از چنین حملاتی است[۴].



شکل ۵: سمت چپ: ضریب خسارت بیمه‌نامه مستقل سایبری در ایالات متحده و نرخ و رشد در معرض قرار گرفتن
سمت راست: حق بیمه جهانی سایبری، میلیارد دلار، تخمین Swiss Re

منبع: National Association of Insurance Commissioners, S&P Global, Swiss Re Institute calculations

---

۱. در شکل ۵ (سمت چپ)، رشد بیمه‌نامه، نماینده‌ای برای رشد میزان مواجهه با ریسک است. اگر بیمه نامه‌ها با شرایط و ضوابط سخت‌تری مانند محدودیت‌های کمتر، محدودیت‌های فرعی جدید، بیمه‌های مشترک یا استثناها نوشته شوند، افزایش مواجهه مؤثر، کمتر و افزایش نرخ، بیشتر از آنچه در نمودار پیشنهاد شده است، صورت می‌گیرد. ضریب خسارت نیز شامل هزینه های دفاعی و جبران خسارت می‌شود.

2. McAfee. op. cit.

۳. این عدد در مقایسه برآورد ۹۰ درصدی انجمن ژنو براساس سناریونویسی خسارت اقتصادی لویدز در مقابل برآورد خسارت سالانه مک‌آفی است. مراجعه کنید به:

Understanding and Addressing Global Insurance Protection Gaps, The Geneva Association, April ۲۰۱۸.

4 G. Davis, The Cyber Insurance Gap: What Is It, and How Can We Close It?, BlackBerry, 10 August 2022.

بازار بیمه سایبری: تکامل و ساختار

ایالات متحده، سهم بالایی از حق بیمه سایبری جهانی داشته و دارای بازار نسبتاً رقابتی می‌باشد.

تخمین زده می‌شود که دوسوم از پوشش‌های فعلی بیمه سایبری جهانی برای مشتریان آمریکایی صادر شده و اکثریت آن‌ها توسط شرکت‌های بیمه مقیم ایالات متحده بوده است. ۱۰ شرکت بیمه مستقیم سایبری برتر، ۵۷ درصد از بازار ایالات متحده را تشکیل می دهند[1]. تمرکز بازار بیمه در این ایالت در رشته‌های شخصی مانند خودرو و اموال کمتر بوده و بیشتر روی رشته‌های بازرگانی و تجاری بزرگ مانند بیمه بیماری و ازکارافتادگی کارگران و مسئولیت عمومی متمرکز بوده است [2]. برای بیمه‌گرانی که ظرفیت کافی برای افزایش سهم بازار و آگاهی از ریسک دارند، بیمه سایبری فرصت رشد قانع‌کننده‌ای را فراهم می‌کند.

جدول ۴: بزرگ‌ترین شرکت‌های بیمه سایبری ایالات متحده، با حق بیمه صادره مستقیم

(میلیون دلار، بر اساس داده های مکمل سایبری NAIC)

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	**۴۸۲۷**	**۲۷۷۴**	**٪ ۷۴**	**٪ ۱۰۰**

منبع: Source: NAIC cyber insurance supplement, S&P Global, Swiss Re Institute

1. Swiss Re Institute analysis of NAIC cyber supplement data.
2. Based on a comparison of Herfindahl-Hirschman Indexes of premium revenues.

بیشتر از ۵۰ درصد از حق بیمه‌های سایبری واگذار می‌شود.

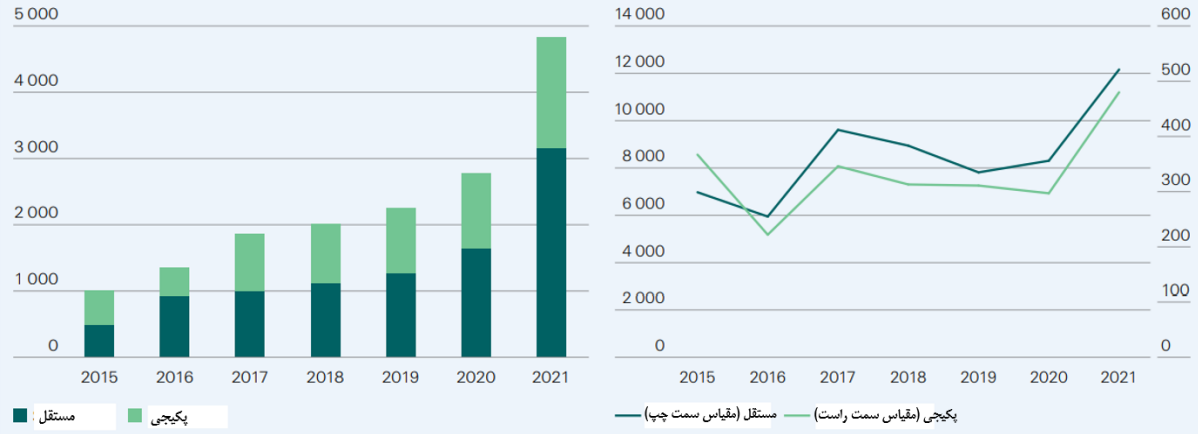
همواره بین صادرکنندگان بیمه‌نامه مستقیم، نمایندگان عمومی[۱] (MGA) و بیمه‌گران عمومی[۲] (MGU) رقابت وجود دارد. تخمین زده شده که حدود ۴۰ تا ۵۰ درصد از حق‌بیمه جهانی سایبری واگذار می‌شود که این میزان، بسیار بالاتر از ۱۵ درصد میانگین حق‌بیمه رشته‌های بازرگانی است. این موضوع، به تازه‌واردان در عرصه صدور کمک می‌کند تا جای پای خود را در بازار محکم کنند. بااین‌حال، ظرفیت بیمه‌نامه سایبری در سطح صنعت در درجه اول به‌دلیل وجود ظرفیت بالقوه رخداد خسارت نظامی بزرگ، محدود می‌باشد.

بیمه سایبری یا به‌عنوان یک محصول مستقل و یا به‌صورت پکیجی، در یک بیمه‌نامه دیگر ارائه می‌شود.

پوشش‌های بیمه سایبری را می‌توان هم به‌صورت مستقل و هم به‌صورت پکیجی و در یک بیمه‌نامه بازرگانی چندخطره موجود ارائه کرد[۳]. بازار بیمه مستقل سایبری، در پاسخ به معرفی استثناهای بیمه‌ای سایبری در بیمه‌نامه‌های دیگر توسعه یافت و حق بیمه 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[۴]. بیمه‌نامه‌های مستقل معمولاً توسط شرکت‌های بزرگ‌تر که دارای اطلاعات و منابع مالی مهم و در معرض خطر هستند، خریداری می‌شوند. براساس داده‌ها و اطلاعات مکمل سایبری ثبت‌شده در NAIC، میانگین حق بیمه در بیمه‌نامه‌های صادره مستقل در سال ۲۰۲۱ به ۱۲،۱۶۱ دلار افزایش یافت، درحالی‌که حق بیمه بیمه‌نامه سایبری پکیجی مانند بیمه‌نامه‌های شاخه مالی (بیمه مسئولیت مدیران و مسئولان شرکت‌ها[۵] (D&O)) یا حرفه‌ای (فناوری و بیمه مسئولیت اشتباه و خطا[۱]

1. Managing general agents (MGA)
2. Managing general underwriters (MGU)
۳. حق‌بیمه‌های سایبری در بیمه‌نامه‌های پکیجی یا به‌صورت دقیق کمی بیان می‌شود و یا برآورد می‌شوند.
4. Cyber Risk Task Force, “Cyber Risk Toolkit”, American Academy of Actuaries, August 2021, updated February 2022.
5. Directors and officers (*D&O*)

(E&O))، افزایش ۴۸۰ دلاری داشته است (میانگین حق‌بیمه بیمه‌نامه مستقل در شکل ۶، سمت راست نشان داده شده است). حدود ۲۵۹،۰۰۰ بیمه‌نامه مستقل در پایان سال ۲۰۲۱ در مقایسه با ۳/۵ میلیون بیمه نامه پکیجی صادر شده است. نود و چهار درصد از بیمه نامه‌های مستقل نیز به جای حادثه-محور، به‌عنوان خسارت-محور طبقه‌بندی شدند[۲]؛ درحالی‌که این نسبت در بیمه نامه‌های پکیجی، حدود ۵۰ درصد حادثه-محور و ۵۰ درصد خسارت-محور بوده است.



شکل ۶: کل حق بیمه صادره مستقیم (میلیون دلار آمریکا) گزارش‌شده در اطلاعات مکمل سایبری ثبت‌شده در NAIC ایالات متحده (سمت چپ)، متوسط حق بیمه (دلار آمریکا) بر اساس نوع بیمه‌نامه (راست)

منبع: NAIC

روند محصول: افزایش تقاضا برای پوشش‌های شخص اول و ثالث

پوشش شخص اول در سال‌های اخیر با گسترش حملات بدافزارها به‌سرعت رشد کرده است.

در پی افزایش حملات باج‌افزاری، پوشش‌های شخص اول نیز با تمرکز شرکت‌ها بر حفاظت از داده‌ها و جلوگیری از وقفه در کسب‌وکار افزایش یافته است. حمله NotPetya در سال ۲۰۱۷ نشان‌دهنده شروع تغییر تقاضا از پوشش شخص ثالث به شخص اول بوده است. برخلاف شکایت‌های گروهی قبلی، خسارت‌های ثبت‌شده در حمله سایبری NotPetya، مربوط به از دست دادن داده‌ها نبوده و اغلب برای

1. *Errors and omissions insurance* (E&O)

۲. بیمه‌نامه‌های خسارت-محور، حوادثی را پوشش می‌دهند که در چارچوب زمانی بیمه نامه رخ می‌دهند و گزارش می‌شوند، درحالی‌که بیمه نامه های حادثه -محور برای حوادثی که در طول دوره بیمه نامه رخ می‌دهند، پوشش مادام‌العمر ارائه می‌دهند.

آسیب‌های مالی و عملیاتی ناشی از حمله بدافزارها بوده است[۱]. تا سال ۲۰۱۹، با گسترش باج‌افزارها و پیچیدگی روزافزون گروه‌های هکر مجرم، شرکت‌ها با خسارت‌های شخص اول زیادی مواجه شدند.

خسارت‌های شخص ثالث را فراموش نکنید: قوانین اخیر حریم خصوصی احتمالاً موجب افزایش تقاضای برای پوشش مسئولیت سایبری می‌شود.

در کنار افزایش خسارات باج‌افزاری و اقدامات مرتبط با آن، قوانین و احکام اخیر حفظ حریم خصوصی نیز در افزایش تقاضا برای پوشش‌های شخص ثالث مانند جریمه‌ها، هزینه‌های قانونی و مسئولیت حفظ حریم خصوصی و امنیت شبکه، مؤثر هستند. نتایج پرونده‌های موجود نشان می‌دهد که سابقه حملات سایبری شرکت‌ها و بیمه‌گران پس‌از اجرای قوانین حفاظت از داده‌ها مانند GDPR اتحادیه اروپا، قانون حفظ حریم خصوصی مصرف‌کننده کالیفرنیا، قانون حفظ حریم خصوصی اطلاعات بیومتریک ایلینوی، و قانون حفاظت از اطلاعات شخصی چین، مشخص شد. علاوه‌بر این موارد، شرکت‌ها باید قوانین جدید را نیز در نظر داشته و مواجهه‌های بالقوه با ریسک سایبری خود را زیرنظر داشته باشند. به‌عنوان مثال، براساس قانون حفاظت از داده‌ها و حریم خصوصی آمریکا، که در ژوئن ۲۰۲۲ در مجلس نمایندگان ایالات متحده معرفی شد، شرکت‌ها باید اقدامات امنیتی را برای محافظت و ایمن‌سازی داده‌های شخصی خود در برابر دسترسی‌های غیرمجاز اجرا کرده و افراد می‌توانند هنگام تخلف از قانون، از آن‌ها شکایت کنند[۲].

روند خسارت‌ها: ریسک‌های نظامی باعث افزایش شدید نرخ می شوند.

