

به گفته آقای داویسون - جنکینز، " همه چیز به سرعت در حال تغییر است به طوری که پیشگامان عرصه بیمه دائماً با ریسک های جدیدی روبرو می شوند و باید راه های پوشش انواع مختلف و جدید دارایی ها را پیدا کنند."

او همچنین افزود، " از نقطه نظر ریسک باید به خاطر داشته باشیم که اینترنت دارای ویژگی های غیرعادی می باشد."

به عنوان مثال اینترنت یک رابط چندگانه است که در آن درجه بالایی از تمرکز فعالیت ها وجود دارد. اینترنت با انتشار اطلاعات بی کران و فوری در سراسر جهان قابل دسترس می باشد؛ در اینترنت محیط قانونی نامطمئن شامل قوانین قدیمی و جدید وجود دارد؛ روابط متقابل در اینترنت ظرفیتی برای مسئولیت های عاریتی (وکالتی) ایجاد می کند. اینترنت محیطی شامل محتویات ارزشمندی است که ممکن است نیاز به طراحی مجدد محتویات آن باشد.

به گفته آقای مایکل فرنچ (Michael French) مشاور ارشد شرکت IT Security, IBM Global Services (خدمات جهانی IBM)، "یک حوزه اساسی و دارای اهمیت روزافزون در تجارت الکترونیک اسرار خصوصی افراد می باشد. به گفته وی سوال

به نظر آقای دومینیک داویسون - جنکینز (Dominic Davison-Jenkins) معاون ارشد شرکت مشاوره ای FINPRO Consulting. Marsh USA آمریکا تجارت الکترونیکی، با تغییر الگوی فعالیت اقتصادی علاوه بر تقویت ریسک های موجود، ریسک های جدیدی را نیز پدید آورده است.

تمام عواملی همچون بازاریابی و تبلیغات، حمایت مشتریان و بازخورد آن ها، ارتباطات داخلی یا اینترنت، ارتباطات صاحبان کسب و کار با یکدیگر، مبادلات و فروش از طریق اینترنت و تهیه تکنولوژی قوی یا زیرساختاری به وسیله برنامه نویسان نرم افزاری، ارتباطات تلفنی، درگاهی، ISPها (تهیه کنندگان سرویس های اینترنت)، خدمات تصدیق و ... که منجر به ریسک می شوند از نوع و دامنه فعالیت تجارت الکترونیک ناشی می شوند.

حفاظت مناسب براساس نیازهای تجاری و تأیید دائمی حفاظت های منتخب به طوری که مشخص شود آیا به طور مؤثر و کارآمد کار می کنند یا خیر؟

آقای داویسون - جنکینز اظهار داشت، " ورود به تجارت الکترونیکی وضعیت ریسک را به شدت تغییر می دهد. و برای درک تغییرات مناسب در وضعیت ریسک باید به همه فعالیت ها توجه شود. زیرا شکل واحدی از ریسک که هر چیزی را در برگیرد وجود ندارد."

ریسک های بحرانی که باعث احتمال خسارت می شوند عبارتند از:

- مسئولیت خسارت های اقتصادی که از طریق حوادثی همچون اشتباهات و از قلم افتادگی به وقوع می پیوندند؛
- مسئولیت دارایی های فکری در نتیجه خطای طراحی، توصیه های نادرست، خدمات معیوب، مسائل ارتباطات داخلی، اثرات ویروس ها، آشکار شدن اطلاعات شخص ثالث بدون مجوز، پروانه ساخت، کپی رایت نرم افزار، اسرار تجارت؛
- مسئولیت رسانه های گروهی و محتویات آن از طریق تبلیغات، مقالات سردبیری و جار و جنجال ها.

اساسی برای مدیران ریسک این است که آیا شرکت شما اطلاعات قابل شناسایی فردی را دسته بندی می نماید. اگر چنین اطلاعاتی به طور عمدی یا غیرعمدی در اختیار یک فرد غریبه یا شخص ثالثی قرار گیرد ممکن است شرکت خساراتی را متحمل شود". چنین اطلاعاتی باید محافظت شوند. هنوز هیچ شرکتی همه این اطلاعات سری را در یک محل امن نمی تواند نگهداری کند.

به گفته وی با این روش، رقابت و فعالیت غیرممکن است و این نوع اطلاعات باید در دسترس افراد باشد به طوری که آن ها بتوانند درستی اطلاعات را کنترل کنند.

