بررسی

نظام بیمه مجازی

و تبیین جایگاه آن در نظام بیمه کشور

گروه

اقتصاد و مدیریت

فضای مجازی

سازمان فضای مجازی سراج

مرکز تحقیقات و آینده پژوهی

بسم الله الرحمن الرحیم

بررسی نظام بیمه مجازی و تبیین جایگاه آن در نظام بیمه کشور

گروه اقتصاد و مدیریت فضای مجازی

شماره اثر: ۹۷۰۱۰۰۳

تیر ۹۷

سازمان فضای مجازی سراج
مرکز تحقیقات و آینده پژوهی

فضای مجازی واقعاً یک دنیای رو به رشدِ غیرقابل توقّف است، یعنی واقعاً آخر ندارد؛ آدم هرچه نگاه می‌کند، آن چیزِ اوّلِ‌بلاآخر، فضای مجازی است. هرچه انسان پیش می‌رود در این فضا، این همین‌طور ادامه دارد. این یک فرصت بزرگی در اختیار هر کشوری می‌گذارد، تهدیدهایی هم در کنارش دارد؛ ما بایستی کاری کنیم که از آن فرصت‌ها حدّاکثر استفاده را بکنیم، از این تهدیدها تا آنجایی که ممکن است خودمان را برکنار نگه بداریم.

مقام معظم رهبری مد ظلّه العالی
بیانات در دیدار رئیس‌جمهور و اعضای هیأت دولت - ۹۵/۶/۳

دیگر تردیدی در این معنا نیست که در روزگار ما فضای مجازی، خاص‌ترین و موثرترین پدیده فناورانه پیرامون ماست. آنچنانکه توانسته است بر همه حوزه‌های مختلف زندگی بشر، اثرگذاری‌های جدی و دگرگون کننده داشته باشد. شاید در دهه‌های قبل، هیچکسی نمی‌توانست کوچکترین تصوری از رشد معجزه آسای این پدیده داشته باشد تا جایی که ظرف سالیانی کوتاه، همه ساحت‌های زندگی نسل بشر را فتح کرده و امتزاجی جدید بیافریند.

آینده‌ای که مهم است

با این تفاسیر، شناخت ماهیت و چیستی فضای مجازی موجود اهمیت به سزایی دارد. همزمان با آن خبر گرفتن از آینده پیش رو و شناسایی روزگار بعد، شایسته تأمل و مطالعه است تا بتوان دست به کار طراحی‌های مؤثری شد تا به فضای مجازی مطلوب و بومی، دست پیدا کنیم. این مقوله امروز در زمره یکی از مهمترین نیازمندی‌های سیاستگذاران و تصمیم گیران کشور است.

این ادعا گزافه نیست که مطمئناً در آینده نزدیک، مدیران کشور در حوزه‌های مختلف (اقتصاد، سیاست، امنیت، فرهنگ و ...) نیازمند شناخت دقیق و تأمل هوشمندانه در باب فضای مجازی خواهند بود.

بسته‌ای برای نگاه به آینده

بسته مطالعاتی حاضر، بر اساس همین ضرورت، تدوین شده که به صورت محدود و تعیین شده، منتشر می‌شود. هدف از این بسته‌های مطالعاتی پژوهشی، کمک به توسعه و عمق بخشی به شناخت و درک ما از پدیده فضای مجازی است. در هر بسته یک موضوع خرد در رابطه با فضای مجازی، انتخاب شده است که ضمن بررسی و مداقه، با یک جمع بندی روشن، نهایی سازی شده است.

مجموعه حاضر می‌تواند برای همه متخصصان در حوزه‌های گوناگون (در لایه سیاستگذار و تصمیم گیر) کمک کننده و یاری رسان باشد تا ضمن دغدغه آفرینی برای ایشان، توان فردی و جمعی آنان را به نفع این پدیده وارد میدان سازد.

مرکز تحقیقات و آینده‌پژوهی سراج

این مطالعات و نظایر آن، به طور مستمر و راهبردی در «مرکز تحقیقات و آینده‌پژوهی سراج» به انجام می‌رسد. در این مسیر تلاش می‌شود ضمن تکمیل قطعات مطالعاتی پژوهشی مورد نیاز در نظام واره های مدیریتی علمی، در جهت شناخت صحیح فضای مجازی موجود و تصویرسازی آینده گام برداشته شود. این کوشش ما را به نقطه‌ای خواهد رساند که بتوانیم به طراحی هوشمندانه فضای مجازی مطلوب، اقدام کنیم.

امیدواریم با عنایت خداوند و تلاش خالصانه پژوهشگران این مرکز، این مرکز در آینده نه چندان دور، به نقش آفرینی‌های جدی‌تر به نفع آرمان‌های انقلاب اسلامی و توانمندسازی نظام جمهوری اسلامی ایران در عرصه‌های جهانی، نائل آید.

فهرست مطالب

۱- مفهوم‌شناسی بیمه مجازی و جوانب مختلف آن..... ۱

۱-۱ مقدمه..... ۲

۱-۲ تبیین چیستی بیمه فضای مجازی..... ۲

۱-۳ تعریف اصطلاحات..... ۵

۱-۳-۱ قرارداد بیمه..... ۵

۱-۳-۲ امنیت فضای مجازی..... ۵

۱-۳-۳ سیاست‌گذاری امنیتی..... ۵

۱-۳-۴ سیستم امنیتی..... ۵

۱-۳-۵ امنیت سخت‌افزار..... ۶

۱-۳-۶ سیستم امنیت داده..... ۶

۱-۳-۷ فضای مجازی..... ۶

۱-۳-۸ تهدید در فضای مجازی..... ۶

۱-۳-۹ سیستم رایانه‌ای..... ۶

۱-۳-۱۰ داده پیام..... ۷

۱-۳-۱۱ سیستم اطلاعاتی..... ۷

۱-۳-۱۲ بیمه فضای مجازی..... ۷

۱-۳-۱۳ احتمال..... ۷

۱-۳-۱۴ کارگزار بیمه..... ۸

۱-۳-۱۵ بیمه غرامت حرفه‌ای..... ۸

۱-۴ سابقه بیمه فضای مجازی در سایر کشورها..... ۸
۱-۵ فروض عمومی حاکم بر بیمه فضای مجازی..... ۹
۱-۶ نمونه‌های بیمه‌نامه فضای مجازی..... ۱۰
۱-۷ انواع بیمه‌های فضای مجازی (بر مبنای شخص اول و شخص ثالث)..... ۱۲
۱-۷-۱ انواع بیمه‌های پوشش شخص اول..... ۱۲
۱-۷-۲ بیمه مخاطرات اموال الکترونیکی..... ۱۳
۱-۷-۳ بیمه اختلال در کسب‌وکار..... ۱۳
۱-۷-۴ بیمه اخاذی سایبری..... ۱۳
۱-۷-۵ بیمه خسارت به اعتبار تجاری..... ۱۳
۱-۷-۶ بیمه دزدی پول و اموال تجاری..... ۱۴
۱-۷-۷ انواع بیمه‌های پوشش شخص ثالث..... ۱۴
۱-۷-۸ بیمه نقض امنیت و محرمانگی..... ۱۴
۱-۷-۹ بیمه مسئولیت رسانه‌ای..... ۱۴
۱-۷-۱۰ بیمه اتلاف داده شخص ثالث..... ۱۴
۱-۷-۱۱ بیمه هزینه‌های آگهی به مشتری..... ۱۴
۱-۷-۱۲ بیمه مسئولیت در قبال شخص ثالث به دلیل ارسال ایمیل یا پیامک..... ۱۴
۱-۷-۱۳ بیمه رمزگیری (فیشینگ)..... ۱۵
۱-۷-۱۴ بیمه مسئولیت عمدی..... ۱۵
۱-۷-۱۵ بیمه مسئولیت خطای فنی و بی مبالاتی..... ۱۵
۱-۸ بیمه فضای مجازی برای فین‌تک..... ۱۶
۱-۸-۱ تعریف فین‌تک..... ۱۶
۱-۸-۲ دسته‌بندی فین‌تک..... ۱۷
۱-۸-۳ اهمیت بیمه برای فین‌تک‌ها..... ۱۹
۱-۸-۴ مخاطرات موجود در ابزارهای فین‌تک..... ۲۱
۱-۹ ضرورت ایمنی فضای مجازی..... ۲۸
۱-۱۰ اهمیت پوشش بیمه برای فضای مجازی..... ۳۰
۱-۱۱ عوامل خطرساز در مسئله فضای مجازی را می‌توان به صورت زیر برشمرد:..... ۳۱
۱-۱۲ مفهوم ریسک در فضای مجازی و انواع آن..... ۳۲
۱-۱۳ تعریف مبانی حاکم بر بیمه فضای مجازی..... ۳۲
۱-۱۳-۱ هک..... ۳۲
۱-۱۳-۲ حمله عدم سرویس‌دهی..... ۳۲

۱-۱۳-۳ اخاذی اطلاعاتی ۳۳
۱-۱۳-۴ خطای نیروی انسانی ۳۳
۱-۱۳-۵ نقص ناشی از نرم‌افزار ۳۳
۱-۱۳-۶ نقض داده ۳۳
۱-۱۳-۷ انتقال ویروس ۳۳
۱-۱۳-۸ حالت عدم فعالیت شبکه ۳۳
۱-۱۳-۹ از بین رفتن فیزیکی سیستم ۳۴
۱-۱۴ سابقه روش‌های محاسبات ریسک در بیمه فضای مجازی ۳۴
۱-۱۵ ابعاد تجاری بیمه‌های فضای مجازی ۳۴
۱-۱۶ متقاضیان بیمه فضای مجازی ۳۵
۱-۱۷ نتیجه گیری ۳۶

۲- بررسی نمونه‌های موفق و تجربه کشورهای پیش‌رو در زمینه بیمه مجازی ۳۸

۲-۱ انواع پوشش‌های بیمه سایبر ۳۹
۲-۱-۱ پوشش شخص ثالث ۳۹
۲-۱-۲ پوشش شخص اول ۳۹
۲-۲ پوشش‌های بیمه سایبر بر حسب میزان تقاضا در بازار ۴۰
۲-۳ نکاتی برای خریداران بیمه سایبری ۴۰
۲-۴ نیازهای ایجاد بیمه مجازی ۴۲
۲-۵ مدل بررسی ریسک سایبری ۴۲
۲-۶ مشکلات بیمه‌گذار فضای مجازی و راه حل‌های آن ۴۶
۲-۶-۱ عدم توانایی تعیین دقیق مبلغ بیمه‌نامه به دلیل کمبود اطلاعات کافی در مورد داده‌های سایبری ..۴۶
۲-۶-۲ انباشت فاجعه‌آمیز حملات سایبری ۴۶
۲-۶-۳ تضعیف قابلیت پیش‌بینی در معرض خطر قرارگرفتن به دلیل تکامل مداوم ریسک‌ها ۴۶
۲-۶-۴ دید محدود بیمه‌گذاران و محدودیت محصولات بیمه سایبری ۴۶
۲-۶-۵ عدم استانداردسازی در تعیین و تهیه ریسک‌های اینترنتی ۴۷
۲-۶-۶ عدم درک کامل اغلب خریداران بیمه از خطرات سایبری و یا گزینه‌های بیمه نامه ۴۷
۲-۶-۷ جریان قانونی و نظارتی ۴۷
۲-۷ فواید اقتصادی بیمه سایبر ۴۸
۲-۸ حوزه‌های کشورهای پیشرو در صنعت بیمه ۴۸
۲-۹ بیمه در ایران ۴۹

۳- وضعیت ایران در بیمه فضای مجازی و چالش‌ها..... ۵۱

۳-۱ بیمه فضای مجازی در ایران..... ۵۲

۳-۲ چالش‌های صنعت بیمه فضای مجازی..... ۵۳

۳-۲-۱ عدم وجود پیشینه تاریخی حوادث..... ۵۳

۳-۲-۲ عدم توانایی تعیین دقیق قیمت بیمه نامه..... ۵۴

۳-۲-۳ تجمع ریسک..... ۵۴

۳-۲-۴ عدم افشای اطلاعات توسط بیمه‌گذار..... ۵۴

۳-۲-۵ عدم آگاهی افراد از این حوزه بیمه..... ۵۵

۳-۲-۶ عدم قابل پیش بینی بودن..... ۵۵

۴- منابع..... ۵۶

۱- مفهوم‌شناسی بیمه مجازی و جوانب مختلف آن

۱-۱ مقدمه

شناخت مخاطرات و به حداقل رساندن آن‌ها جهت برنامه‌ریزی دقیق نیازی انکارناپذیر است، لذا بایستی مخاطرات را در زمینه‌هایی که فعالیت در آن‌ها برنامه‌ریزی می‌شود، شناسایی نمود تا بتوان از حداکثر امکانات برای مقابله با آن‌ها مدد گرفت. میزان بودجه‌ای که دولت‌ها در فضای مجازی برای تأمین امنیت آن صرف می‌کنند رو به افزایش است و این خود نشان دهنده اهمیت فراهم کردن محیط مجازی امن تا حد امکان است.

در این گزارش سعی می‌شود با تأکید بر جنبه‌های عملیاتی طرح، هرچه بیشتر فضا برای ایجاد بیمه‌نامه‌ها و خدمات امنیتی اینترنتی توسط شرکت‌های بیمه داخلی ملموس‌تر شود. لذا ابتدا کلیاتی از بیمه فضای مجازی ارائه می‌شود و سپس اصول و قواعدی که عموماً در بیمه‌نامه‌های فضای مجازی بدان توجه می‌شود، به بحث گذاشته خواهد شد. اهداف عمده طرح عبارت‌اند از:

- ارائه تعاریفی مختصر از اصطلاحات حوزه مورد بررسی
- بررسی کلیات مربوط به بیمه‌های فضای مجازی
- معرفی و طبقه‌بندی انواع بیمه‌های قابل عرضه در فضای مجازی و تجارت الکترونیک
- تبیین روش‌های محاسبه ریسک در بیمه فضای مجازی
- ارائه اصول مربوط به بیمه تجارت الکترونیک و فضای مجازی

در این تحقیق، به بررسی مفهوم بیمه مجازی پرداخته شده است، همچنین مواضع مورد نظر بیمه شناسایی شد. اهمیت بیمه و امنیت در فضای مجازی تبیین گشت و مسأله محاسبه ریسک نیز به بحث گذاشته شد.

۱-۲ تبیین چیستی بیمه فضای مجازی

تقریباً در اوایل قرن ۲۱ که صنعت اینترنت به تازگی توسعه پیدا کرده بود، برخی بیمه‌گران اقدام به ارائه خدماتی کردند که زیان‌های مالی ناشی از نقض داده[1] را پوشش می‌داد؛ این در حالی بود که بسیاری از فعالان تجاری[2] به تازگی به قابلیت اقتصادی اینترنت پی برده بودند و بیمه‌گران هم بیشتر به دنبال بیمه شرکت‌های اینترنتی بزرگی[3] چون یاهو[4]، آمازون[5] و گوگل[6] بودند.

اولین بیمه‌نامه‌های فضای مجازی حول موضوع جرائم این فضا شکل گرفتند و به طور کلی ابتدا بیمه‌های فضای مجازی مربوط به بیمه اموال و مسئولیت بودند (سایبر اینشورنس، ۲۰۱۲). بیمه مسئولیت در فضای مجازی ابتدا هزینه‌ها و مسئولیت‌های ناشی از نقض امنیت سیستم‌های رایانه‌ای بیمه‌گذار را

---

[1] Data breach
[2] Such as Brick and Mortar
[3] Big dotcom companies
[4] Yahoo
[5] Amazon
[6] Google

پوشش می‌داد و بیمه‌نامه‌های اموال نیز اختلال در کسب‌وکار و از بین رفتن اموال اطلاعاتی[1] در اثر نقض داده را تحت پوشش خود در آورده بودند. بیمه‌های اموال همچنین موارد مربوط به بیمه‌های شخص اول شامل مقابله با هکرها، اخاذی اطلاعاتی و مدیریت بحران را نیز در بر می‌گرفتند.

نخستین فعالیت مربوط به کاربرد سیستم توزیع بیمه برای اینترنت، به سال ۱۹۹۴ برمی‌گردد. مبدع استفاده از مدیریت ریسک شامل استفاده از پوشش بیمه‌ای برای اینترنت نیز دان‌گیر[2] بوده است. او نخستین کسی بود که ارتباط مقوله مدیریت ریسک که عموماً در دیگر رشته‌ها و به‌به خصوص در بخش مالی به کار می‌رفت را با اینترنت مطرح کرد. همچنین بارزترین فردی که بیمه اینترنت را در بحث‌های آکادمیک مطرح کرد، بروس شنیر[3] بود که آنچه را که امروزه در مورد نقش بیمه اینترنت بر آن اجماع شده قبلاً تشریح کرده است (یورسیک، ۲۰۰۶)[4].

در همان ابتدا یکی از مهمترین چالش‌های بیمه ضرورت تفهیم مخاطبان بیمه فضای مجازی در مورد لزوم تحت پوشش قرار گرفتن بوده است. به مرور و با وضع قوانین ایالتی در امریکا و توسعه آن در سطح جهان (که مشارکت هر چه بیشتر شرکت‌ها در گزارش نقض داده در فضای مجازی را ایجاب می‌کرد) و همچنین لزوم مقابله هر چه بیشتر با جرائم سازمان یافته سایبری، بیمه‌های فضای مجازی به یکی از مهمترین ملزومات فعالیت در فضای مجازی تبدیل شد. براساس سایت اطلاعات[5] امروزه درآمد سالیانه حاصل از بیمه فضای مجازی بالغ بر یک میلیارد الی دو میلیارد دلار است که می‌تواند به دو برابر رقم مذکور در سال‌های آینده برسد (السان, ۱۳۹۵).

امروزه هیچ کس در دورنمای روشن بیمه فضای مجازی تردید ندارد و بسیاری از کارشناسان حوزه بیمه بر این اعتقادند که بیمه فضای مجازی، سریع‌ترین و رو به رشدترین بیمه در سراسر جهان است؛ زیرا نه تنها شرکت‌های بزرگ متقاضی آن هستند، بلکه شرکت‌های کوچک و سامانه‌های نه چندان امن آن‌ها نیز چون مکرراً مورد حمله قرار می‌گیرند، نیازمند بیمه هستند. افزایش ۵۰ درصدی حق بیمه پرداختی برای بیمه‌های فضای مجازی و نیز افزایش ۲۱ درصدی تقاضا برای محصولات مجازی در سال 2013 موید این مسئله است (کاپی مگزین،۲۰۱۳)[6].

---

[1] Data asset loss
[2] Dan Geer
[3] Bruce Schneier
[4] (Majuca, Kesan, & Yurcik, 2006)
[5] Informationweek.com
[6] (kpmg, 2013)

طبق تحقیقات صورت گرفته میزان تعرض به داده در سال ۲۰۱۴، در بخش بانکی و مالی ۵٫۵ درصد، کسب‌وکار ۳۳ درصد، آموزش ۷٫۳ درصد، دولت و نیروهای نظامی ۱۱٫۷ درصد و بخش بهداشت ۴۲٫۵ درصد بوده است. هرچند که اطلاعات اعلام نشده بسیاری نیز در این بخش‌ها وجود دارد که ارزیابی صحیح و دقیق از مخاطرات را با دشواری روبرو می‌سازد.

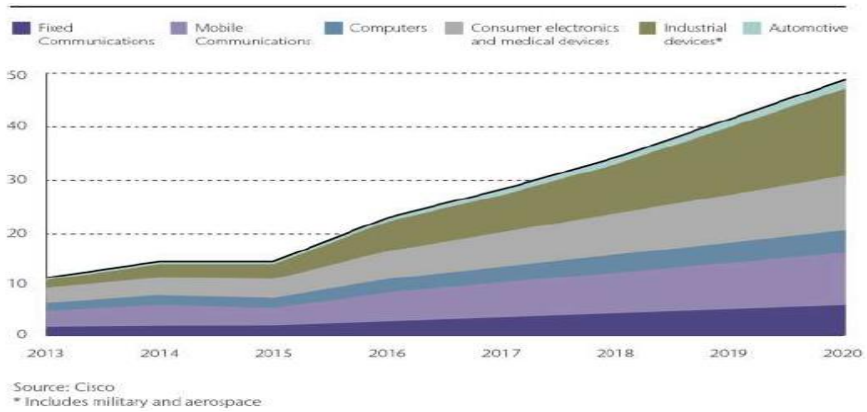
Total Data Breaches in 2014

	No. of breaches (% of all breaches)	No. of records exposed (% of all records exposed)
Banking/Credit/Financial	43 (5.5%)	1,198,492 (1.4%)
Business	258 (33.0%)	68,237,914 (79.7%)
Educational	57 (7.3%)	1,247,812 (1.5%)
Government/Military	92 (11.7%)	6,649,319 (7.8%)
Medical/Health Care	333 (42.5%)	8,277,991 (9.7%)
Totals for all categories:	783 (100%)	85,611,528 (100%)

Source: Identity Theft Resource Center
Note: The ITRC defines a breach as an event in which an individual's name plus Social Security number, driver's license number, medical record, or financial record/credit/debit card is potentially put at risk. Breaches include those identified as of 1/5/2015.

تصویر ۱. افزایش حجم داده‌ها در سال ۲۰۱۴

همچنین پیش‌بینی می‌شود که تا سال ۲۰۲۰ حدود ۵۰ میلیارد دستگاه متصل به اینترنت در سراسر جهان وجود خواهد داشت که از این تعداد، تلفن همراه و رایانه‌ها بیشترین میزان را تشکیل می‌دهند. از طرف دیگر با ورود اینترنت اشیاء[1] به زندگی بشر، تعداد دستگاه‌هایی که به اینترنت متصل می‌شوند، رو به افزایش است. طبق این گزارش‌ها و سایر پیش‌بینی‌های صورت گرفته، لزوم توجه به امنیت اینترنت و فضای مجازی مشخص می‌گردد.



تصویر ۲. پیش‌بینی شرکت سیسکو ازدستگاه‌های متصل به اینترنت در سال ۲۰۲۰

[1] IOT

۱-۳ تعریف اصطلاحات

برای آشنایی بیشتر با بیمه در فضای مجازی و اصطلاحاتی که در بیمه‌نامه‌های معتبر می‌آید، در ادامه به بازتعریف حقوقی عناوین مصطلح در بیمه پرداخته می‌شود.

۱-۳-۱ قرارداد بیمه

قرارداد بیمه یا همان بیمه‌نامه ایجاب می‌کند که مفاهیم مندرج در آن به وضوح تعریف گردد به گونه‌ای که جای هیچ ابهام و اجمالی باقی نماند. از این رهگذر اختلافات حادث، بسیار سریع‌تر و بهتر رفع و رجوع می‌گردد. در ماده ۲۴ بیمه‌نامه‌ای که شرکت چاب[1] منتشر کرده است[2]، به وضوح مفاهیمی که در بیمه‌نامه به آن اشاره شده تعریف گردیده است. در بیمه‌نامه دیگر شرکت مزبور که در رابطه با مدیا منتشر شده است[3]، نیز این تعاریف در ماده ۲ بیان شده است.