این حملات و آگاهی بیشتر از ریسک، باعث افزایش قیمت بیمه سایبری شده است.

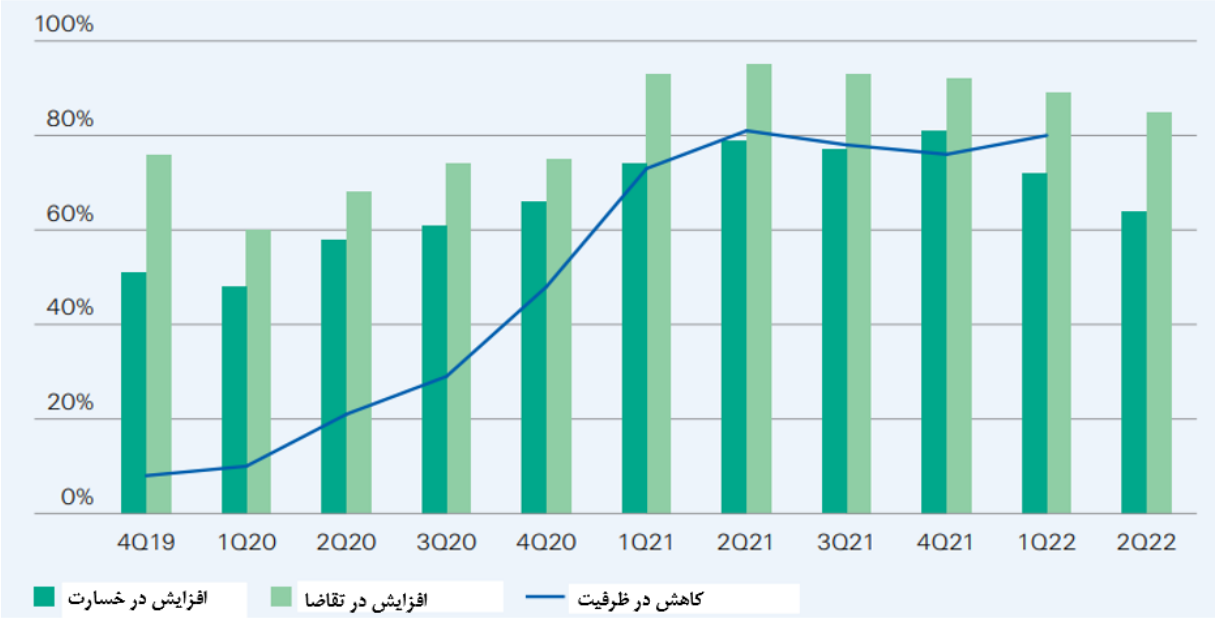
به‌طور خلاصه می‌توان نتیجه گرفت که تقاضا برای بیمه سایبری و آگاهی از ظرفیت بالقوه خسارات نظامی، افزایش یافته است. ظرفیت صدور بیمه نامه، همگام با افزایش میزان تقاضا، افزایش نیافته و همین امر سبب بالاتر رفتن قیمت‌ها شده است؛ طوری که برخی از کارگزاران افزایش سه رقمی

---

۱. به‌عنوان مثال: "FedEx Hit with Cyber Attack-Related Securities Suit", The D&O Diary, 28 June 2019.

2. American Data Privacy and Protection Act, Library of Congress, accessed 22 August 2022.

سال‌به‌سال را در سال ۲۰۲۱ گزارش کرده‌اند[1]. در نظرسنجی سه ماهه دوم شورای نمایندگان و کارگزاران بیمه در سال ۲۰۲۲، ۸۵ درصد از پاسخ‌دهندگان افزایش تقاضا برای پوشش‌های بیمه سایبری و ۶۴ درصد، افزایش خسارت‌ها را گزارش کرده‌اند[2]. این مقادیر در سال ۲۰۲۱ کمتر بوده اما نشان‌دهنده افزایش مداوم تقاضا و ایجاد خسارت نامطلوب می‌باشند. عرضه محصولات بیمه سایبری همواره محدود بوده و تقریباً ۸۰ درصد از پاسخ‌دهندگان در نظرسنجی کاهش ظرفیت را در سه ماهه اول سال ۲۰۲۲ گزارش کرده‌اند[3]. علاوه‌بر افزایش نرخ دو رقمی از اواخر سال ۲۰۲۰، بیمه‌گران محدودیت‌های فرعی را نیز برای پوشش‌های باج‌افزاری، بیمه مشارکتی بالای ۵۰ درصد برای پرداخت باج و فرایند درخواست تجدید نظر، لحاظ نمودند.



شکل ۷. درصد پاسخ‌دهندگان نشان‌دهنده افزایش تقاضای خسارت در مقابل کاهش ظرفیت

منبع: شورای نمایندگان و کارگزاران بیمه، مؤسسه Swiss Re

استانداردهای کاهش خسارت، پیش‌نیاز بررسی ریسک صدور بیمه‌نامه است.

افزایش اخیر حملات باج‌افزاری منجر به به‌روزرسانی‌های هدفمند بیمه‌نامه‌ها شده است.

1. "BRIEF-U.S. Q4 cyber insurance rates soar 130%, UK up 92%-Marsh", Reuters, 2 February 2022.
2. Commercial Property/Casualty Market Index: Q2/2022, Council of Insurance Agents and Brokers (CIAB), August 2022.
3. Commercial Property/Casualty Market Index: Q1/2022, CAIB, May 2022.

بیمه‌گزاران و مشتریان در ایالات متحده و در سطح جهان اکنون باید آمادگی خود را در برابر حملات باج‌افزارها نشان دهند. بیمه‌گران یا شرکت‌های تحلیل‌گر مرتبط، قرار گرفتن در معرض ریسک‌های سایبری را ازطریق اسکن کردن اطلاعات، اهمیت به طرح تداوم کسب‌وکار/طرح بازیابی از فاجعه[1]، کنترل دسترسی‌های خاص، احراز هویت چندعاملی و اسکن/تست فعال[2] مورد بررسی قرار می‌دهند. به‌طور معمول، هنگام صدور بیمه‌نامه و یا در زمان تمدید آن، باید از یک فرم[3] جهت بررسی وضعیت امنیت سازمان در برابر باج‌افزارها استفاده کرد و درصورتی‌که امنیت سازمان پایین باشد، بیمه‌نامه صادر نشده و یا تمدید نگردد.

فرایند صدور بیمه‌نامه می‌تواند انگیزه‌ای برای کاهش ریسک ایجاد کند.

هزینه‌های اجرای اقدامات امنیتی مورد نیاز بیمه‌شدگان به‌منظور رسیدن به سطح پایه بهداشت سایبری را می‌توان از بخش ذخیره حق بیمه جبران نمود. بنابراین، فرایند درخواست و صدور بیمه‌نامه می‌تواند یک سازمان را تشویق کند که ریسک‌های خود را ارزیابی نموده و به سمت اجرای اقدامات امنیتی مبتنی بر ریسک به‌منظور به حداقل رساندن میزان حق‌بیمه سوق دهد. در واقع، پوشش‌های بیمه سایبری، شرکت‌ها را وادار می‌کنند جانب احتیاط را در امور خود رعایت کنند و درنتیجه احتمال خسارت کاهش می یابد[4].

استانداردهای صدور بیمه‌نامه می‌توانند اثرات خارجی بر شرکت‌ها داشته و در دستیابی به اهداف بازدارندگی سایبری کمک کنند.

انجمن بیمه اموال مسئولیت آمریکا[5] تاب‌آوری سایبری را به‌عنوان "یک تعهد اجتماعی" توصیف کرده است؛ به این معنی که شرکت‌ها باید به تاب‌آوری سایبری مانند یک تعهد اجتماعی توجه کنند[6]. به‌دلیل ماهیت بدون مرز فضای سایبری، شرکت‌هایی که فاقد ابزارهای مناسب جهت حفظ امنیت دیجیتال

1. Business continuity/disaster recovery planning
2. Pro-active scanning/testing
3. Supplemental ransomware application
4. I. Ehrlich and G. Becker, “Market Insurance, Self-Insurance, and Self-Protection,” Journal of Political Economy, Vol. 80, No. 4, July–August 1972.
5. *American Property Casualty Insurance Association* (APCIA)
6. E. Gilligan, “APCIA Announces Strong Cyber Extortion/Ransomware Guiding Principles”, American Property Casualty Insurance Association, 1 July 2021.

هستند، خود و اقتصاد جامعه را در معرض خطر قرار می دهند. پس‌از حملات سایبری مهم مانند حمله به نظام‌های فناوری اطلاعات خط لوله کولونیال، قانون‌گذاران اقدام به اعمال فشار در جهت لزوم حفظ امنیت اطلاعات شرکت‌ها نمودند. در این راستا، ایالات متحده استراتژی جدیدی را وضع نمود که شامل قوانینی بود که سازمان‌ها را ملزم به رعایت حداقل استانداردهای امنیت سایبری، مشارکت با بخش خصوصی و اجرای دقیق‌تر هرگونه قوانین جدید می‌نمود[1]. بیمه سایبری با توجه به اینکه می‌تواند نیاز به قوانین مختلف را محدود کرده و همکاری سازنده بین بخش‌های خصوصی و دولتی را ارتقا بخشد، مشوق‌های مالی همسو با اهداف بازدارندگی سایبری بازار و مقامات دولتی را فراهم می‌کند.

شکل ۸: معیارهای صدور بیمه‌نامه و منابع اطلاعات

منبع: Swiss Re, CyberCube

بخش‌های دولتی و خصوصی نیز می‌توانند به‌منظور بهبود استانداردهای امنیت سایبری همکاری کنند.

نهادهای دولتی و خصوصی نیز می‌توانند امنیت سایبری را با هماهنگی در فرایندهایی مانند "طراحی و آزمایش" بهبود بخشند. مشابه کدهای ساختمانی در زلزله یا آتش‌سوزی و آزمایش تصادف برای

---

۱. به‌عنوان مثال، در اوایل سال ۲۰۲۲، کریس اینگلیس، مدیر ملی سایبری ایالات متحده، اظهار داشت: «وقتی که بحث فعالیت‌های حیاتی که در خدمت نیازهای جامعه هستند، مطرح می‌شوند، برخی چیزها اختیاری نیستند.» مراجعه کنید به: " Inside the plan to fix America's never-ending cybersecurity failures" MIT Technology Review, ۱۸March ۲۰۲۲.

خودروها، سخت‌افزارها و نرم‌افزارهایی در حوزه سایبری را می‌توان قبل از انتشار آن‌ها آزمایش نموده و سپس به‌طور رسمی تأیید نمود. اخیراً یک نرم‌افزار جدید برچسب‌گذاری در ایالات متحده با الگوبرداری از نرم‌افزار Energy Star طراحی شده که برای ارتقای بهره‌وری انرژی استفاده می‌شود[1].

مشتریان بیمه می‌توانند از خدمات جانبی نیز بهره‌مند شوند.

شرکت‌های امنیت سایبری با ارائه تخصص‌های فنی و خدمات پشتیبانی، نقش مهمی در فعالیت‌های بیمه ایفا می‌کنند.

شرکت‌های بیمه اغلب با شرکت‌های امنیت سایبری جهت توسعه محصولات سفارشی‌سازی‌شده برای مشتریان، به‌ویژه در بخش زیرساخت‌های حیاتی، همکاری دارند. شرکت‌های امنیت سایبری از وجود تیم‌هایی با قابلیت‌های فنی قوی برخوردار هستند که می‌توانند پروژه را هدایت کرده یا به‌عنوان ارائه‌دهندگان خدمات و مشاوران ریسک عمل کنند. مشارکت شرکت‌های امنیت سایبری با شرکت‌های بیمه، ارائه راه‌حل‌های حفظ امنیت سایبری جامع، ازجمله نظارت مستمر بر ریسک‌های سایبری را افزایش می‌دهد.

بیمه‌گران/ بیمه‌گران اتکایی باید با همکاری شرکت‌های سایبری یک ارزش پیشنهادی یکتا[2] ایجاد کنند.