آقای فرنچ افزود به منظور تصمیم گیری درباره نحوه برخورد با ریسک تجارت الکترونیکی، مدیر باید ریسک ها را شناسایی و آن ها را براساس معیارهایی همچون نام شرکت، وجهه و کیفیت کالاها و خدمات به صورت کمی بیان کند.

او پنج مرحله زیر را برای اجرا و تکمیل برنامه امور خصوصی و پشتیبانی پیشنهاد کرد تعیین موارد نیازمند به حفاظت، تعیین مسائل مربوط به حریم خصوصی افراد، تصمیم گیری در مورد نحوه محافظت از دارایی ویژه، تکمیل

از، ۲۰۰ مدیر ریسکی که مورد بررسی قرار گرفتند حاکی از وجود یک خطر بیمه ای در خارج از ایالات متحده آمریکا می باشد.

آقای AL Kappel mann مشاور مدیر شرکت لیبرتی میوچوآل در گروه مدیریت ریسک جهانی اظهار داشت باید توجه کرد که این روند نه تنها برای شرکت های بزرگ بلکه برای مؤسسات کوچک و متوسط نیز برقرار می باشد.

آقای داریسون جنکینز گفت " برای حمایت مالی در مقابل ریسک های تجارت الکترونیکی علاوه بر بیمه های سنتی که اموال، وقفه تجاری و تخلفات به صورت فردی یا گروهی را پوشش می دهند راه حل های ویژه ای از طرف اغلب بیمه گران عمده ارائه می شود."

محصولات « نسل اول » بیشتر ترکیبی یا به صورت سیاست های تخلف کامپیوتری پیشرفته می باشند.

او اضافه کرد به طور کلی آن ها تمام مسائل اساسی ریسک مانند آسیب به دارایی های غیرمحسوس و اختلالات تجاری غیرفیزیکی را نشان نمی دهند.

« محصولات نسل دوم » تمایل دارند یک روش چندگانه را انتخاب کنند، ساختار

به علاوه ریسک های متوجه طرف اول در فضای الکترونیک در ارتباط با اموال غیرمنقول و خصوصی، زیربنای اقتصادی واقعی و دارایی های نامحسوس، وجود دارد.

به طور کلی زیان ها به دو نوع مستقیم و غیرمستقیم تقسیم می شوند. او گفت، " تخلفات نیز بایستی به عنوان ریسک های طرف اول برای پول، اوراق بهادار و دیگر اموال محسوس در نظر گرفته شود."

علاوه بر این موارد امور غیرمحسوسی مانند پروانه ساخت، کپی رایت، علایم تجاری، اسرار تجاری، خدمات، کالاهای الکترونیکی، سرقتی و کیفیت کالا که می توانند توسط دزدی، تجاوز به حقوق (نقض قانون)، تصرف غیرقانونی، توزیع یا استفاده غیرمجاز و تهدید از بین بروند باید تحت مراقبت قرار گیرند. وی اضافه کرد که تجارت الکترونیکی، ریسک حوزه های نسبتاً کم ریسک یا بدون ریسک را تشدید نموده است.

مطابق تحقیق شرکت لیبرتی میوچوآل (Liberty Mutual) نکته دیگری که باید مورد توجه قرار گیرد افزایش روزافزون روند جهانی شدن است. تحقیقات سالانه بخش مدیریت ریسک شرکت نشان می دهد که اظهارات نیمی

● حدود ۵۰ درصد از آن ها نوعی مزاحمت و استفاده غیرمجاز از سیستم کار رایانه ای را در ۱۲ ماه قبل گزارش کردند.

● بیشتر حوادث توسط افراد داخلی، کارمندان و فروشندگان بوجود آمد.

آقای فرنچ گفت "وقتی لازم باشد کارمندان را با جنبه های مختلف رایانه شرکتی آشنا کنیم، این خود باعث افزایش ریسک می شود. وی ادامه داد هدف اصلی هر عملیات این است که امنیت و حریم خصوصی را توسط فرآیند منطقی و اهداف تجاری در شرکت تلفیق کرد.

با این همه ما هرگز نمی دانیم که فروشنده یا هر شخص دیگری که راه « ورودی سری » سیستم امنیتی را باز کرده آیا فراموش نمی کند که آن را ببیند، منظور این است که تمام این زیر پا گذاشتن امنیت، عمدی نیست بلکه بعضی موارد تصادفی هستند».

او گفت اغلب از شرکت آی بی ام (IBM) یا دیگر شرکت های رایانه ای سوال می شود که آیا آن ها می توانند یک « تأیید قطعی نگهداری خوب » برای برنامه ای کارآمد و مؤثر امنیتی طراحی کنند؟ جواب منفی است.

