مجله علوم مطالعات پژوهشی در علوم کامپیوتر آینده، 1403، دوره ۱، شماره ۱، ص ص ۱-۱۲

مجله علمی مطالعات پژوهشی

در علوم کامپیوتر آینده

www.journalhi.com/com/

ریسک‌های نوظهور در صنعت بیمه؛ فرصت‌ها و چالش‌ها (با رویکرد ریسک‌های سایبری)

پوریا مجدآملی [۱]

۱- کارشناسی ارشد کامپیوتر، دانشگاه خوارزمی، تهران، ایران.

اطلاعات مقاله

مقاله پژوهشی کامل

دریافت: ۲۷ اسفند ۱۴۰۱

پذیرش: ۱۰ اردیبهشت ۱۴۰۲

ارائه در سایت: ۱۲ خرداد ۱۴۰۲

کلید واژگان:

صنعت بیمه

ریسک

ریسک‌های سایبری

چالش‌های صنعت بیمه

چکیده

در این مقاله، ریسک‌های نوظهور در صنعت بیمه با محوریت ریسک‌های سایبری مورد بررسی قرار گرفته‌اند. اگرچه رکود اقتصادی و تغییرات قانونی هنوز در صدر لیست‌های ریسک بیمه هستند، کانون توجه به سمت ریسک‌های جدید کارآفرینی مانند رقابت، اعتبار و شهرت و وقفه در کسب و کار و ریسک‌های سایبری انتقال یافته است. ریسک‌های سایبری پیشامدهایی هستند که می‌توانند باعث ایجاد اختلال یا وارد کردن خسارت در کسب و کار الکترونیکی، شهرت و اعتبار برند شوند. از جمله این ریسک‌ها می‌توان به خطرات امنیت شبکه، ویروس، هک اینترنتی، از کار افتادن شبکه اینترنتی، سرقت‌های هویتی و ... اشاره کرد. بیمه سایبری پوششی برای خسارات و پیشامدهای ناگوار ناشی از ریسک‌های الکترونیکی فراهم می‌کند. انتخاب نامساعد و مخاطرات اخلاقی، از جمله چالش‌های بیمه در حوزه سایبری هستند که در این پژوهش بدانها پرداخته شده و راهکارهایی برای غلبه بر این چالش‌ها ارائه شده است.

emerging risks in the insurance industry; Opportunities and challenges (with the approach of cyber risks)

Pouria Majdaamoli[1]

1- Master of Computer Science, Khwarazmi University, Tehran, Iran.

Article Information

Original Research Paper

Received 18 March 2023

Accepted 02 October 2023

Available Online 04 October 2023

Keywords:

insurance industry

Risk

Cyber risks

Challenges of the insurance industry

Abstract

In this article, the emerging risks in the insurance industry have been examined with a focus on cyber risks. Although economic downturns and regulatory changes are still at the top of insurance risk lists, the focus has shifted to new entrepreneurial risks such as competition, credit and reputation, business interruption and cyber risks. Cyber risks are events that can cause disruption or damage to e-business, reputation and brand credibility. Among these risks, we can mention the risks of network security, virus, internet hacking, internet network failure, identity theft, etc. Cyber insurance provides coverage for damages and mishaps caused by electronic risks. Adverse selection and ethical risks are among the insurance challenges in the cyber field that are addressed in this research and solutions to overcome these challenges are provided.

۱- مقدمه

بیمه عقدی است که به موجب آن بیمه‌گر در ازای دریافت حق بیمه از بیمه‌گزار، متعهد می‌گردد در صورت بروز حادثه موضوع عقد بیمه، از ذی‌نفع بیمه جبران خسارت نماید یا وجه معینی را به او بپردازد (زرین، ۱۳۹۸). عقد بیمه دارای سه عنصر اساسی است: ریسک، حق بیمه و وقوع حادثه. در این میان ریسک نقشی اساسی و تعیین‌کننده‌تر از سایر عناصر دارد. ریسک واقعه‌ای اتفاقی و احتمالی است که منشأ ایراد خسارت خواهد بود. ریسک در برخی مواقع به عنوان خسارت و در مواردی به عنوان موضوع تضمین بیمه به کار می‌رود. از آنجایی که موضوع عقد بیمه، ریسک یا خطر تحقق حادثه خسارت‌بار است، می‌بایست از یک سو بر اساس قواعد حقوق بیمه امری اتفاقی باشد و از سوی دیگر طبق قواعد عمومی تعهدات امری واقعی و مشروع محسوب گردد. ریسک موضوع بیمه باید به طور دقیق و بر اساس اعلام اطلاعات بیمه‌گذار تعیین و مشخص گردد (تاجیک و سرور، ۱۳۹۵). این اعلام نقش مهمی را در قرارداد بیمه و محاسبات ریاضی و آماری حق بیمه و به تبع آن پوشش مناسب بیمه ایفا می‌کند؛ که برای عدم اعلام صحیح، ضمانت اجراهای قانونی همچون بطلان قرارداد در نظر گرفته شده است. همین مسئله تعیین ریسک را به امری پیچیده و حساس تبدیل نموده است. برخلاف قواعد عمومی، در قرارداد بیمه تغییرات موثر در میزان ریسک موجب آثار و احکامی خواهد بود که البته تشدید ریسک باید توسط بیمه‌گذار به بیمه‌گر اعلام گردد. مفهوم تشدید ریسک خود از مفاهیمی است که نیاز به واکاوی حقوقی و تعیین حدود و ثغور دارد. همچنین در برخی نظام‌های حقوقی مانن فرانسه، به بیمه‌گذار اجازه داده شده در صورت کاهش ریسک تقاضای تعدیل حق بیمه نماید. از این رو شناخت ریسک‌های بیمه، نقش مهم و کلیدی در پیشبرد اهداف، سودآوری و در نتیجه بقای صنعت بیمه ایفا می‌کند. از این رو در این پژوهش ریسک‌های سایبری و دیجیتال در صنعت بیمه به عنوان یک ریسک نوظهور مورد بررسی قرار می‌گیرند.

۲- مفاهیم

در این بخش، به صورت خلاصه به تبیین برخی از مفاهیم پژوهش پرداخته می‌شود.

