**به نام خدا**

**موضوع : چالش ها و راهکارها در بیمه نامه سایبری**

**تهیه کننده : حمید شمس اشراق ( معاون اداره سیستم های نوین و هوشمندی کسب و کار )**

**پوشش­­‌های بیمه‌ای سایبری :**

عمده پوشش‌های بیمه‌ای در فضای سایبری می‌توان در بخش خسارات مالی، سرقت اطلاعات صنعتی و فردی دانست که به ۳ دسته تقسیم می‌شود:

۱- پوشش بیمه‌ای شخص ثالث مانند اخاذی در فضای سایبری و کلاهبرداری در زمان انتقال پول الکترونیکی.

۲- پوشش بیمه مسئولیت شخص ثالث مانند ویروسی شدن سیستم‌ها و دزدیده شدن کارت‌های اعتباری و تجاری

۳- بیمه استثنائات مانند کلاهبرداری از سوی شرکت ارائه دهنده خدمات الکترونیک.

شرکت‌های پوشش بیمه‌ای سایبری معمولا برای دریافت اطلاعات طی مراحل ذیل اقدام می‌کنند:

* تعیین نوع پوشش درخواستی
* دریافت اطلاعات کامل سیستم‌های نرم‌افزاری و سخت‌افزاری و میزان آمادگی کاربران و پشتیبانان
* مراحل زمان بندی پوشش بیمه­ای
* تعیین حق بیمه به صورت توافقی
* نگارش متن حقوقی و امضا طرفین

**عمده مشکلات در پوشش بیمه‌ای فضای سایبری :**

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

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

**چرا صنعت بیمه در بیمه‌نامه‌های سایبری ورود جدی نکرده است؟**

بیمه‌گذار هنگام خرید بیمه‌نامه یک ریسک را به شرکت بیمه انتقال می‌دهد یعنی از استراتژی‌های مدیریت ریسک استفاده می‌کند اما باید توجه داشت که در بیمه‌نامه‌های سایبری انتقال ریسک در بعضی از موارد با اصول بیمه‌گری در تناقض است.به عنوان مثال در بیمه نامه های سایبری، انتفاع (بهره بردن) بیمه گذار یا حتی گاهی هزینه های تشخیص اینکه هنگام خسارت چه اتفاقی رخ داده است و اینکه بیمه گذار تقصیری داشته است یا خیر، بالاتر از هزینه خسارت وارده می شود.

کوچکترین بی احتیاطی بیمه گذار ممکن است سبب به وجود آمدن خسارت شود و بیمه گر نمی تواند به سادگی متوجه شود که بیمه گذار از روی عمد این کار را انجام داده  یا به اشتباه.

الان در دنیا بیمه ها به سمت مدل کاهش ریسک یا اجتناب از ریسک می روند و ضریب نفوذ بیمه در زمینه انتقال ریسک رو به کاهش است و به احتمال زیاد مدل کسب و کار نمونه های خارجی بیمه نامه های سایبری هم کاهش ریسک است.

یک نکته دیگر اینکه بیمه گر برای پذیرش هر ریسک باید آن را بسنجد، در بیمه های سایبری هم برای پذیرش ریسک‌ها باید این فرآیند از منابع و کانالهای معتبر انجام بپذیرد که در حال حاضر این منابع تعریف نشده اند، همچنین مدل ارزش گذاری اطلاعات در فضای مجازی نیز از الزامات بیمه سایبری است.

نکته بعدی هم تعریف مشخص جرایم و تفکیک آن از تخلفات مدنی حوزه سایبری است.در حقیقت برای ارائه پوشش سایبری نیاز به اکوسیستم آن است که اجزا آن عبارتست از ارزیابی ریسک، پرداخت خسارت، حقوق فضای سایبری، مدلهای ارزش گذاری، صلاحیت های حرفه ای فعالیت در فضای مجازی و در نهایت شرکتهای بیمه ای، و این ها محرک هایی است که به نظر می رسد مدل کسب کار را به سمت کاهش ریسک سوق می دهد تا انتقال ( روش جاری).

**چالش های بیمه امنیت سایبری :**

یکی از چالش‌های اساسی در بیمه امنیت سایبری تعیین سطح پوشش است. این قضیه هم در سمت بیمه شونده و هم در سمت بیمه گر چالش بزرگی است. به طور مثال دو باج افزار NotPetya و Wannacry تعداد زیادی شرکت را در ۱۵۰ کشور مورد حمله قرار دادند. خسارتی در حدود ۴ میلیارد دلار تخمین زده شد. اما تعیین دقیق این خسارت‌ها قبل از وقوع حادثه یا بعد از آن حتی کار بسیار سختی است. اینکه دقیقا مشخص نماییم در صورت یک رخداد چه خساراتی وارد خواهد شد و بر آن مبنا بیمه گر، حق بیمه و سطح پوشش را مشخص نماید.