بیمه‌گران سایبری می‌توانند در هنگام وقوع حمله، فراتر از کاهش ریسک و عملکرد انتقال آن عمل نمایند. بیمه‌گران خدمات مربوط به پرداخت و جبران خسارت را ارائه داده، درحالی‌که شرکت امنیت سایبری خسارت‌ها را ارزیابی می‌کند. علاوه‌بر خدمات ذکرشده، کمک‌های اضطراری، کنترل فرایند سرقت و بازیابی اطلاعات نیز در دسترس مشتریان قرار دارد. در برخی از کشورها، بیمه‌گران/بیمه‌گران اتکایی و شرکت‌های امنیت سایبری با بخش عمومی همکاری می‌کنند تا تصویری جامع‌تری از ریسک

1 “White House to unveil ambitious cybersecurity labeling effort modeled after Energy Star” Cyberscoop, 11 October, 2022.

۲: Unique value proposition مهم‌ترین عنصر کسب‌وکار که ماهیت وجودی و مزیت شرکت را در مقابل سایر رقبا مشخص می‌کند.

ایجاد شود. موارد ذکرشده می‌تواند دامنه تجارت بیمه‌گران/ بیمه‌گران اتکایی را گسترش دهد، اما این کار نیازمند سرمایه‌گذاری جهت توسعه مهارت‌ها و مشارکت‌های لازم است.

جدول ۵: فرایند بیمه سایبری در یک مدل مشارکت معمولی

قبل از صدور بیمه‌نامه	قبل از حمله سایبری	بعد از حمله سایبری
مصاحبه متخصصین ریسک	پایش ریسک‌های احتمالی و کاهش خسارت	خطوط تماس اضطراری ۲۴/۷
بررسی امنیت سایبری	آموزش مشتریان برای درک بهتر قوانین، مقررات و روند خسارت	فروشنده پاسخ اضطراری اختیاری
بررسی پرونده‌های خسارت	آزمایش نظام برای بهینه سازی اقدمات پیشگیری از خسارت	گزارش بررسی حوادث
ارائه راه‌حل‌های سایبری و قیمت‌گذاری		

منبع: موسسه Swiss Re

پرداختن به ریسک کل[1] و سایر محدودیت‌های بیمه‌پذیری

پرداختن به چالش‌های بیمه‌پذیری می‌تواند رشد بالقوه بازار بیمه سایبری را تقویت کند.

با توجه به عدم اطمینان موجود در ریسک‌های سایبری، ارائه‌دهندگان بیمه ازطریق انتخاب ریسک های بهتر، محدودیت‌های کمتر، بیمه مشترک و شرایط سخت‌گیرانه‌تر در بیمه‌نامه، به‌صورت انتخابی بیمه‌نامه‌ها را صادر می‌کنند[2]. به این طریق، شرکت‌های بیمه اندازه پرتفوی و درنتیجه قرار گرفتن در معرض ریسک سایبری را کاهش داده و بازار، رشد کافی نخواهد داشت. این امر می‌تواند اقتصاد را بیشتر در معرض تهدیدات سایبری قرار دهد و بر تاب‌آوری جامعه تأثیر گذارد. با کاهش عدم اطمینان‌ها، عهده‌داران ریسک[3] می‌توانند ریسک‌های سایبری را بیمه‌پذیر کنند و ظرفیت بالقوه رشد بازار بیمه سایبری را بهبود بخشند. در این بخش، بر افزایش قابلیت بیمه‌پذیری سایبری با بهبود

1. Aggregation risk
2. J. Pendleton, Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market, US Government Accountability Office, 20 May 2021.
3 Risk carriers

دانش ریسک ازطریق داده‌ها و مدل‌سازی، و افزایش شفافیت در حوزه خسارت‌های فاجعه‌بار تمرکز می‌شود.

جدول ۶: بیمه‌پذیری ریسک‌های سایبری

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
معیارهای بیم‌سنجی	فراوانی و شدت ریسک باید به‌طور 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 به‌منظور اهداف امنیتی خودداری کنند. به‌عمد، ماهیت حملات به‌طور مداوم در حال تغییر است تا از تجزیه‌وتحلیل و کاهش آن فرار کنند. مدل‌های سایبری در مراحل ابتدایی خود باقی مانده و توسعه نمی‌یابند.	خلق نوآوری به‌منظور ایجاد پایگاه داده جمعی (تلفیقی)، بهبود استانداردسازی برای مدل‌سازی و تجزیه‌وتحلیل، و تعریف شفاف مواردی که جزء یک حمله سایبری هستند (توصیه ۱).
	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 قبلاً 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[1] (خسارت‌هایی غیر از خسارات فجایع یا مواجهه‌های بزرگ) جدا کنید.
	متوسط مقدار خسارت در هر رخداد قابل پیش‌بینی باشد و تعداد زیادی از رخدادهای خسارت مشابه در سال اتفاق	اساس بازار بیمه سایبری به‌خوبی تثبیت شده است.	افزایش نرخ جذب بیمه در بخش‌ها و اندازه شرکت‌ها؛ جداسازی ریسک‌های فاجعه‌آمیز از خسارت‌های فرسایشی

1 Attritional losses

	معیارهای بیمه‌پذیری	وضعیت فعلی	تغییرات برای بهبود بیمه‌پذیری
	بیفتد.		
	کمبود اطلاعات نامتقارن[1] در این حوزه (به‌عنوان مثال، کژمنشی یا مخاطرات اخلاقی[2]، کژگزینی/ انتخاب نامطلوب[3])	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
معیارهای بازار	برای یک بازار بیمه پایدار، حق بیمه باید از نظر پوشش ریسک، کافی باشد.	میزان خسارت واردشده 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 مؤثر است (توصیه ۲).

منبع:

C. Biener, M. Eling, J.H Wirfs, Insurability of Cyber Risk – An Empirical Analysis, University of St. Gallen, 2015; C. Christophe, P. Liedtke, "Insurability, its limits and extensions", Insurance Research and Practice, vol 18 (2), 2002; B. Berliner, Limits of Insurability of Risks, 1985

بهبود دانش ریسک جهت کاهش عدم قطعیت در تعیین قیمت

داده‌های استاندارد و بهبود مدل‌سازی می‌تواند پوشش‌های موجود ارائه شده را گسترش دهد.

هنگامی که درجه بالایی از عدم اطمینان در میانگین خسارت‌های مورد انتظار وجود داشته باشد، بیمه‌گران تمایل دارند پوشش‌های ارائه‌شده را محدود کنند. برای این منظور، کاهش عدم قطعیت با استفاده از اطلاعات و داده‌ها و بهبود ظرفیت مدل‌سازی، می‌تواند پوشش‌های موجود ارائه‌شده در بازار را گسترش دهد. به‌دلیل فقدان داده‌های استاندارد و محدودیت‌های مدل‌سازی در یک محیط ریسکی

1. Information Asymmetry
2. Moral hazard
3. Adverse selection

در حال تغییر، کمی‌سازی ریسک‌های سایبری دشوار است. اکچوئرها معمولاً ریسک‌های آینده را براساس داده‌های گذشته تفسیر می‌کنند، اما این رویکرد در زمینه ریسک سایبری به دو دلیل امکان‌پذیر نیست: ۱) فقدان داده‌های استاندارد؛ و ۲) داده‌ها و اطلاعات گذشته در یک محیط ریسکی که به‌سرعت در حال تغییر است، کاربرد چندانی ندارد. جمع‌آوری و تجزیه‌وتحلیل داده‌های مناسب برای مدل‌سازی احتمالی[1] و توسعه تخمین خسارت‌های موثق جهت درک بهتر پویایی و پیامدهای خسارت سایبری بسیار مهم است. این امر مستلزم دانش دقیق از دامنه ریسک‌ها، تأثیرات آن‌ها و اعتبار داده‌ها است[2]. معرفی استانداردهای امنیت سایبری همچنین می‌تواند عدم اطمینان خسارت‌های بالقوه را کاهش دهد.

بخش خصوصی و دولتی اقدام به استانداردسازی داده‌ها نموده‌اند.

تلاش‌های بخش خصوصی برای رفع این کاستی‌ها شامل ایجاد شرکت CyberAcuView، کنسرسیومی از بیمه‌گران سایبری پیشرو در جمع‌آوری داده‌های حملات سایبری و خسارت‌ها، و توسعه استانداردهای اطلاعات سایبری می‌شود. در اروپا نیز فدراسیون بیمه و بیمه اتکایی اقداماتی را برای تسهیل دسترسی به داده‌های استاندارد و داده‌های سرقتی جمع‌آوری‌شده تحت GDPR انجام می‌دهد[3]. زمینه برای هماهنگی بین بخش دولتی و خصوصی نیز در حال افزایش است. برای مثال، در مارس ۲۰۲۲ قانون گزارش‌دهی رویدادهای سایبری ایالات متحده برای زیرساخت‌های حیاتی آن‌ها به تصویب رسید که اپراتورهای زیرساخت‌های حیاتی خود را ملزم می‌کنند «حوادث سایبری قابل توجه» را در عرض ۷۲ ساعت به آژانس امنیت سایبری و امنیت زیرساخت وزارت امنیت داخلی و حملات باج‌افزاری را طی ۲۴ ساعت گزارش کنند.

1. Probabilistic modelling
2. sigma 1/2017 op. cit., https://www.insuranceeurope.eu/priorities/27/cyber
3. See Insurers' key role in increasing cyber resilience, Insurance Europe., https://www.insuranceeurope.eu/priorities/27/-cyber

کمی‌سازی ریسک سایبری به‌دلیل تغییر سریع ماهیت آن، به چالش کشیده شده است.

حتی زمانی که بازار بیمه سایبری بالغ شده و داده‌های کافی در دسترس قرار گیرد، تخمین دقیق خسارت با توجه به ماهیت در حال تحول ریسک، چالش‌برانگیز خواهد بود. فناوری‌های نوین، انگیزه‌های جدید، عوامل تهدید و روش‌های حمله، اطلاعات گذشته را به راهنمای ضعیفی برای برآورد آینده تبدیل می‌کند، زیرا توزیع خسارت در مدل‌های جدید، سریع‌تر از روند سنتی تغییر می‌کنند. این ویژگی‌های ریسک سایبری، هر دو مدل احتمالی و سناریویی را با محدودیت‌هایی روبه‌رو می‌کنند. داده‌های مربوط به مشتریان فردی برای ارزیابی ریسک کافی نبوده و باید با داده‌های صنعت تکمیل شود. برای این کار باید از مدل‌هایی استفاده کرد که قادر به اتخاذ روش‌های تحلیلی جدید ازجمله هوش مصنوعی (AI) و یادگیری ماشین (ML) باشند. ماهیت این مدل‌ها پویا هستند؛ به این معنی که به حاکمیت مدل [۱] بیشتری نیاز دارند (به‌عنوان مثال، نظارت بر عملکرد، بررسی داده‌ها و معیار).

با استفاده از مدل‌های مبتنی بر سناریو می‌توان میزان مواجهه بالقوه با ریسک سایبری را بهبود بخشید.

تا به امروز یک فاجعه سایبری واقعی رخ نداده و اطلاعات کافی در این زمینه ثبت نشده است؛ بنابراین، استفاده از سناریونویسی در تخمین میزان خسارت به‌منظور ایجاد درک مقیاس زیان واردشده، و با تأکید بر ظرفیت بالقوه انباشت ریسک و افزایش سطح کلی ریسک، می‌تواند آموزنده باشد (برای انواع روش‌های اصلی برآورد خسارت سایبری به جدول ۷ مراجعه کنید.) و در نهایت به عهده‌دارهای ریسک (بیمه‌گران/ بیمه‌گران اتکایی) اطمینان می‌دهد که می‌توانند ظرفیت بیشتری از سهم شرکت خود را به بخش سایبری اختصاص دهند[۲]. جنگ سایبری، اختلال در دسترسی به فضای ابری در نرم‌افزارهای حیاتی یا استقرار بدافزارها از طریق نرم‌افزارهای رایج، نمونه‌هایی از سناریوهایی هستند که می‌توانند خسارات فاجعه‌باری ایجاد کنند. شرکت‌های بیمه/بیمه‌گران اتکایی و شرکت‌های تحلیل‌گر باید به سناریونویسی اختصاصی خود بپردازند، که با استانداردسازی داده‌ها و تجربه رویدادهای سایبری جدید، اطلاعات در این زمینه بهبود یابد.

