سیر تکامل بیمه فضای مجازی[1]

مترجمان: رامین رشیدی- اعظم رشیدی

- کارشناس‌ارشد معارف اسلامی و اقتصاد
- کارشناس مترجمی زبان انگلیسی

چکیده

بیمه اینترنت[2] ابزاری قدرتمند برای همراه‌کردن انگیزه‌های بازار[3] در جهت بهبود امنیت اینترنتی است. در این مقاله، تکامل بیمه اینترنت از تبدیل بیمه‌نامه‌های سنتی به اولین بیمه‌نامه‌های اینترنت و سپس به محصولات جامع کنونی بررسی می‌گردد. می‌توان دریافت که افزایش ریسکِ امنیت اینترنت به همراه نیاز به تطبیق با قوانین شرکتی به طرز چشمگیری به تقاضا برای بیمه اینترنت کمک کرده است. از زمانی که بیمه‌گران نیازهای تجاری خاص و دورنمای ریسک را بهتر درک کرده‌اند، بیمه‌نامه‌های اینترنت جامع‌تر ارائه می‌شوند. به‌طور دقیق‌تر، بیمه‌گران اینترنت در حال رفع و حل مسائلی هستند که قبلاً لاینحل تلقی می‌شدند (نظیر مسئله انتخاب نامساعد، عدم‌تقارن اطلاعات، مخاطرات اخلاقی و ...) و می‌توانست به شکست راه‌حل مبتنی‌بر بازار بیانجامد. اگرچه برخی مشکلات اجرایی همچنان باقی مانده است اما اعتقاد بر این است که پیشرفت بیمه اینترنت در آینده این مشکلات را همچون مشکلات دیگر حوزه‌های ریسک حل خواهد کرد.

واژگان کلیدی: بیمه اینترنت، اقتصاد امنیت اطلاعات[4]

1. The Evolution of Cyberinsurance

۲. اگر چه معادل فضای مجازی برای کلمه Cyber مناسب‌تر است، اما به دلیل تکرار زیاد عبارت در متن مقاله و همچنین هم‌پوشانی بالای دو مفهوم فضای مجازی و اینترنت درحال‌حاضر، در ترجمه از عبارت «بیمهٔ اینترنت» به عنوان معادل «Cyberinsurance» استفاده شده است. (مترجم)

3. Market Incentives

4. Economics of Information Security

مقدمه

هر قدر سازمان‌ها به دارایی‌ها و اطلاعاتِ شبکه‌ای کامپیوتری خود بیشتر وابسته شوند، در مقابلِ خسارات ناشی از افزایش حملات مکرر و زیان‌باری که به دلیل اتصال به شبکه به‌وجودمی‌آید، آسیب‌پذیرتر می‌شوند. جلوگیری از خسارت در هر سیستم شبکه‌ای کامپیوتری هرگز ۱۰۰٪ و کامل نخواهد بود. در دهه گذشته تکنیک‌های حفاظتی از برخی رشته‌های علم کامپیوتر مانند رمزنویسی و مهندسی نرم‌افزار به طور مداوم پیشرفت‌هایی داشته است، بااین‌حال هنوز هم حملات اینترنتی در حال افزایش است. درحالی‌که رسانه‌های جمعی توجه خود را بر حملات اینترنتی گسترده که به شکل شکاف‌های امنیتی و کرم‌های اینترنتی سریع‌الانتشار است، متمرکز کرده‌اند، حملات داخلیِ کشف و گزارش‌نشده افراد، در داخل سازمان‌ها که از امتیاز دستیابی به شبکه اطلاعات برخوردار می‌باشند با تواتر و شدت بیشتری اتفاق می‌افتد. با اینکه بیشتر فروشندگان خدمات امنیت اینترنتی، محصولاتی را به شکل نرم‌افزار و سخت‌افزار می‌فروشند، اما حفاظت امنیت اینترنتی فرآیندی مستمر است که مردم نیز درگیر و فعال در آن هستند و مسئله امنیت اینترنتی کاملاً با چنین محصولاتی حل نمی‌شود. به‌عبارت‌دیگر اگرچه بیشتر سازمان‌ها بر جلوگیری از حملات اینترنتی تنها از طریق روش‌های تکنیکی متمرکز شده‌اند، اما این امر تنها بخشی از راه‌حل کلی به‌شمارمی‌رود. یک راه‌حل کلی باید در برگیرنده پذیرش و مدیریت ریسک ناشی از حملات اینترنتی باشد چرا که وقوع آنها یک واقعیت است.