۲-۱- ریسک

ممکن است کلمه ریسک ریشه عربی داشته باشد یا از واژه لاتین Risicum ریشه گرفته باشد. واژه یونانی rhiza به خطرهای قایقرانی بادی در اطراف صخره‌های کنار دریا اشاره دارد. واژه فرانسوی risqué به معنای ضمنی qui rien n`alien (خطر نکردن، برابر است با کسب منفعت نکردن) اشاره دارد (دیکسون، ۱۳۹۳). صرف نظر از اینکه کدام یک از ریشه‌های لغوی را در واقع مصدر صدور واژه ریسک بدانیم با ملاحظه در مجموع آن‌ها به این مهم دست می‌یابیم که عنصر مشترک همه این ریشه‌ها «خطر یا واقع شدن در معرض آن» است. با این وجود در زبان انگلیسی، کاربرد ریسک در شرایط مختلف، با تفاوت‌های ظریفی در معنا همراه است که اغلب موجب سو تدبیر و اشتباه می‌شود. در سال ۱۹۳۳ کمیته اصطلاح‌شناسی انجمن بیمه و ریسک آمریکا تعریف عدم اطمینان از پیامد حادثه‌ای که دو احتمال یا بیشتر دارد را تایید کرد؛ لکن هنوز هم درباره معنای ریسک سردرگمی و اختلاف نظر وجود دارد. همچنین در لغت‌نامه کمبریج در خصوص واژه ریسک ۲ معنا ارائه نموده الف) امکان وقوع پیشامد بد در خصوص فعلی که در آن شانس به نتیجه نیز هست ب) امر ناخوشایندی که ممکن است اتفاق بیافتد. واژه‌نامه مدیریت مالی نیز ریسک را به وضعیتی ترجمه کرده که در آن وقوع پیشامدها احتمالی است یا به عبارت دیگر در چنین وضعیتی پیشامدها توزیع احتمال دارند. هم‌چنین این واژه‌نامه مهم‌ترین منبع ریسک را عدم اطمینان درباره وضعیت اقتصادی آینده می‌داند.

به هر صورت واژه ریسک در بیمه به معنای یک خطر بیمه شده (مثل سیل یا زلزله که همه در برابر مخاطرات آن در معرض خطر قرار خواهند گرفت) و یا شخص یا اموال محافظت شده توسط بیمه است. با این اوصاف و از مجموع آنچه بیان شد، به نظر می‌رسد کاربردی‌ترین تعریف که می‌تواند موضوع ریسک در این نوشتار را به صورت جامع تبیین کند، تعریف مؤلف کتاب اصول و مبانی نظری بیمه (مهدوی غدیر و نصیری، ۱۳۹۱) باشد که بیان می‌دارد: «ریسک وضعیتی از دنیای واقعی است که در آن احتمال وقوع خطر ناگواری وجود دارد. به بیان دقیق‌تر ریسک، موقعیتی است که در آن امکان انحراف منفی از نتیجه دلخواه مورد انتظاری وجود دارد که به رخ دادن آن امیدواریم.» از این تعریف مشخص می‌گردد که ریسک اولاً می‌تواند وضعیتی از احتمال خطر باشد. ثانیاً انحراف از نتیجه دلخواه نیز ریسک محسوب می‌شود؛ خواه به معنای عدم دستیابی به نتیجه دلخواه و متحمل شدن ضرر مالی باشد، خواه این عدم نتیجه صرفاً نرسیدن به مطلوب باشد بدون ضرر مالی. ثالثاً نکته مهم تعریف فوق این است که نباید انگاشت که این احتمال باید حتماً قابل اندازه‌گیری و یا محاسبه دقیق باشد؛ بلکه صرف احتمال وقوع و عدم دستیابی به نتیجه دلخواه و برنامه‌ریزی‌شده ریسک نامیده می‌شود.

۲-۲- فضای سایبری

فضای سایبر در معنای عام آن به عنوان مجموعه تعامل¬های انسان¬ها از طریق رایانه و فنآوری¬های نوین ارتباطات، بدون در نظر گرفتن «زمان» و «مکان»، توسط ویلیام گیبسون نویسنده¬ی کتاب نورومونسر در سال ۱۹۸۴ به کار برده شد. وی فضای سایبر را بازنمایی گرافیکی از داده¬ها از نظام¬های رایانه¬ای می¬داند. مفهومی که مورد نظر گیبسون بود؛ شاید به نوعی به هوش مصنوعی و روبوتیک نزدیک¬تر است تا آنچه اکنون به نام «فضای سایبر» شناخته می¬شود (Brier, 2010). این مفهوم نه چندان روشن اولیه، به تدریج دستمایه گفتمانی فلسفی در حوزه سایبر شد و چندی نپایید که حوزه سایبر نه به عنوان محدودهای آزمایشگاهی یا علمی، که خود به مثابه جهانی مستقل، مورد بررسی قرار گرفت (بل، ۱۳۸۹).

این سخن درستی است که با گسترش استفاده از مفهوم نوین «سایبر»، هر آنچه پس یا پیش از واژه «سایبر» قرار گیرد، به نوعی به بیان رابطه انسان و رایانه می¬پردازد. در عین حال، رویکردهای گوناگون به فضای سایبر قابل انکار نیست. مفهوم فضای سایبری معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می¬شود. بدون فنآوری، فضای سایبر بی¬معنا خواهد بود. اکنون، فضای سایبر را با موضوعات علمی - تخیلی مقایسه می¬کنند. این نوعی ناکجاآباد است که در آن می¬توان هویت¬های چندگانه داشت (Haney, 2006).

در واقع، اینترنت دروازه فضای سایبر است؛ اما فضای سایبر، با ویژگی¬هایی چون میزان و چگونگی دسترسی، راهبری، فعالیت اطلاع¬یابی، بالندگی و اعتماد شناخته می¬شود (Folsom, 2007). نگرش فناورانه به فضای سایبر به مؤلفه¬هایی چون سخت¬افزار، نرم¬افزار، کیفیت و کمیت انتقال داده¬ها و تعامل در شبکه می¬پردازد. در حالی که رویکرد روان¬شناسانه، اجتماعی و حقوقی در قالب مقوله¬هایی چون فضای ذهنی، الگوی رفتاری انسان و رایانه، تخیل، هویت و شخصیت، به مرز بین واقعیت و خیال و مانند آن توجه می¬کند. دیدگاه جامعه¬شناسانه درباره فضای سایبر

نیز به دلیل پرداختن به جماعت¬های برخط، شبکه¬های اجتماعی سایبر، و آثار اجتماعی تعامل انسان و رایانه حائز اهمیت است. اما، این در برگیرنده تمامی رویکردهای موجود نیست.