---

۱. Model governance مجموعه ای از فرایندها و چارچوب هایی است که به استقرار ML کمک می‌کند.

2. Cost of a Cyber Incident: Systematic Review and Cross-Validation, CISA, 26 October 2020.

کاهش شکاف مهارت‌های امنیت سایبری در شرکت‌های فناوری و بیمه‌گر/بیمه‌گرهای اتکایی می‌تواند به کسب‌وکارها کمک کند، به ریسک‌های پویا مسلط باشند.

شرکت‌های فناوری و بیمه‌گر/بیمه‌گران اتکایی نیز برای اینکه بتوانند در برابر ریسک‌های نوظهور آماده باشند، باید به‌طور مداوم برای توسعه بیشتر تخصص سایبری نیروی کار خود تلاش کنند. به‌عنوان مثال، در اکتبر ۲۰۲۱، مایکروسافت ابتکاری را برای پر کردن شکاف مهارت‌های امنیت سایبری، با استفاده از ایجاد برنامه و ابزارهای آموزشی رایگان رونمایی کرد[1]. شرکت‌های بیمه/بیمه اتکایی نیز می‌توانند با تقویت مشارکت خود با دانشگاه‌ها جهت توسعه برنامه‌های آموزشی مرتبط با کسب‌وکارشان، به مقابله با کمبود استعدادهای سایبری کمک نمایند. آموزش‌ها می‌تواند شامل مدل‌سازی ریسک سایبری و تحلیل‌های امنیتی برای تقویت مهارت‌های بیم‌سنجی و فنی مورد نیاز در چرخه‌های صدور بیمه‌نامه و مدیریت خسارت‌ها باشد.

ظرفیت پذیرش ریسک‌های سایبری در بازار را می‌توان با استفاده از شفافیت در حوزه ریسک‌های فاجعه‌آمیز افزایش داد.

فعالیت‌های بیمه‌گری و استانداردسازی داده‌ها می‌تواند به بیمه‌گران کمک کند تا خسارت‌های فرسایشی[2] را مدیریت کنند، اما ظرفیت موجود در سایبری تحت تأثیر رویدادهای شدید بالقوه دیگری نیز هستند که سرمایه زیادی لازم دارند. درصورتی‌که به مدل‌سازی ریسک‌های فاجعه‌آمیز سایبری و شفافیت درباره آنچه که موجب خسارت‌های فاجعه‌بار می‌شود، بهای بیشتری داده شود، بیمه‌پذیری ریسک‌های سایبری بهبود یافته و منجر به جذب بیشتر ظرفیت پذیرش ریسک سایبری در بازار می‌شود.

1. Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries, Microsoft, 23 May 2022.
۲. خسارت‌هایی که به فجایع یا رخدادهای بزرگ ریسک مرتبط نیستند.

جدول ۷: انواع روش‌های اصلی برآورد خسارت سایبری

روش	توصیف
تحلیل از پایین به بالا	به داده‌های خرد آماری[1] (مانند داده‌های مربوط به حمله سایبری فردی)، که معمولاً در تحلیل‌های بیم‌سنجی برای ارزیابی ریسک استفاده می‌گردد، تکیه می‌شود.
برآوردهای کل (مقیاس ملی/جهانی)	معمولاً توسط فروشندگان امنیت سایبری برای نشان دادن نیاز به سرمایه گذاری در امنیت سایبری استفاده می‌شود.
روش سناریونویسی	بر حملات شدید با میزان خسارت بالا تمرکز دارد.

منبع: Cost of a Cyber Incident: Systematic review and cross-validation, CISA, Swiss Re Institute

ریسک کل، دغدغه بخش دولتی و خصوصی را به هم مرتبط می‌کند.

برخی از سناریوهای بالقوه سایبری ممکن است منجر به کاهش ظرفیت ریسک‌پذیری شود. به‌عنوان مثال، در سال ۲۰۱۵ لویدز تخمین زد که یک حمله سایبری گسترده به شبکه برق ایالات متحده می‌تواند تا ۱ تریلیون دلار خسارت اقتصادی و ۷۱ میلیارد دلار خسارت بیمه‌ای ایجاد کند[2]. پیامدهای ناشی از این نوع حملات شامل افزایش نرخ مرگ‌ومیر، کاهش میزان معاملات و اختلال در منابع و شبکه‌های حمل‌ونقل است که هرکدام ریسک خاص خود را به جامعه وارد می‌کنند. درنتیجه ریسک کل، امنیت ملی و آسیب‌پذیری‌های زیرساختی حیاتی را با بازارهای خصوصی مرتبط می‌کنند. امنیت ملی، اولویت دولت است درحالی‌که بخش خصوصی معمولاً مالک بخش‌های زیادی از زیرساخت‌های حیاتی است که در برابر حملات آسیب‌پذیر هستند. همکاری بین بخش‌های دولتی و خصوصی برای مقابله با تهدیدات سایبری زیرساخت‌ها می‌تواند قابلیت بیمه را با کاهش میزان ریسک و عدم اطمینان در مورد واکنش به فجایع سایبری گسترش دهد.

بخش دولتی با ارائه‌دهندگان زیرساخت‌های حیاتی همکاری دارد.

حمله سایبری به زیرساخت‌های حیاتی می‌تواند تأثیرات آبشاری در سراسر اقتصاد داشته باشد. فراتر از خسارات اقتصادی، یک حمله موفقیت‌آمیز می‌تواند اعتماد مردم را نسبت به شرکت‌های برق و نظام

1. Statistical microdata
2. Business Blackout: The insurance implications of a cyber attack on the US power grid, Lloyd's, July 2015.

مالی از بین ببرد[1]. بخش‌های دولتی و خصوصی برای شناسایی دارایی‌های حیاتی و تعیین نحوه نگهداری، ارائه خدمات و اجرای شیوه‌نامه‌های پاسخ با هم همکاری دارند.

پرداختن به ریسک کل ازطریق استانداردسازی زبان بیمه‌نامه

صنعت برای پرداختن به رویدادهای بالقوه فاجعه‌آمیز، به دنبال یک زبان استاندارد برای بیمه‌نامه است.

جدید بودن نسبی بازار بیمه سایبری و پیچیدگی ریسک باعث شده استانداردسازی کلوزهای استثنا و شرایط و ضوابط عمومی بیمه‌نامه سایبری به‌راحتی صورت نگیرد. ظرفیت بالقوه رویدادهای فاجعه‌بار ناشی از اقدامات جنگی تحت حمایت دولت، اقدامات سایبری خصمانه یا شکست زیرساخت‌های حیاتی - و عدم شفافیت در مورد مسئولیت متعاقب آن‌ها – عامل‌های مهمی در کاهش ظرفیت بیمه سایبری در بازار هستند. با استفاده از روش سناریونویسی، خسارت‌های حملات سایبری حدود ده‌ها میلیارد دلار برآورد شده‌اند که این میزان، چندین برابر حق بیمه سال ۲۰۲۱ است؛ درحالی‌که میزان خسارات اقتصادی واردشده این حملات، بسیار بیشتر از این مقدار هستند. درنتیجه، معرفی و توسعه یک مدل واحد برای مقابله با خسارت‌های کل، می‌تواند با ایجاد راه‌حل‌های قابل درک برای شرکت‌ها و تقویت ریسک‌پذیری بیمه‌گران، از رشد پایدار حمایت کند.

کاستی‌های زبان مشترک بیمه‌نامه با رویکردهای مختلف برطرف می‌شود، اما این رویکردها ممکن است منجر به نپذیرفتن ریسک سایبری در بازار بدون ارائه راه‌حلی برای رخداد بزرگ‌ترین رویدادها شود.

انجمن‌ها، بیمه‌گران فردی و اتاق‌های فکر گام‌هایی برای استانداردسازی تعاریف ذکرشده در بیمه‌نامه ازجمله جنگ سایبری، عملیات سایبری[2] و علم شناسایی مرتکب و مقصر آن‌ها برداشته‌اند. در نوامبر ۲۰۲۱، انجمن بازار لویدز کلوزهایی را معرفی کرد که به‌منظور حذف پوشش جنگ سایبری و عملیات

1. Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts, GAO, 27 September 2020.
2. Cyber operations

سایبری[1] طراحی شده بود، با این الزام که این موارد یا موارد مشابه از ۳۱ مارس ۲۰۲۳ اعمال شود[2]. تأثیر بیانیه صادرشده لویدز، فراتر از بازار مستقیم بیمه می‌رود، زیرا استثناهایی که مطرح می‌کند باید در تمام بیمه‌های اتکایی که سندیکاهای لویدز با آن‌ها مشارکت دارد، رعایت شود و درنتیجه بیمه‌گران/ بیمه‌گران اتکایی دیگر نیز که فعالیت‌هایی مشابه آن‌ها انجام می‌دهند، باید آن را رعایت کنند.

شناسایی مرتکب و مقصر حمله سایبری یک مشکل اصلی است. بیمه‌گران رویکردهای متفاوتی برای شناسایی آن‌ها اتخاذ می‌کنند.

اما داشتن یک رویکرد هماهنگ و واحد در زبان بیمه‌نامه، همچنان در حد یک آرزو باقی مانده است. یک مشکل اساسی در تعیین پوشش‌ها این است که یک فرایند فنی ساده برای شناسای مقصر و مرتکب سایبری وجود ندارد[3]. برخی از ناظران پیشنهاد می‌کنند که بیمه‌گران از پوشش‌های استثنایی که لویدز مطرح کرده[4]، اجتناب کنند. چند شرکت بیمه در ایالات متحده در حال ایجاد کلوزهای استثنای خود برای رسیدگی به رویدادهای فاجعه‌بار سایبری هستند. شرکت Chubb پوشش‌های مناسبی برای رویدادهای شایع و گسترده، برخورد با باج افزارها و نادیده گرفته شدن آسیب‌پذیری‌های نرم افزارها ارائه کرده[5] و چارچوبی برای قیمت‌گذاری ریسک‌های فاجعه‌بار و آسیب‌پذیری‌های درحال تکامل نیز مطرح کرده است و شرکت Beazley درحال به‌روزرسانی موارد استثنای بیمه‌نامه خود در جنگ سایبری و شکست زیرساخت‌ها است و در عین حال محدودیت‌های فرعی را در مورد رویدادهای سایبری فاجعه‌باری که «تأثیر مخرب عمده» بر عملکرد یک ایالت دارند، قرار می‌دهد[6].

گزارش‌های قبلی ایده‌هایی را برای ایجاد زبان مشترک ارائه می‌دهند که همچنان شفاف نیستند، ازجمله تعاریف جدید رویدادهای سایبری و انواع مختلف پوشش‌های استثناء که مطرح کرده‌اند.

1. Cyber War and Cyber Operation Exclusion Clauses, Lloyd's Market Association, 25 November 2021.
2. "State backed cyberattack exclusions", Lloyd's Market Bulletin, 16 August 2022.
3. Guide to Cyber Attribution, US Office of the Director of National Intelligence, 14 September 2018.
4. "Lloyd's Cyber Insurance Tweaks Stir Coverage Restriction Concern", Bloomberg Law, 26 August 2022.
5. Chubb Addresses Growing Cyber Risks with a Flexible and Sustainable Approach, Chubb, 2021.
6. "Beazley finalises systemic cyber wordings ahead of phased rollout", Insurance Insider, 24 August 2022.