۱-۳-۲ امنیت فضای مجازی

امنیت فضای مجازی، به ایمن بودن در برابر استفاده مجرمانه یا غیرقانونی از داده‌های الکترونیکی یا به اقداماتی که جهت ایجاد این امنیت صورت می‌گیرد گفته می‌شود.[4] به عبارت دیگر امنیت فضای مجازی مجموعه اقداماتی است که جهت حفاظت رایانه یا سیستم رایانه‌ای (در مواقع اتصال به شبکه) برای مقابله با حمله یا ورود غیر مجاز صورت می‌گیرد. برخی منابع نیز امنیت فضای مجازی را به روش‌هایی که برای محافظت از سیستم‌های رایانه‌ای در برابر تهدیدها مانند ویروس انجام می‌گیرد، تعریف کرده‌اند.[5]

۱-۳-۳ سیاست‌گذاری امنیتی

سیاست‌گذاری امنیتی، اصولاً در بردارنده رویه‌ها، قواعد و مقررات مربوط به دسترسی رایانه به شبکه می‌باشد. اینکه یک سازمان چگونه مدیریت شود و اطلاعات محرمانه خود را (اطلاعات مربوط به مراجعان و یا اطلاعات شرکتی) محافظت کند و چارچوب تأمین امنیت مربوط به شبکه رایانه‌ای را فراهم سازد، همگی نشان دهنده خط مشی‌های امنیتی آن سازمان است.[6] در کل به مجموعه قواعدی که مشخص می‌کند چه کسی مجوز دسترسی به چه اطلاعاتی را دارد، تحت چه شرایطی دارای چنین اختیاری می‌شود و همچنین معیارهایی که طبق آن‌ها چنین مجوزی داده شده یا گرفته می‌شود، سیاست‌گذاری فضای مجازی می‌گویند.

۱-۳-۴ سیستم امنیتی

سیستم امنیتی به فرایندی گویند که مسئول کنترل ورود به منابع (اطلاعات محرمانه) سیستم اصلی است و همیشه در حال فعالیت می‌باشد. این سیستم بایستی در بردارنده میزان محافظت کافی برای چنین

---

[1] CHUBB
[2] (Airmic Review of Recent Developments in the Cyber, 2013)
[3] ibid
[4] www.oxforddictionaries.com/definition/english/cybersecurity
[5] dictionary.cambridge.org/dictionary/business-english/cybersecurity
[6] www.webopedia.com/TERM/S/security_policy.html

اطلاعاتی بوده و باید قسمت‌هایی از سیستم را که داده‌ها و سامانه‌ها را پشتیبانی و محافظت می‌کند، کنترل نماید[1] یا به هر شیوه‌ای که برای محافظت از اطلاعات و اموال در برابر طیف بزرگی از مخاطرات لازم است، مجهز باشد.[2]

۱-۳-۵ امنیت سخت‌افزار

به فرآیند استفاده از سخت‌افزارهایی مانند سخت‌افزارهای حافظه برای پشتیبان‌گیری و سخت‌افزارهای موسوم به ثبت‌نام محدود[3] جهت پیشبرد تأمین امنیت سامانه گویند.[4]

۱-۳-۶ سیستم امنیت داده

به صورت کلی وقتی ابزارهایی برای حفاظت داده‌ها از عملیات ارادی یا غیر ارادی افشا، خرابی یا تغییر[5] به کار گرفته می‌شوند.

۱-۳-۷ فضای مجازی

فضای مجازی، دامنه‌ای جهانی درون محیط اطلاعاتی می‌باشد که دربردارنده شبکه به هم متصل زیرساختاری سیستم اطلاعاتی است و شامل اینترنت، شبکه‌های ارتباط راه دور، سیستم‌های رایانه‌ای و کنترل‌گرها و پردازشگرهای آن می‌گردد.

۱-۳-۸ تهدید در فضای مجازی

به هر نوع وضعیت یا اتفاقی گفته می‌شود که از طریق یک سیستم اطلاعاتی، امکان تأثیر نامساعد بر عملیات سازمانی (مأموریت، عملکرد، اعتبار و ...)، اموال سازمانی، افراد و سایر سازمان‌ها را از طریق دسترسی غیرمجاز، خرابی، افشا، تغییر اطلاعات و عدم سرویس‌دهی داشته باشد.

۱-۳-۹ سیستم رایانه‌ای

رایانه‌های به هم متصل با یک سیستم ذخیره را گویند. سیستم رایانه‌ای می‌تواند به طور مستقل عمل کرده و با سایر سامانه‌های فعال در شبکه ارتباط برقرار کند.[6] در تعریف دیگر سیستم رایانه‌ای عبارت از هر نوع دستگاه یا مجموعه دستگاه‌های متصل سخت افزاری-نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده‌پیام» عمل می‌کند. (قانون تجارت الکترونیکی ایران)

---

[1] www.encyclopedia.com/doc/1O11-systemsecurity.html
[2] dictionary.reference.com/browse/security+system
[3] bound registers
[4] www.encyclopedia.com/doc/1O11-hardwaresecurity.html
[5] (Kissel, 2013)
[6] http://thelawdictionary.org/computer-system/

۱-۳-۱۰ داده پیام

داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود (قانون تجارت الکترونیکی ایران). در این مفهوم، داده پیام مفهومی عام‌تر از نوشته الکترونیکی داشته و در واقع هر نوع داده‌ای را شامل می‌شود.

۱-۳-۱۱ سیستم اطلاعاتی

سیستم اطلاعاتی، سیستمی برای تولید، ارسال، دریافت، ذخیره یا پردازش داده پیام است (قانون تجارت الکترونیکی ایران). در واقع، سیستم اطلاعاتی مجموعه‌ای از مولفه‌های وابسته به هم است که با گردآوری، پردازش، ذخیره و توزیع داده‌های اطلاعاتی، از تصمیم‌گیری و کنترل در سازمان‌ها پشتیبانی می‌کند. این سیستم علاوه بر کمک کردن به ایجاد هماهنگی در انجام عملیات سازمانی، به مدیران و کارکنان سازمان‌ها کمک می‌کند تا مسائل سازمان را تحلیل یا شبیه‌سازی کنند.

سیستم‌های اطلاعاتی سه فعالیت عمده را انجام می‌دهند: ورود داده‌ها، پردازش و خروج داده‌ها؛ یعنی داده‌ها وارد سیستم اطلاعاتی شده و بر روی آن عملیات پردازش صورت می‌گیرد تا به اطلاعات در قالب‌های خاص تبدیل شود؛ سپس این اطلاعات در اختیار افراد مصرف‌کننده قرار می‌گیرد تا از آن استفاده کند. در این سیستم‌ها عمدتاً می‌بایست بازخورد نیز وجود داشته باشد که از سوی مصرف‌کنندگان ارائه می‌شود و به منظور بهبود سیستم مورد استفاده قرار می‌گیرد. اگرچه مکانیزم عملکرد سیستم‌های اطلاعاتی با شرحی که گفته شد، شباهت زیادی با یک رایانه دارد، اما ماهیت یک سیستم اطلاعاتی فراتر از رایانه یا نرم‌افزار است. رایانه و نرم‌افزار، ابزارها و اجزایی هستند که یک سیستم اطلاعاتی را تشکیل می‌دهند، اما قادر نیستند به تنهایی اطلاعاتی را که یک سازمان به آن‌ها نیاز دارد، تولید کنند (لاودن & لاودن, ۲۰۱۲).

۱-۳-۱۲ بیمه فضای مجازی

بیمه فضای مجازی برای جبران زیان‌های ناشی از اتفاقات مختلف در فضای مجازی مانند نقض داده، اختلال در کسب‌وکار و صدمه به شبکه طراحی شده است.[1] قانون بیمه این عقد را این گونه تعریف می‌کند: «بیمه عقدی است که به موجب آن یک طرف تعهد می‌کند در ازاء پرداخت وجه یا وجوهی از طرف دیگر در صورت وقوع یا بروز حادثه خسارت وارده بر او را جبران نموده یا وجه معینی بپردازد. متعهد را بیمه‌گر و طرف تعهد را بیمه‌گذار و وجهی را که بیمه‌گذار می‌پردازد حق بیمه و آنچه را که بیمه می‌شود موضوع بیمه می‌نامند».

۱-۳-۱۳ احتمال

هدف از تجارت بیمه برای بیمه‌گر کسب سود بوسیله جمع‌آوری حق بیمه‌های کافی جهت پرداخت خسارات موضوع بیمه است. برای این منظور و حفظ تعادل میان حق بیمه‌ها و سود حاصل و میزان خسارت پرداختی، بیمه‌گران بایستی با دقت به تعیین قیمت‌ها (حق بیمه) بپردازند که اصطلاحاً نرخ‌گذاری نامیده

[1] http://www.dhs.gov/publication/cybersecurity-insurance

می‌شود.[1] حال در این میان بیمه‌گران از یک سری روش‌های محاسباتی استفاده می‌کنند تا احتمال وقوع حادثه را ارزیابی کنند. این عدد میان صفر و یک است و احتمال وقوع حادثه را معین می‌کند.

۱-۳-۱۴ کارگزار بیمه

کارگزار، شخص حقیقی یا حقوقی است که به عنوان واسطه میان بیمه‌گذار (که می‌تواند هر شخص حقیقی یا حقوقی اعم از تجاری و سازمانی باشد) و بیمه‌گر عمل می‌کند. کارگزاران بیمه با در اختیار قراردادن دانش خود در صنعت بیمه به بیمه‌گذاران کمک می‌کنند تا مناسب‌ترین نوع بیمه‌نامه را انتخاب و خود را نسبت به مخاطرات احتمالی تحت پوشش قرار دهند.[2] در واقع کارگزار بیمه متخصص بیمه و مدیریت ریسک است.[3]

۱-۳-۱۵ بیمه غرامت حرفه‌ای

نوعی از بیمه است که شاغلین حرفه‌ای از جمله حسابداران، حقوق‌دانان و مانند آن‌ها را در موارد بی‌مبالاتی و بی‌احتیاطی‌های شغلی بیمه می‌کند. این نوع بیمه‌ها از آن‌جا که حمایت‌هایی را به عمل می‌آورند که در بیمه‌های مسئولیت عمومی وجود ندارد، حائز اهمیت هستند چرا که بیمه‌نامه‌های اخیر خسارت‌هایی که در اثر بی‌دقتی یا عدم انجام صحیح وظایف خاص شغلی ایجاد می‌شود، پوشش نمی‌دهند. عنوان بیمه‌ها در این قسم از بیمه ممکن است بر حسب حرفه موضوع بیمه متفاوت باشد مثلاً بیمه موسوم به بیمه غرامت[4] پزشکی که مخصوص حرفه پزشکی دارویی است.[5]

۱-۴ سابقه بیمه فضای مجازی در سایر کشورها

در اواخر دهه ۱۹۹۰ بیمه‌نامه هکر برای اولین بار طراحی شد. نخستین بیمه‌نامه معروف هکر توسط شرکت‌های فناوری و با همکاری شرکت‌های بیمه‌ای به منظور ارائه خدمات فناوری و بیمه شخص اول به مشتریان عرضه شد تا از فناوری‌های شرکت‌های فناوری حمایت کند یا یک راه‌حل جامع مدیریت کامل ریسک را برای شرکت‌های متقاضی فراهم کند.

به دلیل جدید و ناشناخته بودن این بخش، شرکت‌های بیمه‌ای فعالیت خود را با پوشش‌های کوچک آغاز نمودند؛ بنابراین انجمن بین‌المللی امنیت کامپیوتری[6] اولین گروهی بود که به ارائه بیمه هکر به عنوان نوعی تضمین برای معتبر بودن خدماتش اقدام کرد. این انجمن فعالیت خود را فقط با حداکثر پوشش ۲۵۰ هزار دلار در سال آغاز نمود. علاوه براین تقریباً تمام این بیمه‌نامه‌های هکر، فقط خسارت شرکت خصوصی بیمه‌گذار (شخص اول) را پوشش می‌داد، چگونگی شروع فعالیت اولین بیمه هکر از پوشش‌های ساده و کم در مقابل خسارت حملات هکرها تا بیمه‌نامه‌های متنوع هکر را نشان می‌دهد.

---

[1] (Zhang & Dong, 2011)
[2] http://www.prospects.ac.uk/insurance_broker_job_description.htm
[3] http://understandinsurance.com.au/insurance-brokers
[4] Mal Practice Insurance
[5] http://www.investopedia.com/terms/p/professional-liability-insurance.asp
[6] International Computer Security Association

جدول ۱. شروع فعالیت اولین بیمه هکر از پوشش‌های ساده

سال	شرکت	توضیح	پوشش
۱۹۹۸	ICSA TruSecure	تضمین محصول	پوشش شخص اول: حداکثر تا ۲۰ هزار دلار در هر حادثه؛ حداکثر تا ۲۵۰ هزار دلار در سال
۱۹۹۸	Cigna Corp/Cisco Systems/NetSolve	همکاری بیمه‌ای/ شرکت‌های انتفاعی با شرکت‌های فناوری؛ مشتریان باید خدمات ارزیابی امنیت و نظارت خریداری کنند	شخص اول (خسارت هکر و توقف در کار)؛ ۱۰ میلیون دلار
۱۹۹۸	J.S. Wurzler Underwriting	کارگزار بیمه	شخص اول
۱۹۹۸	IBM/Sedgwick	همکاری بین شرکت فناوری و شرکت بیمه	۱۵-۵ میلیون دلار
۲۰۰۰	Counterpane/ Lloyd's of London	همکاری بین شرکت امنیت اینترنتی با بیمه لویدز	شخص اول؛ ۱۰-۱ میلیون دلار
۲۰۰۰	AIG	ظهور انواع بیمه‌های جامع‌تر و کامل‌تر	شخص اول و ثالث (کپی غیرقانونی از کتابی که حق کپی دارد، لطمات به حیثیت از طریق نگارش مطالب در فضای اینترنت، شایعه و تهمت غیرواقعی، عدم‌دسترسی کاربران غیرمجاز به داده‌های شخصی[محرمانه] افراد، تعرض از طریق شبکه به حریم افراد، خطاها و اشتباهات)؛ ۲۵ میلیون‌دلار
۲۰۰۱	Marsh McLennan/AT&T	مشتریانی که از مرکز اینترنت شرکت AT&T خدمات خریداری می‌کنند از شرکت بیمه تخفیف می‌گیرند	شخص اول

۱-۵ فروض عمومی حاکم بر بیمه فضای مجازی

اگرچه اکثر اصول عام بیمه در مورد بیمه‌های فضای مجازی قابل اعمال است اما در تنظیم بیمه‌نامه‌های فضای مجازی باید به ویژگی‌های خاص فضای مجازی که البته در هر نوع متفاوت خواهد بود توجه داشت. برخی از این ویژگی‌ها که بیمه‌گر باید آن‌ها را مورد توجه قرار دهد، در ادامه بیان شده است.

مکان: مرتکب دزدی اطلاعات یا آسیب به اموال ممکن است در هنگام ارتکاب جرم از طریق اینترنت هزاران کیلومتر دورتر از محل تجارت باشد.

درجه: آثار خسارت یک ویروس می‌تواند از کسب‌وکار هدف فراتر برود و موجب شود کسب‌وکار مورد هدف اولیه، خود به علت وارد کردن خسارت، مسئول شناخته شود.

قابلیت مشاهده: چون کالای موجود در اینترنت داده‌ها می‌باشند، رخنه‌های امنیتی اغلب کشف نمی‌شوند.

ارزش‌گذاری: اصولاً ارزش‌گذاری در بیمه وابسته است به جداول بیمه‌ای که سابقه‌ای طولانی دارد ولیکن اینترنت پدیده‌ای نو است. از طرفی شرکت‌ها جزئیات پرونده‌ها را به علت مسائل امنیتی فاش

نمی‌کنند؛ لذا شرکت‌های بیمه برای بیمه‌های فضای مجازی معیارهای ارزش‌گذاری تعیین کرده‌اند. به همین دلیل، کمیت ریسک‌های فضای مجازی را که به نظر برخی غیر قابل اندازه‌گیری است، تعیین کرده‌اند. اگرچه هنوز این مسئله قابل بحث است که آیا این طرح‌های ارزش‌گذاری صحیح هستند یا خیر و حق بیمه مناسب برای این بیمه‌های جدید چقدر باید باشد.

۱-۶ نمونه‌های بیمه‌نامه فضای مجازی

برخی از نمونه‌های جدید بیمه‌نامه‌های اینترنت شامل نت ادونتج[۱] گروه بین‌المللی آمریکایی[۲]، بیمه‌نامه جامع الکترونیک لویدز لندن[۳]، بیمه‌نامه‌های اینشور تراست دات کام[۴]، جی. اچ. مارش و مک لنان[۵]، شروود[۶]، سی. ان. ای[۷] و زوریخ نورث آمریکا[۸] است. حق بیمه‌ها بسته به نوع پوشش و میزان آن از ۵۰۰۰ تا ۶۰۰۰ دلار برای یک میلیون دلار پوشش بیمه‌ای (از ۰/۵٪ تا ۰/۶٪) متغیر است.

از این‌گونه می‌توان نتیجه‌گیری کرد که بیمه‌نامه‌های جدید فضای مجازی در مقایسه با بیمه‌نامه‌های اولیه هکر، بسیار پیشرفته‌تر هستند. بر خلاف بیمه‌نامه‌های اولیه هکر که بر خسارات شخص اول تکیه می‌کرد، بیمه‌نامه‌های اینترنت جدید، هم خسارات اشخاص اول و هم خسارات اشخاص ثالث را پوشش می‌دهد؛ ضمن اینکه پوشش بالاتری را نیز ارائه می‌کند.

---

[1] Net Advantage
[2] American International Group (AIG)
[3] Lloyds of London’s e-Comprehensive
[4] InsureTrust.com
[5] J.H. Marsh & McLennan
[6] Sherwood
[7] CNA
[8] Zurich North America

جدول ۲. مقایسه انواع بیمه‌نامه‌های اینترنت در پوشش شخص اول و ثالث

پوشش	بیمه‌نامه نت‌ادونتج	بیمه‌نامه جامع الکترونیک	بیمه‌نامه وب‌نت
پوشش شخص اول			
تخریب دارایی‌های اطلاعاتی، ایجاد وقفه در ارائه آنها یا سرقت آنها	✓	✓	✓
توقف در کار اینترنت	✓	✓	✓
اخاذی اینترنتی	✓	✓	✓
اختلاس‌های الکترونیکی	خیر	✓	خیر
حملات DoS		✓	✓
پوشش شخص ثالث			
محتوای اینترنت	✓	✓	✓
امنیت اینترنت	✓	✓	✓
هزینه‌های دفاعی	✓	✓	✓

پوشش شخص اول نوعاً شامل تخریب یا وارد شدن خسارت به دارایی‌های اطلاعاتی، توقف در کار اینترنت، سرقت اینترنتی، خسارت ناشی از حملات DoS و حتی اختلاس‌های الکترونیکی است. پوشش شخص ثالث ادعاهای خسارتی مربوط به محتوای اینترنتی، امنیت اینترنتی، خطاها و اشکالات فناوری و همچنین هزینه‌های دفاعی را شامل می‌شود.

دیگر ویژگی برجسته بیمه‌نامه‌های جدید اینترنت این است که برای انواع مختلف مشتریان هدف، پوشش‌های محدودی دارند. یک دلیل این امر آن است که بیمه‌گران با تعریف پوشش محدود، می‌توانند ریسک حوادثی که از قبل قابل پیش‌بینی نیستند را مستثنی کنند. دلیل دیگر آن است که با تعریف محدود و مشخص پوشش بیمه‌ای، بیمه‌گران اینترنت می‌توانند بیمه‌نامه‌ها را متفاوت کنند و در نتیجه آن‌ها را به بازارهای خاص ارائه دهند. به عنوان مثال بیمه‌گران اینترنت، بیمه‌نامه‌هایی طراحی کرده‌اند که برای شرکت‌هایی است که نگران خسارت به سیستم‌های خودشان هستند؛ علاوه‌براین طراحی بیمه‌نامه برای شرکت‌هایی که فقط پوشش‌های مسئولیت شخص ثالث را می‌خواهند و همچنین طراحی بیمه‌نامه‌هایی برای پوشش مسئولیت وسایل ارتباط جمعی از جمله بیمه‌نامه‌های متفاوت و متنوعی است که در فضای مجازی ارائه شده است.

جدول ۳. بررسی و مقایسه محصولات شرکت

پوشش	محصولات (بیمه‌نامه‌های) AIG						
	نت ادونتج	نت ادونتج حرفه‌ای	نت ادونتج تجاری	نت ادونتج مسئولیت	نت ادونتج اموال	نت ادونتج امنیت	نت ادونتج کامل
مسئولیت امنیت شبکه			✓	✓		✓	✓
مسئولیت محتوای وب	✓	✓	✓	✓		✓	✓
مسئولیت حرفه‌ای اینترنت		✓		✓			✓
وقفه در شبکه					✓	✓	✓
پوشش برای دارایی‌های اطلاعاتی					✓	✓	✓
سرقت شناسه			✓	✓	✓	✓	✓
هزینه‌های مازاد					✓	✓	✓
اخاذی اینترنتی			✓	✓	✓	✓	✓
تروریسم اینترنتی	✓	✓	✓	✓	✓	✓	✓
جوایز کشف مجرمان					✓	✓	✓
هزینه‌های وارد‌شده به روابط اجتماعی بیمه‌گذار ناشی از حملات اینترنتی					✓	✓	✓
هزینه‌ها و جریمه‌های کیفری و تنبیهی	✓	✓	✓	✓		✓	✓
سرقت فیزیکی اطلاعات در سخت‌افزار/ میان‌افزار			✓	✓		✓	✓

جدول بالا به عنوان نمونه نشان می‌دهد که بیمه‌گران اینترنت چگونه برای به دست گرفتن بخش‌های مختلف بازار، با نیازهای بیمه‌ای متفاوت انواع مختلفی از بیمه‌نامه‌های اینترنتی را طراحی و ارائه می‌کنند.[1]

۱-۷ انواع بیمه‌های فضای مجازی (بر مبنای شخص اول و شخص ثالث)

به طور کلی منظور از بیمه‌های شخص اول کلیه بیمه‌هایی است که موضوع آن‌ها شخص بیمه‌گذار و اموال او می‌باشد؛ به عبارت دیگر شخص برای حفاظت خود از هر گونه خسارتی که مستقیماً به او وارد می‌گردد، خود را بیمه می‌کند، مانند خسارتی که ممکن است در اثر ویروس‌های اینترنتی به یکی از تأسیسات الکترونیکی شرکتی تجاری وارد آید؛ اما بیمه‌های شخص ثالث هرگونه خسارتی را که ممکن است شخصی به دیگری وارد کند، بیمه می‌کند، مانند نقض حق محرمانه بودن داده‌های دیگری یا افشای اطلاعات محرمانه متعلق به دیگری که در شبکه موجود است.[2]

۱-۷-۱ انواع بیمه‌های پوشش شخص اول

در این بخش کلیه بیمه‌نامه‌هایی که مخاطرات شخص اول در فضای مجازی را پوشش می‌دهند، ارائه شده است.[3]

---

[1] (American International Group, n.d.)
[2] (Third-Party vs. First-Party Cyber Risk Insurance: Protect Your IT Firm Right, 2013)
[3] (according to: Airmic Review of Recent Developments in the Cyber, 2013)

۱-۷-۲ بیمه مخاطرات اموال الکترونیکی

ورود خسارت به اموال الکترونیکی[1] یا برنامه‌های نرم‌افزاری خطری است که امروزه هر تجارتی در فضای مجازی را تهدید می‌کند. این نوع از بیمه‌ها معمولاً هزینه‌هایی را پوشش می‌دهد که بیمه‌گذار برای موضوع بیمه صرف کرده تا آن را به وضعیت پیش از خسارت برساند.