با توجه به تفاوت رویکردهای موجود درباره فضای سایبر، دیوید بل تعریف این مقوله پیچیده را می¬داند. وی ضمن اشاره به گونه¬های مختلف تفسیری فضای سایبری به توصیف مایکل بندیکت از فضای سایبر اشاره می¬کند که حائز اهمیت است: «یک دنیای جدید، یک دنیای موازی است که با خطوط ارتباطی و کامپیوترهای جهان خلق و نگهداری می¬شود. دنیایی که در آن تردد جهانی دانش، رموز سنجش¬ها، شاخص¬ها، سرگرمی¬ها و عاملیت دیگری انسانی شکل می‌گیرد. تاکنون، هرگز بر روی زمین دیده نشده است که امور دیدنی، صداها و حضورها در یک روشنایی عظیم الکترونیکی شکوفا شوند (بل، ۱۳۸۹). در زبان فارسی مفهوم دقیق و کاملاً پذیرفته‌شده‌ای از اصطلاح «سایبر» وجود ندارد. برخی از صاحب‌نظران معتقدند که مفهوم سایبر در سطح بین‌المللی بسط پیدا کرده و رواج عام یافته است؛ لذا این واژه تبدیل به یک لغت بین‌المللی شده است. با این وجود در زبان فارسی لغت «سایبر» را معادل واژه «مجاز» و لغت «اسپیس» را معادل واژه «فضا» ترجمه کرده‌اند و ترکیب «سایبر اسپیس» را معادل «فضای مجازی» دانسته‌اند. در همین معنا ترکیبات دیگری نظیر «جامعه مجازی» یا «شهروند مجازی» و «فروشگاه‌های مجازی» و امثال آن مطرح می‌شود. همه این ترکیبات در فضای مجازی مطرح می‌شوند (باستانی، ۱۳۸۳).

از لحاظ لغوی سایبر به معنی مجازی و غیر ملموس می‌باشد؛ نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضی‌دانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (و کامپیوترها) است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم برخط نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد (عاملی، ۱۳۹۰). با توجه به بررسی سنجه‌های گوناگون از تعریف فضای سایبر می‌توان گفت که فضای سایبر، «محیطی تشکیل‌یافته از سامانه‌ها و شبکه‌های ارتباطی متصل به هم است که قابلیت هر نوع رفتار متناسب با محیط مبادله داده، ذخیره و انتشار اطلاعات را دارد.» در معنای خاص و تعریف جزئی از فضای سایبری و در نتیجه‌گیری از تعاریف بالا، می‌توان بیان داشت که منظور از فضای سایبری – به ویژه در پژوهش حاضر- فضا و بستری است که در اینترنت و شبکه‌های اجتماعی بر پایه‌ی اینترنت و شبکه‌های کامپیوتری به هر شکل وجود دارد.

۳-۲- ریسک‌های الکترونیکی

ریسک‌های الکترونیکی پیشامدی که می‌تواند باعث ایجاد اختلال یا وارد کردن خسارت در کسب و کار الکترونیکی، شهرت و اعتبار برند شود. مثال: خطرات امنیت شبکه، ویروس، هک اینترنتی، از کار افتادن شبکه اینترنتی که به کسب و کار اینترنتی آسیب می‌زند، اخاذی‌های سایبری، سرقت‌های هویتی و اطلاعات بانکی و یا حمله به حساب‌های بانکی، آسیب به اطلاعات شرکت توسط کارمندان ناراضی داخلی همه از نمونه‌های ریسک الکترونیکی هستند (گریسلدا، ۱۳۹۹).

۴-۲- بیمه سایبری

بیمه سایبری ، بیمه‌ای است که پوششی برای خسارات و پیشامدهای ناگوار ناشی از ریسک‌های الکترونیکی فراهم می‌کند، به طور مثال بیمه سایبری پوششی در مقابل خطرات احتمالی سرقت وجوه نقدی که در حین تراکنش‌های بانکی صورت می‌گیرد ایجاد می‌کند. مصادیق دیگر آن نیز ایجاد پوشش در مقابل زیان‌های ناشی از توقف کسب و کار یا لطمه زدن به اعتبار آن کسب و کار می‌باشد. همه و همه مشروط به این که علت نزدیک در حوزه ریسک‌های الکترونیکی تشخیص داده شود.

۵-۲- بیمه مسئولیت فضای سایبری

در دنیایی که به طور فزاینده در حال جهانی شدن است، ریسک‌های مسئولیت، همراستا با ثروت و دارایی در اقتصادهای نوظهور، که به طور روزافزون در حال پیوند با جهان پیشرفته هستند، بیشتر می‌شوند. برای مثال بیمه مسئولیت فضای سایبری یک محصول جدید است که خسارات مسئولیت ناشی از عواملی همچون سرقت داده‌ها، انتقال ویروس و قطع شبکه طرف‌های ثالث را نشان می‌دهد (تاجیک، ۱۳۹۴).

