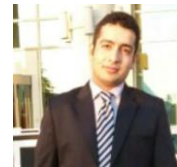




بیمه سایبری؛ نیاز آتی صنعت بیمه ایران

نویسنده: راشد رستمیان



سالی که نکوست از حملاتش پیداست

سال ۲۰۲۰ با یک پاندمی وحشتناک شروع شد که اقتصادهای دنیا را به یک رکود عمیق فرو برد و اواخر سال میلادی نیز با حملات سایبری که ترس ظهور ریسک های خطرناک تر در دهه پیش رو را بیشتر نشان می دهد. آیا ارتباطی بین این دو رخداد، یعنی کرونا و حملات سایبری می توان یافت؟ حمله سایبری هفته گذشته به ایالات متحده که در نوع خود ضمن اینکه بزرگترین حمله سایبری به مراکز حساس تجاری و دولتی آمریکا بود، از لحاظ جدید و شدید بودن و نیز عدم ردیابی آن برای دولت آمریکا بی نظیر بود.

هرچند که انگشت اتهام در این خصوص مجدداً به سمت روسیه و به خاطر نتیجه انتخابات آمریکا نشانه گرفته شد، ولی دلیل محکمی بر این ادعا یافت نشده. چنین حمله ای در اواخر سال میلادی نشان از گسترده شدن تحولات ریسک سایبری در سال آینده دارد. ریسکی که محدوده جغرافیایی حد و مرز نمی شناسد. آنچنان که مایکروسافت اظهار کرده نه تنها آمریکا بلکه شش کشور دیگر نیز تحت تاثیر این حملات قرار گرفتند تا دنیا خود را برای مواجهه با تحولات جدید در حیطه مدیریت ریسک های دهه آتی و مرتبط با تحولات انقلاب چهارم صنعتی حاضر کند.

توجه به ریسک های سایبری چندین سال است که در دنیا مورد توجه ویژه و تحلیل مدیران ریسک بسیاری از شرکت ها و در راس آن بیمه گران قرار گرفته، با این حال توجه به ریسک و خطرات بالقوه آن از سال ۲۰۱۶ و ۲۰۱۷ و با وقوع چند حمله نسبتاً خطرناک و در سطح وسیع بیشتر آن را در کانون توجه قرار داد.

به نظر می رسد ظهور ویروس کرونا هم در بالا رفتن ریسک سایبر بی تاثیر نبوده و باعث توجه بیشتر به بستر الکترونیک برای تجارت در کل دنیا گردید که خود به نحوی علاوه بر اینکه تبادلات الکترونیک را بالا برده امکان سو استفاده از آن و شکل گیری حملات سایبری را نیز بیشتر می کند.





ریسک‌هایی مانند نفوذ تروجان‌هایی که یک سیستم کامپیوتری را قفل و از کار می‌ندازد تا ریسک‌هایی مانند ADP ها که با نفوذ به سیستم کامپیوتری اطلاعات آن راسرقت می‌کنند به شدت بالا رفته است. البته دردسر بزرگتر برای بسیاری از شرکت‌ها و سازمان‌ها در اروپا و آمریکا فقط زیان ناشی از حمله سایبری نیست. بلکه جرایم سنگینی نیز که به واسطه قانون آن کشور برای نشت اطلاعات و عدم تامین امنیت اطلاعاتی به آن سازمان یا شرکت تحمیل می‌شود نیز در نوع خود قابل توجه است.

ریسک‌های سایبر در ایران

آیا سایبر برای شرکت‌های بیمه ایرانی می‌توان تهدید باشد یا فرصتی برای جذب پرتفویی نو است؟ با توجه به رشد فناوری و حرکت فوق‌العاده سریع تکنولوژی‌های نوین و مرتبط با دیجیتال و Insurance4 به نظر تا سال‌های آتی بازار از بیمه‌های سنتی مانند اتومبیل که بخش اعظمی از پرتفوی بیمه‌ای بسیاری از این شرکت‌ها را شکل می‌دهد، به بیمه‌های سایبر نقل مکان نماید، با این حال عامل فوق‌العاده مهمی می‌تواند بیمه‌ها را در جهت پذیرش ریسک‌های سایبر محتاط‌تر نماید و آن هم بحث میزان خسارت وارده است.