نقض امنیت داده می‌تواند خسارت‌های مختلفی را در پی داشته باشد. همچنین، عامل یا مسئول زیان امکان دارد متعهد به جبران انواع مختلفی از خسارت گردد که حسب مورد پیش آمده یا مطرح می‌شوند. خسارت مالی، خسارت به خرده‌فروشی، خسارت جانی، خسارت به خدمات، خسارت به مشتریان، زیان‌های صنعتی، فناوری، حمل و نقل، ارتباطات، آموزش و دارویی از جمله این موارد هستند. این خسارت‌ها ممکن است از بی‌احتیاطی (۳۹ درصد)، افعال مجرمانه یا مغرضانه (۳۷ درصد) یا مشکل در سامانه (۲۴ درصد) ناشی شوند.

به هر حال در پیش‌گرفتن «بیمه فضای مجازی» به عنوان یکی از رویکردهای اصلی سازمان و نهادینه کردن آن در حد مدیران عالی، یکی از رویکردهای ضروری برای مدیریت پایدار سازمان و پیشگیری از تحمیل همه خسارت‌ها به سازمان و وسیله‌ای برای انتقال ریسک به بیمه‌گر محسوب می‌شود.

۱-۷-۳ بیمه اختلال در کسب‌وکار

اختلال در کسب‌وکار حوادثی هستند که بیشتر موجب زیان‌های عدم‌النفعی، افزایش هزینه‌های عملکرد شرکت تجاری و افزایش هزینه‌های ناشی از اقدامات انجام گرفته جهت کاهش خسارت می‌گردد.

۱-۷-۴ بیمه اخاذی سایبری

این نوع از بیمه‌ها اصولاً آن دسته از اخاذی‌هایی را در بر می‌گیرد که دربردارنده هرگونه تهدید در فضای مجازی برای به دست آوردن پول مانند تهدید به صدمه زدن به شبکه، محدود کردن شبکه یا انتشار اطلاعات برگرفته از شبکه است.

۱-۷-۵ بیمه خسارت به اعتبار تجاری

خسارت به اعتبار تجاری[2] کلیه زیان‌های مربوط به اموال معنوی، ضرر درآمدی، از دست دادن مشتری (بازار) یا افزایش هزینه عملکرد را در بر می‌گیرد. نقض حفاظت داده‌ای و به دنبال آن گزارش اطلاعات به‌دست آمده ناشی از این نقض (ولو اطلاعات غلط) متداول‌ترین نوع افعالی است که تحت پوشش قرار گرفتن این نوع بیمه را ایجاب می‌کند.

---

[1] Digital assets
[2] Reputational damage

۱-۷-۶ بیمه دزدی پول و اموال تجاری

این نوع بیمه شخص اول به از دست دادن مستقیم پول و اختلالی که در پی آن در تجارت ایجاد می‌شود، مربوط است که ممکن است ناشی از دزدیده شدن تجهیزات رایانه‌ای، دزدی الکترونیکی صندوق مالی یا پول از طریق هک و سایر جرائم فضای مجازی باشد.

۱-۷-۷ انواع بیمه‌های پوشش شخص ثالث

بیمه‌نامه‌های متنوعی وجود دارند که مخاطرات شخص ثالث را تحت شرایطی بیمه می‌کنند که در این بخش به صورت مختصر به عمده این مخاطرات و بیمه‌نامه‌ها اشاره می‌گردد.[1]

۱-۷-۸ بیمه نقض امنیت و محرمانگی

بیمه‌نامه‌های تعبیه شده برای این بخش به طور عمده هزینه‌های ناشی از بازرسی، دفاع (از اطلاعات و سیستم) و جبران خسارات مدنی را در بر می‌گیرد.

۱-۷-۹ بیمه مسئولیت رسانه‌ای

این نوع بیمه خسارات و هزینه‌هایی را که در اثر افترا، نقض محرمانگی و بی مبالاتی در انتشار هرگونه محتوا در قالب الکترونیکی یا رسانه‌ای و تجاوز به حقوق مربوط به مالکیت فکری شخص ثالث ایجاد می‌شود، تحت پوشش قرار می‌دهد.

۱-۷-۱۰ بیمه اتلاف داده شخص ثالث

بیمه اتلاف داده، مسئولیت از بین بردن و غیرقابل استفاده کردن داده‌های شخص ثالث مانند اطلاعات مربوط به پرداخت خسارت به مشتریان برای عدم اجازه ورود[2]، عدم کارکرد نرم‌افزاری و سیستم امنیتی و ... را شامل می‌شود.

۱-۷-۱۱ بیمه هزینه‌های آگهی به مشتری

حوزه عملکرد این بیمه عبارت است از هزینه‌های قانونی، پستی و تبلیغاتی در مواقعی که الزام قانونی وجود دارد یا در مواردی که نیاز به انجام اقدامات تنظیمی ایجاب می‌کند که به اشخاص اطلاع داده شود نقض امنیتی یا محرمانگی رخ داده است.

۱-۷-۱۲ بیمه مسئولیت در قبال شخص ثالث به دلیل ارسال ایمیل یا پیامک

در صورتی که ایمیل یا پیامک حاوی ویروس یا محتوای غیراخلاقی باشد، حسب مورد می‌تواند مسئولیت فرستنده یا رسا (واسطه) را در پی داشته باشد. این مسئولیت را در صورتی که ناشی از فعل عامدانه نباشد، می‌توان تحت پوشش بیمه قرار داد.

---

[1] (According to: Airmic Review of Recent Developments in the Cyber, 2013)
[2] Denial of access

۱-۷-۱۳ بیمه رمزگیری (فیشینگ)[1]

رمزگیری یا فیشینگ، کنایه از ماهیگیری[2] است که در آن، شکارچی قلاب یا تور خود را در محیط‌هایی که طعمه‌های فراوانی برای صید وجود دارد، (از جمله در فضای مجازی که استانداردهای ایمنی به درستی مراعات نشده باشد یا مشتری برای یک لحظه بی‌احتیاطی کند) پهن می‌کند. در این روش، با ادعای قانونی بودن شرکت یا مؤسسه، از طرق مختلف از جمله نامه الکترونیکی از افراد خواسته می‌شود که شماره کارت اعتباری یا سایر اطلاعات شخصی خود را ارائه نمایند. با توجه به جعلی بودن عنوان و پایگاه اینترنتی مورد استفاده، بزهکاران حرفه‌ای از رمزگیری به عنوان مقدمه‌ای برای تحصیل وجه متعلق به دیگری استفاده می‌کنند.

رمزگیری، در صورتی که تنها با هدف جرائم مالی انجام گیرد، بزهی خاص به شمار می‌آید که نمی‌توان معادل دقیقی در قوانین موضوعه کشورمان برای آن یافت. فعل انجام یافته، در صورتی که منجر به بردن مال شود، کلاه‌برداری یا در حکم آن خواهد بود. با این همه به نظر نمی‌رسد که کلاه‌برداری یا جرایمی همچون سرقت، برای توصیف این جرم کفایت کند. چرا که انجام رمزگیری مستلزم مقدماتی همچون ایجاد پایگاه اینترنتی موهوم یا استفاده از پایگاه موجود است که خود می‌تواند عنوان مجرمانه مستقلی داشته باشد.

۱-۷-۱۴ بیمه مسئولیت عمدی

این نوع بیمه‌نامه پوشش‌دهنده تمام خسارات جانی و مالی ناشی از تصادف است و همچنین تمام خساراتی را که به صورت نوعی از طریق تعرض به حق کپی‌رایت، بازداشت غیر قانونی، سرقت ادبی، تعرض به حریم خصوصی، افترا در تبلیغات و ... وارد می‌شود را تحت پوشش قرارمی‌دهد.

۱-۷-۱۵ بیمه مسئولیت خطای فنی و بی مبالاتی

بیمه‌نامه مسئولیت خطای فنی و بی مبالاتی - همانطور که از نام آن پیداست- خسارات ناشی از بی‌توجهی را پوشش می‌دهد. این بیمه به عنوان نمونه برخی از مسئولیت‌های قراردادی مانند نقض حق نمایندگی و تضمینات قرارداد حرفه‌ای خدمات و همچنین برخی از موضوعات امنیتی و خصوصی که از قواعد قراردادهای خدمات حرفه‌ای ناشی می‌شود را تحت پوشش قرارمی‌دهد.

---

[1] phishing
[2] fishing

۱-۸ بیمه فضای مجازی برای فین‌تک[1]

فضای مجازی از ابزارهایی تشکیل شده است که هرکدام مخاطراتی دارند و باید تحت پوشش بیمه قرار بگیرند. یکی از مهمترین این ابزارها فین‌تک است که برای تحقق اهداف خود، راه‌حل‌هایی دارد و این راه‌حل‌ها در این بخش، مورد مطالعه قرار گرفته است؛ اما قبل از بررسی مخاطرات فین‌تک، لازم است تا این ابزار تعریف گردیده و مفاهیم مربوط به آن تبیین گردد. لذا ابتدا تعریف، دسته‌بندی و اهمیت بیمه برای فین‌تک‌ها بیان گردیده و سپس خطرات موجود در ابزارهای فین‌تک ارائه می‌شود.

نکته حائز اهمیت دیگر که باید به آن توجه نمود این است که وقتی از فین‌تک صحبت می‌شود، باید بین آن و اینشورتک[2] تفکیک نمود. همانطور که در ادامه (در بخش ۱-۸-۱) بیان می‌شود، فین‌تک فناوری‌های مالی صنعتی در فضای اقتصادی است که خدمات مالی را کارآمدتر می‌کند. ولی مراد از اینشورتک مجموعه اقداماتی است که به کمک فناوری در یافتن میزان ریسک افراد کمک می‌کند. برای مثال وقتی بدانیم یک راننده کم ریسک است، باید حق بیمه کمتری پرداخت کند. در این گزارش تنها به بررسی فین‌تک پرداخته شده است و بررسی اینشورتک مجال دیگری می‌طلبد.

۱-۸-۱ تعریف فین‌تک

فین‌تک یا فناوری‌های مالی[3]، صنعتی در فضای اقتصادی است که به شرکت‌هایی اشاره دارد که با کاربرد فناوری تلاش می‌کنند خدمات مالی را کارآمدتر کنند. این شرکت‌ها در ارائه خدمات مالی به مشتری، از به‌روزترین فناوری‌ها استفاده می‌کنند و با توجه به کم‌هزینه‌تر بودن، سرعت بالا در ارائه خدمات و راحتی استفاده، دست مؤسسات مالی سنتی مثل بانک‌ها را از این‌گونه فعالیت‌ها قطع کرده‌اند. عبارت «فناوری امور مالی» از اوایل قرن جدید، در مورد خلاقیت‌های فناورانه که در زمینه ادبیات مالی، بانکداری خرد، سرمایه‌گذاری و حتی پول‌های رمزی مثل بیت‌کوین[4] صورت می‌گیرند، مورد استفاده قرار گرفته است.

از زمان انقلاب اینترنت[5] و انقلاب اینترنت موبایل، فین‌تک‌ها به‌سرعت رشد کرده‌اند. فین‌تک‌ها که اغلب در قالب استارتاپ[6] ظهور پیدا کرده‌اند، هزینه‌ها را کاهش داده و به جایگزینی برای خدمات مؤسسات مالی سنتی تبدیل شده‌اند. به عنوان نمونه نرم‌افزار موبایلی که فین‌تک رابین‌هود[7] برای مبادلات سهام در اختیار مشتریان قرار می‌دهد، رایگان است. همچنین سایت‌های فین‌تک پراسپر[8] و لندینگ کلاب[9] که امکان

---

[1] Fintech
[2] Insurtech
[3] Financial Technology
[4] bitcoin
[5] internet revolution
[6] Startup
[7] Robinhood
[8] Prosper
[9] Lending Club

قرض‌دهی نظیر به نظیر (P2P)[1] را فراهم کرده‌اند، از طریق ایجاد رقابت میان قرض‌دهندگان و قرض‌گیرندگان، نرخ‌های بهره را کاهش داده‌اند.

احتمالاً بسیاری از مردم کشور، حتی نام فین‌تک را نیز تاکنون نشنیده‌اند؛ نامی که تا سال‌های آینده مرزهای ارائه خدمات مالی را جابه‌جا خواهد کرد و تا به امروز نیز، در این کار موفق بوده است. لذا به نظر می‌رسد رشد روزافزون فین‌تک‌ها، آشنایی با چگونگی عملکرد آن‌ها را برای به‌روز ماندن الزامی کرده است؛ بنابراین در ادامه نکات مربوط به شناسایی ضعف‌ها و مشکلات این حوزه و همچنین شناسایی و معرفی اختلالات امنیتی آن مورد بررسی قرار گرفته است.

۱-۸-۲ دسته‌بندی فین‌تک

قبل از بررسی دسته‌بندی مربوط به فین‌تک باید به این نکته نمود که تأکید تشریحات در این حوزه‌ها بیشتر روی چالش‌ها، مسائل امنیتی و نواقصی است که این حوزه‌ها منشأ آن هستند و یا از آن‌ها تأثیر می‌گیرند؛ بنابراین سعی شده است توضیحاتی راجع به هرکدام از موارد فوق و مشکلات موجود ارائه شده و چگونگی رفع این نواقص از طریق پوشش بیمه بیان گردد.

اما قبل از بحث راجع به حوزه‌های فین‌تک باید اذعان نمود که ارتباط بیمه با بحث فین‌تک ارتباطی دوطرفه است؛ یعنی هم شرکت‌های بیمه می‌توانند از فین‌تک استفاده کنند و کیفیت فعالیت‌های خود را ارتقا دهند و هم بیمه می‌تواند با پوشش ریسک‌های ناشی از فین‌تک به فراگیر شدن آن و همچنین گسترش آن کمک کند.

همانگونه که بیان شد، فین‌تک اشاره‌ای است به اپلیکیشن‌ها، فرایندها، محصولات و مدل‌های کسب‌وکار جدید در صنعت خدمات مالی که با توجه به این مسئله، **راه‌حل‌ها به ۵ حوزه قابل تقسیم است:**

- بخش بانکداری یا بیمه که به عنوان بخش‌های بالقوه کسب‌وکار شناخته می‌شوند. راه‌حل‌هایی که برای صنعت بیمه هستند اغلب اینشورتک[2] خوانده می‌شوند.
- راه‌حل‌هایی که به فرایندهای پشتیبانی از کسب‌وکارها اشاره دارند مانند اطلاعات مالی، پرداخت‌ها، سرمایه‌گذاری، تأمین مالی، مشاوره و فرایندهای حمایت متقابل. یک مثال راه‌حل‌های پرداخت موبایلی یا همراه است.
- سومین دسته آن‌هایی هستند که با تمرکز بر بخشی از مشتریان در حوزه‌هایی مانند بانکداری خرد، بانکداری اختصاصی و بانکداری شرکتی و همین‌طور بیمه‌های عمر و غیر آن مشخص می‌شوند. یک مثال بیمه‌هایی هستند که کارمزد و هزینه بیمه‌هایی غیر از بیمه‌های زندگی را از طریق رفتار مشتری محاسبه می‌کنند.

---

[1] Peer to peer
[2] InsurTech

- چهارم، فرم تعاملی کسب‌وکار با کسب‌وکار[1]، کسب‌وکار با فرد[2]، مشتری با مشتری[3] است. به عنوان مثال راه‌حل‌های تجارت اجتماعی سی.تو. سی[4] در این بخش قرار می‌گیرند.
- در نهایت راه‌حل‌هایی هستند که با توجه به موقعیت بازارشان گستره وسیعی را شامل می‌شوند؛ مانند سیستم‌های خدماتی مدیریت مالی شخص[5] و راه‌حل‌های قرض‌دهی نفر به نفر[6].

سرمایه‌گذاری در فین‌تک که در سال ۲۰۰۸ حدود ۹۳۰ میلیون دلار بوده ۱۲ برابر شده و در سال ۲۰۱۴ به بیش از ۱۲ میلیارد دلار رسیده است. آنگونه که شهرداری لندن می‌گوید صنعت نوپای فناوری‌های مالی در سال‌های گذشته شاهد رشد سریعی بوده است. ۴۰ درصد از نیروی کار شهر لندن در بخش‌های خدمات مالی و فناوری کار می‌کنند. برخی از شرکت‌های شناخته شده فین‌تک مانند دایره مالی[7]، جوز هندی[8] و انتقال هوشمندانه[9] در لندن فعالیت می‌کنند. در ایالات متحده آمریکا نیز استارتاپ‌های فین‌تک متعددی مانند تأیید[10]، برتری[11]، آی.ای.اکس[12]، دارنده[13]، از سوی[14]، باشگاه وام[15]، پول خالص[16]، مربع[17]، راه راه[18]، سوفی[19]، رابین هود[20]، پلیدی[21] و ثروتمندانه[22] فعالیت می‌کنند[23].

در اروپا حدود ۱/۵ میلیارد دلار در شرکت‌های فین‌تک در سال ۲۰۱۴ سرمایه‌گذاری شده است که سهم شرکت‌های حاضر در لندن ۵۳۹ میلیون دلار، آمستردام ۳۰۶ میلیون دلار و استکهلم ۲۶۶ میلیون دلار بوده است. در واقع بعد از لندن، استکهلم دومین شهر اروپا است که بیشترین سرمایه‌ها را در ۱۰ سال گذشته جذب کرده است. معاملات اروپایی‌ها در فین‌تک در ۵ فصل متوالی روبه افزایش بوده است و از ۳۷ مورد در فصل چهارم ۲۰۱۵ به ۴۷ مورد در فصل اول ۲۰۱۶ رسیده است.

---

[1] B2B
[2] B2C
[3] C2C
[4] C2C
[5] PFM
[6] peer-to-peer lending
[7] Funding Circle
[8] Nutmeg
[9] TransferWise
[10] Affirm
[11] Betterment
[12] IEX
[13] Fundera
[14] Behalf
[15] Lending Club
[16] Money.net
[17] Square
[18] Stripe
[19] SoFi
[20] Robinhood
[21] Plaid
[22] Wealthfront
[23] (accenture, 2016)

در آسیا و اقیانوسیه، هاب جدیدی برای فناوری‌های مالی در استرالیا از آوریل ۲۰۱۵ شروع به فعالیت کرده است. در حال حاضر بازیگران قوی در صنعت فین‌تک مانند پرداخت‌های تایرو[1]، رشد بی‌صدا[2] و نقطه بورس[3] فعالیت می‌کنند و هاب جدید، شتاب رشد در این منطقه را بیشتر خواهد کرد. یک آزمایشگاه نوآوری در فناوری‌های مالی[4] نیز در هنگ‌کنگ راه‌اندازی شده است که روند نوآوری در خدمات مالی به کمک فناوری را تقویت خواهد کرد. شرکت قابل ذکر دیگر وی.مانی[5] است که در فیلیپین فعالیت می‌کند.

در فوریه ۲۰۱۶ گزارشی توسط موسسه حسابداری ارنست‌اند یانگ[6] به سفارش خزانه علیاحضرت یا خزانه وزارت دولت بریتانیا[7] منتشر شد که هفت هاب پیش‌روی فین‌تک را مقایسه کرده است. این گزارش کالیفرنیا را از منظر استعدادها و سرمایه، بریتانیا را از منظر سیاست دولتی و نیویورک را از منظر تقاضا در جایگاه برتر قرار داده است.

طبق بررسی‌های صورت گرفته در دسامبر ۲۰۱۵، نقش فین‌تک در افزایش رضایت مصرف‌کنندگان در صنعت مالی حدود ۸ درصد بیشتر از بانکداری بوده است. در بخش مشاوره مالی شرکت مانند سرمایه گذاری وفادارانه[8] اخیراً با استارتاپی مانند مشاور آینده[9] شروع به مشورت کرده است که اجازه ورود فناوری به متولیان برجسته را می‌دهد. چهره‌های شناخته‌شده‌ای مانند اسنیپ داگ[10]، جرد لتو[11] و ناس[12] اخیراً منابع‌شان را متوجه استارتاپ‌های نوپای فین‌تک کرده‌اند که مثلاً می‌توان به سرمایه‌گذاری این چند نفر در استارتاپ رابین هود[13] اشاره کرد.

امور مالی یکی از صنایعی است که پیشگام تخریب توسط نرم‌افزارها قرار گرفته چون خدمات مالی مانند انتشارات بیشتر از بیت‌ها درست شده تا محصولات قابل لمس.

۱-۸-۳اهمیت بیمه برای فین‌تک‌ها

به نظر می‌رسد امروزه که رگولاتوری سپری برای خدمات مالی بوده و ترکیدن حباب دات‌کام[14] تاثیری بر آن‌ها نگذاشته است، بانک‌های جهان از موج جدید استارتاپ‌ها ناراضی باشند؛ با این حال اجرای تهاجمی محرمانگی فعالیت‌های بانکی و رگولاتوری انتقال پول، تهدیدی برای شرکت‌های فین‌تک به نظر می‌رسد. علاوه بر شرکت‌های سنتی، شرکت‌های فین‌تک اغلب با دیده شک و تردید از سوی رگولاتورهای مالی دیده

---

[1] Tyro Payments
[2] QuietGrowth
[3] Stockspot
[4] Financial technology innovation lab
[5] VMoney
[6] Ernst & Young
[7] HM Treasury
[8] Fidelity Investments
[9] FutureAdvisor
[10] Snoop Dogg
[11] Jared Leto
[12] Nas
[13] Robinhood
[14] Dot-com bubble

می‌شوند. امنیت داده‌ها یکی دیگر از مسائل رگولاتورها است که به دلیل تهدید هک، آن‌ها را نگران می‌کند که لازم است داده‌های مشتریان و شرکت‌های حساس به خوبی حفاظت شود.