۳- بیمه به عنوان بخشی از مدیریت ریسک

مدیریت ریسک، فرایند مدیریت رویارویی یک سازمان با ضرر و زیان و حفاظت از دارایی‌هایش است (Dorfman, 2008). مدیریت ریسک فرایندی پویا است که شامل شناسایی و اندازه‌گیری مواجهه با ریسک و ایجاد و اجرای طرحی جهت مدیریت توان بالقوه مواجهه با ریسک، مشتمل بر کنترل مدیریت مالی مواجهه با ریسک است. مدیریت ریسک، بخشی جدانشدنی از فعالیت اقتصادی یک شرکت و محیط حقوقی آن است که به قابلیت‌های خاص و متنوعی از جمله دانش فنی، حقوقی، حسابداری و بیمه نیاز دارد. محیط حقوقی که شرکت در آن فعالیت می‌کند، عاملی با اهمیت روزافزون در مدیریت ریسک است. جدای از قوانین مسئولیت و دادرسی کلی که در مورد شرکت‌ها به کار می‌رود، مقررات دیگری وجود دارند که به طور ویژه با جنبه‌های مختلف مدیریت ریسک سر و کار دارند. اولین مقررات قابل توجه و مهم در مدیریت ریسک، منجر به تعیین حداقل استانداردهای ایمنی محیط کار و برنامه‌های اجباری غرامت کارگران[1] را در اوایل قرن ۱۹ شدند. سپس در دهه ۱۹۷۰، اولین قوانین مختص به مسئولیت در قبال محصول عرضه‌شده و به دنبال آن مقررات مربوط به مسئولیت در قبال محیط زیست مطرح شدند. اخیراً فرایند مدیریت ریسک، خود تبدیل به موضوع اصلی کانون رهنمودهای داوطلبانه حاکمیت شرکتی و دستورالعمل‌های الزام‌آور حقوقی شده است. به طور مثال قانون حسابداری کنتراگ آلمان (۱۹۹۸) آشکارا از شرکت‌های تجاری می‌خواهد به منظور مدیریت و سرپرستی ریسک‌های خطرناک بالقوه در شرکت، یک واحد مدیریت ریسک جامع تشکیل دهند.

ریسک‌های نوظهور در صنعت بیمه

پیمایش مدیریت ریسک جهانی، که توسط یک کارگزار بیمه به نام شرکت اِی.اُ.اِن انجام شده است، از شرکت‌ها پرسیده است کدام ریسک‌ها را مهم‌ترین ریسک تلقی می‌کنند و چگونه برای رویارویی با آنها آماده هستند. این پیمایش تاکنون ۳ مرتبه در سال‌های ۲۰۰۹، ۲۰۰۷ و ۲۰۱۱ انجام شده است. مقایسه ۱۰ مورد از مهم‌ترین ریسک‌های درک شده، محدوده وسیعی از ریسک‌هایی را که شرکت‌ها با آن مواجه هستند، نشان می‌دهد و همچنی بیانگر این است که ادراک ریسک می‌تواند سریعاً تغییر یابد. از سال ۲۰۰۷ تا

[1] Worker's Compensation.

۲۰۰۹ بحران اقتصادی و مالی چشم‌انداز موجود را تیره کردند و باعث افزای رابطه درک‌شده بین سایر ریسک‌ها شدند. طبق بررسی سال ۲۰۱۱ بر اساس پاسخ‌های سال ۲۰۱۰ اگرچه رکود اقتصادی و تغییرات قانونی هنوز در صدر این لیست بودند، کانون توجه به سمت ریسک‌های جدید کارآفرینی مانند رقابت، اعتبار و شهرت و وقفه در کسب و کار انتقال یافت. بسیاری از مهم‌ترین ریسک‌های شرکت، ریسک‌های متعارف بیمه‌ای نیستند. برخی از مهم‌ترین ریسک‌ها از جمله محیط بازار، رقابت روزافزون، شکست در جذب و حفظ کارمندان و آسیب به شهرت، مربوط به ریسک راه انداختن یک کسب وکار است. ریسک شماره یک در سال ۲۰۰۷ آسیب به شهرت بود که تهدیدهای مربوط به ارزش برند یک شرکت را نشان می‌دهد .

ریسک تغییرات مقرراتی به نگرانی‌های رو به افزایشی اشاره دارد که به اقدامات دولت در واکنش به بحران مالی مربوط می‌شوند. ریسک‌های کلیدی دیگری که شناسایی شده‌اند، بیمه‌پذیر هستند. کسب و کارها در سال ۲۰۰۷ متوجه شدند که باید برای مقابله با ریسک‌های بیمه‌پذیر مانند وقفه در کسب وکار، مسئولیت شخص ثالث و خطرات مربوط به آسیب فیزیکی آماده شوند. با این که بین سالهای ۲۰۰۹ تا ۲۰۱۱ به واسطه نااطمینانی شدید در فضای کسب وکار شمار ریسک‌ها افزایش یافته است، اما ده مورد اول ریسکهای بیمه‌پذیر همچنان همان موارد قبلی هستند. به هر حال همانطور که بررسی کلی جدیدتر انجام شده توسط آلیانز نشان می‌دهد، ادراک ریسک به سرعت در حال تغییر است (Alianz, 2017). در یک بررسی انجام شده در اروپا که بعد از زلزله ژاپن در سال ۲۰۱۱ انجام شد، ریسک‌های مربوط به شهرت و زنجیره عرضه به ترتیب در رده‌های اول و دوم قرار گرفتند و بعد از آنها ریسک‌هایی مانند ریسک سیاسی، اعتباری و سایبری قرار گرفتند. اکثر ریسک‌های مربوط به اعتبار یا شهرت و برخی از ریسک‌های سیاسی، در آن سوی مرزهای متعارف ریسک‌های بیمه‌پذیر وجود دارند. بخشی از ریسک‌های زنجیره عرضه را می‌توان با بیمه ریسک محتمل‌الوقوع وقفه کسب و کار تعیین کرد اما مواجهه با ریسک‌ها باعث ایجاد چالش در مدل شده و برخی از این وقفه‌ها مطابق قرارداد مشمول بیمه نیستند. ریسک‌های سایبری و اعتبار در پایین این درجه‌بندی بودند اگرچه ریسک اعتبار احتمالاً به واسطه بحران بدهی در اروپا در حال رشد است.