گزارش‌های قبلی گواه این هستند که به سمت یک زبان مشترک بیمه‌نامه پیش رفته و بینش‌هایی برای کمک به تکامل زبان بیمه‌نامه سایبری صنعت نیز ارائه شده است. به‌عنوان مثال، در سال ۲۰۲۰ انجمن ژنو[1] اصطلاح «فعالیت سایبری خصمانه[2]» را برای توصیف اقدامات سایبری که بین جنگ و تروریسم[3] قرار می‌گیرند پیشنهاد کرد، درحالی‌که موقوفه کارنگی[4] پیشنهاد داد از دو پوشش استثنای مکمل برای مقابله با حملات سایبری فاجعه‌آمیز و حملات سایبری مرتبط با جنگ یا ریسک‌های سایبری که با حمایت دولت انجام می‌شوند، به‌صورت مجزا استفاده شود[5]. برخی از شرکت‌ها انتظار دارند که بیشتر تحت تأثیر ریسک‌ها و حملات فاجعه‌آمیز / معمولی قرار بگیرند و کمتر در معرض پوشش استثنای بیمه‌نامه حملات مرتبط با جنگ باشند[6].

شرکت‌های بیمه اقداماتی را برای مقابله با قرار گرفتن در معرض سایبری خاموش انجام داده‌اند.

سایبری خاموش، ریسک بزرگی برای صنعت دارد.

پوشش بیمه سایبری اشاره‌شده در این گزارش، به‌صورت پوشش‌های بیمه‌نامه مستقل است، زیرا ریسک‌ها در بیمه‌نامه به‌صراحت درج شده یا مستثنی شده‌اند. "سایبری خاموش" یک موضوع مرتبط با این موضوع است، که در آن ریسک‌های سایبری به‌صراحت در بیمه‌نامه‌های سنتی فهرست نشده‌اند، اگرچه دارندگان این نوع بیمه‌نامه‌ها ممکن است همچنان طلب خسارت کنند. بنابراین، سایبری خاموش می‌تواند منجر به خسارات قابل توجهی برای بیمه‌گران شود، علی‌رغم اینکه در این نوع بیمه‌نامه، آن‌ها قصد ندارند پوشش سایبری ارائه کنند. مثال روشنی دراین‌باره، حمله NotPetya در اوکراین است که علی‌رغم وقوع یک حمله سایبری، تقریباً ۸۵ درصد از خسارت‌های صنعت بیمه،

1. Geneva Association
2. Hostile cyber activity
3. R. Carter, J. Enoizi, Cyber War and Terrorism: Towards a common language to promote insurability, Geneva Association, 23 July 2020.
4. *Carnegie Endowment*
5. War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions, Carnegie Endowment for International Peace, 5 October 2020.
6. M. Geoghegan, “Episode 122 Dan Trueman: The only way to be in Cyber is to be an expert”, The Voice of Insurance Podcast, 10 May 2022.

ازطریق خسارت‌های ثبت‌شده بیمه اموال بوده که صراحتاً شامل حملات سایبری یا حذف آن نشده بود[۱].

بیمه‌گران سعی کرده‌اند با ارائه بیمه‌نامه‌های بهتر ازجمله ذکر پوشش‌های استثنای جدید، به این مشکل پاسخ دهند.

قرار گرفتن در معرض سایبری خاموش را می‌توان با بیان صریح آن در بیمه‌نامه، یا به‌صورت اعلام و قیمت‌گذاری آن‌ها در بیمه‌نامه‌های پکیجی (غیرسایبری) و یا انتقال ریسک آن‌ها به‌صورت بیمه‌نامه‌های مستقل کاهش داد. ارزیابی ریسک بهتر و قیمت‌گذاری دقیق‌تر، پایداری بازار را بهبود می‌بخشد. شرکت‌های بیمه اقداماتی را برای رسیدگی به ریسک‌های سایبری خاموش، به‌روزرسانی بیمه‌نامه‌ها و شروع استانداردسازی عبارت‌ها، استثناها و الحاقیه‌ها انجام داده‌اند. به‌عنوان مثال، در نوامبر ۲۰۱۹، انجمن بازار لویدز[۲] (LMA) کلوزهایی را برای رسیدگی به حملات سایبری خاموش در بیمه اموال و بیمه باربری دریایی ارائه نمودند[۳].

افزایش ظرفیت بیمه سایبری به‌وسیله عهده‌داران ریسک غیرسنتی

زمینه برای افزایش ظرفیت بیمه سایبری ازطریق مشارکت بیشتر بازار سرمایه وجود دارد ...

یکی از راه‌های رفع کمبود ظرفیت سایبری که ناشی از مدل‌سازی پیچیده و غیرتنوع این گونه ریسک‌ها است، ایجاد بازاری برای اوراق بهادار مرتبط با بیمه سایبری[۴] (ILS) می‌باشد. درحال‌حاضر، تخمین زده شده که سرمایه‌گذاری جایگزین[۵] حدود ۹۵ میلیارد دلار ظرفیت اضافی برای بیمه اتکایی حوادث فاجعه‌آمیز در سال ۲۰۲۲ ایجاد می‌کند که مکمل سرمایه اختصاصی بیمه اتکایی سنتی ۴۳۵ میلیارد دلاری است[۶]. علاقه به رشد روش‌های استفاده از سرمایه‌گذاری جایگزین برای ریسک‌های سایبری در حمایت از یک بازار سایبری پایدار وجود دارد. بااین‌حال، تا به امروز علاقه سرمایه گذاران به استفاده از اوراق بهادار بیمه‌ای به‌علت وجود ریسک کل و عدم قطعیت در مدل‌سازی، محدود بوده

1. Could NotPetya's Tail Be Growing?, PCS, 2019.
2. Lloyd's Market Association
3. Property and Marine Cyber Clauses, Lloyd's Market Association, 3 November 2019.
4. Cyber insurance-linked securities
۵. Alternative capital نوعی از سرمایه‌گذاری که در دارایی‌هایی غیر از سهام سرمایه، اوراق قرضه و وجه نقد انجام می‌شود.
6. Dedicated Reinsurance Capital Growth of 2021 May Not Continue, AM Best Market Segment Report, 22 August 2022.

است. ساختارهای واقعی اوراق بهادار بیمه‌ای (مشابه اوراق مشارکت فجایع[۱]) نیاز به ایجاد محرک‌های عینی دارند که می‌تواند بیمه‌گزار را با ریسک قابل توجهی روبه‌رو کند. مدیران سرمایه‌گذاری جایگزین درحال سرمایه‌گذاری در شرکت‌های اینشورتک بیمه سایبری هستند تا درک ریسک را بهبود بخشند و به‌طور بالقوه سرمایه را برای حمایت از آن گسترش دهند. در ضمن، ساختارهای سرمایه شخص ثالث مبتنی بر خسارت، مانند بیمه/ بیمه اتکایی سایدکار[۲]، می‌توانند ظرفیت جدیدی را برای صدور بیمه‌نامه سایبری ایجاد کنند[۳].

... و مشارکت عمومی – خصوصی

راه‌حل بالقوه دیگر برای رفع کمبود ظرفیت سایبری در بازار، طراحی یک نوع برنامه بیمه‌ای مشارکت عمومی-خصوصی[۴] (PPP) است که در آن پوشش ریسک‌های نظامی بین بیمه‌گران و یک صندوق تحت حمایت دولت (ها) تقسیم می‌شود. در ایالات متحده، دفتر پاسخ‌گویی دولت (دیوان محاسبات)[۵] توصیه کرده که آژانس امنیت سایبری و امنیت زیرساخت و دفتر بیمه فدرال[۶]، ارزیابی مشترکی بر حملات سایبری فاجعه‌بار که به زیرساخت‌های حیاتی آسیب می‌زنند، داشته باشند[۷]. در این ارزیابی بهتر است ساختار، بودجه، الزامات مشارکت و دامنه پوشش ریسک مشخص شده و توسط سیاست‌گذاران خزانه‌داری ایالات متحده[۸] و سایر حوزه‌های قضایی، ارزیابی گردد.

1. Cat bonds
2. Re/insurance sidecars
3. See, for example, “Coalition launches $300m Ferian Re to provide third-party cyber risk capital”, Artemis, 13 October 2022.
4. Public-private partnership (PPP)
5. Government Accountability Office
6. Federal Insurance Office
7. Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, GAO, June 2022.
8. Potential Federal Insurance Response to Catastrophic Cyber Incidents”, Federal Register, Department of the Treasury, 29 September 2022.

نتیجه‌گیری

حدود ۹۰ درصد از افراد و سازمان‌ها تحت پوشش بیمه سایبری قرار نگرفته‌اند.

چشم‌انداز ریسک سایبری به‌سرعت درحال تحول است و با افزایش حملات سایبری، آگاهی از ریسک و تقاضا برای بیمه سایبری نیز افزایش یافته است. بااین‌حال، بیشتر مشاغل و افراد، بیمه نشده یا به میزان کافی تحت پوشش قرار نگرفته‌اند، و حق بیمه سایبری تنها کسری از کل خسارات ناشی از حملات سایبری است. برآوردها نشان می‌دهد که حدود ۹۰ درصد از افراد و سازمان‌ها تحت پوشش قرار نگرفته‌اند. این میزان، اشاره به وجود ظرفیت بالقوه رشدی بزرگ در بازار بیمه سایبری دارد، اما این کار به‌سادگی 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.

کیفیت داده‌ها و مدل‌سازی ریسک نیاز به ارتقا دارند تا جامعه در برابر ریسک‌های سایبری تاب‌آور باشد.

اولین نیاز در توسعه بیمه سایبری، بهبود کیفیت داده‌ها و مدل‌سازی آن‌ها است. به‌دلیل 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 به‌سرعت در حال تغییر هستند، ارزش کمی دارد. معرفی استانداردهای امنیت سایبری باعث شده که داده‌ها از نظر وسعت و شفافیت بهبود یافته، درک ریسک روشن‌تر شده، و قیمت‌گذاری و مدل‌سازی دقیق‌تری را امکان‌پذیر کند. شرکت‌های بیمه نیز باید بر نیروی کار متخصص سایبری سرمایه‌گذاری کنند تا به تقویت مهارت‌های بیم‌سنجی، فنی و حقوقی مورد نیاز برای چرخه‌های بیمه‌گری و مدیریت خسارت کمک شود. بااین‌وجود، درجه بالای عدم اطمینان در مورد خسارت‌های مورد انتظار و ماهیت درحال تحول ریسک، بیمه‌پذیری ریسک‌های کل و فاجعه‌آمیز را به چالش می‌کشد.

بیمه‌گران می‌توانند ازطریق به‌روزرسانی زبان بیمه‌نامه خود به‌منظور وضوح و سازگاری بیشتر، سهم مهمی داشته باشند.

دومین نیاز، به‌روزرسانی زبان بیمه‌نامه‌ها توسط بیمه‌گران/بیمه‌گران اتکایی، به‌منظور 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 به‌راحتی صورت نگیرد. همچنین قرار گرفتن در معرض ریسک‌های نظامی که به‌سختی بیمه می شوند، 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.

طرح های بیمه‌ای عمومی-خصوصی می‌تواند به پوشش حوادث ریسک نظامی کمک نماید.

در نهایت، همچنین نیاز به استفاده از انواع جدیدی از مکانیسم های 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 نظامی 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، بهره برداری از بازار سرمایه جایگزین، مانند توسعه بازاری اوراق بهادار مرتبط با بیمه سایبری است.

