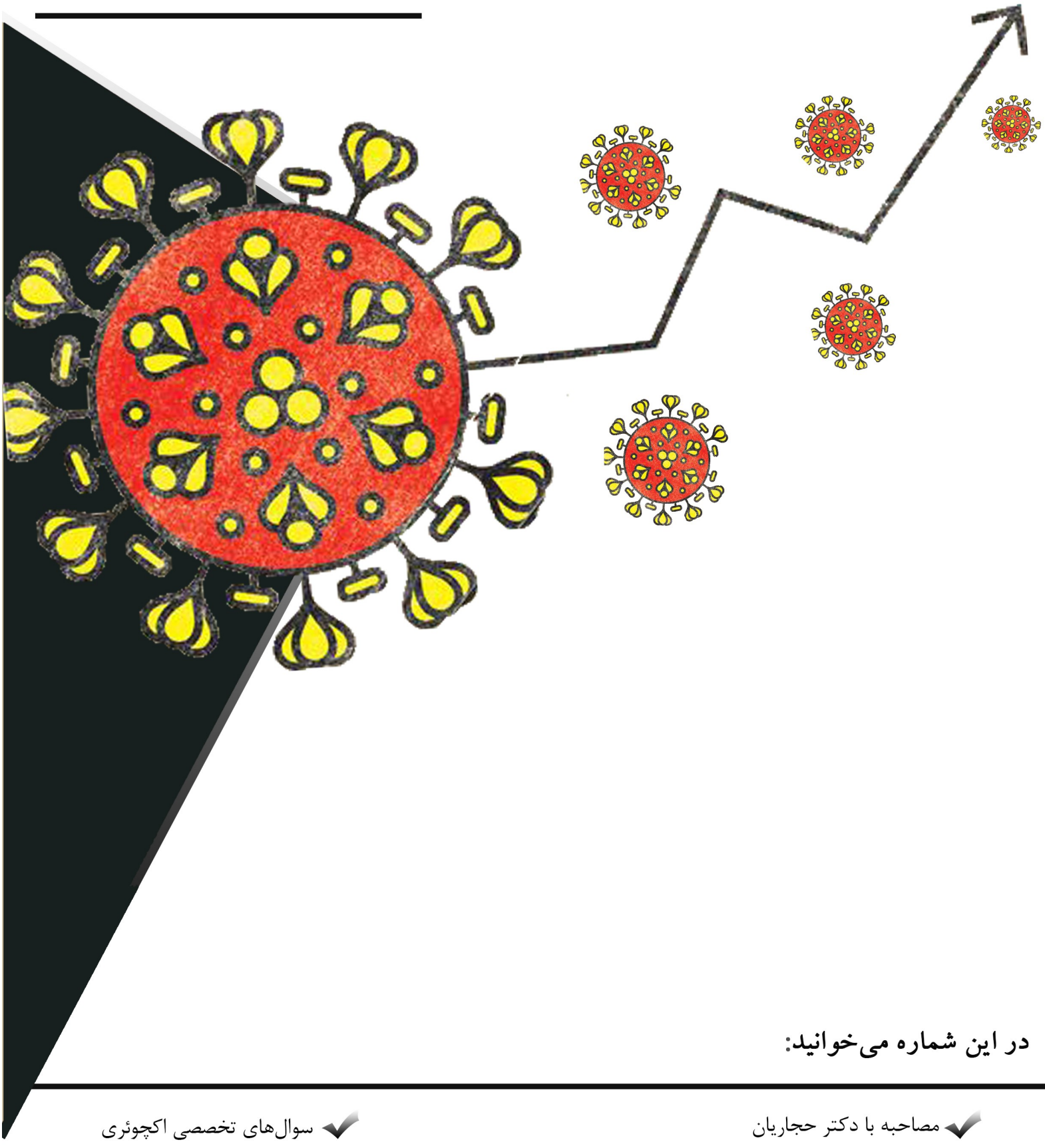
خبرنامه

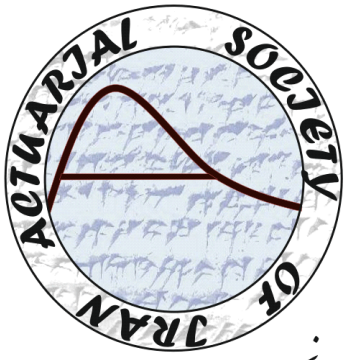
انجمن محاسبات بیمه و مالی ایران / زمستان ۹۸ / شماره ۸

انجمن محاسبات بیمه و مالی ایران



در این شماره می‌خوانید:

- مصاحبه با دکتر حجاریان
- شناسایی ادعاهای خسارت ساختگی
- سوال‌های تخصصی اکچوئری
- بیمه سایبری



خبرنامه

صاحب امتیاز: انجمن محاسبات بیمه ومالی ایران

مدیر مسئول: صابر شیبانی

سردبیر: رحیم محمودوند r.mahmodvand@gmail.com

اعضای هیأت تحریریه:

محمدرضا مشکانی mrmeshkani@gmail.com

مرتضی اعلاباف aalabaf@atu.ac.ir

رضا افقی r.ofoghi@yahoo.com

مریم تیموریان teimorymar@gmail.com

احمد صلاح‌نژاد ahmad.salahnejhad@gmail.com

علیرضا عدالتی aedalati@gmail.com

همکاران این شماره:

محمد قاسم وحیدی اصل — فاطمه علی‌محمدی

محمدرضا اناری — فاطمه سادات آل‌حسینی

فاطمه نصیری — محمد مهدی کاظمی

راضیه نوابی — پگاه پزشک‌نژاد

آزاده فتح‌الله ترشانی — هما نوروزی

طرح جلد: راضیه نوابی

صفحه آرایی: عاطفه مرادی

ویراستاری ادبی: فاطمه نصیری

فهرست مطالب

سرمقاله: تحقیق و اکتشافم آرزوست	۲
ریسک سایبری، شکست‌های بازار و ثبات مالی	۳
بیمه سایبری	۹
مصاحبه با دکتر حجاریان	۱۳
شناسایی ادعاهای خسارت ساختگی	۱۵
مجلهٔ بیمه، اقتصاد و ریاضی	۱۸
انتصاب‌های جدید اکچوئری‌ها	۱۸
طرح یک سوال پژوهشی	۱۸
گزارش برگزاری کنفرانس	۱۹
کنفرانس انجمن محاسبات بیمه و مالی ایران	۱۹
سوال‌های تخصصی اکچوئری شماره ۸	۲۰
پاسخ سوال‌های تخصصی اکچوئری شماره ۷	۲۰
اخبار دانشگاهی	۲۰
فراخوان درج مطلب	۲۱

تذکر: مسئولیت محتوای مطالب و مقاله‌ها به عهده نویسندگان آنهاست و لزوما دیدگاه‌های انجمن محاسبات بیمه و مالی ایران نیست.

نشانی مکاتبه: تهران، اوین، دانشگاه شهید بهشتی، دانشکده علوم ریاضی، گروه آمار

تلفن: ۲۲۴۱۹۴۳۰ (۰۲۱)

صندوق پستی: ۱۹۸۳۹۶۹۴۱۱

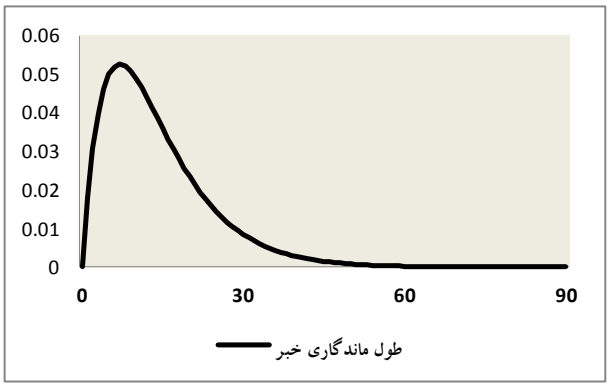
آدرس الکترونیکی: ir.actuary@gmail.com

وب سایت انجمن: www.irsoa.ir

سرمقاله

تحقیق و اکتشافم آرزوست

معمولا هر خبری دورهٔ اوج و فرودی دارد. اگر طول دوره ماندگاری هر خبری در صدر اخبار رسانه‌ها را به عنوان یک متغیر در نظر بگیریم، احتمالا توزیعی مانند نمودار زیر دارد:



این بدان معناست که خبرهای کمی با دوره ماندگاری طولانی منتشر می‌شود. در اغلب موارد خبرهای ناگوار و مخرب یا تصمیم‌های کلان در دولت‌ها در این طیف قرار می‌گیرند. درست یکسال پیش بخش‌های وسیعی از کشور درگیر سیل بود و اخبار آن به صورت داغ تا چندین روز از رسانه‌های رسمی و غیر رسمی منتشر می‌شد. افزایش ناگهانی قیمت بنزین و مسائل مرتبط با آن، ماجرای ترور سردار سلیمانی و سقوط هواپیمای مسافربری اوکراینی در آسمان ایران از جمله خبرهایی بودند که در زمان خودشان برای مدت زیادی در صدر اخبار رسانه‌ها قرار داشتند. جالب آنکه هرچقدر خبر داغ‌تر و طولانی‌تر شود، دامنه شایعات نیز به موازات آن گسترش می‌یابد.

خبر انتشار ویروس کرونای جدید، از زمان انتشار آن در حدود ۳ ماه قبل، همچنان در صدر اخبار رسانه‌های دنیاست و تقریبا تمام دنیا را درنوردیده است. مجددا رسانه‌های رسمی و غیررسمی سعی در پوشش آنی اخبار مربوط به این موضوعِ بحرانی دارند. اما داغ و حساس بودنِ موضوع باعث ترویج اخبار جعلی و نامعتبر در کنار اخبار واقعی نیز شده است. شدت و انبوه هشدارها نسبت به خبرها و گزارش‌های نادرست در مورد کرونا به حدی است که سازمان بهداشت جهانی را بر آن داشته تا صفحه‌ای برای مقابله با شایعات در مورد راه‌های درمان و راه‌های گسترش ویروس به راه بیندازد. صفحه زیر اطلاعات مفیدی در این خصوص منتشر کرده و به صورت مداوم به روزرسانی می‌شود:

https://www.who.int/emergencies/diseases/novel-coronavirus-2019

بخشی از اخبار جعلی متاثر از عدم کنترل شبکه‌های اجتماعی مجازی است. توئیتر، واتس اپ، اینستاگرام، تلگرام، فیس بوک و بسیاری از ابزارهای مشابه در چنین مسیری کم و بیش درگیر هستند. هر چند برخی از آنها مانند وی‌چت اخبار مربوط به ویروس کرونا را سانسور می‌کنند. برخی دیگر، مانند پینترست، در صورت جستجوی تصاویر مربوط به ویروس کرونا نتایج معتبر از سایت سازمان بهداشت جهانی را نمایان می‌کند.

به هر حال این روزها:

- از خطر شیوع بالای این ویروس می‌شنویم؛
- از کم‌شماری (فارغ از درستی یا نادرستی) آمارهای ابتلاء و فوت ناشی از ویروس کرونا می‌شنویم؛
- از گفته‌های متفاوت (و گاه متناقض) تاثیر مواد غذایی و داروهای پیشنهادی بر ویروس کرونا می‌شنویم؛
- از کمبود وسایل بهداشتی برای پیشگیری می‌شنویم؛
- از کمبود ابزارهای تشخیصی و درمانی می‌شنویم.

با این همه باید کوشش تحسین‌برانگیز خادمین و دلسوزان بهداشت و درمان کشور را ارج بنهیم.

البته شکی نیست که ویروس کرونا پیامدهای نامطلوبی در همه حوزه‌های زندگی‌مان به همراه دارد. اما به عنوان یک ریسک پیش‌روی در رفتار با آن بهتر است به صورت منطقی و عقلانی برخورد کنیم. در این راستا از نهادهای علمی، دانشگاه‌ها و پژوهشگران انتظار می‌رود برای یافتن راهکارهای منطقی کوشش کنند. اخیرا در نرم‌افزار R بسته ای تحت عنوان coronavirus افزوده شده است که در آن داده‌های مربوط به ابتلاء و مرگ و میر ناشی از ویروس کرونا در کشورهای مختلف و در برخی کشورها به تفکیک استان‌ها ارائه شده است. منبع داده های این بسته، مرکز سیستم‌های علمی و مهندسی در دانشگاه جان‌هاپکینز آمریکا ذکر شده است. این مرکز داشبوردی نیز برای ارائه آمارهای به روز در زمینه ویروس کرونا فراهم کرده است که از آدرس زیر قابل دسترس است:

https://www.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

به علاوه بسیاری از مجله‌ها شماره‌های ویژه‌ای به ویروس کرونا اختصاص داده‌اند و تلاش می‌کنند سهمی در شناسایی الگوهای شیوع و آگاهی رسانی به جامعه بشری داشته باشند.

انجمن محاسبات بیمه و مالی ایران نیز به پشتوانه دانش حرفه‌ای اعضاء و با توجه به استراحت اجباری که از پی حضور نامیمون ویروس کرونا برای همگان فراهم آمده است می‌تواند گام‌هایی در زمینه ارزیابی این ریسک بردارد. علاوه بر این ارزیابی پیامدهای این ریسک در حوزه‌های مختلف از جمله مواردی است که بسیار ارزشمند است و به زودی مورد نیاز خواهد بود. مانند اغلب موارد خمیرمایه چنین تحقیق‌هایی، داده معتبر است. اندیشیدن به این موضوع نیز بسیار ضرورت دارد و معرفی راهکارهایی برای صحت‌سنجی داده‌ها می‌تواند بسیار مفید واقع شود.

سال ۹۸ رو به اتمام است؛ از دست دادن شادروان دکتر محمدرضا مشکانی، که هم بنیان‌گذار علم بیم‌سنجی در ایران بود و هم یار و همراه خبرنامه تا فصل پائیز ۹۸ بود و در کل سرمایه‌ای گرانبها برای جامعه علمی کشور بود، ضایعه سنگینی بود. ضمن گرامیداشت یاد ایشان از سایر همراهان و مخاطبین خبرنامه سپاسگزاری می‌کنیم و آرزوی سلامتی و بهروزی در سال جدید داریم.

رحیم محمودوند، سردبیر خبرنامه

ریسک سایبری، شکست‌های بازار و ثبات مالی

۱. مقدمه

روند رو به رشد دیجیتالی شدن با وجود افزایش بهره‌وری موسسات مالی انواع متفاوتی از ریسک‌های جدید ایجاد می‌کند. ماهیت این ریسک‌ها، که شامل ریسک‌های سایبری نیز می‌شود، به گونه‌ای است که خیلی سریع تغییر یافته و اشکال متفاوتی به خود می‌گیرد. امروزه کلیه سیستم‌های بانکی در معرض ریسک سایبری قرار دارند. یکی از نقاط ضعف بازارهای مالی وابستگی آنها به مجموعه کوچکی از سیستم‌های فنی محسوب می‌شود و به همین خاطر هدف خوبی برای حملات سایبری هستند.

کلیه موسسات و شرکت‌ها، در معرض ریسک‌های سایبری خصوصاً از جنبه اقتصادی آن قرار دارند به عنوان مثال، موسسات ارائه دهنده خدمات مالی، حملات سایبری زیادی از جمله از کار افتادن سرویس‌ها در انتقال پول از طریق کارت های اعتباری را تجربه نموده اند. خطرناک‌ترین حملات سایبری که موسسات مالی تاکنون تجربه کرده‌اند بر زیرساخت‌های مالی آنها تاثیر گذاشته است. در این حملات معمولاً فایل‌ها و سخت‌افزارها نابود شده و یا این که داده‌ها و سیستم ها به نحوی در معرض خطر قرار می‌گیرند که بر خدمات‌دهی آن موسسه تاثیر منفی بگذارد و در نتیجه اعتماد مردم به سیستم‌های مالی تضعیف شود.

پیچیدگی و ناشناخته بودن اینترنت، شناسایی ریسک‌های سایبری را دچار مشکل نموده است و از آنجایی که ریسک‌های سایبری جدید هستند، اطلاعات کاملی راجع به آن‌ها و اثرات بلند مدت‌شان وجود ندارد و این مسأله برآورد هزینه و احتمال وقوع آنها را با مشکل مواجه کرده است. ریسک‌های سایبری از دسته ریسک‌های سیستماتیک محسوب می‌شوند. وجود اطلاعات نامتقارن، محرک‌های اشتباه استراتژی‌های مکمل و سایر پیامدهای خارجی می‌تواند منجر به نرخ‌گذاری نامناسب ریسک‌های سایبری شود. ماهیت ریسک‌های سایبری سیستماتیک به گونه‌ای است که در معرض شکست‌های دسترسی، تمرکز ریسک‌ها، ارتباط و سرایت به یکدیگر قرار دارند.