اهمیت ریسک‌های سایبری در صنعت بیمه

با مراجعه به گزارش اخیر کمپانی بزرگ اچ‌پی، از خلاصه تهدیدات سایبری سال ۲۰۱۸ میلادی به اعداد و ارقام بسیار قابل توجهی از زیان‌های مالی و سرقت‌هایی که توسط هکرها انجام شده است، دست می‌یابیم. در گزارش مذکور این شرکت بیان می‌دارد که اطلاعات بیش از ۵۶ میلیون کارت اعتباری در دست هکرها است. در نگاه اول این رقم غیر قابل چشم‌پوشی است. چون گزارش شرکت اچ پی مربوط به کل کشورها می‌باشد و قطعاً ایران از این وادی مستثنا نبوده است. در سال‌های اخیر با شکل‌گیری پلیس فتا برای مبارزه با جرائم و سرقت‌های اینترنتی روبرو بوده‌ایم که خود نشانگر پاسخ به نیاز وجود ارگانی مستقل برای رسیدگی به کلیه مسائل سایبری است. با بررسی عمیق‌تر می‌توان متوجه شد که آمار اعلام شده فقط بخشی از حوادثی است که توسط شرکت‌ها یا سازمان‌های ذیربط شناسایی شده است و بسیاری از سرقتها و جرائم از این دست ناشناس باقی خواهند ماند و در این میان کاربران هستند که ضررهای مادی و معنوی را متحمل می‌شوند. اما، با گذر زمان کشورهایی که بیش از پیش هدف حملات سایبری قرار می‌گیرند، متوجه شده‌اند که حتی با پیشرفته‌ترین لایه‌های امنیتی و هزینه‌های گزاف برای ایجاد امنیت باز هم در امان ماندن از حملات هکرها و سارقان سایبری بسیار مشکل است، و این زمانی بود که شرکت‌های بیمه با شناسایی مشکل، راهکاری به نام بیمه سایبری را ارائه کردند. این بیمه نزدیک به دو دهه است که در کشورهایی مثل انگلیس، ژاپن و ایالات متحده در حال عرضه می‌باشد (Mukhopadhyay, 2019).

امروزه امنیت در محیط سایبری بحثی بسیار با اهمیت است؛ چون شکل دارایی‌های سازمان‌ها و نحوه تعاملات آنها نسبت به قبل تغییر کرده است. نمونه‌های سرقت‌های اینترنتی چه از درگاه‌های پرداختی یا چه توسط هکرهایی که به دنبال یافتن اطلاعات کاربران یا شرکت‌ها هستند را کمابیش می‌بینیم. علاوه بر آن، امروز در سطوح بین‌المللی حوادثی مثل قطعی در سرویس اینترنت، جزو حوادثی است، که باعث کاهش سودآوری شرکتها می‌شود و کسب و کار آنها را تهدید می‌کند. این حوادث قطعی می‌تواند مثل حوادث زلزله یا سیل خارج از دست انسان باشد و صرفاً خطاهای سیستمی را در بر گیرد. امّا به هر علتی که این پیشامد رخ بدهد یک کسب و کار را تهدید می‌کند. از منظر کاربران نیز، وجود تضمین برای ایجاد بیشتر امنیت در نقل و انتقالات اینترنتی یا امنیت اطلاعات شخصی در این حوزه بسیار حائز اهمیت است.

کسب و کارها و چالش ریسک‌های سایبری

هر قدر سازمان‌ها به دارایی‌ها و اطلاعات شبکه‌ای کامپیوتری خود بیشتر وابسته شوند، در مقابل خسارات ناشی از افزایش حملات مکرر و زیان‌باری که به دلیل اتصال به شبکه به وجود می‌آید، آسیب‌پذیرتر می‌شوند. جلوگیری از خسارت در هر سیستم شبکه‌ای کامپیوتری هرگز ٪۱۰۰ و کامل نخواهد بود. در دهه گذشته تکنیک‌های حفاظتی از برخی رشته‌های علم کامپیوتر مانند رمزنویسی و مهندسی نرم‌افزار به طور مداوم پیشرفت‌هایی داشته است، با این حال هنوز هم حملات اینترنتی در حال افزایش است. درحالی که رسانه‌های جمعی توجه خود را بر حملات اینترنتی گسترده که به شکل شکاف‌های امنیتی و کرم‌های اینترنتی سریع‌الانتشار است، متمرکز کرده‌اند، حملات داخلی کشف و گزارش‌نشده افراد، در داخل سازمان‌ها که از امتیاز دستیابی به شبکه اطلاعات برخوردار می‌باشند با تواتر و شدت بیشتری اتفاق می‌افتد. با اینکه بیشتر فروشندگان خدمات امنیت اینترنتی، محصولاتی را به شکل نرم‌افزار و سخت‌افزار می‌فروشند، اما حفاظت امنیت اینترنتی فرآیندی مستمر است که مردم نیز درگیر و فعال در آن هستند و مسئله امنیت اینترنتی کاملاً با چنین محصولاتی حل نمی‌شود. به عبارت دیگر اگرچه بیشتر سازمان‌ها بر جلوگیری از حملات اینترنتی تنها از طریق روش‌های تکنیکی متمرکز شده‌اند، اما این امر تنها بخشی از راه حل کلی به شمار می‌رود. یک راه حل کلی باید در برگیرنده پذیرش و مدیریت ریسک ناشی از حملات اینترنتی باشد چرا که وقوع آنها یک واقعیت است (Majuca, 2006).

در کنار همه مزایایی که برای بیمه‌ی الکترونیک (سایبری) ذکر شد، این نکته نیز از اهمیت فراوان برخوردار است که اصولاً کسب و کارها (به ویژه کسب و کارهای الکترونیک) بدون حضور بیمه سایبری (الکترونیک) دارای چالش‌ها و مشکلات عدیده‌ای خواهد بود. در ادامه به عمده‌ترین موارد شناخته‌شده این مشکلات اشاره می‌گردد. یکی از مشکلات جدی در این زمینه مورد استقبال واقع نشدن تجارت الکترونیکی به دلیل فقدان امکانات بیمه‌ای اطمینان‌بخش به طور الکترونیکی است. همان‌طور که می‌دانیم در تجارت الکترونیکی اطمینان دو جنبه اصلی دارد: الف) اعتماد به رسانه (ایمنی شبکه و وجود حمایت‌های قانونی از مبادلات آن) و ب) اعتماد متقابل میان طرفین معامله (طرفین معامله/ مذاکره‌های دوستانه). نقش و اهمیت بیمه الکترونیک در هر دو نوع اعتماد و به ویژه اعتماد دوم کاملاً محسوس و

مشهود است و عدم وجود آن باعث از بین رفتن اعتماد و نهایتاً منجر به نابودی هر نوع تجارتی می‌گردد (Eling, 2016). چالش دیگر سایبری امکان نیافتن تأمین‌کنندگان به ارائه محصولات مختلف از طریق تجارت الکترونیکی است. تنوع محصولات نیازمند تنوع پوشش‌های بیمه‌ای است و تجارت الکترونیکی برای دربرگرفتن محصولات مختلف نیازمند پوشش‌های گسترده الکترونیکی (به ویژه در حوزه ریسک سایبری) است که فقدان تمام یا بخشی از این پوشش‌ها، تأمین‌کنندگان را در ارائه محصولات مختلف از طریق تجارت الکترونیکی ناکام می‌گذارد.