پیوست

۱- حملات سایبری منتخب در هر بخش اقتصادی مهم

بخش‌ها	نام حمله	توصیف	مفهوم
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[۱]. خط لوله کولونیال، بزرگ‌ترین نظام توزیع فراورده‌های نفتی تصفیه‌شده کشور آمریکا است و حدود ۴۵ درصد از کل سوخت مصرفی در ساحل شرقی را تأمین می‌کند. در ۷ می ۲۰۲۱، یک حمله باج‌افزاری شرکت را مجبور کرد تا زمانی که باج را پرداخت کند، تمام عملیات‌ها را متوقف نماید. این شرکت، هشت روز بعداز حمله، عملیات خود را بازسازی کرد. این تعطیلی باعث ایجاد وحشت، کمبود سوخت، افزایش قیمت و اختلالات اقتصادی گسترده شد. به‌عنوان مثال، در جورجیا و کارولینای جنوبی، قیمت بنزین معمولی ۸ درصد افزایش یافت[۲].	از نظر ژئوپلیتیکی، این حمله اهمیت نظارت بر امنیت سایبری نظام‌های انرژی حیاتی کشور را برای ایالات متحده، بالا برد[۳]. از نظر مالی، این شرکت ۴/۴ میلیون دلار باج پرداخت کرد (که ۲/۳ 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 می ۲۰۱۷ رخ داد و با رمزگذاری داده‌ها تا زمانی که باج پرداخت شود، نقاط آسیب‌پذیر نظام عامل ویندوز را هدف قرار داد. برآورد شده که این حمله بیش از ۲۳۰،۰۰۰ رایانه را در سراسر جهان آلوده کرده و خسارتی بالغ بر میلیاردها دلار در حوزه عمومی و خصوصی ایجاد نموده است[۴]. این حمله همچنین خدمات سلامت ملی بریتانیا (NHS) را به‌دلیل قدیمی بودن نظام‌های رایانه‌ای تحت تأثیر قرار داد و منجر به از کار افتادن یا از دسترس خارج کردن تجهیزات و نظام های بهداشتی حیاتی شد[۵].	این حمله، عملکرد خدمات سلامت ملی بریتانیا را به خطر انداخت. وزارت بهداشت و مراقبت‌های اجتماعی تخمین زده که این حمله ۹۲ میلیون پوند برای خدمات سلامت ملی بریتانیا هزینه داشته است که شامل ۲۰ میلیون پوند خسارت به‌دلیل اختلال در خدمات و ۷۲ میلیون پوند برای پوشش هزینه‌های مستقیم فناوری اطلاعات بوده است[۶].
حمل‌ونقل، انرژی، زنجیره تأمین	NotPetya	در ژوئن ۲۰۱۷، نسخه بدافزار NotPetya با سوءاستفاده از آسیب‌پذیری‌های مشابه WannaCry در اوکراین شروع به کار کرد و سازمان‌هایی ازجمله دولت، بانک‌ها، شرکت‌های برق دولتی و نظام‌های کلیدی حمل‌ونقل عمومی (فرودگاه،	شبکه زنجیره تأمین در سراسر صنایع و مرزهای متعدد مختل شد. خسارت شرکت‌های پایین دستی ۷/۳ میلیارد دلار تخمین زده می‌شود که چهار برابر بیشتر از

1. "'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack", Politico, 8 May 2021.
2. "The Colonial Pipeline Crisis Is a Taste of Things to Come", Columbia/SIPA (subscription service).
3. Why the energy sector's latest cyberattack in Europe matters, WEF, 4 February 2022.
4. "Petya' ransomware attack: what is it and how can it be stopped?" The Guardian,28 June 2017.
5. See What is WannaCry Ransomware Attack? Fortinet. https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
6. "Department of Health and Social Care puts cost of WannaCry to NHS at GBP 92m," digitalhealth.net, 12 October 2018.

بخش‌ها	نام حمله	توصیف	مفهوم
		مترو) و حتی نظام نظارت بر تشعشعات در چرنوبیل را تحت تأثیر قرار داد[۱]. نهادهای آلوده به ویروس شامل شعبه‌های محلی گروه‌های بین‌المللی مرتبط با شبکه‌های زنجیره تأمین جهانی مانند FedEx یا Maersk بودند.	خسارت شرکت‌هایی است که به‌طور مستقیم آسیب دیده‌اند[۲].
غذا	حمله JBS	در ماه می ۲۰۲۱، بزرگ‌ترین شرکت فراوری گوشت JBS مستقر در برزیل به‌دلیل 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 ۳ تا ۴ روز متوقف کرد. در نهایت، این حمله با پرداخت ۱۱ میلیون دلار باج به پایان یافت[۳].	این حمله کل زنجیره تأمین گوشت را تهدید کرد و مصرف‌کنندگان با ریسک‌های کمبود عرضه و افزایش قیمت گوشت مواجه شدند.
آب	هک نظام آب تامپا[۴]	در فوریه ۲۰۲۱، هک نظام آب تامپا در فلوریدا رخ داد که در آن هکرها به نظام کامپیوتری یک مرکز تصفیه آب که ۱۵۰۰۰ نفر را تأمین می کرد نفوذ کرده و سعی کردند منبع آب شهر را مسموم کنند[۵].	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[۶].
نفت و گاز	حمله ARA	در بحبوحه بحران انرژی قاره‌ای، یک حمله سایبری به هاب‌های پالایش نفت آمستردام روتردام-آنتورپ[۷] (ARA) در فوریه ۲۰۲۲ عملیات پایانی نفتی را مختل کرد. چندین شرکت گزارش دادند که قربانی یک حمله باج افزاری شده‌اند که بر نظام‌های فناوری اطلاعات آن‌ها تأثیر گذاشته و درنتیجه عملیات بنادر (عمدتاً خودکار) را مختل کرده و باعث تغییر مسیر تانکرها شده است[۸].	علاوه‌بر ریسک اختلال در عرضه انرژی، چنین حملاتی همچنین مانع از اجرای درست قراردادهای تأمین انرژی توسط شرکت‌ها شده و منجر به رخداد مسئولیت های قانونی برای آن‌ها می‌شود.
زنجیره تأمین، چندگانه	هک SolarWind	در سال ۲۰۲۰، هکرها یک کد مخرب را به نظام نرم‌افزاری SolarWind وارد کردند[۹]. این بدافزار از طریق به‌روزرسانی‌های معمول نظام به بیش از ۳۰۰۰۰ مشتری سرایت کرد و هکرها را قادر ساخت تا به نظام‌های فناوری اطلاعات هزاران شرکت و سازمان ازجمله سازمان‌های	این حمله باعث افزایش آگاهی در مورد آسیب‌پذیری سایبری زنجیره‌های تأمین ازطریق تأمین‌کنندگان شخص ثالث شد.

1. https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
2. https://www.mitnicksecurity.com/blog/an-overview-of-the-2021-jbs-meat-supplier-ransomware-attack
3. "An Overview of the 2021 JBS Meat Supplier Ransomware Attack" mitnicksecurity.com, 3 June 2021
4. Tampa water system hack
5. "Hackers try to contaminate Florida town's water supply through computer breach", Reuters, 8 February 2021.
6. "One year after the Oldsmar water breach, some experts question the utility's cybersecurity", WUSF Public Media, 4 February 2022.
7. Amsterdam-Rotterdam-Antwerp (ARA)
8. "Cyberattack causes chaos at key European oil terminals", S&P Global Commodity Insights, 3 February 2022.

۹. SolarWind یک شرکت مستقر در تگزاس است که نرم‌افزار Orion را که به‌طور گسترده توسط شرکت ها برای مدیریت منابع IT استفاده می‌شود، تولید می‌کند.

بخش‌ها	نام حمله	توصیف	مفهوم
		دولتی حساس ایالات متحده نفوذ کنند و از آن‌ها جاسوسی نمایند[۱]. این حمله سایبری یک افشای اطلاعات پیشرفته در زنجیره تأمین است که در یک دوره ۷ ماهه رخ داده است. بعدها این حمله، به هکرهای روسی دولت-ملت[۲] (دولت ملی) نسبت داده شد.	
آلومینیوم	Norsk Hydro	در سال ۲۰۱۹، Norsk Hydro تولیدکننده آلومینیوم مستقر در نروژ - در میان بزرگ‌ترین تولیدکنندگان صنعت جهان با کارخانه‌هایی در ۴۰ 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 نظام‌های کنترل صنعتی خود را بسیار کندتر از زمان عادی مدیریت کند[۳].	سالی که حمله رخ داد، Norsk Hydro هزینه کل حمله سایبری را حدود ۶۵۰ تا ۷۵۰ میلیون کرون (~ ۶۵ تا ۷۵ میلیون دلار آمریکا) تخمین زد[۴].
شبکه‌های برق	هک شبکه برق اوکراین	شبکه برق اوکراین بارها مورد هدف هکرهای مرتبط با روسیه قرار گرفته ، حملاتی که در سال‌های ۲۰۱۵ و ۲۰۱۶ ثبت شده است. در دسامبر ۲۰۱۵، شبکه برق اوکراین هک شد که منجر به قطع برق بیش از ۲۰۰۰۰۰ مصرف کننده در اوکراین برای چند ساعت شد. بعدها این حمله به گروه هک سایبری روسی کرم شنی نسبت داده شد. یک سال بعد، شبکه برق اوکراین دوباره مورد هدف هکرهایی قرار گرفت که یک بدافزار قطع کامل برق را به نظام قدرت وارد کردند. در بحبوحه درگیری‌های مداوم با روسیه در سال جاری، متصدی شبکه ملی اوکراین، Ukrenergo، درخواست ادغام با شبکه برق اتحادیه اروپا را مطرح کرد[۵].	حملات سایبری جدید ریسک حوادث ژئوپلیتیکی را افزایش می دهند، به‌ویژه اگر به‌عنوان حمله علیه اتحادیه اروپا در نظر گرفته شوند.

منبع: تحقیقات مؤسسه Swiss Re

---

۱. ایالات متحده در حال وضع تحریم ها علیه روسیه به‌دلیل حمله سایبری SolarWinds است. در اینجا توضیح ساده‌ای درباره نحوه هک و دلیل آن ذکر شده است:
https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-۲۰۲۰-۱۲?r=US&IR=T

2. Nation-state Russian hackers
3. "Norsk Hydro – A Ransomware Case Study" – cyberbrokers.co.uk, 17 February 2022.
4. Annual report 2019, Hydro., http://cyberbrokers.co.uk/norsk-hydro-a-ransomware-case-study/
5 A Power Struggle over Ukraine's Electrical Grid, Center for Strategic and International Studies, 9 March 2022.

انواع پوشش‌های منتخب بیمه‌نامه سایبری

سطح	پوشش	توصیف	نوع خسارت
شرکت	هزینه‌های مدیریت بحران	۱. هزینه‌های پزشکی قانونی؛ ۲. هزینه‌های اطلاع‌رسانی؛ ۳. نظارت بر اعتبار و هزینه‌های ایجاد مراکز تماس؛ ۴. هزینه‌های روابط عمومی؛ ۵. هزینه‌های حقوقی.	شخص اول
	مهندسی- اجتماعی	خسارت‌های مالی ناشی از کلاهبرداری‌های مهندسی اجتماعی، ازجمله جعل هویت فروشنده، تأمین‌کننده، مدیر اجرایی یا مشتری	شخص اول
	اخاذی	هزینه‌های پاسخ‌گویی و همچنین باج‌هایی که به هکرها برای رمزگشایی یا دسترسی مجدد به داده‌ها یا نظام‌ها پرداخت می‌شود.	شخص اول
	بازیابی اطلاعات	بازیابی داده‌ها و اطلاعات ازطریق پشتیبان‌گیری یا ایجاد مجدد داده‌ها.	شخص اول
	وقفه در کسب‌وکار / وقفه احتمالی در کسب‌وکار[1] (CBI)	از دست دادن درآمد کسب‌وکار و هزینه اضافی متحمل‌شده در طول دوره بازسازی یا از دست دادن درآمد کسب‌وکار ناشی از حادثه. CBI شامل پوشش از دست دادن درآمد کسب‌وکار و هزینه های اضافی ناشی از ناتوانی تأمین‌کننده در ارائه خدمات یا محصولات در نتیجه یک حمله سایبری است.	شخص اول
	جریمه‌ها	جریمه‌های مقام نظارتی که توسط سازمان‌های دولتی و/یا استاندارد امنیت داده‌های صنعت کارت پرداخت (PCI-DSS) وضع می‌شود، و جریمه‌هایی که توسط شرکت‌های کارت اعتباری یا بانک‌ها تحت قراردادهای پردازش کارت پرداخت اخذ می‌شوند.	شخص ثالث
	مسئولیت امنیت شبکه	هزینه‌های ناشی از خسارات مطرح‌شده توسط شخص ثالث برای نقض امنیت نظام بیمه‌شدگان، ازجمله هزینه‌های دفاع قانونی	شخص ثالث
	مسئولیت حفظ حریم خصوصی	هزینه‌های ناشی از خسارات مطرح‌شده توسط شخص ثالث برای نقض حریم خصوصی داده‌ها، ازجمله هزینه‌های دفاع قانونی. چنین حوادثی همچنین می‌تواند ناشی از نقض امنیت باشد.	شخص ثالث
	هزینه‌های حقوقی	هزینه‌های حقوقی برای دفاع در مقابل رسیدگی‌های نظارتی یا اقدامات قانونی	شخص ثالث