در حال حاضر بهترین سیاست برخورد با ریسک‌های سیستماتیک سایبری مشخص نیست و ممکن است این سیاست شامل طراحی مقررات پیشین یا تعیین مسئولیت‌های پس از وقوع خسارت، در کلیه سطوح در شرکت‌ها، دولت، موسسات مالی و همکاری متقابل آنها باشد.

در این مقاله مشخصات ریسک‌های سایبری از جمله تجمع ریسک و تاثیرات میان مدت، علت ناکامی بازارهای خصوصی در تأمین سطح مطلوب امنیت و تعاملات ریسک‌های سایبری سیستماتیک و ریسک ثبات مالی بررسی شده است. به علاوه در راستای کاهش ریسک‌های سیستماتیک بخشی از چارچوب مقررات جاری و رویکردهای نظارتی و تناسب بین آنها ارزیابی شده و در نهایت نیز معیارهایی جهت مقابله با ریسک سایبری بحث و بررسی شده است.

۲. ریسک سایبری

الف. تجمع ریسک‌های سایبری و تاثیرات میان مدت:

شرکت‌ها و موسسات ارائه دهنده خدمات مالی ریسک های سایبری را عمدتاً به‌عنوان مشکلی داخلی در نظر می‌گرفتند. با گذشت زمان، این دیدگاه به ریسک‌های عملیاتی مرتبط با شرکای تجاری و اشخاص ثالث نیز توسعه یافت. در خیلی از موارد نیز شرکت‌ها برای مقابله با مشکل عدم تقارن اطلاعات، از قراردادهای موجود با اشخاص ثالث استفاده می‌کنند. از طرفی مشکل تجمع ریسک مرتبط با فضای مجازی فراتر از ظرفیت مدیریت ریسک در یک سازمان است. ریسک‌ها می توانند تحت تاثیر عوامل بیرونی مانند کشمکش‌های جهانی نیز به وجود بیایند. این ریسک‌ها خارج از کنترل موسسه بوده و بر کل فضای مجازی تاثیر می‌گذارد و نیاز به دخالت دولت در این زمینه است.

گام های مدیریت ریسک شامل پیشگیری (مداوم)، پاسخ (فوری)، مدیریت تاثیر (کوتاه مدت) و درمان و بهبود داد و ستد بنگاه ها است.

پیشگیری: در واقع فعالیت‌های برنامه ریزی شده و مداومی است که سیستم‌ها و داده‌ها را در مقابل تهدیدهای سایبری حفاظت می‌کند.

پاسخ: پاسخ، اولین مرحله پس از حملات سایبری است که ابتدا شامل تحلیل آنچه اتفاق افتاده است و پس از آن اقدامات سریع برای جلوگیری از نفوذ در سیستم، تدوین استراتژی های ارتباطی با مشتری و شرکای تجاری و آمادگی برای دادخواهی احتمالی است.

مدیریت تاثیرات: پس از وقوع حملات سایبری، بایستی اقداماتی نظیر اصلاح زیرساخت ها و فرآیندها، فرایند ارزیابی و ممیزی سایبری و پشتیبانی قانونی انجام گیرد.

درمان و بهبود: پس از وقوع حملات سایبری و تاثیرگذاری روی سیستم باید بر جبران خسارات و پیشگیری از وقایع آتی متمرکز شد. این مرحله شامل طراحی مجدد فرایندها و سیستم‌های تجاری، بازسازی روابط و شهرت و تهیه سیستم های امنیتی بهتر و قابلیت‌های آمادگی است.

ب.برآورد نتایج برای حملات سایبری:

برخلاف بسیاری از خطرات مالی و عملیاتی، اطلاعات مربوط به خسارت‌های سایبری یا در دسترس نیستند و یا اطلاعات مفیدی جهت تحلیل این خسارت‌ها موجود نیست. دلایل این امر شامل موارد زیر است:

۱- معمولاً حملات سایبری توسط مشتری ها گزارش می‌شوند و نه خود شرکت‌ها، بنابراین فرآیند گزارش آنها طولانی می‌شود.

۲- شرکت ها به خاطر ترس از افزایش حق بیمه و تاثیرات منفی روی شهرت خود، اطلاعات را حفظ می‌کنند.

۳- تحلیل های اقتصادیِ کمّی به خاطر ناکافی بودن اطلاعات در مورد تاثیرات آنی و بلند مدت حملات سایبری به ندرت مطرح شده است.

۴- تغییرات سریع و چشمگیر در ریسک‌های سایبری منجر به نامناسب بودن داده‌های گذشته به‌عنوان معیاری برای پیش‌بینی آینده می‌شود.

ج.مدیریت ریسک‌های سایبری:

ریسک‌های شناسایی، ارزیابی و تحلیل شده همواره نیاز به مدیریت داشته و این امر به عنوان بخشی از فرآیند شناسایی تهدیدها تلقی می شود. اساس مدیریت ریسک بر مبنای سه فاکتور اجتناب از ریسک، کاهش ریسک و انتقال ریسک است.

کاهش ریسک: کاهش میزان ریسک موردانتظار یک سازمان و رساندن آن تا حد مطلوب برای آن سازمان.

کاهش ریسک از سه طریق فیزیکی(قفل ها)، دیجیتالی(نرم افزارها) و ابزارهای کنترل انسانی (آموزش) امکان پذیر است. همچنین آمادگی و برنامه ریزی یک شرکت منجر به پیش بینی دقیق و در نتیجه کاهش ریسک یک شرکت می‌شود.

اجتناب از ریسک: یکی از اساسی‌ترین اصول مدیریت ریسک‌های سایبری، طراحی مجدد فعالیت‌ها است که به معنای سازگاری و یا تغییر محصولات و فرآیندها است.

انتقال ریسک : این مرحله شامل خرید بیمه مسئولیت سایبری یا انتقال ریسک عملیاتی به ارائه دهنده خدمات شخص ثالث باشد.

بیمه سایبری با تخصیص کارآمدتر ریسک‌ها مشکل عدم تقارن را تا حدی برطرف می‌کند. تخصیص ریسک بین شرکت‌های درگیر منجر به این امر می شود که هر یک انگیزه کافی برای سرمایه گذاری در جهت افزایش امنیت سایبری پیدا کنند، شفاف‌سازی و اشتراک داده‌ها افزایش یافته و در نهایت سهم حق بیمه پرداختی هر یک نیز کمتر شود. ماهیت ریسک‌های سایبری متغیر است و لذا بیمه‌گرها باتوجه به اطلاعات جزئی که در مورد این نوع ریسک دارند در راستای قیمت گذاری مناسب، پوشش ها را با سقف محدود ارائه نموده و شرایط و استثنائات محدود کننده‌ای نیز بر بیمه‌نامه‌های موجود وضع می‌نمایند. مشکلات اطلاعات نامتقارن، نظارت بر رفتار مشتریان و مخاطرات اخلاقی از جمله مواردی است که در بیمه‌های سایبری نیز وجود دارد.

فعالیت های ایمنی سایبری که توسط اشخاص ثالث دارای مسئولیت غیرمستقیم ارائه می‌شود جایگزینی برای انتقال ریسک محسوب می‌گردد. در سال ۲۰۰۷ نیز روو (Rowe, 2007) این پیشنهاد را مطرح کرد که اگر خدمات مشابه توسط شرکت‌های مختلف ارائه گردد، اشتراک‌گذاری داده‌ها برآیند مثبتی خواهد داشت. به علاوه اگر موسسات مالی به منظور کاهش تمرکز ریسک از تامین‌کننده‌های مختلف استفاده کنند در صورتی که یکی از تامین کننده ها عملکرد خوبی نداشته باشد جایگزین مناسب برای آن وجود دارد. با این حال این ریسک پراکنده می تواند تا حدی دوباره متمرکز شود که تامین کننده خارجی تنها به یک شرکت تامین‌کننده متکی شود. برای مثال ممکن است چندین تامین‌کننده ابر مجازی از سیستم عملیاتی مشترکی استفاده کنند که در این صورت اگر آن سیستم عملیاتی نقصی داشته باشد می تواند باعث ایجاد ریسک همبسته در تمام تامین کننده ها شود. تامین کننده های شخص ثالث و توسعه‌دهنده‌های نرم‌افزار می‌توانند در مقابل ریسک‌های سایبری بیمه باشند یا نباشند با این حال حتی اگر تامین‌کننده‌های شخص ثالث هم بیمه شده باشند محدوده پایین پوشش و ناتوانی در قیمت گذاری سنجیده ریسک ها باعث می شود که در نهایت مقداری از ریسک نزد شرکت‌ها نگهداری شود.

بیمه سایبری

بیمه مسئولیت سایبری برای جبران خسارت‌های بیمه‌پذیر شخص اول و ثالث طراحی شده است. خسارت های وارده به شخص اول شامل هزینه مدیریت بحران، اطلاع رسانی به مشتری، قطعی‌های سیستم و هزینه‌های مرتبط با آن، بازسازی نرم‌افزارهای دارای مشکل و دارایی‌های دیجیتال می‌شود (که به طور معمول تحت پوشش بیمه جامع جرم) قرار می‌گیرند.

خسارت های بیمه پذیر شخص ثالث آن دسته از هزینه هایی هستند که شخص ثالث متحمل شده است. ضرر و زیان شخص ثالث در کل شامل

مسئولیت شخص ثالث در نقص های امنیتی حریم خصوصی داده و از این قبیل موارد است. در سال ۲۰۱۶ نمونه گیری انجام شده توسط نت دلینگنش نشان داد که ۱۳ درصد از خسارت‌ها مربوط به شخص ثالث و ۱۷ درصد اثرات بر بخش خدمات مالی است. مقررات بیمه‌های سایبری به طور معمول هزینه های غیر مستقیم ناشی از حملات سایبری که در میان‌مدت و بلندمدت مشاهده می‌شود مانند ضرر و زیان ناشی از بدنامی از دست دادن اعتماد مشتری و غیره را پوشش نمی‌دهد.

برخی از این استثنائات به هیچ عنوان قابل بیمه شدن نیستند در حالی که بعضی از آنها با اعمال پوشش های محدود و استثنائات قابل بیمه شدن هستند. ارائه این سقف از پوشش‌های بیمه‌ای باعث شده است که مکانیزم جبران خسارت های بیمه پذیر به طور موثر عمل نکند و خسارت‌های غیر قابل قیمت‌ُگذاری در بیمه مسئولیت سایبری، تجمیع ریسک‌های پیچیده و ارتباط همزمان خطر های مختلف در یک حادثه قیمت‌گذاری ریسک را دچار مشکل نموده است. همچنین ریسک های سایبری نسبتاً نوظهور هستند و هم شرکت و هم مشتری‌ها نسبت به ساختار این نوع ریسک‌ها و تاثیری که در بلندمدت می توانند داشته باشند، آگاه نیستند بنابراین تکنیک‌های مدل بندی اکچوئری با مشابه خود در ریسک های بیمه پذیر مقایسه می‌شوند. شرکت های بیمه حق بیمه مازادی را به حق بیمه اصلی اضافه می‌کنند که در نتیجه نسبت به انواع دیگر پوشش ها حق بیمه بالاتر می‌رود. مشکلات موجود جهت قیمت‌گذاری این ریسک‌ها نتیجه کار را تضعیف می‌کند و موجب ناکارامدی تخصیص ریسک می شود. به علاوه در صنعت بیمه نگرانی‌هایی در این خصوص وجود دارد که منابع ریسک در بازار بیمه متمرکز شده‌اند و این باعث می‌شود که شرکت‌های بیمه توان تحمل ریسک‌های بزرگ را نداشته باشند. برخلاف تمام مزایایی که بیمه سایبری دارند نمی توانند جایگزین مدیریت فعال ریسک سایبری در شرکت‌ها شوند. هر چه شرکت‌های بیمه در این زمینه با تجربه‌تر شوند، قیمت گذاری قراردادها و تخصیص ریسک کاراتر شده و در نتیجه بیمه مسئولیت سایبری هم در انتقال و یکپارچه کردن ریسک بهتر عمل می‌کند.

۳. شکست‌های بازار

بازار ممکن است در تعیین سطح مطلوب امنیت به دلیل اطلاعات نامتقارن، محرک های اشتباه، عوامل خارجی، عدم هماهنگی و تمرکز ریسک با شکست مواجه شود. به‌علاوه در خصوص اینکه بین مقررات پیشین و مسئولیت‌های پس از وقوع حادثه ، کدام یک در پیشگیری از شکست در معاملات بهتر عمل می‌کنند ، جای بحث وجود دارد. مقررات پیشین در راستای جلوگیری از خطرات امنیتی هدف‌گذاری شده اند، اما مسئولیت های پس از وقوع، مسئولیت را تعیین می نماید.

الف.اطلاعات نامتقارن:

شرکت‌ها از جمله موسسات مالی اغلب به خاطر کمبود اطلاعات مورد نیاز قادر به تصمیم‌گیری در مورد مدیریت بهینه ریسک‌های سایبری نیستند. بنابراین شرکتها نمی‌توانند مواردی نظیر برآورد شدت ریسک‌های سایبری، تاثیر گذاری سیستم های دفاعی، کیفیت خدمات شرکت سایبری خارجی و انعطاف پذیری بازار را در بلند مدت پیش بینی کنند. می دانیم که اطلاعات نامتقارن منجر به مخاطره اخلاقی و انتخاب نامساعد می شود و انتخاب نامساعد عملکرد سیستم را تحت تاثیر قرار می دهد. نامتقارن بودن داده ها در فضای سایبری ناشی از عوامل متعددی است که از مهمترین آنها می توان عدم وجود تجربه کافی را نام برد که کمی سازی منابع ریسک های سایبری را مشکل می کند. همچنین از آنجایی که ریسک‌های سایبری بر اساس ماهیت خود بسیار متنوع بوده و با سرعت در حال تغییر هستند تعیین مشخصات آنها دشوار به نظر می‌رسد مخصوصا در مواردی که ریسک مستقیماً مربوط به شرکت‌ها و یا شرکای تجاری آنها باشد. علاوه بر این شرکت ها معمولاً اطلاعات مرتبط با هزینه های ناشی از حملات سایبری و ماهیت آنها را به اشتراک نمی‌گذارند که علت این امر نگرانی تاثیر منفی آنها بر میزان تقاضا جهت خدمات شرکت است. همچنین در صورتی که شرکت فوق بیمه داشته باشد افشای اطلاعات منجر به افزایش مبلغ حق بیمه می‌شود.

از آنجا که ریسک های سایبری محدود به مرزهای جغرافیایی و محدوده خاصی نمی باشد و از جمله ریسک‌های جهانی محسوب می‌شود، نیاز به هماهنگی قوانین بین المللی ، هماهنگی هایی تسهیل کننده، پشتیبانی جهت اشتراک گذاری داده‌ها و طراحی قوانین یکسان وجود دارد.

آخرین مشکل مرتبط با اطلاعات ، کفایت یک نوع خاصی ازمحافظت سایبری است. شرکت ها مخصوصاً شرکت های کوچک تر که اطلاعات تخصصی کمتری در خصوص سایبری دارند در تصمیم گیری منطقی انتخاب نرم‌افزار یا تامین کننده امنیت سایبری به مشکل می‌خورند.

یکی از مشکلاتی که پیش از رخداد حملات سایبری وجود دارد تعیین کیفیت خدمات است که بسیار سخت بوده و منجر به سرمایه گذاری نادرست در بخش امنیت یا انتخاب راه حل های غیرامن و ارزان می‌شود.

ب: مکمل های استراتژیک، عدم هماهنگی و عوامل خارجی

به طور کلی عوامل بیرونی زمانی به وجود می آیند که ریسک تاثیرات جانبی رفتارهای یک سازمان بر دیگران تاثیر می گذارند. امنیت سایبری یک شرکت از دو طریق زیر کاهش پیدا می‌کند:

۱- سرمایه‌گذاری بیشتر روی امنیت سایبری شرکت خود.

۲- سرمایه گذاری بیشتر روی امنیت سایر شرکت های موجود در همان شبکه است.