توصیه مدیریت ریسک به بیمه‌گران

شرکت‌های بیمه در صورت ورود به این حوزه باید خود را برای رویارویی احتمالی با زیان در سال‌های اولیه آماده کنند. ماهیت ریسک سایبر با توجه به پیشرفت لحظه‌ای فناوری اطلاعات می‌تواند شدت مواجهه با زیان مالی در این بخش را برای شرکت بیمه در حد بالایی وارد افزایش دهد که حتی اگر هم تقاضای بسیاری برای پوشش‌های سایبری از سوی بسیاری از شرکت‌های بزرگ نیز وجود داشته باشد، با این حال در سال‌های اولیه پذیرش ریسک به دلیل فقدان اطلاعات لازم از احتمال ورود زیان از ناحیه چنین ریسک‌هایی به شدت بالا خواهد بود. نکته مهم اینکه نوع تعهدات و مقیاس آن و فراوانی درصد ریسک پذیرش شده توسط بیمه‌گر نیز بسیار در این خصوص نقش مهمی را بازی نموده و اینکه یک شرکت بیمه چه مقدار از پرتفوی خود را به پذیرش ریسک‌های حوزه سایبر اختصاص داده باشد نیز مهم است.

در کل رشد بیمه سایبری در کشوری مانند ایران تا حدودی به موارد زیر بستگی دارد:

- نوع نگاه شرکت بیمه به این نوع ریسک
- ساخت‌های لازم را برای مدیریت چنین ریسکی‌هایی





یکی از ویژگی های ریسک های سایبری سرعت بالای گسترش آن می باشد و عدم مدیریت موثر چنین ریسکی عواقب سنگینی را برای یک شرکت بیمه به همراه خواهد داشت. کفایت که یک فاجعه سایبری را با یک خسارت یا فاجعه طبیعی مقایسه نمود که در عمل شدت و سرعت گسترش خسارت سایبری قابل قیاس با سایر موارد نخواهد بود. برای مثال می توان تصور کرد در صورتی که سیلی در یک نقطه از کشور واقع گردد، شرکت بیمه تنها درگیر ارزیابی خسارت و مدیریت آن در یک نقطه از کشور می گردد. در حالی که در صورت وقوع یک حمله سایبری می توان گفت در عرض چند دقیقه در کل کشور خساراتی که در نتیجه چنین حملاتی بوجود می آید بسیار سنگین و شاید کنترل ناپذیر بوده و دامنگیر سایر پورتفوهاى بیمه ای نیز گردد.

به نظر می رسد چنین مواردی شرکت های بیمه ایرانی را در پذیرش چنین ریسک هایی محتاط تر خواهد کرد چرا که یک شرکت بیمه کارشناسان خبره فناوری اطلاعات را برای مدیریت و کنترل چنین ریسک هایی لازم داشته و نکته دوم اینست که سرمایه گذاری در حیطه فناوری اطلاعات نیز نیاز به زیرساخت داشته و زمان بر خواهد بود.

از طرف دیگر مسئله ای که خیلی برای شرکت های بیمه در این زمینه مهم است بحث ریسک های خاموش سایبری است که احتمال دارد در خصوص بیمه های اموال و مسولیت بیمه گزار وجود داشته باشد و به صورت قطعی نیز مشخص نگردیده باشد که چنین ریسکی استثنا شده یا خیر. با این حال برداشت های متفاوتی که از آن وجود دارد آن را مبهم نموده است. هرچند که معمولا در بعضی از وردینگ های مهندسی و انرژی و در کل بیشتر وردینگ های فرنگی می توان این مسئله را جزیی از استثنائات بیمه نامه مشاهده نمود، با این حال همین وردینگ ها هم در بعضی جاها این قضیه را مبهم ذکر نموده و در هر حال چنین مواردی نیز کار شرکت بیمه را برای قبول ریسک سخت تر می نماید.