گروه کوچکی از متفکران علوم بین‌رشته‌ای، استفاده از بیمه اینترنت را بخشی از راه‌حل کلی امنیت اینترنتی مطرح کرده‌اند. اولین کاری که کاربرد سیستم توزیع بیمه برای اینترنت را بیان می‌کرد، به سال ۱۹۹۴ برمی‌گردد. دان گیر[1] مبدع استفاده از مدیریت ریسک شامل استفاده از پوشش بیمه‌ای برای اینترنت بوده است. او نخستین کسی بود که ارتباط مقوله مدیریت ریسک که عموماً در دیگر رشته‌ها به‌خصوص در بخش مالی به‌کارمی‌رفت را با اینترنت مطرح کرد. بارزترین فردی که بیمه اینترنت را در بحث‌های آکادمیک مطرح کرد، بروس شنیر[2] بود که آنچه را که امروزه در مورد نقش بیمه اینترنت بر آن اجماع شده است را او قبلاً تشریح کرده است. دیگر مفسران (از جمله نویسندگان مقاله حاضر) جزییات بیشتری در مورد بیمه اینترنت عرضه کرده‌اند. ما در سال ۲۰۰۲ نقش بیمه را در بهبود امنیت اینترنتی بیان کردیم. در تئوری، بیمه اینترنت، امنیت اینترنتی را افزایش می‌دهد چرا که بیمه‌گذار در مقابل کاهش حق‌بیمه، به‌عنوان یک عکس‌العمل منطقی، مراقبت از خود را افزایش می‌دهد. بیمه اینترنت همچنین به ارتقای استانداردهای مسئولیت کمک می‌کند. در سال ۲۰۰۴ ما تئوری اقتصادی را مطرح و مزایای رفاهی بیمه اینترنت را محاسبه نمودیم. در ۲۰۰۵ چندین بیمه‌نامه اینترنت را تجزیه‌وتحلیل نموده و تئوری اقتصادی را با آنچه که در بازار اتفاق افتاده بود تطبیق دادیم.

در این مقاله به پیشرفت بیمه اینترنت در طول زمان از هنگام مطرح‌شدن آن برای اولین بار در اواخر دهه ۱۹۹۰ تا ۲۰۰۵ نگاهی می‌اندازیم. پیشرفت بیمه اینترنت مطمئناً تحت تأثیر حوادث پیش‌بینی نشده‌ای قرار گرفته که در این مقاله به آن می‌پردازیم. باتوجه به اینکه تعمیم‌سازی بازاری که شامل قراردادهای خاص بیمه اینترنت می‌باشد، مشکل است، ما در اینجا صرفاً روندهایی را بررسی و شناسایی می‌کنیم که اتفاق افتاده و ممکن است شناخت و دانش ما را از آینده بیشتر کند. سایر مطالب این مقاله به این ترتیب است: بخش ۱، نفع شخصی منطقی از دیدگاه‌های تجاری مکمل در مورد بیمه اینترنت را ارائه می‌دهد. در بخش ۲، پیشرفت بیمه اینترنت از بیمه‌نامه‌های سنتی تا اولین بیمه‌نامه‌های هکر[3] که به بیمه‌نامه‌های جامع بیمه اینترنت توسعه یافتند را دنبال می‌کنیم. بخش۳ در مورد مشکلاتی که بیمه‌گران اینترنت با آن مواجه هستند و در مورد مکانیسم‌هایی که آنها برای حل این مشکلات بر می‌گزینند، بحث می‌کند. در بخش ۴ خلاصه و نتایج مقاله را مطرح می‌کنیم.

1. Dan Geer

2. Bruce Schneier
3. Early Hacker Insurance Policies

۱. دورنمای تجاری بیمه اینترنت

دو دیدگاه تجاری در بیمه اینترنت وجود دارد:

- بیمه‌گرانی که به دنبال کسب سودآوری از مازاد حق‌بیمه‌ها بر خسارت‌ها از طریق توزیع ریسک خسارت‌های غیرقطعی مشتریان مستقل از هم هستند؛
- فرد یا سازمانی که با مدیریت ریسک خسارت غیرقطعی درصدد ماکزیمم کردن مطلوبیت یا سود خود است.

از دیدگاه بیمه‌گر از آنجایی که نیاز فزاینده‌ای برای حفاظت از دارایی‌های اساسی نظیر زیرساخت شبکه، داده‌ها و اعتبار وجود دارد، بیمه اینترنت فرصت پیشرفت را فراهم می‌کند. اگر یک شرکت بیمه دقیقاً بتواند ریسک‌های اینترنتی را به صورت حق‌بیمه‌های جذاب کمی نماید، این فرصت در شرایطی به سود بادآورده تعبیر می‌شود. اگر حق‌بیمه‌ها بسیار بالا باشد دیگر بیمه‌گران نیز وارد بازار شده و این سود بادآورده را جمع خواهند کرد و اگر شرکت بیمه‌ای در کمّی کردن ریسک‌های اینترنت و تعیین حق‌بیمه، دقیق نباشد به‌گونه‌ای که ریسک‌ها خیلی پایین قیمت‌گذاری شوند ممکن است خسارات زیادی به بار آید و شرکت متضرر گردد.