نقص‌های یک نرم‌افزار باعث افزایش ریسک‌های مربوط به امنیت سایبری می شود. این عوامل خارجی توسط فروشندگان نادیده گرفته می شوند که باعث تاثیر منفی عوامل خارجی بر تمامی سازمانهای آن شبکه می‌شود. برای توسعه دهندگان یک نرم افزار تامین امنیت تا زمان تسلط کامل بر بازار، به دلیل هزینه بر بودن، در اولویت قرار ندارد. به دلیل رقابت موجود میان شرکت‌ها، هر کدام از آنها سعی در ارائه هر چه سریعتر نرم‌افزار خود دارد که این موضوع باعث می شود یک نرم افزار قبل از اصلاح ایرادها به بازار ارائه شود؛ که این موضوع باعث کاهش امنیت سایبری می گردد. عوامل خارجی هنگامی ظاهر می‌شوند که مجموعه‌ای از کاربران از یک نرم افزار خاص استفاده می کنند. کاربران به دو دلیل از یک نرم افزار استفاده می کنند: ویژگی های خود آن نرم‌افزار و تعداد کاربرانی که از آن نرم‌افزار استفاده می‌کنند. هرچه تعداد کاربرانی که از یک نرم افزار خاص استفاده می کنند، افزایش پیدا کند عوامل خارجی مثبت و منفی نیز افزایش پیدا می کند. عوامل خارجی مثبت باعث سوء استفاده می شود. بوهمه (Bohme, 2010) این موضوع را مطرح می کند که با تداوم عوامل خارجی شرکت تمایل به سرمایه گذاری کم روی امنیت سایبری خود و استفاده از امنیت ایجاد شده توسط شرکت‌های دیگر پیدا می‌کند.

ج.تمرکز ریسک:

بازار خدمات سایبری از شمار نسبتاً کمی از شرکت هایی که خدمات مشابه ارائه می دهند تشکیل شده است. این امر باعث افزایش بازدهی شرکتهای فوق و مانع ورود شرکت های جدید با سابقه کم به بازار می شود. انحصار چندجانبه در بازار خدمات سایبری منجر به ایجاد ریسک های همبسته برای موسسات مالی می شود چرا که این تامین کنندگان معمولاً از نرم افزارها، سخت افزارها و مرورگرهایی استفاده می کنند که در معرض ریسک های سایبری مشابهی قرار دارند. این در حالی است که در صورت یک جانبه بودن بازار نیز، شرکت فوق انگیزه قوی برای محافظت از سیستم های خویش خواهد داشت که در نتیجه برکاهش ریسک‌های سایبری صنعت مالی نیز تاثیر مثبتی خواهد داشت؛ از طرفی تهیه بیمه نیز ممکن است منجر به تمرکز ریسک شود. بازدهی افزایشی خدمات سایبری، توسعه خدمات بیمه‌ای را به همراه دارد و از آنجایی که شمار نسبتاً کمی از شرکت‌ها خدمات سایبری ارائه می‌دهند و بین ریسک های سایبری نیز به دلیل برخورداری از منابع مشترک همبستگی وجود دارد، شرکت‌های بیمه بایستی به حفظ ثبات مالی خود در شرایطی که خسارت به طور گسترده و هماهنگ رخ می دهد توجه کافی نمایند چرا که در چنین شرایطی شرکت های بیمه در معرض ریسک به صورت تجمیعی قرار دارند.

۴. تعاملات شکست بازار مرتبط با فضاهای سایبری و ثبات مالی

مدیریت ریسک در موسسات مالی روی ریسک‌های ویژه تمرکز دارد. از آنجایی که ماهیت ریسک سایبری همان ریسک‌های سیستماتیک است، ارزیابی آن در سطح نهادها و اشخاص دقیق نخواهد بود. ریسک سیستماتیک زمانی نمایان می‌شود که ریسک‌های موجود بین موسسات مالی مشابه و همبسته باشد. قرار گرفتن در معرض خطرات سایبری منجر به ایجاد آسیب پذیری، تمرکز ریسک و همبستگی ریسک می‌شود.

دسترسی به نقاط آسیب پذیر: سیستم مالی یکی از متصل‌ترین سیستم ها در اقتصاد جهانی می‌باشد بنا به دلایل تجاری قسمت اعظم سیستم ها در اختیار مشتریان و شرکای تجاری قرار می‌گیرد. این امر منجر به این می‌شود که سیستم در معرض دسترسی به نقاط آسیب پذیر قرار گیرد.

تمرکز ریسک: وجود شرکت های کم که با حجم بالایی از معاملات سروکار دارند در نهایت باعث ایجاد تمرکز ریسک می‌شود.

ارتباط و سرایت ریسک: شوک های سایبری محرک ریسک نقدینگی تامین سرمایه است که می تواند به شوک نقدینگی بازار نیز بیانجامد. در چنین شرایطی شرکت‌ها مجبور به ارائه دارایی با قیمت پایین تر از قیمت واقعی می شوند و این امر منجر به قطع ارتباطات با شرکای بازار می‌شود. شوک‌های ریسک نقدینگی و بازار، موسسات مالی را با مشکلاتی در سطح توانگری‌شان روبرو می‌نماید. ارتباط مستقیم و غیر مستقیم بین بازارهای بین بانکی و بازارهای نقل و انتقال پول، منجر به پخش سریع شوک در سراسر سیستم می‌شود.

ناتوانی موسسه در پرداخت‌ها یا ایفای تعهداتش، که ممکن است به علت به خطر افتادن سیستم‌های پرداخت یا ثبت رکورد اتفاق بیفتد، می‌تواند تاثیر منفی بر نقدینگی سرمایه و موسسات زیرمجموعه بگذارد. کمبود نقدینگی، ارزش گذاری دارایی ها به قیمت پایین را به همراه دارد. در طول زمان خسارت های ناشی از ریسک نقدینگی به کاهش سرمایه و نهایتاً تضعیف توانگری مالی شرکت می‌انجامد.

۵. مقررات مالی ریسک سایبری

الف.سایبری به عنوان یک ریسک عملیاتی

هدف از تنظیم مقررات بخش خدمات مالی ارتقاء رشد اقتصادی بلند مدت و به حداقل رساندن هزینه‌ها و خروجی‌های منفی ناشی از بی ثباتی مالی است. یک سیستم مالی پایدار پیش نیاز یک اقتصاد کارآمد است که از رشد اقتصادی پشتیبانی می‌کند. در یک سیستم مالی پایدار موسسات و بازارها فعالیت خواهند کرد، قیمت ها اصول را منعکس می کنند و نگرانی های کوتاه مدت و نوسانات فقط روی یک حلقه محدود از مشارکت‌کنندگان تاثیر می‌گذارد.

با این وجود برای اثربخش ماندن ممکن است نیاز باشد که این مقررات متناسب با تحولات جدید فناوری و عوامل ریسک مانند ریسک سایبری سازگار گردد.

با توجه به نقش فراگیر فناوری در امور مالی، حداقل استانداردهایی جهت مدیریت ریسک های مرتبط با فناوری اطلاعات تنظیم شده است. اکثر شرکت های خدمات مالی از یک چارچوب نظارتی تنظیم شده مشخص جهت مدیریت ریسک‌های مرتبط با فناوری اطلاعات استفاده می کنند که به طور کلی ریسک های مرتبط با فناوری اطلاعات را به عنوان زیرمجموعه‌ای از ریسک‌های عملیاتی در نظر می گیرد. ریسک عملیاتی کلیه خسارت های ناشی از شکست در فرایندهای داخلی، سیستم ها، اشتباهات افراد و وقایع خارجی را در نظر می گیرد. این تعریف، ریسک قانونی را دربرگرفته اما ریسک استراتژیک و شهرت را شامل نمی شود.

حداقل استانداردهای ریسک های مرتبط با فناوری اطلاعات بر روی مدیریت متمرکز شده است که شامل مواردی مربوط به رسیدگی فجایع بزرگ عملیاتی است (به عنوان مثال برنامه ریزی و بهبود ادامه فعالیت). ناظران با توجه به اینکه سیستم‌های اندازه گیری ریسک عملیاتی حرفه ای را توسعه می دهند، کلیه شرکت های ارائه دهنده خدمات مالی را ترغیب به استفاده از رویکردهای موجود می نمایند. در حالت ایده ال، شرکت ها باید رویکرد یکپارچه و مبتنی بر ریسک را برای مدیریت ریسک های مرتبط با فناوری اطلاعات اتخاذ کند که از طریق عملکرد مدیریت ریسک، شناسایی، مدیریت و گزارش می‌شوند.

در چارچوب های ریسک عملیاتی، ریسک دم را بایستی در محاسبه سرمایه نظارتی لحاظ نمود. استانداردهای سرمایه نظارتی بانک‌ها را ملزم به نگهداری مبلغی به عنوان سرمایه جهت پوشش‌دهی خسارت‌های مورد انتظار ناشی از ریسک‌های عملیاتی می‌نماید. انتظار می رود بانک‌ها نیز سرمایه الزامی نظارتی را بر اساس خسارت‌های مورد انتظار و دور از انتظار محاسبه نمایند.

از طرف دیگر استفاده از تحلیل سناریو بخش جدایی ناپذیر این رویکرد می باشد و در این روش با استفاده از داده‌های خارجی میزان قرار گرفتن در معرض ریسک، در حوادث دم ارزیابی می‌شود.

انتظار می رود در تحلیل سناریو، تاثیر انحراف از مفروضات همبستگی موجود در چارچوب اندازه‌گیری ریسک عملیاتی بانک‌ها ارزیابی شود که شامل ارزیابی خسارات بالقوه عملیاتی ناشی از چندین رویداد به طور همزمان نیز می‌باشد. چنین ارزیابی‌هایی بایستی نسبت به خسارت‌های واقع شده مجدداً ارزیابی و تایید گردد. همچنین نیاز است کلیه بانک‌ها خسارت بالقوه دور از انتظار را نیز برآورد نموده و سرمایه‌ای را به آن تخصیص دهند. برای مدیریت ریسک های مرتبط با فناوری اطلاعات استانداردهایی توسط نهادهای بین‌المللی تنظیم استاندارد (ssb) ایجاد و ملاک عمل قرار گرفته است. برای شرکت های خدمات مالی فعال در سطح جهان، ssb چارچوب نظارتی را با حداقل استانداردها با هدف تخصیص سرمایه جهت خسارت‌های دور از انتظار و تشویق شرکت‌ها برای مدیریت هر چه بهتر ریسک ها از جمله فناوری اطلاعات تعبیه نموده است.

به دلیل اتکای فراوان بازارهای اوراق بهادار و مشتقات به فناوری اطلاعات، استانداردهای شفافی برای انعطاف پذیری امنیت سایبری اجرایی شده است. مشکلات عملیاتی که در سیستم های پرداخت، پردازش و تسویه حساب آنها وجود دارد، نه تنها مانع از کنترل بلکه گاهی باعث تشدید سایر ریسک‌ها نظیر ریسک بازار، نقدینگی و اعتبار نیز می‌شود و بصورتی غیرقابل پیش‌بینی همانند ریسک‌های سیستماتیک عمل نموده و خسارت قابل توجهی را به مشارکت کنندگان وارد می‌نماید.

ریسک های عملیاتی مربوط به پرداخت و تسویه حساب، می توانند در بازارهای مالی گسترش یافته و بر محصولات مالی متنوعی تاثیر بگذارند. لذا در راهنمای IOSCO/CPMI استانداردهای با سطح بالا جهت مدیریت ریسک‌های عملیاتی سیستم‌های پرداخت، پردازش و تسویه الزام شده است.

ریسک‌های سایبری با ریسک‌های معمول فناوری اطلاعات بسیار متفاوت هستند. ماهیت وقایع مربوط به سایبری و توزیع متغیر آنها به گونه‌ای است که نیاز به مقررات و رویکرد نظارتی دارد که به صورت مکرر متناسب با تغییرات ریسک پروفایل اصلاح شود.

اساسی‌ترین اصل مدیریت ریسک در بانک‌ها، مدیریت موثر ریسک‌های عملیاتی مربوط به فناوری اطلاعات است. G7 اولین گام را در استانداردسازی الزامات ریسک های سایبری برداشته است. درواقع G7 مجموعه‌ای از اصول پایه‌ای که اجرای آن نیز الزامی نیست برای بخش مالی نهادهای عمومی و خصوصی طراحی نموده است. این اصول به منزله بلوک‌های ساختمانی هستند که هر یک از آنها می‌تواند به پیاده سازی استراتژی امنیت سایبری کمک نموده و چارچوب عملیاتی را با رویکرد خود برای مدیریت ریسک و فرهنگ آن، پیاده سازی نمایند. این اصول عبارتند از:

اصل ۱: استراتژی و چارچوب امنیت سایبری

اصل ۲: حاکمیت

اصل ۳: ارزیابی ریسک و کنترل

اصل ۴: نظارت

اصل ۵: پاسخ

اصل ۶: بازیابی

اصل ۷: به اشتراک گذاری اطلاعات

انتظار می رود که این اصول توسط ناظران و خود موسسات مالی متناسب با چشم انداز عملیاتی و تهدیدآمیز و الزامات قانونی و نظارتی خود آنها تنظیم شوند. این اصول همچنین مراحل یک فرآیند پویا را ارائه می دهند که از طریق آن نهاد می تواند به طور سیستماتیک، استراتژی و چارچوب امنیت سایبری خود را که به عنوان تحول محیط عملیاتی و تهدید تکامل می یابد، مجددا ارزیابی نماید. مقامات دولتی در داخل و در سراسر حوزه‌های قضایی می‌توانند از این اصول برای هدایت سیاست‌های عمومی، نظارتی و فعالیت های سرپرستی خود استفاده کنند.

یک سیستم گزارش دهی ریسک سایبری که بتوان به آن اعتماد کرد، برای ریسک سایبری حیاتی است. توسعه یک برنامه اولویت بندی اطلاعات سایبری دارایی، اقدام برای استاندارد سازی جمع آوری داده‌ها و ایجاد چارچوب‌هایی برای مدل‌سازی و ریسک سایبری، هسته مرکزی یک سیستم نظارتی کارآمد است. مقامات و مقررات ملی برای اطمینان از گزارش به موقع و دقیق حملات سایبری باید دستورالعمل های مناسبی را ارائه دهند. استانداردهای ریسک سایبری باید مؤسسات مالی را ملزم به ارائه داده های داخلی ریسک سایبری، در ابتدا به صورت دوره‌ای و در نهایت در زمان واقعی نمایند. بررسی قابلیت اعتماد داده ها و پردازش خودکار از وظایف تنظیم کننده های استاندارد است. با توجه به ماهیت کیفری حملات سایبری، ناظران نیاز به هماهنگی با دستگاه‌های مربوطه اجرای قانون دارند. ناظران بخش مالی باید بتوانند به سرعت حمله‌کننده را به دستگاه های اجرایی مربوطه معرفی کنند تا از پاسخ به موقع، چه از جانب مؤسسه حقوقی و چه مالی، اطمینان حاصل شود. در حالت ایده‌آل، تمهیدات رسمی برای تبادل اطلاعات دو طرفه بین سازمان های اجرای قانون و ناظران صورت خواهد گرفت.

ب. دستورالعمل‌ها

در ایالات متحده، موسسات مالی دارای مجوز از یک رویکرد بخش بندی شده در رابطه با ریسک عملیاتی (از جمله ریسک سایبری) استفاده می‌کنند. با استفاده از یک رویکرد یکپارچه برای مدیریت ریسک می‌توان انتظار داشت که ریسک های عملیاتی از جمله ریسک های مرتبط با فناوری اطلاعات و سایبری، شناسایی، مدیریت و گزارش شوند. در آمریکا، مسئولین مربوطه با استفاده از استانداردهای مدیریت ریسک هدفمند و تشدید نظارت در بانک‌ها، تمرکز بر مقابله با سایبری را افزایش داده‌اند. ناظران بانکی ایالات متحده برای محافظت از بازارهای مالی و مصرف کنندگان در برابر حملات آنلاین، استانداردهای امنیت سایبری را به کار گرفته‌اند.