هرگونه رخنه اطلاعاتی، هرچند کوچک می‌تواند خوشنامی شرکت‌های فین‌تک را تهدید کند. بخش‌های آنلاین مالی یکی از اهداف حملات دی. دی. اُ. اس[1] هم هست. بازاریابی یکی دیگر از تهدیدهای شرکت‌های فین‌تک است که معمولاً می‌خواهند با رقبایی بزرگ‌تر از خودشان رقابت کنند. البته این تهدیدها زمانی که بانک‌ها می‌خواستند برای اولین بار به مشتریان‌شان خدمات آنلاین ارائه کنند هم وجود داشت.

در واقع در همین نقطه است که نقش صنعت بیمه پررنگ‌تر خواهد شد. اگر یک حمله سایبری صورت گیرد و بخش زیادی از اطلاعات شرکت‌های فعال در حوزه فین‌تک به سرقت رود، مطمئناً ضربه سنگینی به روند رشد این حوزه وارد خواهد شد و اعتماد زیادی از مردم سلب می‌شود که نتیجه آن خسارت‌های بزرگی برای این شرکت‌های مالی به بار خواهد آورد.

لذا ظهور نقش بیمه در چنین مواقعی است که می‌تواند با نظارت خود امنیت سیستم‌های شرکت‌های فین‌تک را افزایش دهد و علاوه‌براین از طریق پرداخت خسارت و پوشش ریسک، این شرکت‌ها را برای انجام سرمایه‌گذاری‌های بیشتر حمایت کرده و فضای کسب‌وکار پر ریسک در این حوزه را تلطیف نماید. حوزه فین‌تک برای رشد و گسترش خدمات، افزایش سرعت امور و بهبود رضایت مشتریان از ابزارهای ذیل استفاده می‌کند:

- ✓ کلان داده[2]
- ✓ اینترنت اشیا[3]
- ✓ رایانش ابری[4]
- ✓ واقعیت افزوده[5]
- ✓ واقعیت مجازی[6]
- ✓ هوش مصنوعی[7]

استفاده از این ابزارها باعث می‌شود که میزان ریسک موجود در پروژه‌ها افزایش چشمگیری داشته باشد، با این وجود با توجه به کارایی و اثرگذاری آن‌ها نمی‌توان به هیچ صورت از استفاده این ابزارها چشم‌پوشی کرد.

---

[1] DDOS
[2] Big Data
[3] Internet of Things-IOT
[4] Cloud Computing
[5] Augmented Reality
[6] virtual reality
[7] Artificial intelligence

۱-۸-۴ مخاطرات موجود در ابزارهای فین‌تک

در این بخش به تبیین مخاطراتی که استفاده از هر یک ابزارهای حوزه فین‌تک می‌تواند به دنبال داشته باشد، پرداخته می‌شود:

۱-۴-۸-۱کلان داده

از جمله مخاطرات ابزار کلان داده می‌توان به موارد ذیل اشاره نمود:

- ✓ انتقال و حفظ امنیت داده‌ها
- ✓ فناوری نگهداری داده‌های خصوصی کاربران
- ✓ شفافیت داده‌ها
- ✓ صحت و اعتبار داده
- ✓ تعیین معیار عملکرد
- ✓ داده و قابلیت همکاری سیستم

موارد فوق در بخش‌های بعد به صورت دقیق همراه با ابزارهای دیگر و همچنین برشمردن مشکلات و ریسک‌های فضای مجازی تشریح خواهد شد.

۲-۴-۸-۱اینترنت اشیا

- ✓ فرسودن و کم کردن کنترل مردم بر زندگی
- ✓ حریم خصوصی کاربران
- ✓ امنیت داده
- ✓ اطلاعات داده
- ✓ تغییر اجتماع

طی پنج تا ده سال آینده، صنعت بانکداری شاهد تغییرات زیادی با ورود فناوری اینترنت اشیا[1] خواهد بود که بانک‌ها را با چالش‌های امنیتی جدید مواجه می‌کند. لذا وجود اطمینان از امن بودن تمام تجربیات بانکی آنلاین به‌طور فزاینده‌ای برای جلب اعتماد مشتری و کاهش نگرانی مشتریان در خصوص هک شدن داده‌های بانکداری شخصی و کسب‌وکار اهمیت می‌یابد.

داده‌های حساس مشتری از پیشینه مالی گرفته تا پیشینه مکانی وی، چه در جایی ذخیره شوند و چه روی شبکه قرار گیرند، هدف بالقوه تهدیدات امنیت داده‌ها هستند. داده‌ها چه روی یک دستگاه نگهداری شوند، چه روی شبکه از بانک به خودروی هوشمند مشتری منتقل شوند، باید به‌درستی ایمن شوند.

لذا به کار بستن اقدامات امنیتی مانند رمزنگاری برای حفاظت از اطلاعات و ابزار احراز هویت برای اجازه دسترسی به افراد مجاز، حیاتی است. در این رابطه استفاده از داده‌های بیومتریک مانند اثر انگشت،

---

[1] IOT: Internet of Things

نرم‌افزار تشخیص صدا و اسکن عنبیه برای اثبات هویت مشتری در حال گسترش است. در واقع به کمک فراوانی دستگاه‌های اینترنت اشیا بانک‌ها جزئیات بسیار بیشتر و تصویر دقیق‌تر و مفیدتری از مشتری خواهند داشت که در نتیجه آن، نیاز به افزودن لایه‌های امنیتی بیشتر برای همه اکوسیستم اینترنت اشیا (از دستگاه‌های متصل به شبکه تا فضای ابری) دارند.

در این شرایط مجرمان سایبری فرصت‌های بیشتری برای حرکات پنهانی و یا هک شبکه دارند، زیرا نقاط بیشتری برای ورود و اتصال دستگاه‌ها به شبکه وجود دارد. لذا برای آن‌که بانک‌ها کاملاً فناوری اینترنت اشیا را بپذیرند، باید برای ایجاد و ماندگاری اعتماد مشتری، امنیت را از ابتدا و در همه لایه‌ها بازسازی کنند (راه پرداخت, ۲۰۱۷).

۳-۴-۸-۱رایانش ابری

معماری امنیت ابری، فقط در صورتی کارا است که پیاده‌سازی‌های دفاعی صحیح وجود داشته و مسائل امنیتی در سطح مدیریتی را شناسایی کند. برای شناسایی این مسائل نیاز است تا کنترل‌هایی در هر یک از مراحل به کار بسته شود تا به شناخت دقیق از مشکلات منتهی گردیده و راه‌حل برطرف‌سازی آن‌ها مشخص شود. این مراحل عبارتند از: کنترل‌های بازدارنده، کنترل‌های پیش‌گیرنده، کنترل‌های تصحیح کننده و کنترل‌های شناسایی‌کننده.

- ✓ **کنترل‌های بازدارنده**

  این کنترل‌ها به منظور جلوگیری از هر نوع حمله عمدی در یک سیستم محاسبات ابری تنظیم شده است. این کنترل‌ها، باعث کاهش آسیب‌پذیری واقعی یک سیستم نمی‌شوند.

- ✓ **کنترل‌های پیش‌گیرنده**

  این کنترل‌ها به کمک مدیریت آسیب‌پذیری‌ها سبب افزایش قدرت سیستم می‌شوند. کنترل پیش‌گیرنده، از آسیب‌پذیری سیستم محافظت خواهد کرد؛ به نحوی که اگر یک حمله اتفاق بیفتد، بعد از آن این نوع از کنترل‌ها سعی در پوشش حمله و کاهش خرابی امنیت سیستم می‌کند.

- ✓ **کنترل‌های تصحیح‌کننده**

  این کنترل سعی در کاهش اثر حمله دارد. برخلاف کنترل پیش‌گیرنده، کنترل تصحیح‌کننده حین وقوع حمله، عکس‌العمل نشان می‌دهد.

- ✓ **کنترل‌های شناسایی‌کننده**

  این نوع از کنترل سعی در شناسایی حمله حین وقوع آن دارد. در زمان رخداد حمله، کنترل شناسایی‌کننده، سیگنالی برای کنترل‌های پیش‌گیرنده یا تصحیح‌کننده برای مشخص کردن مشکل ارسال می‌کند.

اما در رابطه با مخاطرات امنیتی موجود در رایانش ابری باید گفت که این مشکلات عمدتاً شامل موارد زیر می‌شود که نیاز روزافزون به مشارکت صنعت بیمه را گوشزد می‌نماید.

- ✓ **سرقت اطلاعات**

اگر پایگاه داده چند مستأجری[1] در این معماری ساسز[2] برای سرویس‌های ابر اطلاعاتی[3] شناخته باشیم در نتیجه یک نسخه از نرم‌افزار را بر روی پایگاه داده اجرا می‌کند و از طریق وب به تعداد زیادی از کاربران دسترسی می‌دهد. به همین دلیل نفوذ به یکی از برنامه‌های کلاینت‌ها می‌تواند به مهاجم اجازه دهد که علاوه بر اطلاعات همان کلاینت به اطلاعات کلاینت‌های دیگر دسترسی پیدا کند.

- ✓ **از دست دادن اطلاعات**

اطلاعاتی که در فضاهای ابری نگهداری می‌شوند به دلایلی غیر از هک شدن هم می‌توانند پاک شوند. تا زمانی که شرکت ارائه‌دهنده ابری از اطلاعات بک آپ نگیرد، دلایل زیادی می‌تواند به حذف دائمی اطلاعات منجر شود (مانند پاک کردن تصادفی اطلاعات توسط شرکت ارائه‌دهنده ابر اطلاعات و حوادثی مانند آتش‌سوزی و زمین لرزه). اگر یک مشتری اطلاعاتش را قبل از آپلود روی ابر اطلاعات رمزگذاری کند و سپس کلید رمزنگاری را گم کند، اطلاعاتش را هم از دست می‌دهد.

- ✓ **سرقت اکانت**

در سال ۸۸ هکرها تعداد زیادی از سیستم‌های آمازون را هک کردند و با استفاده از آن‌ها تروجان زئوس[4] را اجرا کردند. در فروردین ماه سال ۸۹ نیز یک حمله از نوع اسکریپت متقابل سایت[5] یا اکس. اس.اس[6] به سایت آمازون صورت گرفت. منشأ این حمله یک باگ در سیستم بود که باعث شد هکرها بتوانند اطلاعات هویتی را از سایت به سرقت ببرند.

- ✓ **رابط‌های کاربری یا ای.پی.آی[7] های ناامن**

تأمین اطلاعات، مدیریت، هماهنگی و نظارت بر اطلاعات از طریق این رابط‌های کاربری انجام می‌شود. از احراز هویت و کنترل دسترسی‌ها گرفته تا رمزنگاری و نظارت بر فعالیت‌ها برعهده ای.پی.آی است. در نتیجه‌ای.پی.آی باید در برابر تلاش‌های تصادفی و یا بدخواهانه برای دور زدن رابط کاربری آماده باشد.

- ✓ **حملات مانع سرویس‌دهی[8]**

به حملاتی گفته می‌شود که در آن کاربران سرویس ابر اطلاعات نمی‌توانند به اطلاعات و یا برنامه‌هایشان دسترسی پیدا کنند. در این حمله سرویس قربانی دچار کمبود منابع سیستمی

---

[1] Multi-tenant database
[2] SaaS
[3] cloud
[4] Zeus
[5] Cross-Site Scripting
[6] XSS
[7] API
[8] Denial of Service

(مانند قدرت پردازشی، حافظه و پهنای باند) می‌شود. مهاجمین در حملات توزیع انکار سرویس[1] سرعت سیستم را تا جایی که امکان دارد پایین می‌آورند و کاربران سرویس را به دلیل عدم پاسخگویی سرویس ناراحت می‌کنند.

- ✓ **همکار خیانت کار**

همکار خیانت کار در یک سازمان کسی است که در حال حاضر یا در گذشته کارمند، پیمانکار یا شریک تجاری سازمان بوده و اجازه دسترسی به شبکه، سیستم یا اطلاعات داشته و از روی عمد از این دسترسی سوء استفاده کرده است، به طوری که روی اطلاعات محرمانه، صحت اطلاعات و اطلاعات سیستم تأثیر گذاشته است.

- ✓ **سوء استفاده از سرویس ابر اطلاعاتی**

یکی از بهترین مزایای پردازش ابری[2] این است که با استفاده از آن سازمان‌های کوچک می‌توانند از مقادیر زیادی از پردازش و حافظه استفاده کنند. برای بسیاری از سازمان‌ها تهیه هزاران سرور مشکل است، اما اجاره همین هزاران سرور امکان‌پذیر است. ممکن است برای هکر شکستن یک کلید رمزنگاری شده با سیستم ضعیفی که دارد چندین سال طول بکشد؛ اما همین هکر اگر به تعداد زیادی از سرورهای ابر اطلاعاتی دسترسی داشته باشد، با استفاده از قدرت پردازشی این سرویس‌ها می‌تواند همان کلید را در عرض چند دقیقه کرک کند. سپس او می‌تواند با استفاده از سرورهای ابر اطلاعاتی یک حمله دی. دی. اُ. اس[3] را پیاده کرده و بدافزارها را گسترش دهد.

- ✓ **کم بودن درجه دیجیتالی شدن**

مزایایی که پردازش ابری دارد (مانند کاهش هزینه‌ها، بهبود امنیت و تاثیرگذاری مثبت بر عملکردها)، بسیاری از سازمان‌ها را به سمت خود می‌کشاند. در این شرایط بسیاری از سازمان‌هایی که منابع کافی دارند به سمت فناوری‌های ابر اطلاعاتی می‌روند، اما مشکل اینجاست که بسیاری از آن‌ها دید کاملی نسبت به این فناوری ندارند.

اگر سازمان‌ها راجع به ارائه‌دهندگان ابر اطلاعات، برنامه‌ها یا سرویس‌هایی که در ابر اطلاعات کار می‌کنند و کارهایی که باید در زمان اجرای ابر اطلاعات انجام شوند، دانش کافی نداشته باشند، دچار ریسک‌های شدیدی می‌شوند که حتی قابل اندازه‌گیری نیست و ممکن است از بسیاری از تهدیدهای رایج خطرناک‌تر باشد.

- ✓ **آسیب‌پذیری فناوری‌های به اشتراک گذاشته شده**

ارائه‌دهندگان سرویس‌های ابر اطلاعات خدماتشان را در سطح مشخصی از زیرساخت‌ها، پلتفرم‌ها و برنامه‌ها ارائه می‌دهند که آسیب‌پذیری را در همه سطوح فوق می‌توان مشاهده نمود.

---

[1] Distributed Denial of Service
[2] Cloud Computing
[3] DDOS

در واقع از هر مدلی که استفاده شود[1]، ریسک و تهدید فناوری‌های به اشتراک گذاشته شده وجود دارد. برای مقابله با این تهدیدها باید استراتژی قوی در نظر گرفت که شامل پردازش، حافظه، شبکه، امنیت برنامه و کاربران و کنترل عملیات‌ها باشد (انجمن تخصصی فناوری اطلاعات ایران).

۴-۴-۸-۱ واقعیت مجازی و واقعیت افزوده

- ✓ **شکستن حریم مکانی با جی.پی.اس**

از آنجا که به راحتی می‌توان هنگام استفاده از برنامه‌ای با قابلیت‌های واقعیت افزوده و واقعیت مجازی، مختصات و مشخصات کاربر را جمع‌آوری کرد، در نتیجه ظرف مدت خاصی تمام اطلاعات مکان‌های پر رفت و آمد و همین طور مکان‌های شخصی و محبوب کاربران در اختیار سرور شرکت ارائه‌دهنده خدمات قرار می‌گیرد.

- ✓ **مشکلات امنیتی ناشی از جی.پی.اس**

یکی دیگر از مسائل این است که شرکت‌های ارائه‌دهنده این خدمات قادر خواهند بود تا به محض استفاده کاربران از این قابلیت، به صورت نامحسوس اطلاعات مکانی سازمان‌ها و مقرهای امنیتی و نظامی را در اختیار خود بگیرند. این مسئله بسیار راحت است و کافی است که شرکت مدنظر یک بازی مانند بازی پوکمون‌گو[2] را ارائه دهد و برای طی کردن مراحل مختلف، اجبارهایی را برای سپری کردن و همین‌طور سر زدن به یکسری مناطق خاص به کاربر تحمیل کند. در اینصورت کاربر بدون اینکه بداند آن منطقه یک منطقه نظامی و یا امنیتی است، به راحتی مشخصات و اطلاعات آن را در اختیار یک شرکت و یا کشور بیگانه قرار می‌دهد.

- ✓ **امنیت اطلاعات خصوصی در ایمیل‌ها و حساب‌های کاربری گوگل**

اولین و مهمترین خطری که کاربران بازی‌های رایانه‌ای را تهدید می‌کند، اطلاعات خصوصی این کاربران در سرویس گوگل است، زیرا به عنوان نمونه برای اجرای بازی پوکمون‌گو می‌توان علاوه بر ثبت‌نام در سایت بازی، از حساب کاربری گوگل استفاده کرد که استفاده از این حساب کاربری، مجوز لازم برای دسترسی به ایمیل‌ها، عکس‌های ذخیره شده در سرویس گوگل، اسناد ذخیره شده در گوگل درایو و ... را در اختیار توسعه‌دهندگان بازی قرار داده و علاوه بر آن، هکرها نیز با نفوذ به دستگاه کاربران یا نفوذ به این بازی می‌توانند به همه این اطلاعات دسترسی یابند.

- ✓ **جاسوسی کامل و نامحسوس**

شما یک تلفن همراه هوشمند در اختیار دارید که به‌خوبی صدا و تصویر را ثبت می‌کند، برای اجرای بازی اینترنت خود را فعال می‌کنید، اپلیکیشن دوربین را اجرا می‌کنید و ضمن ارسال موقعیت مکانی خود در هر لحظه، تصاویری بسیار با کیفیت را به‌صورت آنلاین به سرورهای بازی ارسال می‌کنید. حالا فرض کنید در این شرایط پوکمون موردنظر شما در یک مرکز نظامی یا

---

[1] LaaS, PaaS, Saas
[2] Pokémon GO

امنیتی قرار گرفته باشد. جاسوس‌ها بجز تصویری کاملاً شفاف و آنلاین، به چه چیز دیگری نیاز خواهند داشت؟ باتوجه به این خطر امنیتی بسیار بزرگ، این روزها بسیاری از کارشناسان امنیتی حدس می‌زنند دست‌های پشت پرده‌ای همچون سازمان جاسوسی سیا به اطلاعات کاربران در این بازی دسترسی داشته باشند. همین عامل نیز موجب شده نه تنها در ایران، بلکه در بسیاری از کشورهای دیگر اجرای بازی پوکمون‌گو محدود و حتی غیرممکن شود.

- ✓ **جمع‌آوری افراد در یک مکان برای انجام حملات تروریستی**

چنانچه با این بازی آشنایی داشته باشید می‌دانید قرارگیری یک پوکمون کمیاب می‌تواند تعداد زیادی از کاربران را به یک منطقه خاص بکشاند. این همان چیزی است که این روزها تروریست‌ها دنبال آن هستند. بهانه‌ای برای حضور تعداد زیادی از مردم در یک مکان خاص برای انجام عملیات تروریستی.

- ✓ **مشکلات غیر امنیتی ولی با خطرات جانی**

جالب است بدانید با گذشت کمتر از یک هفته از انتشار این بازی، چند تصادف به دلیل اجرای این بازی گزارش شده است، چند نفر در اثر بی‌دقتی داخل جوی افتاده‌اند یا با تیرهای برق و تابلوهای موجود در خیابان‌ها برخورد کرده‌اند و در این میان بزهکاران نیز هوشمند شده و با کشاندن پوکمون‌بازها به کوچه‌های تنگ و تاریکی که یک پوکمون در آن قرار گرفته است، از قربانیان خود که به تنهایی در نیمه‌های شب به این مکان‌ها رفته و به دنبال پوکمون بوده، زورگیری کرده‌اند.

۵-۴-۸-۱ هوش مصنوعی

پژوهشگران، پنج مسئله اصلی را که منجر به وقوع سوانح و بروز خطا می‌شود، شناسایی کرده‌اند که عبارتند از اثرات جانبی منفی، هک کردن پاداش، نظارت مقیاس‌پذیر، اکتشاف امن و مقاومت در برابر تغییرات توزیعی. آن‌ها علاوه بر بیان این پنج مسئله، زمینه‌های تحقیقاتی مورد نیاز برای حل آن‌ها را نیز پیشنهاد داده و این مسائل را با تکیه بر مثال تمیز کردن یک گلدان توسط یک ربات در محیطی اداری تبیین نموده‌اند.

اثرات جانبی منفی می‌توانند از تمرکز یک جانبه هوش مصنوعی روی یک وظیفه خاص ناشی شوند. به طور مثال، ربات نظافت کار ممکن است سریع‌ترین مسیر را برای تکمیل وظیفه خود فارغ از روش تمیز کردن، محاسبه کند؛ بنابراین تنها چیزی که برای او اهمیت دارد این است که صرفاً کار خود را به اتمام برساند. می‌توان به ربات آموزش داد تا از وارد آوردن فشار اضافی به گلدان هنگام تمیز کردن آن اجتناب کند، اما این راهکاری مؤثر برای تبیین جداگانه تمامی روش‌های مواجهه با موانع برای عامل هوش مصنوعی نیست. محققان بر این نکته تاکید می‌کنند که توسعه یک رویکرد عمومی که در آن هوش مصنوعی وظایف خود را بر اساس محدودیت‌های عقل سلیم انجام داده و به خاطر ایجاد تغییرات عمده در محیط تنبیه شود، می‌تواند زمینه تحقیقاتی جذابی برای آینده باشد.

هک کردن پاداش، تمایل گستاخانه یک عامل هوش مصنوعی برای یافتن و بهره‌برداری از یک میانبر برای رسیدن به هدف خود و پاداش‌های بعدی است که احتمال دارد هدف اصلی او را تضعیف کند. این مسئله با برخی اثرات جانبی منفی همراه بوده و عمدتاً توسط طراحان هوش مصنوعی با اشتباه در تعیین تابع هدف ایجاد می‌شود. به طور مثال، روش تبیین یک کار یا وظیفه به عامل هوش مصنوعی اجازه می‌دهد که هدف خود را برخلاف خواسته برنامه‌نویس، تفسیر کند.

بنابراین ربات نظافت کار ممکن است زمانی پاداش دریافت کند که هیچ آلودگی یا شیء کثیفی را شناسایی نکرده باشد و این به نوبه خود می‌تواند منجر به نادیده گرفتن محیط‌های کثیف توسط او شود. یا اگر بر اساس پاک کردن فعالانه آلودگی به ربات پاداش داده شود، او ممکن است تصمیم بگیرد تا آلودگی بیشتری را برای تمیز کردن تولید کند. بدیهی است که هیچ‌یک از روش‌های پاداش‌دهی یاد شده نمی‌توانند راهی مؤثر برای نظافت محیط یک دفتر اداری باشند.