او اضافه نمود که " این بازار هنوز به سرعت در حال رشد است و در نتیجه احتمال

واحد انعطاف پذیری داشته باشند و راه حل های ابداعی که بیمه را با خدمات با ارزش افزوده ترکیب می کنند مانند کنترل سلامتی ریسک الکترونیکی، بررسی بیمه تجارت الکترونیکی و ارزیابی امنیتی تجارت الکترونیکی را به کار گیرند.

آقای فرنچ گفت به زبان ساده بیمه را نمی توان به تنهایی به عنوان جایگزینی برای فعالیت های مناسب مدیریت ریسک انتخاب نمود، به خصوص که امروزه استفاده از اینترنت به صورت جهانی شدیداً باعث تغییر شکل ریسک شده است.

او آمار قابل ملاحظه ای از نتایج تحقیقات اخیر را ارائه کرد:

● حدود ۷۵ درصد از ۵۶۳ شرکت مورد بررسی، زیان مالی ناشی از نقض موارد مختلف ایمنی رایانه را گزارش کردند.

● زیان برای سازمان هایی که توانستند این زیان ها را کمی کنند به مبلغ ۱۰۰/۲ میلیون دلار رسید.

● حدود ۱۶۵ شرکت مورد بررسی زیان کلی ۱۲/۵ میلیون دلاری ناشی از ویروسی شدن رایانه ها را گزارش دادند.

می رود شاهد تکامل بیشتری در پوشش و فرآیند فعالیت بیمه ای باشیم“ .

مترجم: مهدی شهبیدی

*Ins. Day, May 2001, p. 6.*

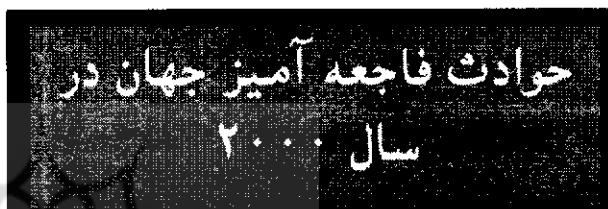
منبع:

از ۱۰/۶ میلیارد دلار خسارت بیمه شده در سال ۲۰۰۰، ۷/۵ میلیارد دلار ناشی از حوادث طبیعی بوده است و ۳ میلیارد دلار مربوط به حوادث ناشی از فعالیت های انسانی. طبق جدول ۱ آن چنان که انتظار می رود حوادث فاجعه آمیز طبیعی با وجود شمار کمتر در مقایسه با حوادث انسانی، خسارت های شدیدتری پدید آورده اند.

به عبارت دیگر حوادث طبیعی با وجود آن که تنها ۳۴/۵ درصد حوادث فاجعه آمیز را تشکیل می دهند ۷۱/۲ درصد از خسارات بیمه شده به این حوادث تعلق می گیرد. در مقابل، در حالی که ۶۵/۵ درصد حوادث فاجعه آمیز ناشی از فعالیت های انسانی بوده است تنها ۲۸/۸ درصد خسارات پرداختی به این گونه حوادث تعلق یافته است.

حدود ۵۰ درصد خسارات بیمه شده جهان در سال ۲۰۰۰ به قاره امریکا تعلق دارد. در این قاره با وقوع ۷۳ مورد حادثه فاجعه آمیز، ۴/۹ میلیارد دلار خسارت پرداخت شده است. در حالی که سهم قاره اروپا از خسارات بیمه شده حدود ۲۷ درصد است.

از این نظر قاره آسیا وضعیت کاملاً متفاوتی دارد با وجود ۱۵۰ حادثه فاجعه آمیز



تهیه و تنظیم: مهدی نمین الحسینی

خسارت های بیمه شده ناچیز در برابر

سیل های عظیم و ویرانگر

شرکت. های بیمه در سال ۲۰۰۰ بابت

۳۵۱ حادثه فاجعه آمیز ۱۰/۶ میلیارد دلار خسارت پرداخت کردند که این رقم بسیار کمتر از ۳۲/۹ میلیارد دلار خسارت بیمه شده در سال ۱۹۹۹ است. در حالی که ۹ مورد از حوادث طوفان و زلزله در سال ۱۹۹۹ هریک بیش از یک میلیارد دلار خسارت ایجاد کردند. در سال مورد بررسی تنها حادثه ای که نزدیک به یک میلیارد دلار خسارت به صنعت بیمه تحمیل کرد سیل توکای (Tokai) در ژاپن بود.