منبع: موسسه Swiss Re

1. Contingent Business Interruption (CBI)

فهرست گزارش موردی‌های منتشرشده (دوره قدیم)

گزارش موردی ۱ (تیر ۱۳۷۷): بازار بیمه کره جنوبی با توجه به شرایط پیشنهادی صندوق بین‌المللی پول

گزارش موردی ۲ (شهریور ۱۳۷۷): مقایسه تطبیقی مالیات بر شرکت‌های بیمه در ایران و ۱۷ کشور جهان

گزارش موردی ۳ (آبان ۱۳۷۷): مقدمه‌ای بر آزادسازی و خصوصی‌سازی صنعت بیمه همراه با تجربه برخی کشورها با توجه به شرایط پیشنهادی صندوق بین‌المللی پول

گزارش موردی ۴ (اردیبهشت ۱۳۷۸): مقدمه‌ای بر لزوم اندازه‌گیری و اهمیت بهره‌وری در صنعت بیمه کشور

گزارش موردی ۵ (تیر ۱۳۷۸): بیمه و بحران پیری

گزارش موردی ۶ (مهر ۱۳۷۸): بررسی ریسک‌های پتروشیمی از نقطه نظر آتش‌سوزی

گزارش موردی ۷ (دی ۱۳۷۸): آشنایی با صنعت بیمه مالزی

گزارش موردی ۸ (شهریور ۱۳۷۹): مبانی بیمه و مدیریت ریسک و گاز

گزارش موردی ۹ (دی ۱۳۷۹): موقعیت بازارهای بیمه آسیا پس از بحران اقتصادی

گزارش موردی ۱۰ (اردیبهشت ۱۳۸۰): بیمه در فیدیک

گزارش موردی ۱۱ (تیر ۱۳۸۰): مروری بر تجارب و دستاوردهای بازار بیمه بنگلادش

گزارش موردی ۱۲ (اسفند ۱۳۸۰): عوامل مؤثر در نرخ‌گذاری بیمه‌های اتومبیل

گزارش موردی ۱۳ (فروردین ۱۳۸۱): توانگری در بیمه

گزارش موردی ۱۴ (اردیبهشت ۱۳۸۲): اصلاح سیستم‌های مقرراتی و نظارتی در بازارهای بیمه در حال گذار

گزارش موردی ۱۵ (مهر ۱۳۸۲): مروری بر بازار بیمه لندن و فعالیت‌های لویدز

گزارش موردی ۱۶ (آذر ۱۳۸۲): نوآوری‌های بازار سرمایه در صنعت بیمه

گزارش موردی ۱۷ (دی ۱۳۸۲): تأثیر تجارت الکترونیکی بر صنعت بیمه

گزارش موردی ۱۸ (بهمن ۱۳۸۲): ابعاد گوناگون نظارت در صنعت بیمه (بخش اول: نظارت در فنلاند، ایسلند و هندوستان)

گزارش موردی ۱۹ (اسفند ۱۳۸۲): قوانین، مقررات و نظارت بیمه (ایجاد سیستم‌های مؤثر تنظیمی و نظارتی بیمه)

گزارش موردی ۲۰ (شهریور ۱۳۸۳): آژانس چند جانبه تضمین سرمایه‌گذاری (MIGA) و تعامل آن با صنعت بیمه

گزارش موردی ۲۱ (خرداد ۱۳۸۴): بازار جهانی بیمه در سال‌های ۲۰۰۲ و ۲۰۰۳

گزارش موردی ۲۲ (تیر ۱۳۸۴): مقدمه‌ای بر بیمه‌های عمر (بخش اول و دوم)

گزارش موردی ۲۳ (مرداد ۱۳۸۴): مقدمه‌ای بر بیمه‌های عمر (بخش سوم)

گزارش موردی ۲۴ (مهر ۱۳۸۴): ابعاد گوناگون نظارت در صنعت بیمه (بخش دوم: مهندسی مجدد نظارت)

گزارش موردی ۲۵ (آبان ۱۳۸۴): بیمه ده ساله عیب‌های اساسی ساختمان در چند کشور منتخب

گزارش موردی ۲۶ (آذر ۱۳۸۴): ابعاد گوناگون نظارت در صنعت بیمه (بخش سوم: استانداردهای نظارتی اعطای پروانه، بازرسی در محل، فعالیت‌های تجاری بین مرزی، مدیریت شرکت‌های بیمه)

گزارش موردی ۲۷ (فروردین ۱۳۸۵): خود بیمه‌گری

گزارش موردی ۲۸ (مرداد ۱۳۸۵): بیمه در بازارهای نوظهور (با تأکید بر چین و هند)

گزارش موردی ۲۹ (آذر ۱۳۸۵): بیمه خودرو در ژاپن

گزارش موردی ۳۰ (دی ۱۳۸۵): بازارجهانی بیمه (درسال‌های ۲۰۰۴ و ۲۰۰۵)

گزارش موردی ۳۱ (خرداد ۱۳۸۶): ابعاد گوناگون نظارت در صنعت بیمه (بخش سوم: توانگری ۲)

گزارش موردی ۳۲ (مرداد ۱۳۸۶): اصلاحات ضروری قانون بیمه در چین پس از الحاق به سازمان جهانی تجارت

گزارش موردی ۳۳ (آبان ۱۳۸۶): بررسی ابعاد نظام آماری صنعت بیمه از نگاه جهانی (ارائه راهکاری برای کشور ایران)

گزارش موردی ۳۴ (فروردین ۱۳۸۷): رتبه‌بندی شرکت‌های بیمه

گزارش موردی ۳۵ (اردیبهشت ۱۳۸۷): اندازه‌گیری سوددهی صدور در صنعت بیمه غیرزندگی

گزارش موردی ۳۶ و ۳۷ (تیرو مرداد ۱۳۸۷): چارچوبی جهانی برای ارزیابی توان واگذاری بیمه‌گر

گزارش موردی ۳۸ و ۳۹ (مهر و آبان ۱۳۸۷): بررسی تجربه بیمه حوادث طبیعی منازل مسکونی در کشورهای منتخب و ارائه راهکارهای مناسب برای ایران

گزارش موردی ۴۰ (دی ۱۳۸۷): اثر تأمین مالی به روش PAYG و خصوصی‌سازی تأمین اجتماعی بر تشدید فقر

گزارش موردی ۴۱ (بهمن ۱۳۸۷): بیمه در بازارهای نوظهور: بررسی اجمالی بیمه اسلامی و چشم‌انداز آن

گزارش موردی ۴۲ (اردیبهشت ۱۳۸۸): اقتصاد واسطه‌های بیمه

گزارش موردی ۴۳ (تیر ۱۳۸۸): بیمه سپرده

گزارش موردی ۴۴ (شهریور ۱۳۸۸): آزادسازی در صنعت بیمه- بحران مالی جهانی

گزارش موردی ۴۵ (آبان ۱۳۸۸): اخلاق بیمه، همجواری تضادها؟

گزارش موردی ۴۷-۴۶ (آذر ۱۳۸۸): تنظیم مقررات و مداخلات در صنعت بیمه (موضوعاتی بنیادین)

گزارش موردی ۴۸ (دی ۱۳۸۸): گزارش بازار جهانی بیمه اتکایی سال ۲۰۰۸ (ارائه شده توسط انجمن بین‌المللی ناظران بیمه)

گزارش موردی ۴۹ (بهمن ۱۳۸۸): تحلیل سناریو در بیمه

گزارش موردی ۵۰ (اردیبهشت ۱۳۸۹): مطالعه تطبیقی بیمه شخص ثالث با دنیا و ارائه راهکارهای توسعه فرهنگ رانندگی

گزارش موردی ۵۱ (تیر ۱۳۸۹): صنعت بیمه و تغییر اقلیم (قسمت اول)

گزارش موردی ۵۲ (شهریور ۱۳۸۹): صنعت بیمه و تغییر اقلیم (قسمت دوم)

گزارش موردی ۵۳ (آبان ۱۳۸۹): صنعت بیمه و تغییر اقلیم (قسمت سوم)

فهرست گزارش موردی‌های منتشرشده (دوره جدید)

گزارش موردی ۱ (دی ۱۳۸۹): کلیات اقتصاد برنامه‌های بیمه اجتماعی

گزارش موردی ۲ (اسفند ۱۳۸۹): آمارهای حوادث جاده‌ای در کشورهای منتخب و تحلیل خسارت‌های پرداختی بیمه شخص ثالث در ایران

گزارش موردی ۳ (فروردین و اردیبهشت ۱۳۹۰): اوراق بهادار بیمه‌ای

گزارش موردی ٤ (خرداد و تیر ۱۳۹۰): نقش شاخص‌ها در انتقال ریسک در صنعت بیمه

گزارش موردی ٥ (مرداد و شهریور ۱۳۹۰): شاخص‌های پایه‌ای نرخ بیمه زلزله ساختمان‌های ایران

گزارش موردی ٦ (مهر و آبان ۱۳۹۰): اصلاح سیستم خدمات درمانی در ژاپن: کنترل هزینه‌ها، ارتقای کیفیت و تضمین برابری

گزارش موردی ۷ (آذر و دی ۱۳۹۰): بیمه در کشورهای درحال‌توسعه: بهره‌گیری از فرصت‌های موجود در بیمه‌های خرد

گزارش موردی ۸ (بهمن و اسفند ۱۳۹۰): پولشویی و روش‌های جلوگیری از آن در صنعت بیمه

گزارش موردی ۹ (فروردین و اردیبهشت ۱۳۹۱): کاربرد ملی مقررات ساختمان در مدیریت ریسک و نرخ‌گذاری بیمهٔ آتش‌سوزی

گزارش موردی ۱۰ (خرداد و تیر ۱۳۹۱): پیشگیری شناسایی و مقابله با کلاهبرداری در بیمه

گزارش موردی ۱۱ (مرداد و شهریور ۱۳۹۱): تجربه کشور هندوستان در حذف تعرفه‌های بیمه‌های غیرزندگی

گزارش موردی ۱۲ (مهر و آبان ۱۳۹۱): تدوین بیمه‌نامه زلزله در بخش مسکن و ارائه مدلی کاربردی جهت بررسی نقش بیمه در بهبود کیفیت ساختمان در ایران

گزارش موردی ۱۳ (آذر و دی ۱۳۹۱): رابطه بیمه و رشد اقتصادی- تحلیل نظری و تجربی

گزارش موردی ١٤ (بهمن و اسفند ۱۳۹۱): ارزیابی وتحلیل ریسک قراردادهای بیمه زندگی: ترکیب رویکردهای اکچوئرال و مالی

گزارش موردی ۱۵ (فروردین و اردیبهشت ۱۳۹۲): دوگزارش بیمه‌ای: ارزیابی عملکرد صنعت بیمه کشور و تبیین چشم‌انداز آینده (مقاله اول)- بررسی و سنجش سطح رضایت‌مندی بیمه‌گذاران (مشتریان) شرکت‌های فعال در صنعت بیمه کشور (مقاله دوم)

گزارش موردی ١٦ (خرداد و تیر ۱۳۹۲): بیمه سلامت و بیمه نوین سلامت (مطالعه موردی: کشورهای چین، ژاپن و کره جنوبی)

گزارش موردی ۱۷ (مرداد و شهریور ۱۳۹۲): راهکارهای عملی افزایش تقاضای بیمه زندگی انفرادی و تدوین چهارچوبی برای ارائه بیمه‌های زندگی جدید

گزارش موردی ۱۸ (مهر و آبان ۱۳۹۲): چهارچوب نظارتی انجمن بین‌المللی ناظران بیمه

گزارش موردی ۱۹ (آذر و دی ۱۳۹۲): کاربرد منطق فازی، شبکه عصبی و الگوریتم ژنتیک در صنعت بیمه

گزارش موردی ۲۰ (بهمن و اسفند ۱۳۹۲): بررسی عملکرد ساختمان‌ها و تأسیسات زیربنایی و عملکرد صنعت بیمه در زلزله مرداد ۱۳۹۱ آذربایجان شرقی

گزارش موردی ۲۱ (فروردین و اردیبهشت ۱۳۹۳): مطالعه تطبیقی مقررات‌گذاری و نظارت صنعت بیمه در کشورهای منتخب توسعه یافته

گزارش موردی ۲۲ (خرداد و تیر ۱۳۹۳): مطالعه عوامل ریسک و فاکتورهای مؤثر بر محاسبه حق‌بیمه در بیمه‌های اتومبیل در ایران و جهان

گزارش موردی ۲۳ (مرداد و شهریور ۱۳۹۳): مطالعه روش‌های محاسباتی و ارزیابی ریسک‌های مختلف بیمه‌های زندگی

گزارش موردی ٢٤ (مهر و آبان ۱۳۹۳): مشتری مداری در صنعت بیمه

گزارش موردی ۲۵ (آذر و دی ۱۳۹۳): بیمه ریسک در قراردادهای تأمین مالی پروژه.