چالش‌های زیادی نیز سمت بیمه شونده برای یافتن سطح پوشش مناسب وجود دارد. در مورد تجارت‌های کوچک و متوسط قضیه چندان پیچیده نیست. اما در ارتباط با سازمان‌ها و تجارت‌های بزرگ موضوع پیچیدگی‌های زیادی دارد. طبق قوانین محافظت از داده در بسیاری از کشورها شرکت‌ها و تجارت‌هایی که افشای اطلاعات در آن‌ها رخ می‌دهد و اطلاعات کاربرانش در اختیار افراد غیر مجاز قرار می‌گیرد، ملزم به پرداخت جریمه‎‌های مالی سنگین هستند. پس یکی از انگیزه‌ها برای بیمه شدن، می‌تواند همین خسارت‌های احتمالی در آینده باشد. دلیل دیگر ضررهایی است که به اعتبار و آبروی یک سازمان در صورت درز و نشر اطلاعات خواهد خورد که بی اعتمادی مشتریان و یا سقوط ارزش سهام می‌تواند از جمله آن‌ها باشد. دیگری، ضررهای مالی به جا مانده ناشی از توقف کار، راه اندازی عملیات جرم شناسی بعد از واقعه و غیره می‌باشد که تاثیر آن‌ها در درآمد سالیانه آن تجارت‌ها قابل توجه است. تمامی این موارد باید توسط بیمه شونده مورد بررسی قرار گیرد و مشخص شود چه سطح پوششی می‌تواند برایش بهترین باشد.

**هشت چالش مهم شرکت‌های بیمه‌ای برای فروش بیمه نامه سایبری کدامند؟**

شرکت‌های بیمه‌ای که برای تأمین پوشش کافی بیمه سایبری به مشتریان خود تلاش می‌کنند، باید بر چالش‌های زیادی غلبه کنند.

**1-کمبود اطلاعات تاریخی:**

برای مثال، زمانی که بیمه گران [خسارات ناشی از سیل](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14) را تحت پوشش قرار می دهند، به تاریخچه ای غنی از این نوع بلایای طبیعی دسترسی دارند و می توانند یک مدل موجه برای این نوع خسارات تدوین کنند.

اما هیچ داده تاریخی درمورد **حملات سایبری** وجود ندارد و این نوع حملات یکی از مشکلات نوظهور به شمار می روند.

**2-عدم وجود داده های مفید موارد سایبری:برای فعال کردن یک متن دقیق :**

نه تنها بیمه گران با  فقدان داده های تاریخی در این زمینه مواجه اند بلکه در بسیاری از موارد، قانون سازمان ها را ملزم به آشکار کردن نقض قوانین سایبری نکرده  مگر مواردی که بر اطلاعات مصرف کننده تاثیر می گذارد.

این امر بیمه گران را از داده های لازم برای اندازه گیری تمام [هزینه های حمله سایبری](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14/10496-%D9%87%D8%B4%D8%AA-%DA%86%D8%A7%D9%84%D8%B4-%D9%85%D9%87%D9%85-%D8%B4%D8%B1%DA%A9%D8%AA-%D9%87%D8%A7%DB%8C-%D8%A8%DB%8C%D9%85%D9%87-%D8%A7%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%81%D8%B1%D9%88%D8%B4-%D8%A8%DB%8C%D9%85%D9%87-%D9%86%D8%A7%D9%85%D9%87-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%DA%A9%D8%AF%D8%A7%D9%85%D9%86%D8%AF?pr=1) محروم می کند و نوشتن **سیاست های بیمه ای** موثر سایبر برای آن ها دشوار است.

**3-شکاف آگاهی:**

عدم آگاهی سازمان ها در مورد آمادگی داخلی آن ها در برابر حملات سایبری، اقدامات موثر را برای بیمه گران بسیار دشوار می سازد.

**4-اشکال در تعریف یک حمله سایبری:**

بیمه گران هنوز در تلاشند تا برای حملات سایبری و تأثیر فناوری های جدید تعاریف دقیقی ارائه دهند.

بدون تهدیدهای واضح تعریف شده و درک نحوه تأثیر آن ها بر بیمه گذاران، بیمه نامه سایبر می تواند فاقد اثربخشی باشد و سازمان ها را در صورت بروز حملات سایبری مهم در معرض [خسارت های سنگین](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14) قرار دهد.

**5- کمبود آگاهی درباره خطرات**:

بسیاری از سازمان ها از دامنه کامل خطرات سایبری تهدیدکننده آن ها و گزینه های [پوشش بیمه ای](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14) موجود آگاه نیستند.این امر گاهی اوقات مانع از جستجوی هرگونه پوشش بیمه‌ای می شود.

**-6فقدان محدودیت جغرافیایی:**

مکان های جغرافیایی نسبت به [فضای سایبری](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14) برای پوشش بیمه ای بسیار آسان تر هستند چرا که هیچ چارچوب مشخصی برای فضای سایبر وجود ندارد و مهاجمان سایبری می توانند آزادانه بدون محدودیت جغرافیایی حرکت کنند.

**7-تضاد فعالیتی :**

[بیمه سایبری](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14) اساساً با سایر انواع پوشش در یک حوزه کلیدی متفاوت است که سیمانتک آن را "پارادوکس فعالیتی" می نامد.در این صورت، اگر پاسخ آن ها به این حملات خطرات آتی را کاهش داده باشد، آیا بیمه گر می تواند [حق بیمه](http://www.chabokonline.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%A8%DB%8C%D9%85%D9%87-14) کمتری را برای شرکت های قبلی که با خطر سایبری مواجه شده اند هزینه کند؟

**8-پیشگیری یا بیمه:**

یک بحث در بین سازمان ها وجود دارد که آیا باید برای خرید یک سیاست سایبری سرمایه گذاری کنند یا اینکه پول را صرف بهبود فایروال و محافظت در برابر سایبر کنند. تکلیف این موضوع هنوز معلوم نیست.

**موفق باشید**