انتظار می رود شرکت های بزرگ هلدینگ بانکی (BHC) پیشرفته ترین قابلیت های دفاعی را داشته و بتوانند طی دو ساعت از هرگونه حمله‌ای بهبود یابند. از سال ۲۰۱۳، بانک ها بخشی از سناریوهایی را که برای آزمون استرس سالانه خود ارائه می دهند به ریسک های سایبری و عملیاتی اختصاص داده‌اند. بانک ها این سناریوها را به عنوان بخشی از آزمون های استرس مورد نیاز تحت قانون Dodd-Frank تهیه می کنند. آژانس های مسئول نظارت به BHCها هشدارهای قابل ملاحظه‌ای برای تصمیم گیری در مورد استانداردهای پیشرفته مدیریت ریسک سایبر را صادر کرده اند . این استانداردها به همراه استانداردهای پیشرفته در خصوص عملکرد اصلی بخش مالی تنظیم شده اند که البته این استانداردهای پیشرفته در مورد بانک های عمومی اعمال نمی‌شوند.

شرکت‌های مالی که در بازارهای اوراق بهادار فعالیت می کنند نیز با یک چارچوب نظارتی جامع روبرو هستند به دلیل اتکای فراوان بازارهای اوراق بهادار و مشتقات به فناوری اطلاعات، رویکرد لایه ای برای طراحی مقاومت در برابر ریسک سایبری در کمیته پرداخت و زیرساخت های بازار و هیئت مدیره بین المللی کمیسیون اوراق بهادار تدوین شده است. رویکردی کلی برای صنعت اوراق بهادار و زیرساخت‌های بازار مالی توسعه یافته است اما این چارچوب برای سایر شرکت‌کنندگان در بخش مالی نیز مناسب است. عناصر اصلی این رویکرد به حاکمیت قوی، شناسایی اطلاعات سیستماتیک دارایی (جواهرات تاج)، شناسایی تهدیدهای سایبری، ایجاد محافظت در برابر حملات سایبری، تشخیص وقایع غیر طبیعی، کاهش هزینه های بازیابی از طریق برنامه ریزی برای پاسخ به حادثه و تست جامع استرس سیستم ها و فرایندها نیاز دارند.

۶. اقدامات برای تقویت مقاومت در برابر ریسک سایبری

الف.کاهش آسیب‌پذیری‌های دسترسی با وجود افزایش مقاومت

صرف نظر از اندازه موسسه اقدامات اساسی ذیل باید برای مقابله با ریسک‌های سایبری خاص انجام گیرد:

لیست سفید برنامه: استفاده از تنظیمات پیکربندی سیستم امنیت استاندارد، انجام فرآیندهایی برای تعمیر کردن سیستم و نرم افزارهای کاربردی در مدت زمانی کوتاه، محدود کردن تعداد افراد دارای حق امتیاز مدیر

افزایش مقاومت در برابر حملات سایبری نیاز به آموزش های موثر دارد: امنیت کامل هیچ وقت اتفاق نمی افتد و شرکت ها همیشه در معرض ریسک های سایبری قرار دارند لذا باید اقدامات دفاعی مناسب جهت افزایش مقاومت و رهایی سریع از حملات را اتخاذ کنند.

ب.کاهش عدم تقارن اطلاعات

داده های سایبری کمیاب هستند و این امر رسیدن به یک مدل بندی بهینه را دشوار کرده است، جمع آوری و به اشتراک گذاری داده هایی مانند نوع و فراوانی تهدیدها و تاثیر مادی آنها منجر به رسیدن به مدل بندی بهتر و پیش بینی دقیق تر آینده خواهد شد. تجزیه و تحلیل ماهیت و اندازه ریسک های سایبری باعث بهبود برنامه ریزی های مالی خواهد شد.

ج. طراحی سیاست های موثر

ریسک های سایبری باید با استفاده از دو رویکرد مقررات پیشین و یا مسئولیت‌های پس از وقوع مدیریت شوند. در صورت عدم تقارن اطلاعات بین ناظران و شرکت ها، مقررات قادر به طراحی موثر استانداردها نیستند و مقررات پیشین بدون اثر می گردد. رویکرد مسئولیت‌های پس از وقوع نیز در صورت پاسخگو نبودن شرکت‌ها یا محدودیت مسئولیت‌های آنها بی فایده است لذا تنها راه افزایش مقاومت جهت ایجاد نوآوری، ایجاد تعادل بین این دو رویکرد است. با توجه به ماهیت متمایز ریسک های سایبری باید ساختار نظارتی همواره به‌روزرسانی شود. دیجیتال‌سازی به سرعت در حال پیشرفت است و استفاده از فناوری‌های جدید در بخش مالی روبه رشد است لذا سازمان نظارتی ضمن اینکه به موسسات این امکان را می دهد تا ریسک ها را به روشی که مطلوب می دانند برطرف کنند باید به طور مداوم هیئت ها و مدیران ارشد را از طریق سرمایه گذاری در امنیت سایبری ترغیب به ایجاد مقاومت کند، با این حال اقدامات کشورهای مختلف و فقط شرکت کنندگان در بخش مالی کافی نخواهد بود. برای همگام شدن با ریسک‌های سایبری در حال تحول لازم است که استانداردها در صنعت به طور مداوم توسعه یابند حتی اگر برای موسسات آسیب‌دیده هزینه‌های انطباق ایجاد کند.

د. شکست های هماهنگی آدرس دهی و مدیریت ریسک سیستماتیک سایبری

در ارتباط بین سیستم فناوری اطلاعات و مالی، هماهنگی موثر ملی و بین‌المللی بسیار مهم خواهد بود. دولت‌ها باید اطمینان حاصل کنند که آژانس های مختلف به طور منسجم همکاری و از تکثیر و ابتکار عمل جلوگیری می کنند. از آنجا که ریسک سایبری محسوب به محدوده سیاسی و جغرافیایی خاصی نیست هماهنگی سیاست در سطح بین الملل نیز لازم است. در اینجا سازمان های بین المللی مانند بانک تسویه حساب های بین المللی، هیئت مدیره ثبات مالی یا صندوق بین المللی پول می‌توانند در صورت ظهور نقش اساسی در تسهیل هماهنگی حمایت از اشتراک داده ها، طراحی سیاست های هماهنگ و کمک به حل اختلافات داشته باشند. ریسک های سایبری بسیار متمرکز و پیچیده هستند که باید در سطح شرکت‌ها یا کشورها اداره شوند این یک منبع جهانی از ریسک سیستماتیک است که باید در یک سطح چندجانبه مورد بررسی قرار گیرد.

منبع:

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability.

آزاده فتح‌الله ترشانی (بیمه پارسیان)؛ هما نوروزی (بیمه دانا) و پگاه پزشک‌نژاد (بیمه پارسیان)

بیمه سایبری

۱. مقدمه

امروزه سازمان‌های تجاری و خدماتی مختلف در دنیا در فضای پر تلاطم اقتصادی به منظور حفاظت از سرمایه‌های اطلاعاتی (مانند اطلاعات مالی، سرمایه‌گذاری و پرسنلی) با چالش‌های جدی و پرهزینه‌ای مواجه هستند. همگام با پیشرفت‌های تکنولوژی صورت گرفته در دنیای دیجیتال، شمار تهدیدهای سایبری نیز افزایش یافته و تهدیدات سایبری در زمره‌ی پنج تهدید مهم جهانی قرار گرفته است. از این رو، امنیت در فضای سایبری به یکی از مهم‌ترین چالش‌های پیش روی دولت ها و سازمان‌های خصوصی تبدیل شده است؛ به گونه‌ای که یکی از موضوعات مورد بحث در نشست مجمع جهانی اقتصاد را نیز به خود اختصاص داده است.

بیمه‌ی سایبری، محصول بیمه‌ای است که به منظور محافظت از کسب و کارها و کاربران از خطرات مبتنی بر اینترنت و به طور کلی، از خطرات مربوط به زیرساخت‌های فناوری اطلاعات استفاده می‌شود.

گزارش بازرسی نفوذ اطلاعاتی شرکت ورایزون در سال ۲۰۱۵، سه صنعت خدمات عمومی، خدمات اطلاعاتی و خدمات مالی را به عنوان صنایعی که بیشتر از همه در معرض نفوذ اطلاعاتی هستند شناسایی کرد؛ درحالیکه گزارش پژوهش‌های نهادی پونِمون در همین سال نشان می‌دهد بهداشت و درمان، آموزش و دارو بیشترین هزینه های سرانه را به خود اختصاص می‌دهند. پیام مهم هر دو گزارش این است که هیچ شرکتی از حملات سایبری در امان نیست. بر اساس آخرین تحقیقات منتشر شده توسط یک شرکت بیمه در قاره آسیا تنها ۱۰ درصد از شرکت‌های تجاری در این قاره در برابر حملات سایبری بیمه هستند.

۲. ادبیات موضوع

در حوزه‌ی بیمه‌ی فضای سایبری، پوشش‌های بیمه‌ای در مقابل خسارات وارد بر سیستم‌های رایانه‌ای بانک‌ها به علت دسترسی فیزیکی غیرمجاز کاربران از دهه ۹۰ در ایالات متحده آمریکا ارائه شده است. با افزایش کاربرد رایانه و نیز ایجاد شبکه اینترنت در سال ۱۹۹۵، تنها در سال ۲۰۰۰ در ایالات متحده آمریکا خسارت وارده به سایت‌ها و مراکز فروش اینترنتی رقمی معادل نیم میلیارد دلار اعلام شده است. اوج این حملات سایبری را می‌توان در سال ۲۰۰۱ و پس از حملات تروریستی ۱۱ سپتامبر به برج‌های دوقلوی نیویورک دانست که در کمتر از یک هفته قریب به ۱۲۰۰ سایت دولتی و خصوصی بزرگ تحت حملات سایبری قرار گرفته و هک شدند. این عوامل سبب شد تا تقاضا برای پوشش بیمه‌ای فضای سایبری به طور روزافزون افزایش یافته به طوریکه بر اساس آمار اعلامی موسسه اطلاعات بیمه تنها در سال ۲۰۰۵ بیش از ۲.۵ میلیارد دلار صرف این پوشش شده است. بر این اساس، ۴۰ درصد شرکت‌ها در آمریکا، آلمان و انگلستان از بیمه سایبری استفاده می‌کنند. جدول زیر نمونه‌ای از حملات سایبری سال‌های اخیر به شرکت ها/ موسسات نمایش داده شده است.

برخی از شرکت‌های بزرگ فعال در حوزه بیمه سایبری عبارتند از:

American International Group
The Chubb Corporation
Zurich Insurance Co
XL Group Ltd
Berkshire Hathaway
Allianz Global Corporate & Specialty
Munich Re Group
Lloyds
Lockton Companies

نام سازمان	تعدا افراد هک شده	نوع سازمان	روش حمله سایبری	منبع
Center for Medicare & Medicaid Services	۷۵۰۰۰	مراقبت‌های بهداشتی	هک شده	Deccan Chronicle 2018
Facebook	۵۰۰۰۰۰۰۰	شبکه اجتماعی	ایمنی ضعیف	Perez 2018, Wong 2018
Ticketfly	۲۶۱۵۱۶۰۸	توزیع بلیط	هک شده	Motherboard 2018
MyHeritage	۹۲۲۸۳۸۸۹	شجره نامه	نامشخص	Cimpanu 2018
Google Plus	۵۰۰۰۰۰	شبکه اجتماعی	ایمنی ضعیف	Goodin 2018
BMO and Simplii	۹۰۰۰۰	بانکداری	ایمنی ضعیف	CIBC 2018
Orbitz	۸۸۰۰۰۰	سایت اینترنتی	هک شده	Colascione 2018
Popsugar	۱۲۳۸۵۷	مد	هک شده	Brinza 2018
Under Armour	۱۵۰۰۰۰۰۰۰	کالاهای مصرفی	هک شده	BBC 2018
SingHealth	۱۵۰۰۰۰۰	دولت، پایگاه داده	هک شده	Cheng 2018
British Airways	۳۸۰۰۰۰	حمل و نقل	هک شده	Sandle 2018

۳. انواع پوشش‌ها

ریسک‌های تحت پوشش بیمه سایبری به نوع بیمه‌نامه، اندازه و ماهیت فعالیت‌های تجاری بیمه‌گذار در ارتباط است. عمده پوشش‌های بیمه ای در فضای سایبری را می‌توان در بخش خسارات مالی، سرقت اطلاعات صنعتی و فردی، وقفه در تجارت و نیز ارتباطات دانست. این پوشش‌ها در این بخش عمدتا به دو دسته کلی تقسیم می‌شوند:

۱- پوشش بیمه شخص اول: شامل پوشش از دست دادن یا خرابی سیستم‌های اطلاعاتی، اخاذی در فضای سایبری و نیز کلاهبرداری در زمان انتقال پول الکترونیکی؛

۲- پوشش بیمه شخص ثالث: شامل پوشش آلوده شدن سیستم ها به ویروس و بدافزار و دزدیده شدن اطلاعات کارت‌های تجاری و اعتباری؛

بیمه سایبری شخص اول و شخص ثالث متفاوت از یکدیگرند. پوشش بیمه‌ی شخص اول ضرر مالی خود شخص و صاحب شرکت را جبران و پوشش بیمه شخص ثالث، ضرر وارد شده به یک شخص خارج از شرکت مانند مشتریان یا اعضای عمومی شرکت را جبران می‌کند. این پوشش‌ها به تفکیک زیر دسته‌بندی می‌شوند:

- ✓ پوشش سرقت هویت: هر نوع دسترسی غیر مجاز و جعلی برای استفاده، حذف یا تغییر داده‌های شخصی
- ✓ پوشش مسئولیت رسانه‌ی اجتماعی: هزینه دفاع و پیگرد قانونی علیه سرقت هویتی در حساب کاربری شخصی یا اجتماعی شخص
- ✓ پوشش تهدیدات سایبری: استفاده مکرر از ارتباطات دیجیتال برای آزار و اذیت یا ترساندن افراد
- ✓ پوشش زیان‌های ناشی از سرقت اطلاعات: هزینه‌های ایجاد شده به علت سرقت اطلاعات فرد توسط شخص ثالث
- ✓ پوشش بدافزارها: هزینه‌ی خرابکاری برنامه کامپیوتری که از طریق پیامک، انتقال فایل، دانلود فایل از کامپیوتر یا تلفن همراه و بدون رضایت شخص به سیستم و اطلاعات او آسیب می‌رساند
- ✓ پوشش ایمیل‌های فیشینگ: هر گونه تلاش برای به دست آوردن اطلاعات حساس مانند نام کاربری، رمز عبور و اطلاعات کارت اعتباری به قصد انجام کلاهبرداری
- ✓ پوشش ایمیل جاسوسی: جعل یا دستکاری غیرمستقیم ایمیل و پست های الکترونیکی به طوری که پیام ظاهرا از منبع واقعی منشا گرفته است
- ✓ پوشش خسارت‌های مسئولیت رسانه‌ای: هرگونه مسئولیت ناشی از انتشار ناخواسته یا پخش هرگونه محتوای دیجیتال ناشی از حمله سایبری در سیستم کامپیوتری فرد و تلفن همراه او
- ✓ پوشش اخاذی سایبری: تهدیدات صورت گرفته برای ایجاد سرقت اطلاعات خصوصی و سرقت داده‌ها سرقت اطلاعات خصوصی و سرقت اطلاعات توسط شخص ثالث.

مثالی از پوشش‌های سایبری ارایه شده توسط شرکت‌های بیمه در جدول پیش‌رو نمایش داده شده است. به طورکلی، حملات سایبری ممکن است بروز هر یک از آسیب‌های زیر را برای شرکت‌ها به دنبال داشته باشد:

- از دست رفتن داده‌ها
- وقفه در کسب و کار
- تقلب و تخلفات کامپیوتری
- اخاذی سایبری
- کاهش مستقیم پول نقد از طریق سرقت الکترونیکی
- تلفات ناشی از اخاذی DDoSیا باج افزارها
- هزینه‌های رفع و بررسی حادثه
- از دست دادن اطلاعات به دلیل خرابی
- هزینه‌های حقوقی
- هزینه‌ی خسارت به داده و سیستم‌ها و هزینه‌های مربوط به بازگرداندن سیستم‌ها به حالت عادی.