محققان بر این باورند که حل مسئله هک کردن پاداش به دلیل روش‌های متعددی که یک هوش مصنوعی ممکن است وظیفه یا محیط خود را تفسیر کند، بسیار دشوار خواهد بود اما آن‌ها در مقاله خود چندین پیشنهاد را برای تحقیقات آتی مطرح کرده‌اند. آگاه سازی یک عامل هوش مصنوعی از سازوکار اعطای پاداش به او ممکن است از دست‌کاری سیستم امتیازدهی فیزیکی توسط او جلوگیری کند و دانشمندان می‌توانند با توسعه سنجه‌هایی برای ارزیابی موقعیت ربات، از دخالت او در فرآیند پاداش‌دهی ممانعت به عمل آورند.

نظارت مقیاس‌پذیر به این مسئله اشاره دارد که چگونه یک عامل هوش مصنوعی از قرارگیری در مسیر صحیح، اطمینان حاصل کرده یا نتایجی را به بار می‌آورد که دلخواه و مطلوب انسان است. یک تابع هدف مختلط به این معناست که یک عامل هوش مصنوعی می‌تواند به طور مرتب توسط یک ناظر انسانی پایش شود، اما انجام این کار در اغلب موارد، آزار دهنده و غیر بهره‌ور است. برای غلبه بر این مشکل، محققان نیاز دارند که روش‌هایی را برای پیاده‌سازی اصول پاداش‌دهی بدون تضعیف اهداف کلی پیدا کنند.

بخش عمده‌ای از یادگیری ماشین، فرآیند اکتشاف است که در آن، عامل هوش مصنوعی با چندین روش، آزموده شده، نتایج را مشاهده و عملکرد خود را برای دریافت پاداش ارزیابی کرده و تصمیم می‌گیرد که آیا باید در آینده آن عمل را انجام دهد یا خیر. این یک تابع بسیار کارآمد برای بیشتر بخش‌ها است، اما به‌وضوح می‌تواند منجر به بروز برخی از اثرات نامطلوب شود. هک کردن پاداش، ممکن است باعث وارد آمدن آسیب به ربات، محیط یا افراد پیرامون آن شود. شما به دنبال این هستید که ربات نظافت کار، روش‌های متفاوت شست‌وشو را امتحان کند اما قطعاً نمی‌خواهید که او یک پریز برق را بشوید. دانشمندان پیشنهاد می‌کنند که فرآیند تعلیم عوامل هوش مصنوعی در محیط‌های شبیه سازی شده، انجام شده تا فرآیند اکتشاف منجر به وارد آمدن آسیب به دنیای واقعی نشود. آن‌ها بر این باورند که تحقیقات آینده باید با تنظیم پارامترهایی، راه را برای اکتشاف ایمن ربات‌ها در محیط، هموار کند.

در نهایت، هوش مصنوعی نیاز دارد تا در برابر تغییرات ناشی از توزیع، مقاوم شود. اگر فرآیند تعلیم یک هوش مصنوعی در یک محیط بسته انجام شود، احتمالاً در آینده عملکرد عامل با اختلال مواجه خواهد شد،

چرا که درس‌های آموخته شده به او ممکن است قابل تعمیم به محیط‌های دیگر نباشند. به طور مثال، احتمال دارد ربات نظافت کار، برای نظافت کف یک کارخانه، استفاده از مواد شوینده قوی را مؤثر بداند اما قطعاً متوجه نخواهد شد که این مواد برای شست‌وشوی یک فرش در یک دفتر اداری کوچک، مناسب نیستند. عوامل هوش مصنوعی در این مورد، بسیار آسیب‌پذیر هستند، چرا که برخلاف انسان، ربات‌ها در یک محیط جدید در آموخته‌های خود تردید نکرده و با اعتماد به نفس کامل دست به کار می‌شوند و این به نوبه خود می‌تواند منجر به وقوع سلسله رخدادهای آسیب‌زا شود.

مواجهه با این مسئله نیز می‌تواند در قالب بهبود و توسعه روش‌های سنجش بهتر، مطرح گردد. به طور مثال، عامل هوش مصنوعی تخصیص توان به یک شبکه برق می‌تواند به جای ارقام گسسته از درصد استفاده کند تا از مقایسه شبکه‌ها با اندازه‌های متفاوت، جلوگیری شده و از تحمیل اضافه‌بار به یک سیستم انرژی ممانعت به عمل آید.[1]

نکته پایانی اینکه تمام عوامل تشریح شده در بالا به نوعی خطر و ریسک‌های این حوزه را گوشزد و ضرورت استفاده هوشمند بیش از پیش را متذکر می‌گردند؛ اما برای شرح دقیق معنای ریسک و روشن شدن بیشتر موضوع نیاز است که توضیحی در مورد ریسک هر یک از این حوزه‌ها ارائه شود که در ادامه این مهم مورد بررسی قرار می‌گیرد.

۱-۹ ضرورت ایمنی فضای مجازی

امروزه تأمین امنیت فضای مجازی از نخستین اولویت‌های سیاست‌گذاری در عرصه اجرا و قانون‌گذاری در کشورهای توسعه‌یافته و در حال توسعه است؛ چرا که توسعه روزافزون فضای مجازی همان‌طور که زمینه رشد اقتصادی و تجارت جهانی را فراهم ساخته، زمینه‌های ارتکاب جرائم و تهدیدات امنیتی را در پی داشته‌است. امروزه منافع صنعت، فناوری و دولت‌ها در تأمین امنیت برای مبادلات الکترونیکی و فعالیت‌های مختلفی است که عمدتاً اقتصادی بوده و کاربران و مؤسسات مالی اقتصادی در فضای مجازی بدان مشغولند و تدریجاً فعالان تجاری و دولت‌ها در این عرضه هماهنگ‌تر عمل می‌کنند. دولت‌ها برای رشد و رونق اقتصادی، بهره‌وری و تأمین امنیت ملی نیازمند زیرساخت‌های جهانی دیجیتالی امن هستند و شرکت‌های فناورانه در صدد فراهم ساختن حفاظت کافی در سیستم‌ها و محصولات خود می‌باشند.[2]

در این میان برای عملکرد بهتر دولت‌ها در سیاست‌گذاری‌ها و همچنین حرکت بهینه‌تر مؤسسات تجاری فعال در فضای مجازی اصولی چند در رابطه با امنیت فضای مجازی پیشنهاد شده است از جمله:[3]

---

[1] (Google,OpenAI,Stanford uni,Berkeley, 2015)
[2] (The IT Industry's Cyber security Principles for Industry and Government, information technology industry council, 2011)
[3] (Rhoades, The Truman|CNP Cyberspace & Security Program)

- **اقدام برای بهبود امنیت فضای مجازی بایستی در جهت بهتر شدن وضع مشارکت‌های خصوصی- دولتی و بر مبنای منابع تخصیصی و نوآوری‌های موجود باشد**

بیش از ده سال است که صنعت تکنولوژی با همکاری دولت‌ها توانسته است ابتکارات، منابع کافی و هدایتگری مناسبی در همه ابعاد امنیت فضای مجازی فراهم سازد؛ به عبارت دیگر تلاش برای مهیا نمودن فضای مجازی امن وقتی کارآمدتر است که بر مبنای نوآوری‌های روز بوده و به مسئله سرمایه‌گذاری و مشارکت‌ها (خصوصی- دولتی) توجه ویژه کند.

- **اقدام برای بهبود امنیت فضای مجازی بایستی با توجه به خصیصه جهانی، متصل و بدون مرز فضای مجازی باشد**

فضای مجازی محلی برای صلاحیت و قلمرو دولت خاصی است و فارغ از مرزهای جغرافیایی موجود تعبیر می‌شود و فعالان فضای مجازی یعنی مصرف‌کنندگان، مؤسسات مالی، دولت‌ها و مالکان و ارائه‌دهندگان زیرساخت‌های این فضا به دنبال فعالیت مداوم امن در فضای مجازی هستند.

- **تأمین امنیت فضای مجازی بایستی مطابق با جدیدترین مخاطرات فضای مجازی، فناوری و الگوهای تجاری و مبتنی بر مدیریت خطر[1] صورت گیرد**

عرصه فناوری به سرعت در حال پیشرفت است و شرکت‌های بزرگ با سرمایه‌گذاری در بخش تحقیق و توسعه[2] (سرمایه‌گذاری جهت رسیدن به فناوری جدیدتر) نیاز مبرمی به وجود عوامل امنیتی متناسب با آن در فضای مجازی پیدا می‌کنند. البته بایستی دقت نمود که تأمین امنیت در فضای مجازی برای این مقصود است که یک سازمان یا به طور کلی کاربر فعال در آن به درستی توانایی تشخیص مخاطرات در این محیط را داشته باشد و با دقت بیشتری برنامه‌ریزی کند. برای این مهم است که امروزه مراکز سی.آی.اُ[3] به ارائه تجزیه و تحلیل‌هایی در رابطه با دنیای فناوری و چگونگی به کارگیری آن برای رسیدن به اهداف اقتصادی فعالیت می‌کنند و مأموران موسوم به سی.آی.اس.اُ[4] (که مسئول تضمین حمایت اموال اطلاعاتی[5] و فناوری یک مؤسسه می‌باشند) می‌کوشند تا حد امکان مخاطرات فناوری اطلاعات که کاربران با آن مواجه هستند را کاهش دهند.[6]

- **حفاظت از فضای مجازی مسئولیت مشترک است**

هیچ نهادی از جمله دولت یا مراکز قدرتمند اینترنتی به تنهایی نمی‌تواند تأمین امنیت فضای مجازی را تضمین کند، چراکه فضای مجازی فرای مرزهای جغرافیایی تعریف می‌شود و امنیت فضای مجازی نیازمند هماهنگی و تعاون میان نهادهای دولتی، فدرال، منطقه‌ای و خصوصی است.[7]

---

[1] Risk Management
[2] R&D
[3] CIO
[4] CISO
[5] Information assets
[6] (Durbin, 2013)
[7] (Rhoades, Cyber First Principles, 2014)

- **تأمین امنیت فضای مجازی به معنای حفظ حریم خصوصی است**

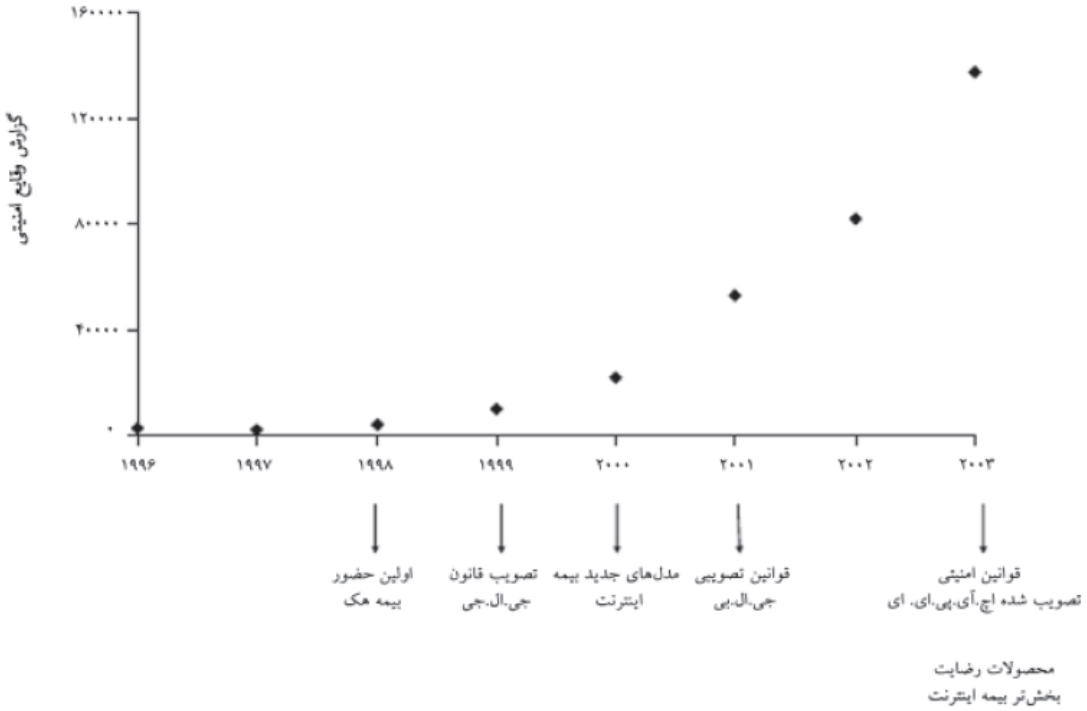
در واقع تأمین امنیت فضای مجازی به حمایت از افراد، شرکت‌ها و دولت‌ها نسبت به نفوذ غیرمجاز به محیط مجازی اختصاصی آن‌ها می‌انجامد و این تصور غلطی است که تأمین امنیت بیشتر منجر به کاهش میزان حریم شخصی می‌شود.

۱-۱۰ اهمیت پوشش بیمه برای فضای مجازی

اگرچه قبل از یازدهم سپتامبر ۲۰۰۱ حوادث اینترنتی بسیاری وجود داشت، اما بعد از آن سال بود که درک و تصور از ریسک و نگرش به آن به طرز قابل توجهی تغییر یافت. سه مورد از جدی‌ترین حملات کرم‌های اینترنتی در طول سه ماه حدود سپتامبر ۲۰۰۱ به وقوع پیوست.

این حملات نه تنها مانع ارائه خدمات ۵ وب‌سایت از ده وب‌سایت معروف اینترنتی به مشتریان گردید بلکه سرعت اینترنت را هم کاهش داد (کی نوت سیستمز[1] تخمین زد که در عملکرد ۴۰ وب‌سایت دیگر که مورد حمله واقع نشده بودند، ۶۰٪ تنزل ایجاد گردید).

هم‌زمان با افزایش ریسک حملات اینترنتی، در رابطه با استفاده قانونی از اطلاعات الکترونیکی و حفظ آن‌ها مقرراتی تدوین شد. بسیاری از این قوانین در پاسخ به نیاز برای استانداردهای به روزشده در رابطه با اطلاعات رایانه‌ای به وجودآمدند و سپس با حوادث گسترده توسعه یافتند.



نمودار ۱. رابطه مثبت بین افزایش وقایع امنیتی و وضع قوانین مرتبط

[1] Keynote Systems

نمی‌توان انکار کرد که مخاطرات فضای مجازی، همراه دائمی این فضا هستند. انواع جرائم و ناهنجاری‌هایی که به وقوع می‌پیوندد و نیز اخلال در ارائه خدمات از جمله این مشکلات است. لذا بیمه می‌تواند در این زمینه که نمی‌توان مخاطرات آن را به طور کامل حذف کرد، به خوبی نقش ایفا کند. با این حال، هنوز هم علاقه به خرید این بیمه کمتر از میزان مورد انتظار است. کما اینکه مطالعات نشان می‌دهد که ۷۲ درصد از مدیران ریسک در ۱۵۳ شرکت در آمریکای شمالی اقدام به خرید بیمه‌های مورد نیاز برای حریم خصوصی و مسئولیت در فضای مجازی نکرده‌اند.[۱]

درک صحیح از برنامه بیمه یک شرکت، یکی از نکات کلیدی در افزایش ایمنی آن در برابر مخاطرات مجازی است. در ایالات متحده، کمیسیون اسناد تجاری و مبادلات[۲] از تأمین مالی شرکت، دفترچه راهنمایی را در این خصوص منتشر کرده است که به موجب آن شرکت‌ها مکلفند وفق قوانین و مقررات داخلی راجع به بازار بورس و مبادلات اسناد، اقدام به ارائه یا افشای اطلاعات راجع به تهدیدات فضای مجازی نمایند.[۳]

۱-۱۱ عوامل خطرساز در مسئله فضای مجازی را می‌توان به صورت زیر برشمرد:

- **در معرض خطر بودن داده‌ها از سوی بزهکاران**

طبق گزارش سالانه مؤسسه پدیده در سال ۲۰۱۱، تعرض به داده آثار مخرب جدی بر سازمان‌ها داشته است[۴] که این امر ضرورت طراحی و اجرای سازوکارهای پایدار و واقع‌بینانه در خصوص مدیریت ایمنی داده‌ها را می‌طلبد. واقعیت‌ها نشان می‌دهد که با وجود پیشرفت‌های حاصله در زمینه ارتقای ایمنی داده‌های مجازی، این داده‌ها که مربوط به بخش و صنایع مختلف اعم از بازی‌های رایانه‌ای، خدمات بازاریابی، خرده فروشان، صنعت بهداشت، بانک‌ها، بیمه‌ها، مؤسسات و شبکه‌های اجتماعی و مؤسسات مالی و اعتباری هستند، به شدت در معرض خطر قرار دارند. تا جایی که در ۳۶۶۹ حمله تا ماه مارس ۲۰۱۳، بیش از ۶۰۰ هزار سابقه الکترونیکی مورد حمله قرار گرفته‌اند.

افزایش حملات فضای مجازی دلالت بر این واقعیت مهم دارد که هزینه‌های مربوط به مخاطرات مجازی در حال افزایش است. برای مثال، هرگاه سازوکار منظمی برای کنترل سازمان‌ها در خصوص ایمنی داده وجود داشته باشد و این داده‌ها مورد حمله قرار گیرد، سازمان مکلف است برای ارتقای خود به حدودی که در سازوکارهای اعلامی آمده است، هزینه هنگفتی متحمل شود. در ایالات متحده، چنین مقرراتی در ۴۶ ایالت و علاوه بر آن در چند کشور وابسته مانند کلمبیا، گوام، پورتوریکو و جزایر ویرجین ایالات متحده وجود دارد.[۵]

---

[1] (watson, 2012)
[2] Commission on Trade Documents and Exchanges
[3] (Commission on Trade Documents and Exchanges of Corporate Financing, 2011)
[4] (ponemon Institutes, 2012)
[5] (State Security Breach Notification Laws, 2012)

همچنین شرکت‌های مرتبط با فضای مجازی ممکن است مشمول بازرسی‌های منظم و نیز جریمه‌ها، مجازات‌ها و دعاوی باشند که برای مطالبه خسارت ناشی از سرقت داده، نقض حریم خصوصی، سوء استفاده از مالکیت فکری یا دسترسی به اطلاعات محرمانه و سایر آثار ناشی از تعرض به داده‌ها وجود دارد.

۱-۱۲ مفهوم ریسک در فضای مجازی و انواع آن

مخاطره فضای مجازی یعنی احتمال صدمه دیدن و تحمل خسارت و ضرر به دلیل در معرض بودن یک عامل الکترونیکی که می‌تواند منجر به ایجاد آثار سوء بر یک کسب‌وکار شود[1] یا در معنایی عام‌تر مخاطره فضای مجازی عبارت از مخاطره مربوط به فعالیت‌های اینترنتی آنلاین، تجارت الکترونیک، سیستم‌های الکترونیکی و شبکه‌های فناوری و همچنین ذخیره اطلاعات شخصی است.[2]

گرچه مخاطرات در فضای مجازی بسته به نوع فعالیت متفاوت است اما آنچه اصولاً ریسک به معنای واقعی خوانده‌می‌شود و شرکت‌های بزرگ تجاری در صددند تا خود را از آن مصون دارند اصولاً بالغ بر موارد زیر است:

۱-۱۳ تعریف مبانی حاکم بر بیمه فضای مجازی

۱-۱۳-۱ هک

منظور از هک، هک شدن اطلاعات شخصی توسط هکرها است. هک می‌تواند موجب تضعیف میزان محرمانگی سازمانی یک شرکت شود که خود باعث پایین آمدن اعتبار آن شرکت خواهد بود، چرا که هک ممکن است عملکرد یک شرکت نسبت به امنیت داده‌ها و از دست دادن اطلاعات محرمانه را در معرض قضاوت عموم قرار دهد.

۱-۱۳-۲ حمله عدم سرویس‌دهی[3]

در حملات عدم سرویس‌دهی[4] از یک رایانه یا ارتباط اینترنتی برای پرکار کردن[5] پهنای باند و منابع سرور مبدأ استفاده می‌شود که در نتیجه آن سرور توان ارائه خدمات نداشته و اصطلاحاً مشغول می‌گردد؛ بنابراین، حمله قطع یا اخلا در خدمات، به معنای حمله یک یا چندین شخص از طریق ارسال میزان بسیار زیادی از داده‌های الکترونیکی به سامانه رایانه‌ای به منظور کاستن از ظرفیت آن می‌باشد که در نتیجه افراد مُجاز نتوانند برای امور قانونی خود به سامانه دسترسی پیدا کرده و به مبادله اطلاعات بپردازند. در صورتی که پرشدن ظرفیت سامانه بدان جهت باشد که ظرفیت آن با حجم اطلاعاتی که معمولاً بدان وارد می‌شود، هماهنگ نیست؛ حمله قطع‌کننده خدمات که مشمول بیمه باشد، تحقق نخواهد یافت.

---

[1] http://www.investopedia.com/terms/p/professional-liability-insurance.asp
[2] (Greisiger, 2010)
[3] Denial of service attacks
[4] DOS
[5] overloading

۱-۱۳-۳ اخاذی اطلاعاتی[1]

به طور کلی اخاذی در فضای مجازی هنگامی ارتکاب می‌یابد که شخصی از طریق اینترنت دیگری را تهدید به برآورده کردن مطالبات خود مانند دادن مبلغی پول، تحویل کالایی مشخص یا انجام کاری خاص (مانند برقراری رابطه جنسی) می‌کند. تهدید می‌تواند شامل طیفی از صدمه زدن به شخص، عِرض و آبرو و یا اموال وی باشد.[2]

۱-۱۳-۴ خطای نیروی انسانی

با وجود تمام تلاش‌هایی که شرکت‌های تجاری برای مقابله با امنیت داده به عمل می‌آورند باز هم خطای انسانی یکی از مهم‌ترین مخاطرات فضای مجازی است. طبق گزارش[3] شرکت آی.بی.ام[4] از موارد نقض امینت داده‌ای آن شرکت در سال ۲۰۱۳، خطای انسانی در نود و پنج درصد موارد دخیل بوده است.

۱-۱۳-۵ نقص ناشی از نرم‌افزار

شرکت‌ها اصولاً برای به کارگیری فعالیت‌های خود از نرم‌افزارهای رایانه‌ای فراوانی استفاده می‌کنند که گاهی عدم بازدهی مناسب این برنامه‌های رایانه‌ای ممکن است منجر به ورود خسارت شود.

۱-۱۳-۶ نقض داده

نقض داده حادثه‌ای است که در اثر آن اطلاعات محرمانه، محافظت شده و سری به طور پنهانی و بدون مجوز بررسی و دزدیده شده یا مورد استفاده قرار گرفته است.[5]

۱-۱۳-۷ انتقال ویروس

ایجاد اختلال در سیستم‌های خدمات‌رسان از طریق انواع ویروس‌ها[6]، کرم‌ها[7] و مرجان‌ها[8] ممکن است صورت بگیرد.