پیش نیاز های بیمه سایبری

یکی دیگر از مسایل پیش رو در خصوص بیمه ریسک های حوزه فناوری اطلاعات، شفافیت در ارائه پوشش و تعهدات است که شرکت های بیمه شاید در شناسایی نیاز مشتری و به دلیل جدید بودن موضوع بیمه و نیز عدم وجود متخصص حوزه ریسک مربوطه در ارائه پوشش مطلوب به بیمه گزار موفق نبوده و یا اینکه در خصوص عبارت های مبهمی که در بیمه نامه وجود داشته باشد تفاسیر شخصی شرکت بیمه و کارشناسان آن را ارائه دهند که خود موجب نارضایتی و بروز اختلاف را فراهم خواهد آورد.

با این حال توجه به وجود و ظهور چنین ریسک مهم و حیاتی در وضعیت حال حاضر جهان امروز و کشور ایران ناگزیر بوده و بیمه گران ایرانی نیز همپای نیاز های کشور و صنایع باید به ارائه پوشش برای چنین ریسک





هایی در حوزه های مختلف بیمه ای اقدام نمایند و مدیریت و برنامه ریزی برای بیمه نمودن چنین ریسکی که متعاقب آن می تواند پوشش بیمه ای برای بخش های دیگر مانند توقف کسب و کار و زیان درآمدی و شهرت یک شرکت یا بنگاه اقتصادی یا ... رابه همراه داشته باشد از سوی شرکت های بیمه ضروری بوده و می بایست به صورت جدی توجه ویژه به آن صورت پذیرد و این سرمایه گذاری بر روی فناوری اطلاعات و زیر ساخت های آن در شرکت های بیمه ای امری اجتناب ناپذیر و بسیار ضروری بوده و شرکت های بیمه می بایست بودجه بخش فناوری اطلاعات خود را بیشتر از سایر بخش ها در نظر بگیرند.

با توجه به این موارد و اگر بحث مربوط به اینشورتک ها که در این خصوص سرمایه گذاری فناوری اطلاعات نقش حیاتی برای آنها داشته و زیر ساخت و امکانات لازم در این خصوص نیز دارند، را استثنای امر کرده باشیم، کسب و کاری از نظر بیمه گری درحوزه عمومی، زندگی و اتکایی در پنج سال آتی موفق خواهد بود که بیشترین سرمایه گذاری را بر روی بستر دیجیتال و مدیریت ریسک های آن و ارایه پوشش بیمه ای بسیار باکیفیت و مبتنی بر ریسک مربوطه را ارائه نموده باشد چرا که اینکه آینده صنعت بیمه در پوشش های بیمه ای پارامتریک و مبتنی بر Solution بوده که بیمه های سایبری هم از این قضیه مستثنی نخواهند بود .

خوشبختانه به تازگی چند نمونه بیمه سایبری از سوی شرکت ها ارایه گردیده است که حرکت بسیار مثبتی در زمینه پذیرش ریسکهای مرتبط با این بخش است با این حال با توجه به نو بودن رشته بیمه ای مذکور، پوشش و مدیریت چنین ریسک هایی با نظر به شدت و اثرات سنگین درخصوص خسارت های مادی و معنوی، سرمایه گذاری فوق العاده گسترده ای را در این بخش و بستر مناسب و زیر ساخت قوی در حوزه فناوری اطلاعات را طلب می نماید و پوشش اتکایی مطلوب و ابزارهای کنترلی دیگر برای کنترل فجایع ناشی از خسارت های آن امری ضروری و اجتناب ناپذیر است