از جمله دیگر چالش‌های کسب و کارها در این زمینه، مختل شدن مدیریت ریسک شرکت‌هایی است که مایل به تجارت الکترونیکی می‌باشند. مدیران ریسک در شرکت‌های مختلف برای پیشبرد فعالیت‌ها نیازمندند تا شمایی از ریسک‌های مختلف و بیمه‌های مرتبط را ترسیم نمایند. ورود شرکت‌ها به عرصه تجارت الکترونیکی ریسک‌های جدیدی را به وجود می‌آورد و فقدان بیمه الکترونیکی برنامه‌ریزی و مدیریت ریسک‌ها را با اختلال مواجه می‌سازد.

مهم‌ترین چالش‌های صنعت بیمه در مواجهه با ریسک‌های سایبری

در یک دنیای ایده‌آل، طرفین قرارداد در رابطه با قرارداد و تصمیماتشان اطلاعات کامل دارند. اما در دنیای واقعی در بسیاری از موارد، ممکن است یکی از طرفین در مورد ماهیت محصول مورد توافق، اطلاعات کمتری در اختیار داشته باشد. در قراردادهای بیمه‌ای این مشکلات زمانی بروز می‌کند که بیمه‌گر نسبت به اینکه متقاضی بیمه، دارای ریسک بالاست یا پایین، بی‌اطلاع باشد. ازآنجایی که متقاضی خود می‌داند که ریسک بالا یا پایین دارد ولی بیمه‌گر نمی‌داند، یک عدم تقارن اطلاعاتی بین آنها وجود دارد که این همان چیزی است که در ادبیات اقتصادی به مسئله انتخاب نامساعد معروف است. با توجه به پیچیدگی فضای سایبری، به نظر می‌رسد این چالش، در حوزه‌های بیمه سایبری بسیار قابل توجه باشد.

مشکل عمده‌ی دیگری که بیمه‌گران در در ارائه پوشش بیمه‌ای مربوط به ریسک‌های سایبری باید مدنظر قرار دهند، مسئله مخاطرات اخلاقی است. این مسئله زمانی بروز می‌کند که شرکت‌های بیمه‌گذار، خود تعمداً باعث بروز خسارت شوند یا برای جلوگیری از وقوع خسارت اقدامات لازم را انجام ندهند؛ به عنوان مثال زمانی که شرکت‌ها تحت پوشش بیمه‌ای هستند در انجام کارهای امنیتی (مربوط به امنیت سایبری) تعلل و سستی ورزند. بنابراین ممکن است این شرکت‌ها در زیرساخت‌های امنیتی (سایبری) سرمایه‌گذاری نکنند یا برای حفظ یا ارتقای سطح امنیتی موجود انگیزه نداشته باشند.

تفاوت بین مسئله مخاطرات اخلاقی و مسئله انتخاب نامساعد در دو مقوله هزینه‌ها و ساختار انگیزشی آنهاست. حل مسئله انتخاب نامساعد مستلزم صرف هزینه‌های سرمایه‌گذاری در زیرساخت‌های لازم برای تصمیم‌گیری در مورد تعیین نوع ریسک متقاضیان بالقوه‌ای است که ممکن است لازم نباشد دائماً بازنگری شوند. در مقابل مسئله مخاطرات اخلاقی، سرمایه‌گذاری در زیرساخت‌هایی را می‌طلبد تا بر متقاضیانی که لازم است به طور مستمر مورد بررسی قرار گیرند، نظارت شود. از طرف دیگر، در حالی که مسئله انتخاب نامساعد به بررسی انگیزه بیمه‌گذاران با ریسک بالا در مورد پنهان کردن اطلاعات در مورد نوع ریسکشان به بیمه‌گر می‌پردازد (به همین دلیل است که در علم اقتصاد، مسئله انتخاب نامساعد به مسئله اطلاعات پنهان نیز معروف است،) مسئله مخاطرات اخلاقی به انگیزه بیمه‌گذاران برای تعلل و کوتاهی در اقداماتشان می‌پردازد (به همین دلیل است که در علم اقتصاد مسئله مخاطرات اخلاقی، مسئله اقدامات پنهان نیز نامیده می‌شود.) در ادبیات اقتصاد بیمه‌ای، یک روش معروف برای بیمه‌گران برای حل مسئله مخاطرات اخلاقی وجود دارد و آن مشاهده سطح مراقبت بیمه‌گذار جهت ممانعت از خسارت و مرتبط ساختن مبلغ حق بیمه به این سطح مراقبت است. بدین ترتیب، وجود بیمه با چنین خصوصیتی می‌تواند سطح مراقبت از خود، توسط بیمه‌گذار را افزایش دهد.