۱-۱۳-۸ حالت عدم فعالیت شبکه

این اصطلاح زمانی به کار می‌رود که سیستمی برای مدت به خصوصی قادر به ارائه خدمات نباشد. ایجاد چنین وضعیتی برای سیستم‌های خدمات‌رسان به سایر مراکز فعال مانند نیروگاه‌های هسته‌ای، بانک‌ها و سایر مؤسسات مالی موجب اختلال در انجام امور اصلی آن‌ها خواهد شد و ممکن است عواقب ناگواری برای آن‌ها در پی داشته باشد.

---

[1] Information extortion / Cyber extortion
[2] definitions.uslegal.com/c/cyberextortion/
[3] (IBM Security Services 2014 Cyber Security Intelligence Index, Analysis of cyber attack and incident data from IBM's worldwide security operations., 2014)
[4] IBM
[5] (Rouse, 2010)
[6] Viruses
[7] worms
[8] corals

۱-۱۳-۹ از بین رفتن فیزیکی سیستم

فعالیت در محیط مجازی نیازمند سیستم فناوری اطلاعات است که از تجهیزات عینی متعددی تشکیل شده است. صدمه به این تجهیزات می‌تواند در اثر هر عامل بیرونی از جمله آتش‌سوزی، تغییرات دمای اتاق سرور و حتی سیل یا نوسانات الکتریکی به وقوع بپیوندد.[1]

۱-۱۴ سابقه روش‌های محاسبات ریسک در بیمه فضای مجازی

اولین بیمه‌نامه‌های فضای مجازی حول موضوع جرائم این فضا شکل گرفتند به طوری که اولین کاری که کاربرد سیستم توزیع بیمه برای اینترنت را بیان می‌کرد، مربوط به سال ۱۹۹۴ می‌شود. دان گیر[2] مبدع استفاده از مدیریت ریسک شامل استفاده از پوشش بیمه‌ای برای اینترنت بوده است. او نخستین کسی بود که ارتباط مقوله مدیریت ریسک که عموماً در دیگر رشته‌ها به خصوص در بخش مالی به کار می‌رفت را با اینترنت مطرح کرد. بارزترین فردی که بیمه اینترنت را در بحث‌های آکادمیک مطرح کرد، بروس شنیر[3] بود که آنچه را که امروزه در مورد نقش بیمه اینترنت بر آن اجماع شده‌است را او قبلاً تشریح کرده‌است (یورسیک، ۲۰۰۶)[4].

اصولاً ارزش‌گذاری در بیمه وابسته است به جداول بیمه‌ای که سابقه‌ای طولانی دارد ولیکن اینترنت پدیده‌ای نو است. از طرفی شرکت‌ها جزئیات پرونده‌ها را به علت مسائل امنیتی فاش نمی‌کنند. فلذا شرکت‌های بیمه برای بیمه‌های فضای مجازی معیارهای ارزش‌گذاری تعیین کرده‌اند. به همین دلیل، کمیت ریسک‌های فضای مجازی را که به نظر برخی غیر قابل اندازه‌گیری است تعیین کرده‌اند. اگرچه هنوز این مسأله قابل بحث است که آیا این طرح‌های ارزش گذاری صحیح هستند یا خیر و حق بیمه مناسب برای این بیمه‌های جدید چقدر باید باشد.

۱-۱۵ ابعاد تجاری بیمه‌های فضای مجازی

پوششی که امروزه برای مخاطرات فضای مجازی بوسیله بیمه‌نامه‌های مختلف فضای مجازی مهیا شده است نسبت به دو تا پنج سال اخیر افزایش چشم‌گیری نشان می‌دهد. حق بیمه‌های پرداختی در بازار ایالات متحده امریکا بالغ بر ۵۰۰ میلیون دلار تخمین زده می‌شود که این حجم درآمدی خود به توسعه بیمه در فضای مجازی کمک می‌کند. در برخی اتحادیه‌های تجاری نیز طرح‌های عملیاتی برای شرکت‌های عضو در بردارنده بیمه‌نامه‌های استاندارد شده، دارای بند پوشش بیمه‌ای در فضای مجازی است. همچنین بایستی دقت نمود که امروزه بیمه فضای مجازی خود به عنوان فرصت مناسبی برای بیمه‌گذاران تلقی می‌شود چرا که هم درآمد خوبی عاید شرکت‌های بیمه‌گر می‌کند و هم زمینه مساعدی جهت توسعه محصول به حساب

---

[1] (Ltd, 2011)
[2] Dan Geer
[3] Bruce Schneier
[4] (Majuca, Kesan, & Yurcik, 2006)

می‌آید. البته هنوز محاسبه هزینه‌ها برای پوشش بیمه با وجود در نظر گرفتن عوامل متعدد مانند بخش کسب‌وکار بیمه‌گذار، تعداد رکوردی که به وسیله سازمان مربوطه حفظ می‌شود و ... دغدغه بیمه‌گران است[1].

طبق گزارش بترلی[2] در سال ۲۰۱۳، بازار بیمه فضای مجازی به خصوص در بخش مراقبت سلامت[3] و بخش‌های کوچک و متوسط مقیاس تجاری که شامل بنگاه‌ها و شرکت‌های تجاری کوچک می‌شود، رو به گسترش است.[4] همه بیمه‌گران به رشد حق بیمه‌ها اذعان داشته‌اند و اکثراً مقدار این افزایش را بین ۱۰ الی ۲۵ درصد و برخی میان ۲۵ الی ۵۰ درصد گزارش کرده‌اند. گرچه افزایش ۱۰۰ درصدی توسط برخی بیمه‌گران نیز مشاهده شده است.

در این گزارش احتمال افزایش حق بیمه‌ها پیش‌بینی شده است که معلول گسترش روز افزون نقض داده‌ها و حساسیت افکار عمومی نسبت به لزوم حفاظت از حریم شخصی می‌باشد که تبعا منجر به افزایش مبالغ پرداختی برای جبران خسارت می‌گردد. آنچه بیش از هر چیز وضعیت این بازار را مبهم می‌کند ریسک جمعی[5] است که میل بیمه‌گران اتکایی به بیمه فضای مجازی را کاهش داده است.

ویژگی برجسته بیمه‌نامه‌های اینترنت این است که برای انواع مختلف مشتریان هدف، پوشش‌های محدودی دارند. یک دلیل این امر آن است که بیمه‌گران با تعریف پوشش محدود، می‌توانند ریسک حوادثی که از قبل قابل پیش‌بینی نیستند را مستثنی کنند. دلیل دیگر آن است که با تعریف محدود و مشخص پوشش بیمه‌ای، بیمه‌گران اینترنت می‌توانند بیمه‌نامه‌ها را متفاوت کرده و در نتیجه آن‌ها را به بازارهای خاص ارائه دهند.

امروزه هیچ کس در دورنمای روشن بیمه فضای مجازی تردید ندارد. راجر اسمیت از شرکت بیمه آلیانز[6] بر این اعتقاد است که بیمه فضای مجازی، سریع‌ترین و رو به رشدترین بیمه در سراسر جهان است؛ زیرا نه تنها شرکت‌های بزرگ متقاضی آن هستند، بلکه چون هکرها امروزه مکرراً شرکت‌های کوچک و سامانه‌های نه چندان امن آن‌ها را مورد حمله قرار می‌دهند، پس مشتریانی بین شرکت‌های خرد هم دارند.

۱-۱۶ متقاضیان بیمه فضای مجازی

شرکت‌ها، مؤسسات و افرادی که با فناوری اطلاعات سر و کار دارند و برای پیشبرد امور تجاری، اداری و روزانه (شخصی) خود از آن بهره می‌برند، متقاضیان بیمه فضای مجازی و تجارت الکترونیک محسوب می‌شوند. با توجه به حجم روزافزون مبادلات و فعالیت‌ها در فضای مجازی امروزه یکی از مهمترین خدمات بیمه‌ای، بیمه‌های فضای مجازی و تجارت الکترونیک می‌باشند که روز به روز در حال توسعه می‌باشد. در ادامه فهرست مختصری از مخاطبان مذکور ارائه می‌شود:

- ✓ شرکت‌ها و مؤسسات فعال در حوزه تجارت الکترونیک

---

[1] (Airmic Review of Recent Developments in the Cyber, 2013)
[2] betterely
[3] Health care
[4] (. Cyber/Privacy Insurance Market Survey, 2013)
[5] Accumulation risk
[6] Allianz SE

- ✓ مؤسسات دولتی و غیردولتی مانند بانک‌ها و مؤسسات مخابراتی[1] که نسبت به امکانات و خدمات ارائه شده از سوی خود به موجب قانون، قرارداد یا عرف در قبال خسارات وارده به اشخاص ثالث مسئولیت مدنی دارند؛
- ✓ اشخاصی که در فضای مجازی این احتمال نسبت به آن‌ها وجود دارد که قربانی سرقت هویت، سرقت شماره و شناسه‌های بهادار (رمز کارت اعتباری و ...) و جعل سمت شوند؛
- ✓ شرکت‌های مرتبط با رایانه‌هایی که از آن‌ها برای انعقاد قرارداد یا تبادل داده استفاده می‌شود؛
- ✓ هر مؤسسه‌ای که اقدام به ذخیره الکترونیکی اطلاعات می‌نماید و این داده‌ها از طریق شبکه جهانی اینترنت یا شبکه داخلی توسط افراد مجاز یا غیر مجاز قابل دسترس است؛
- ✓ مؤسساتی که به صورت آنلاین (برخط) اقدام به فعالیت‌های نشر، پخش و ارتباط با عموم یا مخاطبان خاص می‌نمایند (بیمه ارتباطات و رسانه)؛
- ✓ شرکت‌ها و مؤسساتی که به طور قابل توجهی در فعالیت‌های تجاری، صنفی یا حرفه‌ای خود از نامه الکترونیکی استفاده می‌کنند؛
- ✓ شرکت‌هایی که به هر نحو از فناوری بهره‌مند می‌شوند و به دلیل وجود دو عامل «استمرار بهره‌مندی» و «ارتباط عمومی یا خصوصی قابل توجه» در معرض مخاطرات امنیتی قرار دارند؛
- ✓ مؤسساتی که دارای پایگاه اینترنتی فعال برای ارتباط با مشتریان یا مخاطبان هستند؛
- ✓ افرادی که اقدام به دریافت کالا و خدمات از طریق اینترنت نموده یا به طور مستمر از این شیوه برای خرید یا اطلاع از وضعیت روز بازار استفاده می‌کنند؛
- ✓ اشخاصی که اطلاعات آن‌ها دارای ماهیت خاصی است که به دلیل ارزش تجاری، امنیتی، شخصی و ... مخاطرات بیشتری در مقایسه با سایر اطلاعات آن‌ها را تهدید می‌کند؛
- ✓ کسانی که از کارت‌های اعتباری یا دیگر سامانه‌های الکترونیکی و اینترنتی به طور مکرر در معاملات و فعالیت‌های روزمره خود استفاده می‌کنند.

۱-۱۷ نتیجه گیری

استفاده از فضای مجازی هر روز بیشتر می‌شود و ابعاد جدید و گسترده‌تری از زندگی فردی و اجتماعی ما را در بر می‌گیرد. این گستردگی در کنار مزیت‌هایی که دارد مشکلات و مخاطراتی نیز به همراه دارد که لزوم توجه و هوشمندی بیشتر بخش‌های مختلف جامعه را نیازمند است؛ اما رونق و توسعه صنعت بیمه در فضای مجازی می‌تواند بسیاری از مخاطرات و ریسک‌ها را از بین برده و هزینه بسیاری از مشکلات را کاهش دهد.

در واقع همان‌طور که روند جهانی این مهم شروع شده است، لازم است در کشور تمهیداتی اندیشیده شود تا بتوان در آینده نزدیک وارد بخش اجرایی و عملی این حوزه شده و بیمه‌نامه‌هایی را طراحی نمود که

[1] شرکت‌ها یا مؤسسات ارائه کننده خدمات اطلاع رسانی و اینترنتی

ابعاد مختلف ریسک‌های فضای مجازی را پوشش دهد. عدم آمادگی نظری و اجرایی برای مواجهه با مسائل این حوزه موجب بی سر و سامانی و مبهم بودن فضای کسب‌وکار خواهد شد که این مسئله می‌تواند هزینه‌های گزافی بر دولت و مردم تحمیل کند.

۲- بررسی نمونه‌های موفق و تجربه کشورهای پیش‌رو در زمینه بیمه مجازی

۲-۱ انواع پوشش‌های بیمه سایبر

به طور کلی پوشش‌های بیمه سایبر به دو بخش شخص ثالث و اول تقسیم می‌شوند؛

۲-۱-۱ پوشش شخص ثالث

- دادگستری و مقررات: هزینه‌های مربوط به پرونده‌های مدنی، قضاوت‌ها، حل و فصل یا مجازات‌های ناشی از یک رویداد سایبری.
- هزینه‌های پاسخگویی خدمات حقوقی، فنی و قانونی لازم برای کمک به بیمه گذار در پاسخ به سؤالات دولتی مربوط به حمله سایبری و پوشش جریمه‌ها، مجازات‌ها، تحقیقات و یا سایر اقدامات نظارتی.
- مدیریت بحران: هزینه‌های مربوط به مدیریت بحران
- پوشش هزینه‌های روابط عمومی و آموزش مشتریان در مورد رویدادهای سایبری و پاسخ به بیمه گذار
- نظارت بر اعتبار: هزینه‌های نظارت بر اعتبار و نظارت بر تقلب و یا سایر خدمات مرتبط با آن به مشتریان یا کارکنان تحت تأثیر یک رویداد سایبری.
- مسئولیت چند رسانه‌ای (مدیا): پوشش نقض حق نسخه برداری، علامت تجاری یا علامت‌های خدماتی ناشی از انتشار آنلاین توسط بیمه گذار
- حریم خصوصی: پوشش هزینه آسیب کارمندان یا مشتریان برای نقض حریم خصوصی آن‌ها توسط یک رویداد مخرب سایبری.

۲-۱-۲ پوشش شخص اول

- سرقت و تقلب: تخریب یا از دست دادن اطلاعات بیمه گذار به عنوان یک نتیجه از یک رویداد سایبری جنایی یا جعلی، از جمله سرقت و انتقال وجوه.
- تحقیق قضایی: شامل خدمات حقوقی، فنی و یا قانونی لازم برای ارزیابی اینکه آیا حمله سایبری رخ داده است یا خیر و همچنین ارزیابی تأثیر حمله و توقف حمله.
- وقفه کسب و کار: درآمد از دست رفته و هزینه‌های مربوطه که در آن یک دارنده بیمه قادر به انجام کسب و کار به دلیل یک رویداد سایبری و یا از دست دادن اطلاعات نیست.
- اخاذی: پوشش هزینه‌های مربوط به تحقیق در مورد تهدیدهای حملات سایبری را علیه سیستم‌های بیمه گذار و پرداخت وجوه به مجرمانی که بیمه گذار را تهدید به انتشار اطلاعات حساس می‌کنند.
- از دست دادن و ترمیم کامپیوتر: شامل آسیب فیزیکی و یا از دست دادن کارایی دارایی‌های مرتبط با کامپیوتر، از جمله هزینه‌های بازیابی داده‌ها، سخت افزار، نرم افزار و یا سایر اطلاعاتی که در نتیجه حمله سایبری تخریب و یا آسیب دیده‌اند.

۲-۲ پوشش‌های بیمه سایبر بر حسب میزان تقاضا در بازار

- نقض امنیت و محرمانگی با میزان فراوانی ۹۲٪.

  بیشترین درصد پوشش مربوط به نقص امنیت و محرمانگی می‌باشد که شامل؛ هزینه جبران خسارت و پاسخ دادن به یک رویداد مانند انتشار اطلاعات، هزینه‌های داخلی و هزینه‌های قانونی می‌باشد.
- بیمه مخاطرات اموال الکترونیکی ۸۱٪، هزینه بازسازی اطلاعات و یا نرم افزارهایی که حذف، خراب و یا از دست رفته‌اند.
- هزینه پاسخ به حوادث ۸۱٪، هزینه‌های مستقیم برای تحقیق و اتمام حادثه برای به حداقل رساندن هزینه‌های پس از وقوع.
- اخاذی سایبری ۷۳٪
- اختلال در کسب‌وکار ۶۹٪، از دست‌دادن سود و یا هزینه‌های اضافی ناشی از عدم دسترسی به سیستم‌ها و یا داده‌ها به عنوان نتیجه حملات سایبری و یا دیگر مخرب‌های فناوری اطلاعات.
- مسئولیت چند رسانه‌ای (مدیا) ۶۵٪، هزینه برای تحقیق، دفاع و خسارات مدنی ناشی از دروغ‌گویی، نقض حق نسخه‌برداری، علامت تجاری، غفلت در انتشار هرگونه مطلب در رسانه‌های الکترونیکی و همچنین نقض مالکیت معنوی شخص ثالث.
- دادگستری و مقررات ۶۲٪، خدمات حقوقی، فنی و یا قانونی لازم برای بیمه‌گذار در پاسخ به سؤالات حکومتی و یا حقوقی مربوط به یک حمله سایبری، پوشش جریمه، مجازات و هزینه‌های دفاعی.
- خسارت به اعتبار تجاری ۴۶٪، هزینه از دست دادن درآمد ناشی از کاهش مشتریان و حجم معاملات که ممکن است در اثر نقض حریم خصوصی ایجاد شده باشد.
- تلف داده شخص ثالث ۲۳٪[1]

۲-۳ نکاتی برای خریداران بیمه سایبری

- اولین گام در خرید بیمه سایبر، شناخت ماهیت و میزان خطرات شرکت شما است. برای برخی از کسب و کارها مانند، بانک‌ها و خرده فروشان، نگرانیشان سرقت اطلاعات مالی اشخاص است. به طور نمونه، خطر اصلی برای یک شرکت در حوزه برق یا انرژی، اختلال کسب و کارهای بحرانی و یا عملیات فیزیکی از طریق حمله به شبکه است از این رو شرکت‌ها باید پوشش خود را با خطراتی که با آن روبرو هستند، مطابقت دهند.
- درک پوشش فعلی خود؛ شرکت شما باید سیاست‌های اول و شخص ثالث استاندارد خود را فراهم سازد تا بتواند به درک پوشش موجود خود برسد و قادر به خرید بیمه سایبری که شرکت به آن نیاز دارد، باشد.

---

[1] (Managing cyber insurance accumulation rick, 2016)

- آنچه به آن نیاز دارید خریداری کنید. با توجه به انواع پوشش ارائه شده توسط بیمه‌گران در بازار امروز مهم است که بر اساس اصول شرکت تمرکز کنید و در نظر بگیرید که آیا شما به تمام پوشش‌هایی که ارائه شده است نیاز دارید؟
- شاید مهمترین گام برای یک شرکت ارزیابی ارزش بیمه سایبر باشد، مقایسه هزینه‌های پیش بینی شده در ارتباط با نقض اطلاعات با محدودیت‌های مسئولیت در دسترس و هزینه‌های آن مرتبط است. هزینه پاسخ دادن به نقض اطلاعات نیز می‌تواند قابل توجه باشد. برآوردها متفاوت هستند، اما در سال ۲۰۱۱ میانگین هزینه نقض شده ۵/۵ میلیون دلار بوده است. شرکت شما باید سعی‌کند محدودیت‌های مسئولیت خود را با مواجهه واقعی خود در صورت از دست دادن سایبر مطابقت دهد.
- پوشش برای اعمال و اتهام شخص ثالث را در نظر بگیرید. بسیاری از شرکت‌ها پردازش داده یا ذخیره سازی را به فروشنده ثالث منتقل می‌کنند. مهم است که سیاست بیمه سایبر شما پوشش‌هایی را برای ادعاهایی که از سوء رفتار با یکی از فروشندگان شما ایجاد می‌شود پوشش دهد.
- پوشش ارائه داده شده برای هزینه‌های بازسازی داده‌ها را ارزیابی کنید. بسیاری از سیاست‌های بیمه سایبر پوشش هزینه‌های مربوط به جایگزینی، ارتقاء یا نگهداری سیستم کامپیوتری را که نقض شده است پوشش نمی‌دهد. هزینه‌های ترمیم داده‌ها به طور بالقوه مبهم هستند. هر شرکتی که با ریسک نقض اطلاعات مواجه است باید اقدامات لازم را انجام دهد تا اطمینان حاصل شود که پوشش اخذ شده هزینه‌های وقفه کسب‌وکار شرکت را در موقعیتی که قبل از نقض آن بود، پوشش می‌دهد.
- بسیاری از حرفه‌ای‌ها امروز در رایانه‌ها و تبلت‌ها در خارج از دفتر کار می‌کنند. اگر چه بسیاری از شرکت‌ها لپ تاپ‌های متعلق به شرکت را رمزگذاری می‌کنند، کامپیوتر شخصی و دستگاه‌های ذخیره سازی متعلق به آن‌ها نیستند. برای شرکت‌هایی که از طریق کامپیوتر شخصی فعالیت انجام می‌دهند، مهم است که بیمه‌ای را خریداری کنند که این ویژگی را پوشش دهد.
- پوشش برای اقدامات مقرراتی در نظر بگیرید. از دست دادن اطلاعات می‌تواند نه تنها منجر به از دست دادن اطلاعات شود، بلکه می‌تواند منجر به اقدامات نظارتی در برابر شرکت شما شود. سازمان‌های دولتی و فدرال در پاسخ به از دست دادن داده‌ها و نقض حریم خصوصی فعال‌تر شده‌اند. شما باید در نظر بگیرید که آیا بیمه شرکت شما پوشش برای تحقیقات قانونی یا یک اقدام قانونی ناشی از حادثه سایبری را پوشش می‌دهد.

حق بیمه برای بیمه سایبری می‌تواند به طور گسترده‌ای متفاوت باشد. گاتنر. ای.ان.سی، اخیراً گزارش داد که حق بیمه سایبری از ۱۰،۰۰۰ دلار به ۳۵،۰۰۰ دلار برای ۱ میلیون دلار پوشش می‌دهد. در حالی که پوشش بیشتری نیز در دسترس است، بیمه گذاران همچنان به درک خود در مورد خطرات اینترنتی ادامه می‌دهند.[۱]

۲-۴ نیازهای ایجاد بیمه مجازی

چه کسانی نیازمند بیمه سایبری می‌باشند؟ در حقیقت، هرکسی که میزبان یک وب سایت است و با عموم ارتباط برقرار می‌کند، یک نامزد برای بیمه مسئولیت سایبری است. این شامل کسب‌وکارهای تجاری و دارندگان وب سایت هم می‌شود.