پوشش بیمه سایبری		Allianz	QBE	AEGIS	CAN	InsureTrust	CDRMLL	Travelers	Zourich	ACE	Hiscox	Insureon	Marsh	Chubb	AIG
شخص اول	ضرر یا خسارت به دارایی‌های دیجیتال	×	×	×	×	×		×	×	×	×	×	×	×	×
	وقفه در کسب و کار	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	اخاذی اینترنتی (سایبری)	×	×	×	×	×	×	×	×			×	×		×
	سرقت پول و دارایی‌های دیجیتال	×	×		×		×	×	×	×	×	×	×	×	
شخص ثالث	از بین رفتن امنیت و حریم خصوصی	×	×	×	×	×	×	×	×	×	×	×	×	×	×
	جمع‌آوری مدارک مهم جرم از رایانه برای ارائه به دادگاه	×	×	×	×	×	×			×		×			×
	هزینه اطلاع رسانی به مشتریان	×	×		×	×	×	×	×	×		×		×	×
	مسئولیت چند رسانه‌ای	×	×	×		×		×	×	×					×
	از دست دادن اطلاعات شخص ثالث	×		×	×	×	×	×	×	×	×	×	×	×	
	پرداخت خسارت شخص ثالث طبق قرارداد		×			×			×	×				×	

در بیمه‌نامه‌های سایبری هرگونه خسارت ناشی از موارد زیر تحت پوشش بیمه قرار نمی‌گیرد (استثنائات):

- اعمال نادرست عمدی، جنایی، کلاهبرداری؛
- تخلف در انجام کارها و وظایف و قراردادها توسط فرد بیمه شده؛
- هرگونه خسارت ناشی از اعمال غیرقانونی و غیر اخلاقی؛
- جنگ، اعمال تروریستی، غارت اموال حکومتی؛
- خطرات طبیعی مانند میدان الکترومغناطیسی یا رادیواکتیوی و زمین لرزه؛
- پخش مکاتبات و ارتباطات به طور مخفیانه (چه در فرم فیزیکی و چه از طریق الکترونیکی).

عمده مشکلات در پوشش بیمه‌ای فضای سایبری را می‌توان در موارد زیر دانست:

۱- عدم شناخت کافی دو طرف قرارداد از خواسته‌ها در هنگام صدور، کارشناسی‌های مشترک و نیز پرداخت خسارت

۲- عدم رشد بیمه‌های اتکایی در این بخش همانند سایر بخش‌ها برای توزیع منطقه‌ای و جهانی ریسک.

۴. تعیین حق بیمه

در تعیین حق بیمه‌ی بیمه سایبری، شناسایی ریسک فاکتورها بسیار حائز اهمیت است. افزایش استفاده از فناوری اطلاعات در کسب و کارهای روزمره از طریق گسترش شبکه‌های اجتماعی، دستگاه‌های تلفن همراه، فناوری‌های بی‌سیم و غیره منجر به افزایش آسیب‌پذیری سازمان‌ها شده است. ریسک‌های این بخش بسته به اینکه تا چه میزان بر عملکرد شرکت‌ها اثرگذار باشند، درجه‌بندی و استانداردسازی شده و بیمه‌ها به نسبت آن با اخذ حق بیمه از مشتریان پوشش بیمه ای لازم را ارائه می‌کنند.

عمده علل عدم ارائه بیمه سایبری از سوی شرکت‌های بیمه را می‌توان به نبود اطلاعات و نیز دانش فنی در حوزه ارائه‌ی طرح و نیز نبود شناخت این سازمان‌ها از این نوع پوشش‌های بیمه‌ای و نبود کافی شفافیت مالی از سوی شرکت‌های متقاضی اینگونه بیمه‌نامه‌ها دانست.

ازآنجایی که دارایی‌های تحت پوشش بیمه‌ی سایبری عمدتا غیرفیزیکی (ناملموس) بوده، تغییرات ریسک در آن به سرعت اتفاق می‌افتد و ارزیابی بیمه‌پذیری مشتریان بالقوه همزمان با دوباره ارزیابی کردن ریسک‌های مشتریان فعلی نیازمند منابع زیادی است، فرآیند کمّی سازی ریسک‌های اینترنتی به منظور تعیین نرخ حق بیمه بهینه را پیچیده خواهد ساخت. در تعیین نرخ حق بیمه‌ی بهینه برای بیمه‌نامه های مختلف اینترنتی، بیمه‌گران با چالش اصلی دیگری همچون گسترش ریسک در بین بسیاری از مشتریان مستقل از هم نیز مواجه هستند. در رابطه با بیمه سایبری باید گفت که بسیاری از کرم‌های اینترنتی جدید و حملات ویروسی آنچنان تاثیرات جهانی داشته که یافتن مشتریانی که ریسک‌هایشان وابسته نباشد، بسیار دشوار است. به طور سنتی، قیمت‌گذاری محصولات بیمه‌ای به جداول اکچوئریال ساخته شده از دیتای سوابق گذشته متکی است. برخلاف بیمه‌نامه‌های سنتی، بیمه‌ی امنیت سایبری فاقد سیستم‌های ثبت داده استاندارد یا جداول اکچوئریال برای نرخ‌گذاری است. ریسک‌های امنیت سایبری نسبتا جدید بوده و داده‌های مربوط به شکست امنیت و ایجاد خسارات امنیتی یا وجود نداشته یا تنها در مقیاس کوچک دردسترس است. این مشکل ممکن است با عدم تمایل سازمان‌ها به فاش کردن جزئیات مرتبط با شکست امنیت به دلیل از دست دادن سهم بازار، از دست دادن شهرت و ... بیشتر شود، البته حتی اگر داده‌های گذشته در این خصوص در دسترس باشد، این اطلاعات به سرعت در حال تغییر بوده که قطعا آمار این داده‌ها را تحت تاثیر قرار خواهد داد.

مطالعات بسیاری در زمینه‌ی مدل‌بندی ریاضی ریسک سایبری انجام شده است. برای مثال، گوردن و همکاران[۳] به بحث در خصوص یک چارچوب کلی در قیمت‌گذاری و مباحث انتخاب نامساعد در بیمه‌ی سایبری پرداخته و یک طرح تصمیم‌گیری چهار مرحله‌ای را برای ریسک سایبری پیشنهاد کرده‌اند. بومِه و کاتاریا[۴] همبستگی بین ریسک‌های سایبری را بررسی و از مدل ریسک پنهان تک عاملی و بتای دوجمله‌ای در مدل‌بندی استفاده کرده‌اند. آنها همچنین به بحث در خصوص همبستگی داخلی ریسک سایبری درون یک شرکت و همبستگی کلی این ریسک در سطح جهانی پرداخته‌اند. یک رویکرد شبکه‌ای بیزی در مدل بندی ریسک سایبری نیز توسط موخپدهی[۵] و همکاران، معرفی شده است. حق بیمه‌های این پوشش نیز به عنوان تابعی از مقدار مورد انتظار شدت خسارت محاسبه شده است. هرات و همکاران[۶] نیز یک مدل اکچوئریال مبتنی بر کاپولا را در قیمت‌گذاری ریسک سایبری پیشنهاد کرده، که دارای سه متغیر ریسک است: وقوع پیشامد، زمان پرداخت و مقدار پرداخت. حق بیمه‌ها برای خسارت‌های شخص اول با توجه به حملات اپیدمی و با استفاده از سه نوع مدل بیمه نامه (بیمه نامه بدون فرانشیز، با فرانشیز و بیمه نامه با بیمه اتکایی و محدوده) محاسبه شده است.

در مقاله‌ی موآچوآ[۷] و همکاران از فرآیندهای تصادفی (مارکوفی و غیرمارکوفی) در توصیف پویایی انتشار اپیدمی در طول زمان استفاده شده است، درحالیکه در بیشتر مقالات قبلی اپیدمی ایستا در نظر گرفته شده است. همچنین در این کار از کاپولا در نمایش وابستگی بین توزیع های زمان سرایت استفاده شده است، درحالیکه در ادبیات اغلب مطالعات فرض استقلال متصور بوده است. آنها از شبیه‌سازی‌های مونت-کارلو برای ارزیابی سطح امنیت شبکه‌ها استفاده کرده‌اند؛ سطح امنیت شامل تعداد حوادث، احتمال ابتلای نودها و زیان‌های کلی است.

البته عوامل متعددی در تعیین و پذیرش ریسک یا اعمال تعدیلات در نرخ حق بیمه، جدا از بحث مبانی محاسباتی حق بیمه، وجود دارد که می‌بایست قبل از پذیرش ریسک بررسی و در تعیین نرخ نهایی حق بیمه اعمال نمود. این اطلاعات به تعیین در معرض خطر بودن شرکت و تعیین محدودیت‌های پوشش بیمه‌ای کمک خواهد کرد. نمونه‌ای از این اطلاعات عبارتند از:

اطلاعات عمومی:

- نام بیمه شده‌ها
- آدرس و اطلاعات تماس
- زمان شروع به کار شرکت
- خلاصه‌ای از فعالیت تجاری اشخاص بیمه شده
- اطلاعات مربوط به درآمد (آخرین سال مالی انجام شده، سال مالی جاری، پیش بینی سال مالی بعدی)
- تعداد کارکنان
- تعداد لپ تاپ‌ها و تعداد سرورها
- افرادی که به اطلاعات شرکت دسترسی دارند (کارمندان، مشتریان خارجی، همکاران، ادارات دولتی، فروشندگان).

اطلاعات شرکت متقاضی:

- میزان پرداخت و دریافت الکترونیکی
- نوع اطلاعات شخصی جمع آوری، پردازش و ذخیره شده (اطلاعاتی درباره کسب و کار مشتری، اطلاعات بهداشتی، حسابداری مالی، اطلاعات کارت اعتباری، شماره پرونده مالیاتی، شماره تامیه اجتماعی و ...)
- میزان خسارت وارده احتمالی
- میزان به اشتراک گذاشته اطلاعات شخصی و حساس شرکت
- میزان ارتباط با شخص ثالث
- تغییر در شرکت (انتظار تغییر چشمگیری در عملکرد شرکت یا محصولات جدید وجود دارد؟)
- کارکنان شرکت (قرارداد کارمندان IT را در ۱۰ ماه گذشته فسخ شده؟ در هنگام استخدام کارمندان جدید، بررسیهای دقیقی انجام شده است؟).

امنیت شبکه:

- نحوه کار با برنامه‌های کاربردی و زیرساخت‌های پشتیبانی (که اطلاعات شخصی را جمع آوری کرده، پردازش و یا ذخیره می‌کنند
- استفاده از تکنولوژی فایروآل
- زمان آزمایش میزان آسیب‌پذیری‌های داخلی و خارجی و آزمایش نفوذ در داده برای بهبود آن
- استفاده از تایید اعتبار دومرحله‌ای برای تمام دسترسی های از راه دور (به عنوان مثال VPN) به شبکه داخلی

مدیریت سازمانی:

- بررسی مسئول مدیریت اطلاعات شرکت؛
- زمان ارزیابی ریسک‌های امنیتی برای اطمینان از بهبود سیاست‌های امنیتی (ماهیانه، سالیانه ، دو سال یکبار)؛
- نوع اقدام هنگام رخ دادن یک حادثه سایبری (استفاده از طرح تداوم کسب و کار، استفاده از طرح پاسخگویی به حوادث هنگام ویروسی شدن یا از دست دادن اطلاعات)؛
- آزمایش طرح‌های موجود؛
- تهیه نسخه پشتیبان از همه اطلاعات ارزشمند و حساس شرکت؛
- نحوه بروزرسانی نرم افزارها.

مدیریت داده‌ها:

- تعداد و نوع داده‌های مربوط به اطلاعات شخصی بیمه‌شدگان؛
- سیاست حفاظت از اطلاعات شخصی؛
- استفاده از آنتی ویروس؛
- میزان رمزنگاری اطلاعات.

چندرسانه‌ای:

- چندرسانه‌ای بودن شرکت (شرکت دارای وبلاگ، خبرنامه، فیلم، پادکست یا سایر نشریات است؟)؛
- استفاده از مالکیت معنوی افراد شخص ثالث در شرکت.

تاریخچه‌ی ادعای خسارت/ سرقت داده‌ها و بیمه‌ی سایبری:

تحولات شرکت در ۵ سال گذشته (قبلا از بیمه سایبری استفاده شده؟ حداکثر پوشش خسارت مورد نیاز و پوشش‌های اضافی مورد نیاز چقدر است؟ هرگونه ادعای خسارت (موفقیت آمیز یا ناموفق) یا شکایت علیه شرکت، کارکنان یا شرکای فعلی، مدیران فعلی یا گذشته صورت گرفته؟ آیا شرکت با سایر شرکت‌ها ادغام شده یا از آنها جدا شده‌اند؟).

در پوشش بیمه‌ی سایبری، اعمال فرانشیز یـا سـهـم بیمه‌گذار از خسارات نیز بر اساس ریسک متفاوت است، اما حدود آن در برخی کشورها تا مرز ۵ میلیون دلار می‌رسد.

در مجموع، تعیین دقیق حق بیمه در این رشته، درکنار درنظر گرفتن کلیه‌ی ریسک فاکتورها، سقف پوشش‌ها، سقف فرانشیز و سایر ملاحظات بیمه‌گری، نیازمند مبانی تئوری به جهت مدل‌بندی ریسک، تعیین حداقل و حداکثر ریسک موجود و قابل پذیرش بر اساس فروض مشخص همچون وابستگی ریسک های تحت پوشش، فراوانی و شدت توزیع ریسک در صورت وقوع بین تمامی سطوح موضوع بیمه است. برای مثال، حق بیمه سالانه پوشش سایبری برای یک مرکز مراقبت درمانی در ایالات متحده با وضعیت عادی حدود ۱.۵۰۱ دلار در هر سال تخمین زده شده است.

نمونه‌ای از استعلام حق بیمه پوشش سایبری در مسیر زیر قابل دریافت است:

http://calculatecyberinsurance.com/calculator.php

بر اساس بررسی‌های انجام شده و فهرست بیمه‌نامه‌های دارای مجوز در بیمه مرکزی ج.ا.ا تاکنون در ایران شرکت بیمه‌ای به ارایه‌ی این پوشش نپرداخته و البته آماری از نرخ های شکست امنیت و وقوع هک در موسسات حقوقی به جهت برآورد موردی حق بیمه در ایران در دسترس نمی‌باشد.

۵. فرآیند پرداخت خسارت

در صورت ادعای خسارت بیمه گذار، اطلاعات و مدارک زیر به جهت پرداخت خسارت مورد نیاز خواهد بود:

- ارسال فرم تکمیل و امضا شده درخواست خسارت؛
- تصویری از گزارش پلیس / مقامات سایبری؛
- تصویری از اطلاعیه حقوقی دریافت شده از هر فرد / نهاد آسیب دیده؛
- تصویر احضاریه از دادگاه‌هایی که افراد یا نهادهای آسیب دیده در آن شکایت کرده‌اند؛
- تصویر مکاتبات با مؤسسات مالی در پرونده‌های مربوط به خسارات سرقت IT؛
- اطلاعیه حقوقی به موسسات مالی در پرونده‌های مربوط به خسارات سرقت IT؛
- تصویر اطلاعیه حقوقی به اشخاص ثالث در پرونده‌های مربوط به سرقت اطلاعات یا نفوذ به حریم خصوصی افراد؛
- تصویر پرونده‌های کیفری علیه شخص ثالث در کلوزهای بیمه‌ای مطرح شده؛
- تصویر فاکتورهای لازم در مواجهه با هزینه‌های ترمیم؛
- تصویر فاکتورهایی که بیمه‌گذار برای پوشش خدمات مشاوره‌ای IT هزینه کرده؛
- فاکتورهای مربوط به هزینه‌های پرونده جنایی/ ادعای خسارت علیه شخص ثالث؛
- ارایه‌ی مدارکی که نشان دهد داده‌ها و اطلاعات شخصی به سرقت رفته، متعلق به بیمه‌گذار بوده است؛
- ارایه ی مدارکی که نشان دهد خسارت و زیان پیش آمده به بیمه‌گذار وارد شده است.

طبیعتا سرفصل های فسخ قرارداد، داوری، شرایط تمدید و تشدید خطر با توجه به ماهیت این پوشش در این بیمه‌نامه نیز متصور خواهد بود.

منابع

1. L. A. Gordon, M. P. Loeb, and T. Sohail. A framework for using insurance for cyber- risk management. *Communications of the ACM*, 46(3):81–85, 2003
2. R. Bohme and G. Kataria. Models and measures for correlation in cyber-insurance. In *Fifth Presented at Workshop on the Economics of Information Security*, University of Cambridge, UK, June 2006.
3. A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan. e-Risk management with insurance: A framework using copula aided Bayesian belief networks. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, vol. 6, 126.1–126.6. Hoboken, NJ: IEEE, 2006.
4. V. S. B. Herath and T. C. Herath. Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2:7–20, 2011.
5. Maochao, Xu. And Lei Hua, ASA. Cybersecurity Insurance: Modeling and Pricing, Society of Actuaries, 2017.