میزان ایمنی را به طورکامل می‌توان قبل از توافق و امضای قرارداد و بعد از آن (طی دوره اعتبار پوشش) مشاهده نمود، به طوری که وجود بیمه سایبری باعث افزایش میزان مخارج شرکت‌های بیمه‌گذار برای مراقبت از خود به شکلی منطقی، کاهش حق بیمه را به دنبال دارد، که این امر باعث افزایش سطوح امنیت فناوری اطلاعات در جامعه می‌شود. بنابراین ارزیابی‌های مفصل ریسک که توسط بیمه‌گران جهت ارائه پوشش بیمه سایبری انجام می‌شود، برای شناسایی نوع ریسک بیمه‌گذار (و در نتیجه حل مسئله انتخاب نامساعد) و همچنین مرتبط ساختن طبقه‌بندی ریسک به مشوق‌های حق بیمه‌ای (برای حل مسئله مخاطرات اخلاقی) کاربرد دارد. در بررسی شیوه عمل رایج صنعت بیمه و همچنین بررسی چند ویژگی بیمه‌نامه‌های سایبری، می‌توان دریافت که بیمه‌گران با گنجاندن چند مکانیسم در قراردادهای بیمه سایبری می‌توانند مسئله مخاطرات اخلاقی را حل کنند. بیمه‌گران سایبری با وضع حق بیمه براساس طبقه‌بندی‌های ریسک، متقاضیان را به پذیرش ارزیابی امنیتی قبل از انعقاد قرارداد ملزم می‌کنند. از نگاه بیمه‌گران سایبری، شرکت‌هایی که سطح حفاظت الکترونیکی پایین و تجارت آنلاین بالا دارند یا دارای تجارت یا نوع کار با مقررات زیاد و همچنین در معرض جریمه‌های بالا هستند (نظیر شرکت‌های مالی) شرکت‌های با ریسک بالا تلقی می‌شوند. بنابراین یک بیمه‌گر سایبری باید شرکت متقاضی را برحسب یکی از چندین طبقه‌بندی ریسک طبقه‌بندی کند و حق بیمه را با ایمنی شرکت مرتبط سازد و به شرکت‌هایی که پروسه‌های ایمن‌تری دارند تخفیف بیشتری دهد.

درصورتی که نظارت کامل بر سطح ایمنی شرکت بیمه‌گذار ممکن نباشد، برای حل مسئله مخاطرات اخلاقی، مکانیسم‌های تشویقی دیگری در بیمه‌نامه‌های استاندارد سایبری گنجانده شده است؛ به عنوان مثال، محدودیت‌های مسئولیت و سهم نگهداری به گونه‌ای طراحی و گنجانده شده که بیمه‌گذار مانند یک بیمه‌گر مشترک باشد که در جلوگیری از وقوع خسارت ذینفع باشد. مثلاً بیمه‌گذار، اولین خسارت‌ها (سهم نگهداری) را پوشش می‌دهد و بیمه فقط مازاد بر این حد (که در بیمه‌نامه نیز تصریح شده است) را پوشش می‌دهد. ذکر این نکته لازم است که سهم‌های نگهداری عموماً برای هر خسارتی به کار می‌رود. دیگر شروطی که برای حل مسئله مخاطرات اخلاقی در نظر گرفته شده‌اند، استثنائاتی از پوشش خسارات است که در نتیجه انجام اقدامات متقلبانه (فریبکارانه) و نادرست بیمه‌گذار باشد، همچنین خسارات ناشی از مسئولیت طرف‌های تجاری بیمه‌گذار مستثنا شده است. بنابراین بر اساس سطح احتیاط اعمال‌شده توسط بیمه‌گذار، بیمه‌گران سایبری می‌توانند میزان حق بیمه را بر مبنای سرمایه‌گذاری شرکت بیمه‌گذار در اقدامات امنیتی تعیین نمایند، که منجر به ایجاد انگیزه‌های بازارمحور در تجارت الکترونیک جهت افزایش امنیت اطلاعاتی می‌شود.

چالش دیگر قابل توجه در بحث بیمه سایبری از آن جهت است که در مقوله امنیت سایبری به دلیل وابستگی‌های ناشی از ارتباطات فراوان، صرفه‌های جانبی ایجاد می‌گردد. امنیت سیستم‌های کامپیوتری به گونه‌ای به هم وابسته است که یک حادثه در یک سیستم ممکن است بر همه

سیستم‌های مشابه تأثیر بگذارد حتی اگر آن سیستم‌ها تحت کنترل ناظر اجرایی دیگری باشند. بنابراین اگر کد مخربی از طریق یک دستگاه معیوب به سیستم نفوذ کند، می‌تواند از این دستگاه به عنوان سکوی پرتابی برای حملات بعدی استفاده کند؛ به عنوان مثال اگر شخص یا شرکتی از نرم‌افزار آنتی‌ویروس استفاده نکند، در صورتی که سیستم آلوده شود، ممکن است سیستم‌های دیگر را که تحت کنترل ناظر اجرایی دیگری می‌باشند نیز آلوده کند. به دلیل این پدیده، یعنی به صورت جمعی در معرض ریسک اینترنتی بودن، مسئله مهم در عرضه پوشش بیمه سایبری، امکان بالقوه وقوع حادثه در یک سیستم است به گونه‌ای که همزمان خساراتی به بیمه‌گذاران زیادی وارد آورد. بیمه‌گران از چندین مکانیسم که برای کاهش معضل ریسک‌های به هم وابسته طراحی شده است، استفاده می‌کنند. ممکن است بیمه‌گران جهت حفاظت خودشان از پرداخت خسارت‌های بزرگ ناشی از ریسک‌های به هم وابسته، برخی حوادث را از پوشش استثنا کنند. به عنوان مثال، یک استثنای رایج به خسارت‌های ناشی از نقص تجهیزات الکتریکی و وسایل ارتباط از راه دور مربوط می‌شود. این استثنائات برای حمایت از بیمه‌گران از یک ریسک که منجر به خسارت در مقیاس وسیع می‌شود، گنجانده شده است.

مشکل دیگر در عرضه بیمه سایبری، عدم وجود استاندارد بیمه‌گری است. از آنجا که ریسک‌های اینترنتی پیچیده‌اند، ارزیابی ایمنی شرکت ممکن است هزاران دلار هزینه در بر داشته باشد. به عنوان نمونه، ارزیابی امنیتی شرکت آلفا تراست که اینشور تراست آن را بیمه کرده است ۲۰۰۰۰ دلار هزینه داشته، همچنین ارزیابی امنیتی مارش ۲۵۰۰۰ دلار هزینه در بر داشته است. با درک این مطلب که بررسی مفصل و از بالا تا پایین ممکن است برای خریداران پوشش مشکل باشد، برخی بیمه‌گران روشهای صدور بیمه‌نامه را تسهیل کرده‌اند. مثلاً اینشـــوردات‌کام یک پرسشنامه به صورت آنلاین عرضه کرده، درحالی که AIG فرآیند صدور سه مرحله‌ای بیمه‌نامه را برگزیده است.