اگر بخشی از کسب‌وکار خود را به صورت آنلاین انجام می‌دهید یا از مشتریان می‌خواهید تا با اطمینان کامل به شما یا فروشنده ثالث اعتماد کنند، باید به طور جدی خرید بیمه سایبر را در نظر بگیرید. خرید تمام انواع بیمه - ماشین، خانه، سیل، آتش - یک عمل معمول است. این موارد در صورت وقوع حادثه، دارایی‌های فیزیکی را حفظ می‌کنند؛ اما در مورد دارایی‌های دیجیتال چگونه؟ با حرکت به سمت تحول دیجیتال، دارایی‌ها به آرامی، اما به طور پیوسته به دنیای دیجیتال منتقل می‌شوند. حملات سایبری و نقض آن می‌تواند برای کسب و کار زیان آور باشد و اغلب از دست دادن مجدد آن‌ها بسیار خطرناک است؛ بنابراین بیمه سایبری در جهان امروز ضروری است.

همانطور که کسب‌وکارها بیشتر به تکنولوژی وابسته می‌شوند، خطر رنج از دست‌دادن مربوط به مشکلات سیستم‌های کامپیوتری و یا نگه‌داشتن اطلاعات حساس مشتری همچنان رشد می‌کند. بیمه فضای مجازی نمی‌تواند سازمان شما را از جرائم اینترنتی محافظت کند، اما می‌تواند کسب‌وکار شما را بر اساس پایه مالی حفظ کند. فناوری، رسانه‌های اجتماعی و معاملات آنلاین نقش کلیدی در تجارت سازمان‌ها ایفا می‌کنند و همچنین نکته قابل توجه این است که این امکانات و وسایل تجارت الکترونیک خود می‌توانند نقش دروازه‌ای برای حملات سایبری باشند.

سازمان‌ها بر اساس طرح مدیریت ریسک خود تصمیم می‌گیرند کدام ریسک‌ها را، اجتناب و یا کاهش دهند و در رویه‌های مالی ریسک را نگه داری کنند و یا انتقال دهند. بیمه یک ابزار مدیریت ریسک است که از طریق انتقال ریسک یا تسهیم آن، ریسک‌های سازمان، افراد و بنگاه‌ها را مدیریت می‌کند. حال اگر رویه سازمان انتقال ریسک باشد، نیاز به بیمه فضای مجازی برای انتقال ریسک ناشی از حملات سایبری را دارد.

۲-۵ مدل بررسی ریسک سایبری

تهدیدهای سایبری یکی از بزرگترین تهدیدات امروز است، بیمه گران نیاز به درک خطر مالی و احتمالی انباشت ریسک را دارند بدون یک استاندارد اطلاعات یا مکانیسم واحد، درک ریسک کاری دشوار است. ریچارد متیو استالمن[۲] (آر.ام.اس) در فوریه سال ۲۰۱۶، آن را به یک سیستم مدیریت محتوا[۱] که یک

---

[1] (A buye`s Guide to cyber Insurance, 2013)
[2] Richard Matthew Stallman (RMS)

استاندارد برای اطلاعات در معرض خطر سایبری به عنوان اولین مدل برای درک مبتنی بر ریسک ارائه و منتشرکرد. این سیستم توسط بسیاری از فعالین سایبری پیشرو در سراسر بازار به تصویب رسید است. در ماه مه سال ۲۰۱۷ آر.ام.اس یک نسل دوم سایبر تولید کرد که بالغ بر ۱۴ ماه تحقیق و توسعه وسیع در مورد در معرض خطر قرار گرفتن سایبری و اجزای اساسی آن است. این به روزرسانی، پیشرفت‌های قابل توجهی را برای مدل‌های خطرناک سایبری ارائه می‌دهد و بینش‌های جدیدی را در مجموعه‌ای از وقایع احتمالی سایبر فراهم می‌آورد.[۲].

کریستر پرسن[۳]، مدیر عامل توسعه مشتری در آر.ام.اس، اذعان نمود: «جمع‌آوری مخاطرات سایبری بسیار پیچیده است و از نظر جغرافیایی محدود نیست، بر خلاف خطراتی مانند طوفان و زلزله.»

وب دارای تأثیرات و ضررهای بالقوه بسیار زیاد است و بیمه‌گرها به طور فزاینده‌ای در مورد انباشت روبه‌رشد در خط مشی کسب‌وکار بیمه سایبری با مشکل روبه‌رو کرده است و سیستم مدیریت سایبر انباشت آر.ام.اس[۴] آن‌ها را قادر می‌سازد تا این انباشت را درک و کنترل کند تا امکان ارائه بیمه سایبر به عنوان یک خط جدید کسب و کار را به حداکثر برساند."

پیشینه تاریخی محدود برای این خطرات، باعث می‌شود که بیمه گران برای تعیین سطح ظرفیت خود آن را به چالش بکشند. بدون درک ارزشمندی رویدادهای سایبر که توسط سیستم مدیریت انباشت سایبری ارائه شده است، بسیاری از بیمه گران باید دیدگاه محافظه کارانه را در مورد خطر در نظر بگیرند، زیرا قادر به تعیین حداکثر ضرر احتمالی برای فاجعه‌های سایبری نیستند. این می‌تواند خط مشی بالقوه رشد سودآوری کسب‌وکار و همچنین مدیریت کارآمد سرمایه شرکت را محدود کند و خطری جدی محسوب شود.

مدیریت سایبر انباشت آر.ام.اس دارای شیوه داده‌های منبع باز خورد است که یک رویکرد مشترک برای در معرض خطر قرار گرفتن را فراهم می‌کند. در این طرح داده‌ها به طور فزاینده‌ای به عنوان استاندارد بازار برای خطر سایبری در نظر گرفته شده است و با بیش از ۲۰ بیمه سایبری که در حال حاضر از آن استفاده می‌کنند، به تصویب رسیده است. سیستم مدیریت انباشت سایبر آر.ام.اس همچنین گزارشات نظارتی را کاهش می‌دهد، هزینه‌های مازاد بیمه‌گران را نیزکاهش می‌دهد. مدل جدید همچنین شامل تغییرات قابل توجه و به روزرسانی در مورد سناریوهای معتبر سایبری آن است که شامل تغییر الگوهای نمونه برداری از داده‌ها می‌شود. مدل جدید همچنین شامل سناریوهای فیزیکی اینترنتی مانند آتش سوزی و انفجارهای ناشی از هکرها می‌شود و این شامل ارزیابی مواجهه‌های خاموش در برخی از سیاست‌هایی است که در مورد حملات سایبری مبهم است.[۵]

آر.ام.اس سناریوهای انباشتی را بررسی می‌کند که چقدر ممکن است یک نمونه بیمه شدت داشته باشد و به مدیران کمک می‌کند تا مواجه خود را زیر مجموعه‌ای از این چارچوب ریسک پذیری قرار دهند. تعریف

---

[1] CMS
[2] (Managing cyber insurance accumulation rick, 2016)
[3] Christen Pehrson
[4] RMS Cyber Accumulation QBE
[5] (Amerding, 2017)

حداکثر ضرر برای بیمه‌های سایبری چالش برانگیز است. تاریخچه این نوع حملات کوتاه است و همانطورکه تهدید به سرعت در حال تحول است، حتی تجربیات چند سال پیش هم کاربرد خود را به عنوان چشم انداز ریسک فعلی از دست می‌دهند.

ماهیت سیستماتیک خطر سایبری با شواهدی از قبیل آلودگی گسترده نرم افزارهای مخرب در جمعیت کم کامپیوترهای امن آشکار است اما هنوز از دست دادن یک سیستم عامل واقعاً وجود ندارد. بسیاری از ادعای بزرگ از بیمه ناشی از یک دلیل واحد «تجربه شده توسط صنعت بیمه» است. در عوض سناریوهای انباشتی آر.ام.اس نیاز به الگویی مبتنی بر شواهد از پتانسیل تلفات و ارزیابی محدودیت‌های واقع گرانه به میزان تأثیرات سیستماتیک هر فرآیند مخرب دارد. جدول زیر ارائه دهنده‌ی چارچوبی برای مدیریت ریسک انباشته می‌باشد.

جدول ۴ ماتریس تحلیل ریسک

Cyber Loss Process:	Data Exfiltration	Denial-of-Service	Cloud SP Failure	Financial Theft	Cyber Extortion
Accumulation Scenario:	Leakomania	Mass DDoS	Cloud Compromise	Financial Transaction Interference	Extortion Spree
Insurance Coverage Category					
Breach of privacy event	3	1	2	1	1
Data and software loss	3	2	2	1	2
Incident investigation and response costs	1	1	1	1	1
Liabilities	2	2	2	2	1
Financial theft	2		1	3	1
Business interruption	1	3	3	1	2
Cyber extortion	1	2	1	1	3
Intellectual Property (IP) theft	1		1		1
Impact on reputation	2	2	1	2	2

3	Potentially High Impact
2	Potentially Significant Impact
1	Potentially Some Impact
	No Impact Likely

در جدول ۴، سناریوهای از دست دادن سایبر که بیشترین تأثیر را بر روی کسب و کارها و همچنین بسیاری از دسته‌های معمول پوشش که در بازار بیمه مسئولیت سایبری ارائه می‌شود، در نظر گرفته شده است. این پنج فرآیند از دست دادن سایبر نه تنها فرآیندهای است که می‌تواند باعث آسیب اینترنت شود، بلکه پیشرو در فرآیندهای آسیب سایبری می‌باشند و چارچوبی برای تولید انواع تست‌های مدیریت انباشته برای نمونه کارها را فراهم می‌کنند. علت داده‌های از دست رفته است که قابل تمرکز برای فهم مدیریت ریسک‌های بیمه سایبر بوده است نه نحوه‌ی فرآیند از دست دادن داده‌ها. از نکات حائز اهمیت از دست رفتن سایبر، این است که تعداد زیادی ادعا از یک علت اصلی ایجاد می‌شود. این ممکن است به «درآمد ناشی از»

خطاهای خاص در سایر نمونه‌های بیمه مشابه باشد و این امر برای بیمه‌گران منطقی خواهد بود که فرایندهای از دست دادن سایبر را که به عنوان دسته‌های اصلی از علل از دست دادن سایبر شناسایی شده‌اند، در نظر بگیرند و به طور بالقوه بر اساس این کدها مدیریت ریسک‌های خود را نشان دهند، اما در یک فرایند از دست دادن سایبر، ممکن است یک فاجعه سایبری را تجربه کنید که در آن تعداد زیادی از ادعاها به هم وابسته هستند، زیرا آن‌ها از یک علت مشترک هستند.

علل وابستگی عبارتند از:

- آسیب پذیری در سیستم‌های فناوری اطلاعات باعث آسیب گسترده در بسیاری از شرکت‌های می‌شود.
- مجرمان از منابع یا تکنیک‌هایی استفاده می‌کنند که می‌توانند حملات خود را در تعداد زیادی از شرکت‌های هدف مورد بررسی قرار دهند.

نمونه از طبقه بندی سازمان‌های بیمه گذار:

- بخش کسب‌وکار و فعالیت
- مالیات شرکت
- اندازه شرکت
- تعداد کارکنان
- تجربه تاریخی رویدادهای سایبری
- وابستگی تجاری به فناوری اطلاعات
- حجم معاملات آنلاین (برخط)
- تعداد پروژه‌های مرتبط با عموم مردم

میزان تأثیر:

- بدون تأثیر
- اثرات کم
- تأثیرات بالقوه قابل توجه
- تأثیرات بالقوه بالا

فرآیندهای مدیریت ریسک:

- مدیریت روانشناسی ریسک سازمان
- طراحی پاسخ حادثه
- مقررات و انطباق پی.سی.ای[1]
- رویه فسق قرارداد با کارمندان
- تعیین روش‌های دسترسی از راه دور
- آگاهی و آموزش کارمندان درمورد امنیت فناوری اطلاعات

[1] PCI Local Bus

۲-۶ مشکلات بیمه‌گذار فضای مجازی و راه حل‌های آن

۲-۶-۱ عدم توانایی تعیین دقیق مبلغ بیمه‌نامه به دلیل کمبود اطلاعات کافی در مورد داده‌های سایبری

اکثر شرکت‌ها طبق قانون اجباری به افشای حملات سایبری در حیطه شرکت خود مگر مرتبط با مصرف‌کننده ندارند و به این ترتیب بسیاری از حملات اینترنتی گزارش نشده‌اند؛ بنابراین صنعت بیمه با گزارش‌های شایع یکطرفه و غیرمنصفانه مواجه می‌باشد که تبیین سیاست‌گذاری را برای آن سخت و همراه با مشکل می‌کند.

راه حل: برای غلبه بر این مشکل بیمه‌گران می‌توانند مدل‌های پیش‌بینی ریسک را به جای مدل‌های پیش‌بینی قطعی و تجزیه اطلاعات در سراسر صنعت بیمه به منظور بهینه‌سازی بیمه‌نامه تحت پوشش قرار دهند.

۲-۶-۲ انباشت فاجعه‌آمیز حملات سایبری

ممکن است برخی از بیمه‌گران ترس از مواجه با تجمیع ناگهانی تلفات را داشته باشند. به طور مثال بیمه‌گر با یک سرویس شخص ثالث که با طیف وسیعی از کسب‌وکار، کار می‌کند و این سرویس مورد حمله قرار گیرد و منجر به توقف خدمات برای همه کاربران آن شود. این نوع رویداد سیستماتیک می‌تواند منجر به هرج‌ومرج برای بیمه‌گران شود.

راه حل: بیمه‌گذاران باید سیاست‌های تضمین قانونی دقیق‌تری را آغاز کرده تابه حداقل رساندن خطر تجمیع، کمک کنند.

۲-۶-۳ تضعیف قابلیت پیش‌بینی در معرض خطر قرارگرفتن به دلیل تکامل مداوم ریسک‌ها

در این زمینه قرارگرفتن در معرض خطر به‌طور مداوم تغییر پیدا می‌کند. بیمه‌گران تنها به یک نوع حمله سازگارند و در این حوزه بیمه‌گر به طور مداوم با پیشرفت تکنولوژی و به تبع تکامل خطرات آن مواجه است. در نتیجه مدیریت ریسک با این مشکل که قابل پیشگیری می‌باشد، مواجه است. در عمل نوآوری‌ها در کسب‌وکار مانند IOT[1] فرصت‌های جدید برای حمله سایبری فراهم می‌کنند که باید مورد ارزیابی و بیمه قرار بگیرند.

راه حل: کلید اصلی آن برای پیشگیری می‌تواند در تبدیل شدن به یک مدیر کامل ریسک سایبر و همچنین طریقه اصلی انتقال ریسک باشد.

۲-۶-۴ دید محدود بیمه‌گذاران و محدودیت محصولات بیمه سایبری

بسیاری از بیمه‌گران در هنگام نوشتن سیاست‌های سایبری، دید تونلی دارند و تمرکز اصلی آنان بر روی بازاریابی سایبر برای شناسایی اطلاعات هک و نادیده گرفتن بسیاری از دیگر مخاطرات سایبری که

[1] Internet Of Things

شرکت با آن مواجه است. این پوشش به سرعت در حال تبدیل شدن به کالا، حساس به قیمت، محدود کردن رشد بلند مدت بیمه‌گران و پتانسیل سود است.

راه حل: برای مقابله بیمه‌گران می‌توانند محصولات را در حین افزایش آگاهی ریسک در میان خریداران متمایز کنند.

۲-۶-۵عدم استانداردسازی در تعیین و تهیه ریسک‌های اینترنتی

پوشش سایبری اغلب از طریق سیاست‌های سفارشی نوشته می‌شوند و اصطلاحات مختلفی از حامل به دستگاه کاربر وارد می‌شود. به نظر می‌رسد شکاف‌های احتمالی پوشش بیمه دلیل اصلی نگرانی بسیاری از کسب‌وکارهایی است که نیاز به بیمه سایبری دارند.

راه‌حل: بیمه‌گذاران می‌توانند با همکاری با یکدیگر برای ایجاد سیاست استاندارد شده برای این مشکل غلبه کنند.

۲-۶-۶ عدم درک کامل اغلب خریداران بیمه از خطرات سایبری و یا گزینه‌های بیمه نامه

نه فقط خریداران ساده لوحی که در حال اجرا کسب و کارهای کوچک‌اند بلکه اغلب بیمه‌گذاران حتی از خطرات سایبری آگاه نیستند و راه مقابله با آنان را نمی‌دانند، چه رسد به گزینه‌های پوشش بیمه.

راه حل: صنعت بیمه باید در ایجاد مصرف‌کنندگان تحصیل کرده بهتر عمل کند که در نتیجه باعث تشویق بیشتر شرکت‌ها برای اجرای برنامه‌های مدیریت ریسک و خرید پوشش می‌شود، یک راه برای انجام این کار افزایش تلاش‌های تبلیغاتی مستقیم از طریق بازاریابی و تبلیغات است. بیمه‌های سایبری می‌توانند با آگاهی دادن نسبت به انواع ریسک و کنترل خطر، از عوامل و کارگزاران حمایت کنند. این می‌تواند شامل؛ بروشورها، وب سایت‌ها و پادکست‌ها و همچنین ارجاعات به متخصص امنیت سایبری باشد.

۲-۶-۷جریان قانونی و نظارتی

قانون درمورد پوشش سایبر هنوز واضح و روشن نیست. از آنجایی که منازعات پوشش سایبری از طریق سیستم دادگاه به راه خود ادامه نداده است، خریداران از ادعای تعهدات متضاد به دلیل اختلاف نظر در مورد سیاست‌های اعمال شده و سیاست پوشش متفاوت، نگران می‌باشند. علاوه براین، مقررات دولتی اغلب بیش از حد و یا متناقض می‌باشند که منجر به ایجاد شکاف پوشش می‌شود.

راه حل: ایزو[1] اشاره کرد که استانداردسازی اصطلاحات و سیاست‌ها می‌تواند به جلوگیری از اختلافات پوشش و دادرسی طولانی و هزینه‌های آن، کمک کند. در دراز مدت، استانداردسازی موارد اختلافات احتمالی پوشش را کاهش می‌دهند که ادعای هزینه‌های مدیریت برای بیمه‌گران و تضعیف اعتماد مصرف‌کننده را از بین می‌برد.[2]

---

[1] IOS
[2] (Jayleen, 2017)

۲-۷ فواید اقتصادی بیمه سایبر

- بیمه منجر به افزایش سطح سرمایه گذاری امنیتی، افزایش سطح ایمنی اطلاعات می‌شود.
- تسهیل استانداردها و ارائه مدل‌های امنیتی برای ریسک انسان به بهترین شیوه ممکن
- ایجاد یک بازار بیمه فضای مجازی

در نهایت می‌توان نتیجه گرفت که بیمه سایبر منجر به افزایش رفاه عمومی اجتماعی می‌شود.

۲-۸ حوزه‌های کشورهای پیشرو در صنعت بیمه

شرکت محافظت سایبری آلیانز

حوزه‌های پوششی:

نقض پوشش داده‌ها برای داده‌های شخصی و شرکت

هزینه‌های نقض اطلاعات از جمله هزینه‌های اطلاع رسانی و گزارش تحقیقات فناوری اطلاعات

تعهد امنیت شبکه برای سیستم‌های هک شده یا به خطر افتاده مانند انکار حملات

تعهد رسانه‌ها برای نشریات دیجیتال

وقفه‌های کسب و کار ناشی از حمله سایبری

هزینه‌های بازیابی برای داده‌ها و برنامه‌ها ناشی از وقفه کسب و کار مجازی

بیان بحران برای کاهش آسیب اعتباری

پوشش سرقت هکر براساس سرقت پول

تعهد وجه پرداختی پول الکترونیکی؛ برطبق جریمه‌های نقدی محدوده گسترده فضای مجازی و پوشش‌های حریم خصوصی با عبارات شفاف و روشن فرآیند سریع و آسان بدون نیاز به بررسی ریسک

شرکت بیمه سایبر وان اچ اس بی

پوشش‌های این شرکت شامل پوشش تعهد بدهی شخص ثالث است. پوشش بیمه شخص ثالث می‌تواند با ارائه «یک دادخواست الزام به انجام تعهد امنیت شبکه‌ای» به دست آید. اقدام مدنی، یک فرایند ثانویه حل اختلاف یا یک درخواست کتبی برای دریافت پول است که درآن ادعا ضعف سیستم امنیتی رایانه بیمه شده ارائه شد و منجر به یکی از رخدادهای ذیل می‌شود: نقض اطلاعات حرفه شخص ثالث، انتشار ناخواسته بدافزارها، انکار حمله‌ای که در آن فرد بیمه شده ناخواسته حضور داشته است.

در صورت پیگیری دادخواست الزام انجام تعهد امنیت شبکه، بیمه سایبر وان اچ اس بی هزینه‌های حمایتی، قضاوت قضایی را پوشش می‌دهد. هزینه حمایتی ارائه شده در محدوده‌های تحت پوشش بیمه و بیمه تحت پوشش شخص ثالث می‌تواند مستقل از بیمه پوششی شخص اول عرضه شود.

بیمه نامه تخصصی تعهد اینترنتی این شرکت به منظور حافظت از بیمه گذار در برابر خطرات بیشمار یک حمله هدفمند سایبری طراحی شده است که شامل خدماتی ازجمله دسترسی به خط تلفن پاسخ گو اینترنتی کارشناسان امنیت اطلاعات می‌باشد و درزمینه های که در زیر به آنها اشاره شده از بیمه گذار حمایت می‌کند:

هزینه‌های بازگرداندن داده‌ها و تجهیزات، مطلع کردن مشتریان، برآورده کردن تقاضاهای باج گیری، هزینه‌های دفاع حقوقی و خساراتی که باید قانوناً به دیگر اشخاص، توسط بیمه گذار پرداخت شود.

پوشش خطرات سایبری مارکل

پوشش بیمه سایبری به طورانحصاری تنها با سیاست‌های شرکت بیمه مارکل حاصل می‌شود که در زیر به آن‌ها اشاره شده است:

خطرات حرفه‌ای (از جمله رسانه، فناوری و حرفه‌های گوناگون) خطرات رفاه اجتماعی، مراقبت و خیریه، خطرات زیست پزشکی و علوم زیستی.

۲-۹ بیمه در ایران

علی رغم گسترش بیمه مجازی در سراسر دنیا به خصوص کشورهای پیشرفته، متأسفانه این نوع بیمه در ایران در حال حاضر جایگاهی در بیمه کشور ما ندارد. شرکت‌های بیمه‌ای بسیاری در این زمینه در دنیا مشغول به فعالیت هستند تا مخاطرات و ریسک‌های فضای مجازی را کاهش دهند.

در ایران، بیمه مرکزی که زیرنظر تأمین اجتماعی فعالیت می‌کند، موظف به برنامه ریزی بیمه‌ای می‌باشد به این نحو که بیمه مرکزی لایحه فعالیت‌های خود را به تأمین اجتماعی می‌دهد و از این طریق وارد مجلس می‌شود و راجع به آن تصمیم گیری می‌شود، سپس به اجرا در می‌آید.