مصاحبه با دکتر حجاریان

۱. لطفاً شرح کوتاهی از سابقه و کارهای آموزشی، پژوهشی و اجرایی تان برای خوانندگان بیان بفرمایید.

من تحصیلاتم را از سال ۱۳۵۳ در دانشگاه علم و صنعت شروع کردم. کارهای آموزشی خود در بعد از انقلاب را از سال ۱۳۶۶ شروع کردم. در دانشگاه‌های امام حسین، تهران و پلی‌تکنیک تدریس کردم و نهایتاً عضو هیات علمی دانشگاه علامه طباطبائی شدم. از سال ۱۳۹۲ یا ۹۳ تا سال ۱۳۹۵ که دیگر بازنشسته شدم، به‌صورت افتخاری در آن جا تدریس می‌کردم. بعداز آن، دیگر به صورت رسمی و ساختاریافته کار آموزشی انجام نداده‌ام. در مورد کارهای پژوهشی هم مقالات بسیار زیادی داشتم، و با دانشجوها برای انتشار چندین مورد کتاب همکاری کرده‌ام. من بیشتر مؤسس بودم، یعنی در واقع ساختارها و سازمان‌هایی که ریشه آموزشی داشتند، نظیر دانشگاه امام حسین و انجمن حرفه‌ای صنعت بیمه را تاسیس کردم. در زمینه کارهای اجرایی هم تاسیس نهادهای عملیاتی نظیر بیمه ملت، سرمایه‌گذاری بهمن، گروه فن‌آوا که یک هلدینگ آی‌تی هست و گروه بهمن که خودرویی هست را بر عهده داشته‌ام.

۲. با چه شاخه‌هایی از اکچوئری بیشتر آشنایی داشته‌اید؟

در مورد رشته اکچوئری، به حوزه مدیریت ریسک و محاسبه ریسک فعالیت‌های مختلف، هم در حوزه بیمه و هم حوزه سرمایه‌گذاری بسیار علاقه‌مند هستم. در محاسبات مربوط به مدیریت پرتفوی و ریسک پرتفوهای مختلف کارهای زیادی انجام داده‌ام و حتی پایان‌نامه‌ی دوره فوق‌لیسانس و دکترای من هم به نوعی تلفیق ریسک و بازده و مربوط به محاسبات ریسک برای افراد مختلف و ایجاد پورتفو با یک زنجیره هوشمند از محاسبات اکچوئری متکی بر ریسک بوده است. در زمینه توانگری مالی فعالیت‌های زیادی انجام داده‌ام. فکر می‌کنم اساساً بیمه مرکزی با پیگیری‌های مداومی که من در این حوزه انجام دادم، بالاخره پذیرفت که آیین‌نامه توانگری مالی را تصویب کرده و کنترلی بر روی میزان ریسک قبولی شرکت‌های بیمه بوجود آورد. هرچند این آیین نامه با مشکلاتی روبرو هست اما به هر صورت چارچوب قابل‌قبولی را در صنعت بیمه پیاده‌سازی کرده است.

۳. علاوه بر دانش اکچوئری، به اکچوئری ها آشنایی با چه حوزه‌های دیگری را پیشنهاد می‌کنید؟

به نظر من اکچوئرهای ما باید علاوه بر محاسبات تئوریک ریاضی، بر روی کاربرد آن درس‌ها در بیمه، به ویژه در شناخت و محاسبات ریسک بیشتر کار کنند. توصیه می‌کنم که از مدل‌های ریسک در بازار سرمایه استفاده کنند. بخش قابل‌توجهی از عملیات شرکت‌های بیمه باید در بازار سرمایه شکل بگیرد. شرکت‌های بیمه ایران متأسفانه از بازار سرمایه فاصله زیادی دارند و تمرکزشان بر فعالیت بیمه‌گری است. درصورتی که منابعی که بیمه‌گر از بخش بیمه‌گری به دست میاورد، باید در بازار سرمایه به بهره‌برداری و به سود برسد و لذا در آن‌جا نباید ریسک زیادی را متقبل شود و باید بازده قابل قبولی با ریسک محدود داشته باشد. چون در صنعت بیمه و بخش بیمه‌گری به اندازه کافی ریسک قبول می‌کند. مثلاً الان این اشکال در آیین‌نامه توانگری ما هم وجود دارد که شرکت‌های بیمه سهام شرکت‌های بیمه‌ی دیگر را می‌خرند. درحالی‌که، سرمایه‌ای که در شرکت‌های بیمه هست برای پوشش ریسک بیمه‌گذارها است. اگر با آن سرمایه، سهام شرکت بیمه دیگری را بخرند، در واقع باید آن مبلغ سرمایه از صورت توانگری مالی‌شان حذف شود ولی بر اساس آئین‌نامه کنونی در حال حاضر نمی‌شود و این موضوع درنظر گرفته نمی‌شود. توصیه می‌کنم که اکچوئرها به بازار سرمایه و حوزه بیمه‌ها و ریسک‌های اعتباری نیز هم توجه داشته باشند. اگر اکچوئرهای ما باید بتوانند وارد مسائل بیمه‌های اعتباری شوند، برای کشور کار بسیار بزرگ و با اهمیتی انجام داده‌اند. اما ما متأسفانه هنوز نتوانستیم در زمینه بیمه‌های اعتباری مطالعات درستی بکنیم تا رتبه اعتباری افراد را بتوانیم اندازه‌گیری کنیم. توصیه می‌کنم بخشی از اکچوئرها مسائل مربوط به ریسک اعتباری و اعتبارسنجی مشتریان را مطالعه و محاسبه کنند. ان شاء ا... به زودی پوشش‌های اعتباری در کشور گسترش پیدا می‌کند و قوانینی نوشته می‌شود که شرکت‌های بیمه موظف به صدور بیمه‌های اعتباری و تضامین می‌شوند. این‌ها همه نیازمند این است که مطالعات اکچوئری به آن سمت گرایش پیدا کرده و حوزه های عملی آن بررسی شوند.

۴. با توجه به این که سال‌ها به عنوان مدیرعامل شرکت بیمه در صنعت بیمه ایران فعالیت داشته‌اید، چه کارهایی برای افزایش حوزه فعالیت یا در جهت خدمت به این رشته در صنعت بیمه ایران انجام داده‌اید؟

در بیمه ملت به عنوان مدیرعامل اقدام به ایجاد واحد مدیریت ریسک کردم و تعداد قابل توجهی از همکاران اکچوئر را در آن واحد جذب کرم. در انجمن حرفه ای صنعت بیمه هم مرکزی را تحت عنوان "مرکز رتبه‌بندی مدیریت ریسک" ایجاد کردم که کار آن مرکز، اندازه‌گیری و رتبه بندی مدیریت ریسک شرکت های بیمه و بیمه گذارها برمبنای استانداردهای ایزو است.

فکر می‌کنم این دو کار، جزء کارهای بزرگی بود که برای کمک به بخش اکچوئری در صنعت بیمه انجام داده‌ام. غیر از آن، بنده اولین کسی بودم که به یک اکچوئر را به عنوان مدیر بیمه‌های زندگی انتخاب کرده و پس از آن به عنوان معاون فنی شرکت به کار گرفتم و به اکچوئرها در سمت های اجرایی فرصت ارائه دانش خود را دادم. همچنین در انجمن حرفه ای صنعت بیمه نیز یک کارگروه بیمه های زندگی داریم که فعالیت‌هایی را در حوزه بیمه‌های زندگی انجام می‌دهد. در مورد اکچوئر رسمی هم همکاری های مشترکی را در زمینه طراحی سوالات آزمون اکچوئر رسمی که بیمه مرکزی برگزار می‌کند، با انجمن اکچوئری دانشگاه شهید بهشتی (انجمن محاسبات بیمه و مالی ایران) انجام داده‌ایم که کم کم اکچوئر رسمی هم در کشور به رسمیت شناخته شود و ان شاء ا... صورت‌های مالی شرکت‌های بیمه از این به بعد، مانند اکثر کشورهای دنیا با امضای اکچوئر رسمی به تصویب برسد.

۵. یکی از اهداف انجمن محاسبات بیمه و مالی ایران برگزاری آزمون‌های تخصصی اکچوئری است، به نظر شما امکان چنین کاری وجود دارد؟

امکان این کار حتماً وجود دارد. چون ما با همکاری انجمن محاسبات مالی و بیمه ایران، آزمون اکچوئر رسمی را اجرا کردیم که می‌توان آن را گسترش داد و آزمون‌ها را برقرار کرد. اما فکر می‌کنم رسالت اصلی انجمن محاسبات بیمه و مالی ایران بیشتر تعمیق علم اکچوئری هست. چون انجمنی علمی است و انجمن حرفه‌ای یا اجرایی نیست. این انجمن باید بتواند منابع علمی و خصوصاً کاربردی بهتر، اساتید مجرب و قوی‌تری را برای کشور تامین کند و دوره‌های پژوهشی و تخصصی بیشتری را برگزار کند و دستاوردهای پژوهشی داشته باشد، یعنی از این انجمن انتظار می رود که ابعاد ناشناخته اکچوئری را برای ما بشناساند. در نتیجه من توصیه ام این است که این انجمن بیشتر به توسعه و تعمیق دانش اکچوئری که تنها مرجع این کار است پرداخته و برگزاری آزمون‌ها را به نهادهای اجرایی تر واگذار نماید. به نظر من برگزاری آزمون، کار یک انجمن حرفه‌ای است اما باید انجمن علمی اکچوئری پشتوانه این کار بوده و ناظر علمی اجرای چنین کاری باشد. اما این‌که انجمن با انجمن‌های حرفه‌ای دنیا چه رابطه‌ای داشته باشد و مدارکی که ما می‌دهیم با مدارک جهانی چه ارتباطی باید داشته باشد، باید بگویم که ما باید سطح حرفه‌ای بودن خود را با آن‌ها منطبق کنیم و حتی شاید بالاتر از آن‌ها درنظر بگیریم. اما اصلاً قبول ندارم که بخواهیم مدارک آن انجمن‌ها را در کشورمان بدهیم. به نظر من، ما باید به طور مستقل نیازهای خود را رتبه‌بندی کرده و کارشناسانمان را به صورت ملی سطح بندی کنیم.

۶. آینده این تخصص را در ایران چگونه می‌بینید؟

با توجه به این‌که تعداد شرکت‌های بیمه در سال‌های اخیر زیادتر شده‌اند و رعایت حقوق بیمه گذار جزو دستورات و دغدغه های دولت و بیمه مرکزی قرار گرفته است، من آینده این تخصص را بسیار خوب می‌بینم. توصیه می‌کنم که متخصصین این رشته روی کسب و کار متکی به رشته خودشان متمرکز شده و از آن خارج نشوند و البته موضوع اکچوئر رسمی را جدی بگیرند. به‌طور حرفه‌ای وارد این تخصص بشوند و بدانند که تمام چند ده میلیون نفر بیمه گذار کشور چشم‌شان به امضای آن‌هاست و امضای آن‌ها یک ارزش تخصصی سطح بالایی است. مسئولیت‌پذیری، کار سالم، کار عمیق را سرلوحه کار خود قرار داده و درواقع ارزش خودشان را حفظ کنند و ان شاءالله درآینده جایگاه بسیار خوبی خواهند داشت و از نظر درآمدی هم فکر می‌کنم از بالاترین درآمدهای صنعت بیمه بهره‌مند خواهند شد.

۷. آینده انجمن محاسبات بیمه و مالی ایران را چگونه می‌بینید؟ چه راه‌هایی برای پیشرفت این انجمن در کشور پیشنهاد می‌دهید؟

این انجمن به نظر من آینده بسیار خوبی دارد. راه پیشرفت آن را در این می‌بینم که ما پژوهشکده اکچوئری در کشور راه‌اندازی کنیم و دانشگاه شهید بهشتی هم دانشگاه بسیار خوبی است که می‌تواند این‌کار را انجام دهد. اگر پژوهشکده‌ای تاسیس شود، جایگاه بسیار بالایی خواهد داشت. به نظر من انجمن محاسبات بیمه و مالی می تواند همکاری مشترکی با پژوهشکده بیمه در ایجاد یک دپارتمان اکچوئری، ابتدا در پژوهشکده بیمه و سپس به صورت مستقل در دانشگاه انجام دهد که در این پژوهش‌کده اساتید دانشگاه سوپر وایزر باشند و دانشجویان دکتری رو به تحقیقات بیشتر به کار بگیرند، تا پروژه‌های تحقیقاتی کاربردی زیادی را در این رشته در صنعت بیمه داشته باشیم.

۸. در آخر اگر مطلبی یا پیشنهادی دارید لطفا بفرمایید؟

این خبرنامه ای که راه اندازی کرده اید کار بسیار خوبی است. توصیه می‌کنم آن را تقویت کنید و همچنین با کسانی که در این رشته تحصیل کرده‌اند، شبکه‌های اجتماعی در کانال‌ها ایجاد کنید تا ارتباط مستمری را با همه اکچوئرهای کشور با هدایت و سرپرستی این انجمن به وجود آورید. انشاءالله.

مصاحبه از فاطمه نصیری، شرکت بیمه رازی

راهبردهایی برای شناسایی ادعاهای خسارت ساختگی در صنعت بیمه اتومبیل

۱. مقدمه

تقلب در شرکت‌های بیمه به یک آسیب قابل توجه مبدل شده است و در صورتی که به درستی به آن پرداخته نشود، نه تنها سودآوری بیمه‌گر را در معرض خطر قرار می‌دهد، بلکه اثر منفی بر زنجیر ارزش صنعت بیمه دارد و می‌تواند بینهایت مضر برای ساختار اقتصادی و اجتماعی رسمی باشد. علاوه بر آن، تمام بیمه‌گذاران صادق قربانی می‌شوند.

در این مقاله، با استفاده از یادگیری الگوریتمی ادعاهای خسارت را از لحاظ مشکوک بودن به تقلب رتبه‌بندی می‌کنیم. پس از شرح مباحث فنی مجموعه‌ای از داده‌های واقعی مورد بررسی قرار می‌گیرد. این داده‌ها شامل پرونده‌های خسارت مختومه اتومبیل در کشور اسپانیا است که توسط کارشناسان حوزه (شناسایی تقلب) مورد تحقیق و تفحص واقع شده و برای آنها ریز اطلاعات هزینه‌ای در اختیار است.

۲. تصمیم‌سازی حساس به هزینه

مدل سازی آماری و تحلیل داده‌رهنمون، فرصتِ مدرن سازی فرایند شناسایی تقلب با استفاده از ابزارهای هوشمند مانند یادگیری نظارت شونده و غیر نظارت شونده را فراهم می‌کند. یکی از مهم ترین کارکردهای یادگیری نظارت شونده، رده‌بندی است. در فنون رده‌بندی، با استفاده از یک مجموعه داده آموزشی که دارای رده معلومی هستند تلاش می‌شود به صورت الگوریتمی اشیاء جدید (به عنوان بردارهای پیشگو) به آن رده‌ها تخصیص داده شود. هر چند تخصیص اشیاء جدید به رده‌های معلوم با استفاده از الگوریتم‌های یادگیری توام با خطاست اما در عمل کاهش هزینه رده‌بندی (یا عوارض تخصیص‌های نادرست) بسیار مهم‌تر است. به عنوان مثال فرض کنید در معاینه افراد دو رده مبتلا به یک بیماری کشنده و عدم ابتلا به آن بیماری وجود دارد. اگر نتیجه بررسی (رده‌بندی) به اشتباه فرد بیمار را به رده سالم (غیر مبتلا) تخصیص بدهد آنگاه هزینه‌ی آن مرگ فرد است که به مراتب پرهزینه‌تر از تخصیص یک فرد سالم به رده مبتلا به بیماری است.