۴- نتایج

هدف اصلی بیمه، مدیریت ریسک است. بیمه‌گران با محاسبات اکچوئری خود با بهره بردن از قانون اعداد بزرگ، پرتفوی‌هایی تشکیل می‌دهند که این پرتفوی‌ها منابع جبران خسارت در زمان بروز آنهاست. از دیدگاه دیگر، بیمه، مکانیزمی است که از طریق آن به جای اینکه یک نفر مسئول جبران خسارت باشد، گروهی از افراد (بیمه‌گذاران) به واسطه حضور شرکت بیمه اقدام به جبران خسارت می‌کنند. این اختراع عظیم بشر پیشرفت‌های بزرگی را در انجام پروژه‌ها و پذیرش و مدیریت ریسک‌ها به واسطه سرمایه‌های حاصل شده از خدمات بیمه‌گری باعث گردیده است. هر تکنولوژی و خدمات نوین به همراه خود مخاطرات (ریسک‌هایی) نیز به ارمغان آورده است که برخی اوقات مخاطرات آن بیش از منافع آن بوده است. از جمله ریسک‌های نوظهوری که صنعت بیمه با آن روبه‌روست، ریسک‌های سایبری است.

ریسک سایبری، نوعی از ریسک است که به سرعت در حال ظهور است و به همین دلیل برخی از شرکت‌های بیمه آن را به طور محدود پوشش می‌دهند. هرچند مدل‌سازی و قیمت‌گذاری بیمه به صورت یک چالش باقی مانده است. مطابق با مطالعات مؤسسه استمرار کسب و کار، حمله‌های سایبری، سومین عامل اختلال بخش خدمات مالی در سال ۲۰۱۸ بوده‌اند. در این پژوهش، تعاریفی از ریسک، فضای سایبری، ریسک سایبری و بیمه سایبری ارائه گردید، همچنین مشـــخص گردید که شرکت‌های بیمه سایبری قادرند با مسائل و چالش‌های این حوزه دست و پنجه نرم کنند. به عنوان مثال، بیمه‌گران با طبقه‌بندی دقیق و موشکافانه میزان ریسک بیمه‌گذار، به مسئله انتخاب نامساعد و مخاطرات اخلاقی پرداختند و تکالیفی در خصوص ایمنی که از بیمه‌گذار انتظار می‌رود را در بیمه‌نامه‌ها گنجاندند. نتیجه آن که محصولات و پوشش‌های مختلف بیمه سایبری، اینترنت را محیطی امن‌تر می‌سازد زیرا بیمه‌گران سایبری با ارائه مشوق‌های اقتصادی، شرکت‌ها را ترغیب به حداقل کردن خسارت نموده و افراد/سازمان‌ها به طور روزافزون، به دنبال بیمه سایبری در راستای منافع شخصی خود هـتند. بیمه‌گران می‌توانند اطلاعاتشان را در مورد ریسک‌ها بیشتر کنند، آسیب‌پذیری‌های سیستم‌ها را شناسایی کنند، از بیمه‌گذار بخواهند که حسابرسی‌های قبلی را بپذیرند و راهبردهای کنشگرایانه پیشگیری از خسارت را برگزینند. این موارد شـــبیه همان چیزی است که در دیگر صنایع اتفاق افتاده، مثلاً بیمه منجر به افزایش ایمنی در پیشگیری از آتش‌سوزی، حوادث هواپیما، بویلر و آسانسور گردید.

مراجع

[۱]- باستانی، ب.، جرائم رایانه‌ای و اینترنتی، انتشارات بهنامی، تهران، ایران (۱۳۸۳)

[۲]- بل، د.، درآمدی بر فرهنگ‌های سایبر، انتشارات جامعه‌شناسان، تهران، ایران (۱۳۸۹)

[۳]- تاجیک، ح.، سرور، ف.، ریسک و بیمه: Risk & insurance، گسترش علوم نوین، بجنورد.، ایران (۱۳۹۴)

[۴]- تاجیک، ح.، اصول نوین مدیریت بیمه (ارتباط بانک - بیمه - سیستم‌های مستمری)، گسترش علوم نوین، بجنورد.، ایران (۱۳۹۴)

[۵]- دیکسون، د.، ریسک و ورشکستگی در بیمه، پژوهشکده بیمه وابسته به بیمه مرکزی جمهوری اسلامی ایران، تهران، ایران (۱۳۹۳)

[۶]- زرین، ک.، عقد بیمه و مبانی مناقصه و تضمینات آن: مبانی نظری، شیوه عملی تنظیم، آراء محاکم قضایی و نظریه‌های مشورتی، کلک زرین، تهران، ایران (۱۳۹۸)

[۷]- عاملی، س.، رویکرد قضایی به آسیب‌ها، جرائم و قوانین و سیاست‌های فضای مجازی، انتشارات امیرکبیر، تهران، ایران (۱۳۹۰)

[۸]- گریسلدا، د.، تئوری ریسک و بیمه اتکایی، کانون نشر علوم، تهران، ایران (۱۳۹۹)

[۹]- مهدوی، غ.، نصیری، ف.، اصول و مبانی نظری بیمه، پژوهشکده بیمه وابسته به بیمه مرکزی جمهوری اسلامی ایران، تهران، ایران (۱۳۹۱)

[۱۰]- Brier S., (2010), Cybersemiotics and the question of knowledge, World Scientific Publishing Co.

[۱۱]- Eling, M., (2016), What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance, Volume 17 Issue 5.

[۱۲]- Dorfman, M.S., (2008), Introduction to risk management and insurance, 9th ed, Englewood Cliffs: Prentice Hall.

[۱۳]- Folsom, T., (2007), Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality), Tulane Journal of Technology & Intellectual Property, Vol. 9.

[۱۴]- Haney, M., (2006), An introduction to cyber peacekeeping, Computers in Human Behavior, Volume 61, Pages 22-48.

[۱۵]- Majuca, R., (2006), The Evolution of Cyberinsurance, Department of Economics; National Center for Supercomputing Applications (NCSA), College of Law, University of Illinois at Urbana-Champaign.

[۱۶]- Mukhopadhyay, A., (2019), Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance, Information Systems Frontier, Volume 21, Issue 5, Pages 997–1018.