به گفته سعید صحت، یکی از کارشناسان بیمه مرکزی، به دلیل عدم گسترش فضای مجازی در ایران نسبت به کشورهای پیشرفته، نه تنها در زمینه بیمه مجازی کاری صورت نگرفته است بلکه در زمینه‌های دیگه از بیمه هم کار خاصی نشده است. اکثر فعالیت‌های بیمه‌ای در ایران حول بیمه عمر یا حوادث می گردد، زیرا فعلاً سرمایه گذاری‌ها بیشتر در این زمینه تجمع یافته است. با توجه به عدم فعالیت بیمه مرکزی در این زمینه، متأسفانه قانون یا لایحه‌ای در مجلس تصویب نشده است. فقط در قانون مجازات اسلامی در بخش جرائم رایانه‌ای، مجازاتی برای جرائم در فضای مجازی در نظر گرفته شده است که با گسترش روزافزون فضای مجازی در همه زمینه‌های کاری و اجتماعی، کافی به نظر نمی‌رسد و برای فعالیت‌های مجازی مصونیت قطعی به عمل نمی‌آورد و شرکت‌ها را با فضای اطمینان مواجه نمی‌سازد.

با توجه به گسترش فضای مجازی و گسترش زمینه کاری در فضای مجازی، الزام قانون گذاری و فعالیت در این زمینه در ایران ضروری به نظر می‌رسد تا با کاهش ریسک فعالیت در فضای مجازی، زمینه ورود شرکت‌ها و افراد به این زمینه هموار شود.

وی افزود: یکی از دلایل عدم گسترش بیمه مجازی، عدم امنیت سایت‌ها و فضای مجازی در ایران است. برای مثال سیستم‌های امنیتی و اینترنتی در ایران در مواجهه با هک و سایر خطرات سایبری بسیار ضعیف و ناامن است، بنابراین بیمه کردن فضای مجازی در ایران، هزینه‌های گزافی برای شرکت‌های بیمه ایجاد می‌کند. در کنار عدم امنیت فضای مجازی، عدم اطمینان به کارهای مجازی و الزام عرفی به انجام امور به صورت حضوری، مردم و شرکت‌های بیمه‌ای، تمایلی برای حضور و فعالیت در زمینه مجازی ندارند جز برخی از شرکت‌ها که تنها به ارائه بیمه نامه به صورت مجازی و غیر حضوری بسنده کردند.

یکی دیگر از دلایل عدم گسترش بیمه مجازی، رقابتی که بین شرکت‌ها برای فروش و بیمه وجود دارد و مانع از گسترش این زمینه می‌شود زیرا گسترش بخش مجازی برای این شرکت‌ها هزینه‌بر و موجب کاهش سودشان می‌شود و در بلندمدت به دلیل نداشتن فناوری لازم، مجبور به ترک بازار و فضای اقتصادی خواهند شد.

همانطور که بالاتر ذکر شد، در بیمه مرکزی و مرکز پژوهش‌های بیمه و شرکت‌های بیمه‌ای، هیچ گزارشی از فعالیت در این زمینه منتشر نشده است و در مجلس شورای اسلامی نیز تنها به بخش حقوقی و مجازات بعضی از جرائم در این زمینه فعالیتی شده است که کافی نمی‌باشد زیرا مجازات تعیین شده در مقابل آسیب‌ها و خسارت‌هایی که ممکن است وارد بشود، تاثیری ندارد.

دکتر عربی، کارشناس سازمان مدیریت و برنامه ریزی بودجه کشور؛ «می‌توان این نکته را ذکر کرد که صنعت بیمه در ایران هنوز پیشرفت چشمگیری نداشته و به دلیل سود بیمه‌های عمر و حوادث، تلاش‌ها به سمت گسترش و پیشرفت در این زمینه‌ها بوده است. در کنار پیشرفت انواع بیمه در کشورهای اروپایی، کشورهای اسلامی در زمینه تکافل کار کرده‌اند و پیشرفت‌های چشمگیری هم داشته‌اند. به دلیل عدم مشکل بیمه از منظر فقه امامیه، خروجی در زمینه تکافل نداشته‌ایم و متأسفانه سودگرایی مانع پیشرفت بیمه در ایران شده است».

۳- وضعیت ایران در بیمه فضای مجازی و چالش‌ها

۳-۱ بیمه فضای مجازی در ایران

علی رغم گسترش بیمه مجازی در سراسر دنیا به خصوص کشورهای پیشرفته، متأسفانه این نوع بیمه در ایران در حال حاضر جایگاهی در صنعت بیمه کشور ما ندارد. شرکت‌های بیمه‌ای بسیاری در این زمینه در دنیا مشغول به فعالیت هستند تا مخاطرات و ریسک فضای مجازی را کاهش دهند.

در ایران، بیمه مرکزی که زیرنظر تأمین اجتماعی فعالیت می‌کند، موظف به برنامه‌ریزی بیمه‌ای می‌باشد به این نحو که بیمه مرکزی لایحه فعالیت‌های خود را به تأمین اجتماعی می‌دهد و از این طریق وارد مجلس می‌شود و راجع به آن تصمیم‌گیری می‌شود، سپس به اجرا در می‌آید.

به گفته سعید صحت[1]، یکی از کارشناسان بیمه مرکزی، به دلیل عدم گسترش فضای مجازی در ایران نسبت به کشورهای پیشرفته، نه تنها در زمینه بیمه مجازی کاری صورت نگرفته است بلکه در زمینه‌های دیگر از بیمه هم کار خاصی نشده است و از کشورهای دیگر در این زمینه هم عقب افتادیم. اکثر فعالیت‌های بیمه‌ای در ایران حول بیمه عمر یا حوادث می‌گردد، زیرا فعلاً سرمایه‌گذاری‌ها بیشتر در این زمینه تجمع یافته است. با توجه به عدم فعالیت بیمه مرکزی در این زمینه، متأسفانه قانون یا لایحه‌ای در مجلس تصویب نشده است. فقط در قانون مجازات اسلامی در بخش جرائم رایانه‌ای، مجازاتی برای جرائم در فضای مجازی در نظر گرفته شده است که با گسترش روزافزون فضای مجازی در همه زمینه‌های کاری و اجتماعی، کافی به نظر نمی‌رسد و برای فعالیت‌های مجازی مصونیت قطعی به عمل نمی‌آورد و شرکت‌ها را با فضای اطمینان مواجه نمی‌سازد.

با توجه به گسترش فضای مجازی و گسترش زمینه کاری در فضای مجازی، الزام قانون‌گذاری و فعالیت در این زمینه در ایران ضروری به نظر می‌رسد تا با کاهش ریسک فعالیت در فضای مجازی، زمینه ورود شرکت‌ها و افراد به این زمینه هموار شود.

وی افزود: یکی از دلایل عدم گسترش بیمه مجازی، عدم امنیت سایت‌ها و فضای مجازی در ایران است. برای مثال سیستم‌های امنیتی و اینترنتی در ایران در مواجهه با هک و سایر خطرات سایبری بسیار ضعیف و ناامن است، بنابراین بیمه کردن فضای مجازی در ایران، هزینه‌های گزافی برای شرکت‌های بیمه ایجاد می‌کند. در کنار عدم امنیت فضای مجازی، عدم اطمینان به کارهای مجازی و الزام عرفی به انجام امور به صورت حضوری، مردم و شرکت‌های بیمه‌ای، تمایلی برای حضور و فعالیت در زمینه مجازی ندارند جز برخی از شرکت‌ها که تنها به ارائه بیمه نامه به صورت مجازی و غیرحضوری بسنده کردند.

رقابتی که بین شرکت‌ها برای فروش و بیمه وجود دارد، مانع از گسترش این زمینه می‌شود زیرا گسترش بخش مجازی برای این شرکت‌ها هزینه بر و موجب کاهش سودشان می‌شود و در بلندمدت به دلیل نداشتن فناوری لازم، مجبور به ترک بازار و فضای اقتصادی شوند.

---

[1] کارشناس مرکز پژوهش بیمه مرکزی و استاد دانشگاه
عضو هییت علمی دانشگاه علامه طباطبایی تهران

در قانون مجازات اسلامی، بخش جرائم رایانه‌ای، مجازاتی برای متخلفین فضای مجازی در نظر گرفته شده است و بدین ترتیب قسمتی از نگرانی‌های فعالین بخش مجازی را کاهش می‌دهد اما مجازات تعیین شده در مقابل آسیب‌ها و خسارت‌هایی که ممکن است وارد بشود، کافی و مانع نمی‌باشد. قانون گذاران نباید صرفاً به افزایش مجازات توجه کنند و آن را تنها اهرم خود برای جلوگیری از جرائم و خسارات بدانند بلکه از طریق وضع قوانین جامع‌تر به مقابله با ناامنی در فضای مجازی بروند.

دکتر عربی[1] در ارتباط با صنعت بیمه در ایران بیان داشتند: می‌توان این نکته را ذکر کرد که صنعت بیمه در ایران هنوز پیشرفت چشمگیری نداشته و به دلیل سود بیمه‌های عمر و حوادث، تلاش‌ها به سمت گسترش و پیشرفت در این زمینه‌ها بوده است. در کنار پیشرفت انواع بیمه در کشورهای اروپایی، کشورهای اسلامی در زمینه تکافل کار کرده‌اند و پیشرفت‌های چشمگیری هم داشته‌اند. به دلیل عدم مشکل بیمه از منظر فقه امامیه، خروجی در زمینه تکافل نداشته‌ایم و متأسفانه سودگرایی مانع پیشرفت بیمه در ایران شده است.

برای پیشرفت در زمینه بیمه مجازی، لازم است که شرکت‌های بیمه، زیرساخت‌های خود را تغییر دهند و از لحاظ ابزار و علم بیمه از کشورهایی که در این زمینه فعالیت دارند الگو بگیرند و تغییراتی را در ساختار بیمه ایجاد کنند، اما این تغییرات که اولین تأثیر خود را در افزایش هزینه بیمه و سپس در کاهش رغبت مردم به بیمه کردن نشان می‌دهد، موجب جایگزین کردن شرکت‌های بیمه و کاهش سود شرکت‌های بیمه می‌شود که یکی دیگر از عوامل عدم پیشرفت بیمه در ایران است. در ضمن دولت و مجلس نیز باید در این زمینه با شرکت‌های بیمه همکاری داشته باشند که متأسفانه اقدامی از طرف دولت‌مردان صورت نگرفته است تا مردم و شرکت‌های بیمه‌ای رغبتی به زمینه بیمه مجازی پیدا کنند که یکی از علل آن عدم احساس نیاز به ورود در این زمینه است و علت دیگر عدم تحقیق و پیشنهاد کارها از سوی بیمه مرکزی به مجلس است.

۳-۲ چالش‌های صنعت بیمه فضای مجازی

۳-۲-۱ عدم وجود پیشینه تاریخی حوادث

بزرگ‌ترین چالش بیمه‌گران عدم وجود اطلاعات مربوط به حوادث امنیتی سایبری است که این اطلاعات باعث فراهم شدن شناخت بیشتر مشتریان بر اساس خطر می‌شود و همچنین منجر به ایجاد حمایتی برای ارزیابی ریسک است. اطلاعات بسیار کم واقعیت‌های سایبری را به خوبی منعکس نمی‌کنند. بیمه‌گذاران در تلاش برای جمع آوری جداول مورد نیاز برای ساخت و قیمت پوشش‌های سایبری هستند. تأسیس پایگاه داده‌های مخفی برای حوادث سایبر، به بیمه‌گران کمک خواهد کرد تا خطر بیشتری را درک کنند و پوشش بیشتری را ارائه دهند جمع‌آوری اطلاعات مفید فعلی شامل سوابق آماری به بیمه‌گران اجازه

[1] کارشناس بخش اقتصاد کلان سازمان مدیریت و برنامه ریزی بودجه کشور

خواهد داد برای ارزیابی احتمال از آن استفاده کنند. همانند سیاست‌های پوشش بیمه زندگی، اتومبیل و... (cyber Insurance: Recent Advances, good practices and challenges, 2016)

۳-۲-۲عدم توانایی تعیین دقیق قیمت بیمه نامه

چالش دیگر که بیمه‌گر با آن روبه‌رو است تعیین قیمت دقیق بیمه‌نامه است تا از این طریق بتواند تقاضای بازار را جواب دهد بیمه‌گران مشغول به کار در زمینه بیمه سایبری، به دنبال اطلاعاتی جدید هستند تا از آن‌ها در ایجاد الگوهای ریسک کامپیوتری کمک بگیرند. هدف آن‌ها تعیین دقیق قیمت انواع پوشش های سایبر است تا تقاضا برآورده شود؛ و همچنین هزینه‌های تخمین زده شده برای زیان‌ها بسیار پایین‌تر از کل حق بیمه جمع‌آوری شده در طول زمان باشد. (Filkins, 2016)

بنابراین بیمه‌گران می‌خواهند به طور کامل درک کنند که چگونه شرکت‌ها مورد حمله قرار می‌گیرند. آن‌ها به ویژه می‌خواهند بدانند که سازمان‌های امنیت اطلاعات چه کاری انجام می‌دهند تا دزدان اطلاعات، جاسوسان، مجرمان، افراد غیر مجاز و گروه‌های مخالف را دفع کنند. دقیق‌تر، آن‌ها حملات را درک می‌کنند در نتیجه می‌توان از دانش آن‌ها در این زمینه برای بالا بردن دقت و اتخاذ سیاست‌هایی کاربردی‌تر و حق بیمه‌های معین استفاده کرد. با داده‌های تاریخی اندکی که در دسترس است، ممکن است لازم باشد برای ارزیابی خطر از داده‌هایی که نشان دهنده خطر در آینده است، طراحی شود.

۳-۲-۳ تجمع ریسک

یکی از دشواری‌های این حوزه وابستگی سیستمی می‌باشد. در صورت هرگونه نفوذ به سیستم احتمال آسیب به کل آن و گسترده شدن خطر نیز وجود دارد. «طوفان کامل» یکی دیگر از بزرگترین ترس‌های بیمه‌گران و افسران اطلاعات امنیت است. خطر «تجمع» یا طوفان کامل، حملات سایبری به بسیاری از حوزه‌ها است که منجر به تلفات مالی نامحدود می‌شود. برطرف کردن این مسئله ممکن است سخت‌ترین وظیفه برای بیمه‌گران و طرفداران امنیتی باشد. به طوری که به کل سسیتم یک شرکت تحت پوشش نفوذ کرده و یا اگر ۱۰ شرکت مختلف تحت پوشش داشته باشند و آن‌ها را هک کنند این تجمع ریسک بیمه‌گر بسیار مخوف خواهد بود.

نگرانی در حال افزایش در میان تعدادی از بیمه‌گران عدم اطمینان در مورد جمع‌آوری ریسک است. برای مثال، مشتریان ممکن است داده‌های خود را در فضای ابر ذخیره کنند. در صورتی که یک حادثه اتفاق بیافتد، بیمه‌گر نمی‌تواند در مورد تعداد مشتریان و میزان آسیب وارد شده مطمئن باشد. یک مثال دیگر می‌تواند در مورد فروشندگان شخص ثالث باشد، جایی که یک رابطه بر اساس اعتماد شکل گرفته می‌تواند توسط یک هکر مورد آسیب قرار گیرد و آسیب وارده به‌راحتی قابل جبران نباشد.

۳-۲-۴عدم افشای اطلاعات توسط بیمه‌گذار

عدم افشای اطلاعات توسط بیمه‌گذار از چالش‌های مربوط به جمع‌آوری اطلاعات در مورد مدیریت امنیت سایبر است. به خصوص برای مشتریان شرکت‌های چند ملیتی و با فعالیت‌های متنوع است.

مشتریان به راحتی حاضر به بحث در مورد اطلاعات مربوط به شرکت نیستند و معمولاً فقط اطلاعاتی را منتشر می‌کنند را که به موجب قانون مجبور به افشا هستند. به طور مثال اشتراک اطلاعات با اسناد رسمی (به عنوان مثال گزارش حادثه سایبری، گزارش حسابرسی و...).(Gemalto, 2017)

۳-۲-۵ عدم آگاهی افراد از این حوزه بیمه

از جمله چالش‌های که می‌توان بیان کرد عدم آگاهی مشتری در مورد بیمه سایبری است که در کشور ما اهمیتی ویژه دارد زیرا در این حوزه هیچ فعالیتی نشده است و برای ایجاد بازاری جدید ابتدا باید مخاطبان آن را شناسایی کرد و سعی در افزایش اطلاعات آنان داشت.

۳-۲-۶عدم قابل پیش بینی بودن

از جمله چالش‌هایی که بیمه‌گران با آن مواجه هستند عدم قابل پیش بینی بودن خطرات سایبری است. ماهیت غیر قابل پیش بینی بودن حملات سایبری را از خطر آتش سوزی، حوادث هوایی و بلایای طبیعی با تاریخ شناخته‌شده‌تر ارزیابی، متفاوت‌تر کرده است. فورمن می‌گوید: «این خطر طبیعی شما نیست.» (در حملات سایبری) دلیل ایجاد این خطر وجود انسان شیطانی در طرف دیگر حصار است.

دون بیان، افسر امنیت اطلاعات ارشد سیستم فدرال رزرو، در کنفرانس آر.اس.ای[1]، گفت: برای افزایش سرعت پیشرفت در این حوزه از بیمه، سازمان‌ها باید یک مدل مشترک را پیدا کنند و «همان مدل را با همان لحن بگویند».

توماس فورمن[2]، مدیر عامل شرکت مشاوره مارش ریسک[3]، در کنفرانس امنیتی سال ۲۰۱۶ در سانفرانسیسکو، گفت: هیچ یک از بیمه‌گران اطلاعات کافی برای ساخت مدل‌های ریسک واقعاً خوب در بیمه‌های سایبری ندارند.

---

[1] RSA
[2] Thomas Fuhrman
[3] Marsh Risk

۴- منابع

1. (n.d.).
2. (2013). Cyber/Privacy Insurance Market Survey. The Betterley Report.
3. A buye`s Guide to cyber Insurance. (2013).
4. accenture. (2016).
5. according to: Airmic Review of Recent Developments in the Cyber. (2013). 7.
6. According to: Airmic Review of Recent Developments in the Cyber. (2013). 9.
7. Airmic Review of Recent Developments in the Cyber. (2013). 11.
8. Airmic Review of Recent Developments in the Cyber. (2013). 9.
9. Amerding, T. (2017). what good cyber insurance?
10. American International Group. (n.d). American International Group. Retrieved from http://www.aig.com
11. Commission on Trade Documents and Exchanges of Corporate Financing. (2011). SEC Division of Corporation Finance, Cybersecurity, CF Disclosure Guidance.
12. Crews, & Wayne, C. (2005). Cybersecurity Finger-pointing Regulation vs. Markets for Software Liability, Information Security, and Insurance.
13. Cyber Insurance: An Efficient Way to Manage Security and Privacy Risk in the Cloud? (2012). InfoLawGroup LLP.
14. cyber Insurance: Recent Advances, good practices and challenges. (2016). enisa.
15. Durbin, S. (2013). Managing the Risks of Cyberspace.
16. Filkins, B. (2016, march). Quantifying risk.
17. Gemalto. (2017). The challenges Facting Acturaies in measuring cyber risk. enterprise security.
18. Google,OpenAl,Stanford uni,Berkeley. (2015).
19. Greisiger, M. (2010). how to protect your business in the digital age. Crain communications inc., 3.
20. (2014). IBM Security Services 2014 Cyber Security Intelligence Index, Analysis of cyber attack and incident data from IBM’s worldwide security operations.
21. Iwata, E. (2016). challenges and opportunities ahead for cyber insurance industry.
22. Jeyleen, R. H. (2017). 7 challenges insurers face in the cyber insurance market. www.propertycasualty360.com.
23. Kissel, R. (2013). Glossary of Key Information Security Terms. Editor, 60.
24. kpmg. (2013). http://www.kpmg.com/za/en/issuesandinsights/articlespublications/financial-services/pages/cyber-insurance-market-matures.aspx.
25. Ltd, M. (2011). Cyber risks explained, what they are, what they could cost and how to protect against them.
26. Majuca, R., Kesan, J., & Yurcik, W. (2006). سیر تکامل بیمه فضای مجازی.
27. Managing cyber insurance accumulation rick. (2016). university cambrige.
28. Menlo Park, C. (n.d.). The Top 5 Cyber Insurance Carriers in the Market. CyberPolicy.
29. Newman, D., & Analyst, D. (n.d.).
30. O. Schinnerer, V. (2011). Healthcare report, Protecting Hospitals and Healthcare Operations from Cyber Liability.
31. ponemon Institutes. (2012). Cost of Cyber Crime Study.
32. PwC’s Global State of Information Security Survey in 2010, Incentives and barriers of the cyber insurance market in Europe. (2012). ENISA, 16.
33. Rhoades, M. (2014). Cyber First Principles. 3.

34. Rhoades, M. (n.d.). The Truman|CNP Cyberspace & Security Program. 1-4.
35. Rouse, M. (2010). definition of data breach.
36. Stanbridge, G. (2012). A brief history of Cyber Insurance Cover.
37. State Security Breach Notification Laws. (2012). National Conference of State Legislatures.
38. Tamm v. Hartford Fire Insurance Co. (2003).
39. The IT Industry's Cyber security Principles for Industry and Government, information technology industry council. (2011). 5.
40. (2013). Third-Party vs. First-Party Cyber Risk Insurance: Protect Your IT Firm Right. Brenna.
41. watson, t. (2012). Risk and Finance Manager Survey. Retrieved from towerswatson: www.towerswatson.com/downloadmedia.aspx
42. Zhang, W., & Dong, W. (2011). Insurance Probability:Comparison & Analysis of Consumer Psychology and Pricing Strategy in U.S. and China. 3.
43. Zurich American Insurance. (n.d.). New York.

۴۴. السان, م .(1395) .بیمه فضای مجازی: مفاهیم اساسی و برنامه عملیاتی .تهران: پژوهشکده بیمه.

۴۵. انجمن تخصصی فناوری اطلاعات ایران. (n.d.). Retrieved from https://itpro.ir .

۴۶. راه پرداخت. (2017). Retrieved from http://way2pay.ir .

۴۷. قانون تجارت الکترونیکی ایران. (بدون تاریخ).

۴۸. لاودن, ک., & لاودن, ج. (۲۰۱۲). *سیستم‌های اطلاعاتی مدیریت.*

پژوهشگران و علاقه مندان محترم می توانند جهت دریافت سایر بسته های مطالعاتی و محصولات مرکز تحقیقات و آینده پژوهی سراج، از طریق راه های ارتباطی ذیل اقدام نمایند.

شماره تماس: ۰۲۱-۷۷۴۱۹۸۱۶
ایمیل: Futures@seraj.ir

سازمان فضای مجازی سراج
مرکز تحقیقات و آینده پژوهی