به طور مشابه در ارزیابی ادعاهای خسارت بیمه‌ای با استفاده از غربالگری خودکار می‌توان یک گردش کار مطلوب برای رده‌بندی ادعاهای خسارت فراهم کرد. ادعاهای خسارتی که فاز غربالگری (خودکار) اولیه را می‌گذرانند طبق روال همیشگی به سرعت و با هزینه‌ی پردازشِ پائین، تسویه می‌شوند. اما ادعاهای خسارتی که برچسب مشکوک می‌خورند، وارد فرایند هزینه‌بر و زمان‌بر تحقیق و تفحص می‌شوند. بر این اساس طراحی تصمیم بهینه برای غربالگری ادعاهای خسارت باید این نامتقارنی در هزینه‌ها را در نظر بگیرد. در عمل بر اساس سوابق پیشین رده‌ای از ادعاهای خسارت تقلبی وجود دارد که معمولا نادر است اما در صورتی که شناسایی نشود هزینه نسبتا سنگینی به دنبال دارد. رده‌بندی خودکاری که به این مسئله حساس نیست احتمالاً موفقیت آمیز هم نخواهد بود. به همین دلیل برخی از پژوهشگران مخالف در نظر گرفتن نرخ خطا به عنوان ملاک ارزیابی عملکرد رده‌بندی هستند. زیرا در روش مبتنی بر نرخ خطا، فرض بر یکسان بودن هزینه رده‌بندی نادرست است. در حالی که با شرحی که در بالا گفته شد در عمل در بسیاری اوقات چنین نیست. تحت فرض یکسان نبودن هزینه رده‌بندی نادرست، تصمیم گیری حساس به هزینه مناسب‌تر است.

۲.۱- رده‌بندی حساس به هزینه ادعاهای خسارت

ابتدا باید متذکر شویم که در این مقاله تنها حالت دو رده‌ای در نظر گرفته شده است. بر این اساس و با استفاده از تصمیم بهینه‌ی بیزی بردار x در فضای $\mathbb{R}^k$ باید به نحوی به دو رده $t\in\{0,1\}$ تخصیص داده شود که متوسط هزینه رده‌بندی مینیمم شود. به عبارتی تصمیم بهینه‌ی بیزی، رده‌بندی را با رویکرد زیر انجام می‌دهد:

$$\arg\min_{t\in\{0,1\}} \sum_{j=0}^{1} p\left(j\,|x\right) C_{t,j}\left(x\right)$$

که در آن $p(j|x)$ احتمال شرطی رده j به شرط بردار پیشگوی x، و $C_{t,j}(x)$ هزینه رده‌بندی یک داده با بردار پیشگوی x و رده‌ی واقعی j در رده‌ی t است. اطلاعات هزینه موجود معمولا به صورت ماتریس هزینه C بیان می شود.

$$C=\begin{bmatrix} C_{0,0}(x) & C_{0,1}(x) \\ C_{1,0}(x) & C_{1,1}(x) \end{bmatrix}$$

در این ماتریس، کد ۰ برای وضعیت درست و کد ۱ برای وضعیت ساختگی (تقلب) استفاده می‌شود. تحت برخی شرایط می‌توان نشان داد که اگر:

$$\mathrm{p}\left(j=1|x\right) > \frac{C_{1,0}(x)-C_{0,0}(x)}{C_{1,0}(x)-C_{0,0}(x)+C_{0,1}(x)-C_{1,1}(x)}$$

آنگاه x به رده ۱ و در غیر این صورت به رده صفر تخصیص داده می‌شود. برای محاسبه احتمال در رابطه بالا از رگرسیون لوژستیک استفاده می‌شود:

$$\mathrm{p}\left(j=1|x\right)=\frac{\exp\left(b'+w^T x\right)}{1+\exp\left(b'+w^T x\right)}\;;b'=b+\ln\left(\frac{p(j=1)}{p(j=0)}\right)$$

که در این رابطه w بردار ضرایب رگرسیونی و b مقدار ثابت مدل رگرسیونی است. به علاوه $p(j=1)$ و $p(j=0)$ احتمال‌های پیشینی مربوط به دو رده دارای ادعاهای ساختگی و ادعاهای درست هستند.

می توان با استفاده از داده‌های آموزشی برآوردهای درستنمایی ماکسیمم بردار ضرایب و مقدار ثابت مدل رگرسیونی را برآورد کرد. هر چند ممکن است با توجه به شرایط داده‌های آموزشی نتایج به دست آمده اریب باشند که در این صورت استفاده از رگرسیون لوژستیک موزون می‌تواند مفید باشد.

۲.۲- داده‌ها و فرض ساختار هزینه

نمونه تصادفی از ادعاهای خسارت اتومبیل در اثر حادثه برای یک شرکت بیمه بزرگ مربوط به کشور اسپانیا در طی سال ۲۰۰۰ در اختیار است. تمام ادعاهای خسارت مورد بازرسی قرار گرفته‌اند و شرکت بیمه پس از فرایند تحقیق و تفحص آنها را به دو رده ساختگی و صادقانه رده‌بندی کرده است. این مجموعه داده شامل ۲۴۰۳ ادعای خسارت است که از بین آنها ۲۲۲۹ ادعای موجه (درست) و ۱۷۴ مورد ساختگی بودند. بر این اساس ۷.۲۴٪ از ادعاهای خسارت ساختگی هستند. جدول پیش رو متغیرهای لحاظ شده در مجموعه داده‌های تحت بررسی را نشان می‌دهد.

نام	نوع	شرح	نام	نوع	شرح
fraud	اسمی	نوع ادعای خسارت	policyage	پیوسته	سال‌هایی که بیمه شده با شرکت بیمه بوده است
cov۱	اسمی	مسئولیت شخص ثالث برابر یک، در غیراین صورت صفر	fault	اسمی	راننده دیگر مقصر بودن در تصادف را قبول کند برابر یک، صفر در غیر این صورت
cov۲	اسمی	مسئولیت شخص ثالث باضافه حریق/دزدی/ شکست شیشه برابر یک، در غیر این صورت صفر	NFS	اسمی	استفاده از سیستم بدون کروکی برابر یک، در غیر این صورت صفر
veh۱	اسمی	اتومبیل برای استفاده شخصی برابر یک، صفر در غیر این صورت	weekend	اسمی	رخداد تصادف در آخر هفته برابر یک، در غیر این صورت برابر صفر
veh۲	اسمی	موتورسیکلت برابر یک، صفر در غیر این صورت	delay	اسمی	ادعای خسارت در دوره قانونی مقرر به شرکت گزارش نشده یک، صفر در غیر این صورت
age	پیوسته	سن راننده بیمه شده در زمان وقوع تصادف	claim amount	پیوسته	قیمت گذاری بیمه گر بر زیان های وسیله نقلیه (به محض این که مبالغ کسر شدنی در صورت وجود کسر شود)
gender	اسمی	راننده بیمه شده مرد برابر یک، صفر در غیر این صورت	audit cost	پیوسته	هزینه تحقیق و تفحص درباره تخلف
records	پیوسته	تعداد ادعاهای خسارت قبلی بیمه شده			

در عمل فرض می‌شود که بازرسی ادعای خسارت ماهیت واقعی ادعای خسارت را به طور دقیق مشخص می‌کند. از آن جا که گواهی ساختگی بودن ادعای خسارت دلیلی برای عدم پرداخت ادعای خسارت است، ساختار هزینه را به صورت جدول زیر به دست می‌آوریم.

واقعیت / رده‌بندی	خسارت واقعی	خسارت ساختگی
خسارت واقعی	صفر	مبلغ ادعای خسارت
خسارت ساختگی	هزینه بازرسی	هزینه بازرسی منهای مبلغ ادعای خسارت

۳. بحث و نتایج

در این مقاله شش سناریو مورد مطالعه قرار گرفته است. تفاوت این سناریوها در نحوه دسترسی به اطلاعات هزینه‌ای در فرایند غربالگری ادعاهای خسارت‌هاست.

۳.۱- سناریو یک: رده‌بندی بدون در نظر گرفتن هزینه

در این سناریو فرض بر این است که هیچ اطلاعات هزینه‌ای در زمان رده‌بندی در شرکت بیمه موجود نیست. در نتیجه برای شرکت بیمه هیچ گزینه‌ای به جز رده‌بندی مبتنی بر خطا باقی نمی‌ماند.

هنگامی که متغیرهای اکتشافی در مدل گنجانده می شود آماره آزمون نسبت درستنمایی ۴۰.۲۸ با ۱۲ درجه آزادی است که نشان می‌دهد بهبود معنی‌داری در مدل در مقایسه با مدل محدود شده شامل عبارت ثابت، رخ می‌دهد. بر اساس احتمال تقلب به نظر می‌رسد که پوشش بیمه نامه، نوع وسیله نقلیه، جنسیت طرف بیمه شده و تعداد سال‌های همراهی طرف بیمه شده در شرکت از نظر آماری معنی‌دار هستند.

بر اساس این سناریو هر ادعای خسارت ورودی که احتمال تقلب برای آن بیشتر از ۵۰ درصد پیشگویی شود به عنوان ادعای خسارت ساختگی و در غیر این صورت به عنوان ادعای خسارت صادقانه برچسب زده می‌شود. هزینه‌ی ارزیابی ادعاهای خسارت و رده‌بندی در این سناریو جمعا برابر ۲۱۰۰۷۹.۶۳ یورو شد. با این وجود بر اساس خروجی‌های به دست آمده از این سناریو تمام ادعاهای خسارت در رده صادقانه قرار گرفتند. در نتیجه به نظر می‌رسد که این سناریو برای اهداف شناسایی تقلب مناسب نیست. هر چند ممکن است با افزودن مبالغ ادعاهای خسارت پیشگویی حاصل از مدل بهبود پیدا کند.

اگر به طور شهودی آستانه رده‌بندی را برابر ۰.۰۷۲۴، که همان درصد پرونده های ساختگی در نمونه تصادفی است، در نظر بگیریم نتایج بهتری از این سناریو به دست می‌آید. با این تغییر، سناریوی رده‌بندی بدون در نظر گرفتن هزینه، ۶۵.۵٪ رده‌بندی درست فراهم می‌کند؛ به طور دقیق‌تر ۵۴٪ پیشگویی درست در موارد ساختگی و ۶۶.۴٪ پیشگویی درست در موارد صادقانه انجام گرفت. توجه کنید که

$$0.54\times0.0724+0.664\times(1-0.0724)=0.655$$

با این تغییر در سناریوی یک، هزینه کل رده‌بندی برابر مقدار مثبت ۷۱۰۴۹.۲ می‌شود. علاوه بر این محاسبات نشان داد که گنجاندن مبلغ ادعای خسارت در بین پیشگوهای مدل، نتایج را بهبود بخشیده و منجر به هزینه منفی کل ۵۶۶۹۳.۳۴- یعنی سود برای شرکت می شود.

۳.۲- سناریو دوم: رده‌بندی با داشتن فهرست کامل هزینه‌ها

در این سناریو فرض بر این است که شرکت بیمه به تمام اطلاعات هزینه انفرادی، یعنی مبلغ ادعای خسارت و هزینه بازرسی در زمان غربالگری دسترسی دارد. مدل رگرسیونی لوژستیک برای پیشگویی احتمال ادعای خسارت با تمام متغیرهای پیشگو به کار برده می‌شود. سپس مقدار آستانه‌ای برای رده‌بندی بر اساس نظریه شرح داده شده در بخش دوم محاسبه می‌شود. این مدل در ۹۹.۴۲٪ موارد رده‌بندی درستی فراهم کرده است. علاوه بر این هزینه سناریوی دوم برابر ۱۶۳۰۳۱.۴- شد. البته باید توجه داشت که این سناریو قابلیت اجرای عملی ندارد، زیرا هزینه دقیق تحقیق و تفحص برای یک ادعای خسارت خاص معمولا تا تکمیل تحقیق و تفحص معلوم نیست. با این وجود، این سناریو را می‌توان به عنوان یک مرجع برای سناریوهای بعدی در نظر گرفت.

۳.۳- سناریو سوم: رده‌بندی با داشتن متوسط هزینه‌ها

در این سناریو فرض بر این است که شرکت بیمه در زمان غربالگری ادعاهای خسارت به میانگین مبلغ ادعای خسارت و میانگین هزینه بازرسی دسترسی دارد. برای داده‌های اتومبیل کشور اسپانیا میانگین مبلغ هزینه بازرسی ۷۲.۲۶ یورو و میانگین مبلغ ادعای خسارت ۸۱۸.۱۴ یورو است.

از آنجا که اطلاعات هزینه‌ای در دسترس ربطی به ماهیت ادعای خسارتِ در حال غربالگری ندارد، از یک آستانه رده‌بندی ثابت برابر ۰.۰۴ برای این سناریو استفاده شد. بر این اساس دقت پیشگویی رده ادعاهای خسارت ضعیف بود به نحوی که تنها ۲۳.۵۱٪ موارد درست پیشگویی شده است. با این حال درصد پیشگویی صحیح در ادعاهای خسارت ساختگی ۸۹.۶٪ بود که نسبتا مطلوب است. اما برای ادعاهای خسارت صادقانه پیشگویی صحیح برابر ۱۸.۳۵٪ بود. در این سناریو هزینه کل برابر ۳۸۵۳۳.۴۸- یورو است.

۳.۴- سناریو چهارم: رده‌بندی با داشتن مبلغ ادعای خسارت انفرادی و متوسط هزینه بازرسی

در این سناریو فرض بر این است که شرکت بیمه مبلغ ادعای خسارت انفرادی و میانگین هزینه بازرسی برای هر ادعای خسارت ورودی در زمان غربالگری را دارد. مقدار آستانه‌ای برای رده‌بندی با در نظر گرفتن اطلاعات موجود درباره مبلغ ادعای خسارت انفرادی و میانگین هزینه بازرسی محاسبه می‌شود. این سناریو به طور کلی ۶۲.۶۳٪ پیشگویی درست داشته است؛ که ۶۶.۶۷٪ در پرونده‌های ساختگی و ۶۲.۳۱٪ در پرونده‌های صادقانه بوده است. هزینه ناشی از این سناریو برابر ۷۱۸۳۲.۲- یورو می شود.

۳.۵- سناریو پنجم: رده‌بندی با داشتن مبلغ ادعای خسارت انفرادی و هزینه بازرسی پیشگویی شده از یک مدل واحد

این سناریو شبیه به سناریو قبلی است با این تفاوت که به جای استفاده از متوسط هزینه بازرسی، مقدار هزینه بازرسی از یک مدل رگرسیون خطی پیشگویی می‌شود. برای تعیین مقدار آستانه از اطلاعات موجود درباره مبلغ ادعای خسارت انفرادی و هزینه بازرسی پیشگویی شده استفاده می‌شود. با این مقدار آستانه ۵۸.۱۸ درصد از ادعاهای خسارت به درستی رده‌بندی می‌شوند. به طور دقیق‌تر ۷۱.۲۶٪ از ادعاهای خسارت ساختگی و ۵۷.۱۶٪ از ادعاهای خسارت صادقانه به درستی تشخیص داده می‌شوند. هزینه کلی این سناریو نیز برابر ۷۰۵۶۹.۴۱ - یورو می شود.

۳.۶- سناریو ششم: رده‌بندی با داشتن مبلغ ادعای خسارت انفرادی و هزینه بازرسی پیشگویی شده از مدل چندگانه

در این سناریو سعی بر این است که پیشگویی هزینه بازرسی با استفاده از دو مدل رگرسیون خطی جداگانه (یک مدل برای پرونده‌های ساختگی و دیگری برای پرونده‌های صادقانه) بهبود داده شود. منطق بنیادین این تصمیم آن است که هزینه بازرسی بسته به این آیا یک ادعای خسارت در واقعیت ساختگی است یا نه، گرایش به نمایش رفتار متفاوت دارد.

به محض این که هزینه بازرسی مورد انتظار برای یک ادعای خسارت ورودی محاسبه می‌شود، به همراه اطلاعات مبلغ ادعای خسارت انفرادی و احتمال ساختگی بودن ادعای خسارت برای محاسبه آستانه رده‌بندی مورد استفاده قرار می گیرد. این سناریو به درصد طبقه بندیِ درستِ ۵۸.۸۹٪ یعنی ۷۰.۹۶٪ و ۵۹.۴۷٪ به ترتیب برای زیر نمونه‌های پرونده‌های ساختگی و صادقانه منجر می‌شود. این سناریو هزینه کلی برابر ۷۱۳۹۶.۲۷- به همراه دارد. خلاصه ۶ سناریوی مطرح شده به شرح زیر است

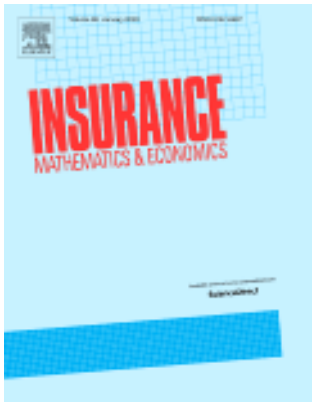
سناریو	تشخیص ساختگی (درصد)	تشخیص کلی (درصد)	هزینه کل (یورو)
اول	۵۴	۶۵,۵	۷۱۰۴۹
دوم	۹۹,۴۳	۹۹,۴۳	-۱۶۳۰۳۱
سوم	۸۹,۶	۲۳,۵۱	-۳۸۵۳۳
چهارم	۶۶,۶۷	۶۲,۳۳	-۷۱۸۳۳
پنجم	۷۱,۲۶	۵۸,۱۸	-۷۰۵۶۹
ششم	۷۰,۹۶	۵۸,۸۹	-۷۱۳۹۶

منبع:

Viaene S., Ayuso S., Guillen M., Van Gheel D., Dedene G.(2007).”Strategies for detecting fraudulent claims in the automobile insurance industry”. European Journal of Operational Research 176 (2007) 565–583.