گزارش موردی ٢٦ (بهمن و اسفند ۱۳۹۳): تعیین روش بهینه محاسبه سیستم پاداش ــ جریمه در بیمه‌های شخص ثالث

گزارش موردی ۲۷ (فروردین و اردیبهشت ۱۳۹٤): حفظ سلامت افراد در بازارهای نوظهور با حمایت بیمه

گزارش موردی۲۸ (خرداد و تیر ۱۳۹٤): سیری در پیشرفت‌های اخیر بیمه‌های دریایی و هوایی

گزارش موردی ۲۹ (مرداد و شهریور ۱۳۹٤): بیمه‌گری ریسک‌های تجاری دائم‌التغییر

گزارش موردی ۳۰ (مهر و آبان ۱۳۹٤): بررسی وضعیت اتکایی اجباری در ایران و کشورهای منتخب

گزارش موردی ۳۱ (آذر و دی ۱۳۹٤): بررسی ساختار و کارکرد ناظر بیمه‌ای در ایران و کشورهای منتخب

گزارش موردی ۳۲ (بهمن و اسفند ۱۳۹٤): معرفی قراردادهای بیمه زندگی متصل به سهام و روش‌های قیمت‌گذاری

گزارش موردی ۳۳ (فروردین و اردیبهشت ۱۳۹۵): بازار بیمه وسایل نقلیه موتوری در اروپا، نوامبر ۲۰۱۵ (قسمت اول)

گزارش موردی ۳٤ (خرداد و تیر ۱۳۹۵): بازار بیمه وسایل نقلیه موتوری در اروپا، نوامبر ۲۰۱۵ (قسمت دوم)

گزارش موردی ۳۵ (مرداد و شهریور ۱۳۹۵): مطالعه تطبیقی شرایط عمومی بیمه‌نامه آتش‌سوزی و ارائه پیشنهادهای اصلاحی

گزارش موردی ۳٦ (مهر و آبان ۱۳۹۵): مطالعه تطبیقی طرح‌های مستمری بازنشستگی خصوصی در کشورهای منتخب

گزارش موردی ۳۷ (آذر و دی ۱۳۹۵): مطالعه عوامل ریسک و فاکتورهای مؤثر بر محاسبه حق‌بیمه در رشته بیمه‌های باربری

گزارش موردی ۳۸ (بهمن و اسفند ۱۳۹۵): حاکمیت شرکتی در مؤسسات بیمه

گزارش موردی ۳۹ (فروردین و اردیبهشت ۱۳۹٦): بررسی شرایط عمومی بیمه بدنه اتومبیل در ایران و سایر کشورها

گزارش موردی ٤۰ (خرداد و تیر ۱۳۹٦) بررسی شرایط پوشش حوادث راننده توسط بیمه‌گران خارجی و ارائه شرایط عمومی پیشنهادی برای ایران

گزارش موردی ٤۱ (مرداد و شهریور ۱۳۹٦): مطالعه شرایط عمومی بیمه‌های باربری و ارائه پیشنهادهای اصلاحی

گزارش موردی ٤۲ (مهر و آبان ۱۳۹٦): یافته‌های تجربی در خصوص قیمت‌گذاری بیمه وسایل نقلیه موتوری در آلمان، اتریش و سوئیس

گزارش موردی ٤۳ (آذر و دی ۱۳۹٦): مدیریت ریسک‌های کلیدی

گزارش موردی ٤٤ (بهمن و اسفند ۱۳۹٦): اصول اساسی بیمه انجمن بین‌المللی ناظران بیمه (اصول ۱ الی ۱۳)

گزارش موردی ٤۵ (فروردین و اردیبهشت ۱۳۹۷): اصول اساسی بیمه انجمن بین‌المللی ناظران بیمه (اصول ۱٤ الی ۱۷)

گزارش موردی ٤٦ (خرداد و تیر ۱۳۹۷): اصول اساسی بیمه انجمن بین‌المللی ناظران بیمه

گزارش موردی ٤۷ (مرداد و شهریور ۱۳۹۷): فن‌آوری و نوآوری در بخش بیمه

گزارش موردی ٤۸ (مهر و آبان ۱۳۹۷): راهنمای نظام نظارت مبتنی‌بر ریسک برای شرکت‌های بیمه

گزارش موردی ٤۹ (ویژه‌نامه سمینار توسعه بیمه‌های زندگی): بیمه زندگی: تمرکز بر مصرف‌کننده

گزارش موردی ۵۰ (ویژه‌نامه بیست‌وپنجمین همایش بین‌المللی بیمه و توسعه): تحولات فناوری مالی در صنعت بیمه

گزارش موردی ۵۱ (بهمن و اسفند ۱۳۹۷): شناسایی و مطالعه ضوابط و مقررات نحوه حضور مؤسسات بیمه خارجی در کشور چین

گزارش موردی ۵۲ (فروردین و اردیبهشت ۱۳۹۸): کلان داده و بیمه: پیامدهایی برای نوآوری، رقابت و حریم خصوصی

گزارش موردی ۵۳ (خرداد و تیر ۱۳۹۸): گزارش توانگری و شرایط مالی شرکت هانوفر ری

گزارش موردی ۵٤ (مرداد و شهریور ۱۳۹۸): گزارش تحلیل مغایرت با استانداردهای حسابداری در خصوص ذخیره فنی تکمیلی و خطرات طبیعی و ارائه پیشنهاد اصلاحی

گزارش موردی ۵۵ (مهر و آبان ۱۳۹۸): سیستم شناسایی تقلب بیمه‌ای

گزارش موردی ۵٦ (آذر و دی ۱۳۹۸): بررسی عملکرد ماده ۳۰ قانون الحاق برخی مواد به قانون تنظیم بخشی از مقررات مالی دولت (۲) و بند الف تبصره ۱۰ قانون بودجه سالیانه (عوارض قانونی بیمه اجباری شخص ثالث)

گزارش موردی ۵۷ (بهمن و اسفند ۱۳۹۸): بیمه زندگی در عصر دیجیتال؛ تحولات بنیادی پیش‌رو

گزارش موردی ۵۸ (فروردین و اردیبهشت ۱۳۹۹): گزارش ریسک‌های آینده گروه آکسا و اوراسیا

گزارش موردی ۵۹ (خرداد و تیر ۱۳۹۹): وضعیت حاکمیت شرکتی در کشورهای عضو سازمان همکاری و توسعه اقتصادی در سال ۲۰۱۷

گزارش موردی ٦۰ (مرداد و شهریور ۱۳۹۹): درک سودآوری در بیمه زندگی

گزارش موردی ٦۱ (مهر و آبان ۱۳۹۹): بررسی اجمالی شبکه فروش صنعت بیمه و چگونگی نظارت بر آن در کشورهای توسعه یافته و درحال‌توسعه

گزارش موردی ٦۲ (آذر و دی ۱۳۹۹): ضرورت بهره‌وری در صنعت بیمه

گزارش موردی ٦۳ (فروردین و اردیبهشت ۱٤۰۰): تحول دیجیتال صنعت بیمه در کشورهای منتخب: فناوری‌ها، قوانین و مقررات و نهادسازی

گزارش موردی ٦٤ (خرداد و تیر ۱٤۰۰): تغییر اقلیم و صنعت بیمه: انجام اقداماتی به عنوان مدیران ریسک و سرمایه‌گذاران از دیدگاه مدیران سطح C در صنعت بیمه

گزارش موردی ٦۵ (مرداد و شهریور ۱٤۰۰): هوش مصنوعی و کاربردهای آن در صنعت بیمه

گزارش موردی ٦٦ (مهر و آبان ۱٤۰۰): ملاحظات مقرراتی مدل‌های کسب‌وکار بیمه دیجیتال

گزارش موردی ٦۷ (آذر و دی ۱٤۰۰): ایجاد ارزش مبتنی بر فناوری در بیمه

گزارش موردی ٦۸ (بهمن و اسفند ۱٤۰۰): درس‌هایی درباره مقررات‌گذاری و نظارت بر بیمه برای کشورهای در حال توسعه

گزارش موردی ٦۹ (فروردین و اردیبهشت ۱٤۰۱): ارزیابی ریسک تغییر اقلیم برای صنعت بیمه؛ چارچوب تصمیم‌گیری جامع و ملاحظات کلیدی برای هر دو سمت ترازنامه

گزارش موردی ۷۰ (خرداد و تیر ۱٤۰۱): بازار جهانی بیمه تکافل- ترسیم نقشه راه دستیابی به بازارهای انبوه

گزارش موردی ۷۱ (مرداد و شهریور ۱٤۰۱): صنعت تکافل در مالزی

گزارش موردی ۷۲ (مهر و آبان ۱٤۰۱): بیمه داده محور

گزارش موردی ۷۳ (آذر و دی ۱٤۰۱) موضوعاتی در باب مقررات‌گذاری و نظارت بر تکافل‌خُرد

گزارش موردی ۷٤ (بهمن و اسفند ۱٤۰۱) بررسی ریسک‌های ناشی از آلودگی پلاستیک در صنعت بیمه اولین گزارش جهانی بر صنعت بیمه در ارتباط با مدیریت ریسک‌های ناشی از آلودگی پلاستیک، پسماندهای پلاستیکیِ دریایی و میکروپلاستیک‌ها

گزارش موردی ۷۵ (فروردین و اردیبهشت ۱٤۰۲): ریسک بیشتر: طبیعت در حال تغییر فرصت‌های بیمه‌های اموال و مسئولیت تا سال ۲۰٤۰

گزارش موردی ۷٦ (خرداد و تیر ۱٤۰۲): تکافل خرد ابزاری مناسب جهت حمایت از کسب‌وکارهای خرد با هدف شمول مالی و توسعه پایدار

گزارش موردی ۷۷ (مرداد و شهریور ۱٤۰۲): خودکارسازی رباتیک فرایندها در صنعت بیمه

گزارش موردی ۷۸ (مهر و آبان ۱٤۰۲): چارچوب واسطه‌گری مبتنی بر ارزش برای تکافل

Working Paper

Bimonthly Journal of Insurance Research Center (IRC)

New Edition,Vol.13, No.5, December & January, 2024, Serial No. 79

Concessioner: Insurance Research Center (IRC)

Director- in- Charge: Yaghoub Mahmoodian (PhD)

Editor- in- Chief: Mohammad Mahdi Asgari (PhD)

Translator: Somayeh Mireh (PhD)

Scientific Editor: Asma Hamzeh (PhD)

Internal Manager: Shabnam Refoua (PhD)

Layout & Cover Designer: Ali hossein Safari

Publication Address: No. 43, West Sarv Ave., Saadat Abad, Tehran/ Iran

P.O. Box: 19395 -4499

Tel: (+9821) 22084084

Fax: (+9821) 22092265

Workingpaper@IRC.ac.ir

All rights reserved for IRC. Quoting the content is allowed if acknowledged.
The views expressed in this journal are those of the authors and do not necessarily reflect the views of IRC. Working Paper reserves the right to edit the articles.