محمد رضا اناری، مدیر گروه مطالعات و مدیریت بازار شرکت بیمه ایران

مجلهٔ بیمه: ریاضیات و اقتصاد



مجلهٔ بیمه: ریاضیات و اقتصاد Insurance: Mathematics and Economics پژوهش‌های شاخص فراگیرندهٔ کلیهٔ حوزه‌های تحقیقات علم بیم‌سنجی را چاپ می‌کند. این مجله شش شماره در سال منتشر می‌شود و جامع‌ترین مجله در تحقیقات علم بیم‌سنجی در سراسر جهان است.

بیمه: ریاضیات و اقتصاد یک مجلهٔ دانشگاهی بین‌المللی است که هدفش تقویت ارتباط بین افراد و گروه‌هایی است که نتایج تحقیقات خود را در علم بیم‌سنجی به دست آورده و آن را به کار می‌گیرند. این مجله تعهد ویژه‌ای برای تسهیل همکاری نزدیک‌تر بین کسانی که در زمینهٔ ریاضیات بیمه و اقتصاد بیمه کمّی دست به تحقیق می‌زنند، و بیم‌سنجان کارورزی که علاقه به پیاده‌سازی این نتایج دارند، در خود حس می‌کند. برای این منظور، مجلهٔ بیمه: ریاضیات و اقتصاد مقاله‌های با کیفیت بالا و مورد توجه گسترده در سطح جهانی را که یا مربوط به نظریهٔ ریاضیات بیمه و اقتصاد بیمهٔ کمّی یا کاربرد مبتکرانهٔ آن هستند، از جمله نتایج تجربی یا آزمایشگری، را منتشر می‌کند. به‌خصوص مقاله‌هایی که چندین مورد از این جنبه‌ها را باهم ترکیب می‌کنند، از توجه ویژه‌ای برخوردارند.

موضوعات مورد توجه مجله مشتمل‌اند بر نظریه، مدل‌ها و روش‌های بیمهٔ زندگی (ازجمله سیستم‌های بازنشستگی، بیمه‌های اجتماعی و بیمه‌های درمانی)، بیمهٔ غیرزندگی، و بیمهٔ اتکایی و سایر تمهیدات توزیع مخاطره. این موضوعات همچنین کاربردهای نوآورانهٔ بیمه‌ای نتایج حاصل در حوزه‌های مرتبط، ازجمله احتمال و آمار، علوم کامپیوتر و آنالیز عددی، اقتصاد کمّی، ریاضیات مالی، تحقیق در عملیات و علم مدیریت و به ویژه مدیریت مخاطرهٔ کمّی را شامل می‌شوند. پایگاه‌های نمایه‌کنندهٔ این مجله عبارت‌اند از:

- Mathematical Reviews
- Current Index to Statistics
- UMI Data Courier
- Zentralblatt MATH
- INSPEC
- Current Contents
- IAR
- RePEc
- Science Citation Index
- Social Sciences Citation Index
- CIS
- Journal of Economic Literature
- Scopus
- ABI/Inform

محمد قاسم وحیدی اصل، استاد دانشگاه شهید بهشتی

انتصاب‌های جدید اکچوئری‌ها

فاطمه نصیری

ایشان اخیرا به عنوان رئیس اداره ریسک و اکچوئری بیمه‌های غیرزندگی در شرکت بیمه رازی منصوب شده‌اند. همزمان با این سمت، ایشان اکچوئری بیمه‌های غیرزندگی شرکت بیمه رازی نیز هستند. پیش‌تر نیز به عنوان اکچوئر بیمه‌های غیرزندگی با شرکت بیمه ملت همکاری داشته‌اند.

فاطمه سادات آل‌حسینی

ایشان اخیرا به عنوان رئیس اداره ریسک، اکچوئری و تطبیق مقررات شرکت بیمه کارآفرین انتخاب شده‌اند. پیش‌تر در سمت معاون اداره ریسک به همکاری با این شرکت مشغول بوده‌اند. ایشان مدتی نیز به عنوان کارشناس اداره محاسبات فنی بیمه‌های زندگی و اکچوئری داخلی با بیمه کارآفرین همکاری داشته‌اند. علاوه بر این سرکارخانم آل‌حسینی دارنده پروانه اکچوئری رسمی بیمه مرکزی در حوزه بیمه‌های زندگی نیز هستند.

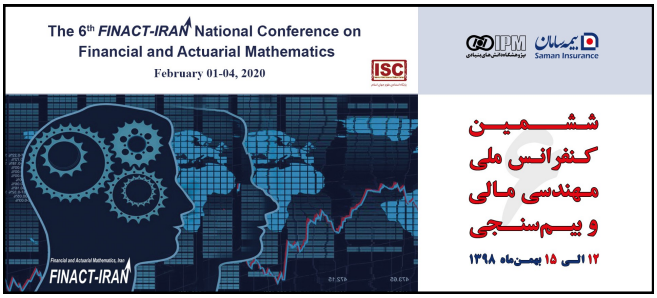
طرح یک سوال پژوهشی

سیستم‌های پاداش-جریمه، به عنوان رویکردی برای تعدیل نرخ حق بیمه و کنترل پیامدهایِ منفی استفاده از بیمه، در حوزه بیمه‌های اتومبیل بسیار رایج شده و در عمل نیز استفاده می‌شود. با توجه به کارکردهای این سیستم‌ها آیا امکان استفاده از آنها در سایر بیمه‌ها نیز وجود دارد؟

به عنوان مثال آیا می‌توان چنین سیستم‌هایی را برای بیمه‌های درمان نیز به کار گرفت؟ در این صورت آیا می‌توان امیدوار بود که هم مراجعه‌های غیرضروری برخی از بیمه‌گذاران به مراکز درمانی کم شود و هم افرادی که هیچ مراجعه‌ای نداشته‌اند به تمدید بیمه‌نامه ترغیب بشوند.

رحیم محمودوند، عضو هیات علمی دانشگاه بوعلی سینا

گزارش کنفرانس‌های برگزار شده



ششمین کنفرانس ملی مهندسی مالی و بیم‌سنجی با همت گروه مهندسان مالی و بیم‌سنجی ایران و با حمایت بیمه سامان و انجمن محاسبات بیمه و مالی ایران و سایر نهادها در نیمه نخست بهمن سال جاری برگزار شد.

یکی از نکات متمایز این کنفرانس نسبت به دوره‌های پیشین، حضور دو استاد غیرایرانی برجسته در حوزه بیم‌سنجی و ارائه سخنرانی و برگزاری کارگاه توسط آنها بود. پروفسور دن کوسروفسکی از دانشگاه نیو برونزویک کانادا در زمینه احتمال ورشکستگی به ارائه سخنرانی پرداختند. همچنین پروفسور خوزه گریدو از دانشگاه کنکوردیا کانادا نیز در زمینه مدل‌بندی مرگ و میر سخنرانی کردند. پروفسور گریدو علاوه بر سخنرانی در نخستین روز کنفرانس، کارگاهی نیز درباره کاربردهای یادگیری ماشین در بیمه در روزهای بعدی کنفرانس ارائه کردند.

تنوع در سخنرانی‌ها و پرداختن به فنون جدید، به ویژه در حوزه کاربردهای یادگیری ماشین و علم داده در بیمه و مالی، از جمله ویژگی‌های جذاب دیگر این کنفرانس بود.

با وجود آنکه تامین هزینه‌های برگزاری کنفرانس در شرایط فعلی بسیار دشوار شده است، کنفرانس مهندسی مالی و بیم‌سنجی با رایزنی‌های قابل تقدیر برای دومین سال و به منظور تشویق ارائه دهندگان مقاله، جوایزی را برای مقاله‌های برتر در بخش دانشجویی و غیردانشجویی در نظر گرفته بود.

حضور چهره‌های دانشگاهیِ برجسته از دانشگاه‌های مختلف کشور، دانشجویان تحصیلات تکمیلی، علاقمندان و سیاستگذاران از صنعت بیمه، نهادهای مالی و سایر موسسه‌های مرتبط در این کنفرانس بدون شک باعث اثربخشی بیشتر و تحقق اهداف آن خواهد شد.

ضمن سپاس از برگزار کنندگان این کنفرانس امید داریم حرکت در مسیر پویایی و آشتی صنایع با دانش فنی دانشگاهیان و تبادل و تضارب آراء آنان با ابتکار عمل برگزار کنندگان چنین کنفرانس‌هایی مستدام و رو به ارتقاء باشد.

رحیم محمودوند، عضو هیات علمی دانشگاه بوعلی سینا

کنفرانس‌های آتی

انجمن محاسبات بیمه و مالی ایران (انجمن اکچوئری ایران) در تابستان سال ۱۳۹۹ افتخار میزبانی اندیشمندان، صاحب نظران، اساتید، مدیران ارشد، کارشناسان و دانشجویان را در کنفرانس بین‌المللی «توانگری در بیمه‌های زندگی و طرح‌های بازنشستگی» خواهد داشت. بی تردید برگزارکنندگان همایش با تمام توان خود تلاش خواهند کرد تا این رخداد علمی را به فرصتی ارزشمند برای ارائه ایده‌های جدید و هم‌افزایی دانش و تجربه‌های نوین در بهبود روش‌ها و فرایندهای شناسایی، سنجش و مدیریت ریسک و ظرفیت‌های ارزیابی و بهبود توانگری مالی در صنعت بیمه و طرح‌های بازنشستگی تبدیل کنند. اهداف این همایش به شرح زیر است:

- شناخت مدل‌های ارزیابی توانگری در بیمه های زندگی و طرح‌های بازنشستگی
- مروری بر تجارب موفق جهانی در توانگری با تأکید بر بیمه‌های زندگی و طرح‌های بازنشستگی
- آشنایی با ماهیت، ابعاد و مدیریت ریسک‌های مالی و غیرمالی در بیمه‌های زندگی و طرح‌های بازنشستگی
- بررسی گزینه‌های بهبود مدیریت دارایی‌ها و بدهی‌ها و سرمایه گذاری‌های بیمه‌های زندگی و طرح‌های بازنشستگی

اطلاعات تکمیلی درباره محورهای کنفرانس، تاریخ‌های مهم و نحوه مشارکت در این کنفرانس در irsoa2.ir قابل پیگیری است.

سوال‌های تخصصی اکچوئری شماره ۸

فرض کنید تابع احتمال توام متغیرهای تصادفی X، Y و Z به صورت زیر است:

f(x,y,z)	x	y	z
۰.۱۰	۳۰	۱۰	۶۰
۰.۱۰	۲۰	۳۰	۳۰
۰.۳۰	۲۰	۳۰	۱۰
۰.۳۰	۰	۳۰	۳۰
۰.۲۰	۶۰	۴۰	-۴۰

۱. مقدار در معرض ریسک (VaR) را برای X، Y، Z، X+Y، X+Z، Y+Z و X+Y+Z در سطح ۶۰ درصد محاسبه کنید.

۲. مقدار سرمایه توانگری حساب شده با $VaR_{0.60}$ برای X+Y+Z را به بخش‌های X، Y و Z به روش:

الف- تناسبی (proportional)

ب- حاشیه‌ای (marginal principle)

توزیع کنید.

پاسخ سوال‌های تخصصی اکچوئری شماره ۷

۱. امید ریاضی سود شرکت بیمه به صورت زیر مدل زده می‌شود:

سود = n(۱۰×احتمال عقد قرارداد) -۲۰۰۰۰۰ (۱-

=۰٫۵n-۲۰۰۰۰۰

بر این اساس از نامنفی بودن سود نتیجه می‌شود که حداقل تعداد بیمه‌گزار با توجه به صورت مسئله برابر ۴۰۰۰۰۰ است.

۲. مانند قسمت اول با فرض ۳۵ درصد برای احتمال عقد قرارداد حداقل تعداد بیمه‌گزار برابر ۱۰۰۰۰۰ است. از آنجا که تعداد بیمه‌گزاران برابر ۲۵۰ هزار است احتمال عقد قرارداد برای باقی ۱۵ هزار بیمه‌گزار برابر است با

$$\frac{100000}{250000}\times 0.35+\frac{150000}{250000}\times x=0.15$$

$$x=0.0167$$

۳. از آنجایی که داشتمان بیمه بسته است و تعداد بیمه‌گزاران نسبتا کم است تحقق ۳۵ درصد بیمه تکمیلی به نظر غیرممکن است. توجه کنید که:

- ارائه اطلاعات بیمه‌گزاران به شرکت بیمه ثالث باعث افزایش ریسک شهرت (reputation risk) می‌شود؛
- به علت بسته بودن داشتمان مبلغ سود حاصل از این توافق محدود است.

بنابراین پیشنهاد شرکت «بازار بیمه» جذاب نیست و پیشنهاد می‌شود هیات مدیره نسبت به کاهش هزینه ثابت و متغیر این پیشنهاد چانه زنی کند.

علیرضا عدالتی، اکچوئر

اخبار دانشگاهی

نام و نام خانوادگی: مریم شریف اوقلو

عنوان پایان نامه:

یک رویکرد بیزی سلسله مراتبی در پیش‌بینی پرداخت‌های خسارت بیمه‌ای

استاد راهنما: دکتر فرید روحانی

تاریخ دفاع ۳۰ بهمن ۹۸

نام و نام خانوادگی: صادق شیراوند

عنوان پایان نامه:

مقایسه نرخ‌گذاری کسرپذیری در رهیافت‌های ماکسیمم درست‌نمایی و رگرسیون

استاد راهنما: دکتر محمد ذکایی

تاریخ دفاع ۲۳ دی ۹۸

فاطمه علی محمدی، دانشگاه شهید بهشتی

فراخوان مطلب برای درج در خبرنامه

خبرنامه انجمن محاسبات بیمه و مالی ایران با هدف درج اخبار مربوط به حوزه بیم‌سنجی در ایران و جهان، آشنایی با مسائل حرفه ای بیم‌سنجی و ایجاد ارتباط میان اعضای انجمن با یکدیگر در پایان هر فصل منتشر می‌شود. برای نیل به اهداف فوق و پربارتر شدن خبرنامه، از همکاری و هم‌فکری همه علاقمندان به گرمی استقبال می‌شود. به این منظور کافی است مطلب مورد نظر خود را در قالب فایل ورد یا دست‌نویس، به صورت خوانا، تهیه نموده و برای ما ارسال کنید. فرآیند همکاری به صورت زیر است:

- مطالب به نشانی سردبیر، اعضای هیئت تحریریه یا دبیرخانه انجمن ارسال شود؛
- خبرنامه، در انتخاب، تلخیص و ویرایش مطالب ارسال شده آزاد است؛
- مطالب دریافت شده، بازگردانده نمی‌شود.

برخی از رئوس مطالب پیشنهادی برای درج در خبرنامه به شرح زیر است:

- ✓ اطلاع‌رسانی درباره همایش‌ها، نشست‌ها، کارگاه‌ها و سخنرانی‌های تخصصی در حوزه‌های مرتبط با بیمه و مالی
- ✓ مسائل حرفه‌ای (آزمون‌های حرفه‌ای، استانداردها، مباحث آئین نامه‌ای، مباحث مربوط به صنعت بیمه و بازارهای مالی و ...)
- ✓ مسائل آموزشی (واژه‌گزینی، مقاله‌های آموزشی، نرم افزار و بسته‌های محاسباتی)
- ✓ معرفی دانشمندان و پژوهشگران برجسته در حوزه‌های مرتبط
- ✓ معرفی سایر انجمن‌های علمی و حرفه‌ای
- ✓ معرفی کتاب

قابل ذکر است که خبرنامه ممکن است با توجه به محتوای مطالب دریافتی و حجم در نظر گرفته شده برای هر شماره، برخی از مطالب دریافت شده را در شماره‌های بعدی منتشر کند.

Newsletter

Actuarial Society of Iran /Winter 2020 No.8

Actuarial Society of Iran