کمّی کردن ریسک‌های اینترنتی برای تعیین نرخ حق‌بیمه بهینه کار مشکلی است چرا که: دارایی‌هایی که قرار است بیمه شوند عمدتاً غیرفیزیکی (ناملموس) بوده، تغییرات ریسک به سرعت اتفاق می‌افتد (خطرات خلق‌الساعه[1]، ناگهانی ظاهر می‌شوند) و ارزیابی بیمه‌پذیری مشتریان بالقوه هم‌زمان با دوباره ارزیابی کردن ریسک‌های مشتریان فعلی، منابع زیادی می‌طلبد. اما درهرحال متناسب ساختن ریسک و هزینه ریسک (حق‌بیمه) در صنعت بیمه چیزی است که قرن‌ها انجام شده است و کارگزاران برای این به‌وجودآمده‌اند تا با هماهنگ کردن مشتریان و بیمه‌گران فرصتی تجاری فراهم کرده و سودی ببرند.

جدای از تعیین نرخ حق‌بیمه بهینه برای بیمه‌نامه‌های مختلف اینترنتی، بیمه‌گران با چالش اصلی دیگری همچون گسترش ریسک در بین بسیاری از مشتریان مستقل از هم مواجه هستند. در رابطه با بیمه اینترنت باید گفت که بسیاری از کرم‌های اینترنتی جدید و حملات ویروسی آنچنان تأثیرات جهانی داشته که یافتن مشتریانی که ریسک‌هایشان وابسته نباشد، دشوار است. یک بیمه‌گر ممکن است به دنبال توزیع ریسک در عرصه‌های مختلف سخت‌افزاری و نرم‌افزاری، سازمان‌های بزرگ و کوچک و ... باشد. اما این سؤال همچنان مطرح است که آیا ریسک‌های اینترنتی به‌دلیل پیوستگی ذاتیشان قابل تفکیک هستند یا نه.

از دیدگاه فرد یا سازمان، غیرقطعی‌بودن در مورد ریسک‌های اینترنتی، نمادی از ریسک واقعی ایجاد خسارت به‌شمارمی‌رود. چهار گزینه برای مدیریت این‌گونه ریسک‌ها وجود دارد:

- اجتناب از ریسک؛
- نگهداری ریسک؛
- کاهش ریسک؛
- انتقال ریسک در مقابل وجه.

گزینه اول یعنی اجتناب از در معرض ریسک‌های اینترنتی قرار گرفتن از طریق عدم‌تکیه بر کامپیوترها، دستگاه‌های شبکه‌ای یا وب‌سایت‌ها ممکن است. برای برخی افراد و سازمان‌ها این امر شدنی است، اما برای اکثر سازمان‌های تجاری غیرممکن است. گزینه دوم یعنی نگهداری ریسک مبتنی‌بر یک تصمیم آگاهانه است، تصمیم آگاهانه‌ای که جذب هر خسارت به‌صورت داخلی را ازنظر هزینه به صرفه‌تر می‌داند یا اینکه دیگر گزینه‌های مدیریت ریسک قابل انجام نیست. ممکن است فرد یا سازمان این گزینه را برمبنای قضاوت آگاهانه یا رفتار ریسک‌پذیریش انتخاب کند. متأسفانه در برخی مواقع به‌دلیل کمبود منابع مالی، نگهداری ریسک تنها گزینه است. گزینه سوم کاهش ریسک با استفاده از اقدامات و فرآیندهای مدیریتی و فنی است. این امر شامل سرمایه‌گذاری روی افراد و ابزار برای شناسایی تهدیدها و تدارک اقدامات ضد آن با اصلاح مداوم و مستمر فرآیندهای امنیتی است. اگرچه این گزینه،

1. Zero Day Threats

دهه‌ها است که کانون توجه منحصربه‌فرد متخصصین امنیت کامپیوتری بوده، اما باید به خاطر داشت که این فقط یکی از گزینه‌های مدیریت ریسک است. گزینه چهارم انتقال ریسک به شخص ثالث در قبال پرداخت وجهی است، که این شخص ثالث باید به‌عنوان یک شرکت بیمه برای انجام این کار مجوز داشته باشد. بیمه به فرد یا سازمان اجازه می‌دهد که پرداخت‌هایش برای حوادث غیرقطعی (هزینه‌های خسارت که متغیر و نامعلوم است)، را به‌صورت هزینه‌های دوره‌ای قابل پیش‌بینی(یعنی همان پرداخت حق‌بیمه) هموارسازی نماید.

فرد یا سازمان، ترکیبی از این راه‌های مدیریت ریسک یعنی نگهداری بعضی ریسک‌ها، کاهش برخی ریسک‌ها و بیمه‌کردن بقیه ریسک‌ها را به‌طور هم‌زمان به‌کارمی‌برد. به‌عنوان‌مثال ممکن است شرکتی بخواهد وب‌سایت اینترنتی داشته باشد که با فرآیندهای امنیتی حفاظت شود اما از برخی ریسک‌های معاملات اینترنتی مشخص اجتناب کند. یک رویکرد رایج مدیریت ریسک، نگهداری همه ریسک یا قسمت بیشتر ریسک و هم‌زمان انتقال اقدامات و عملیات کاهش ریسک به اشخاص ثالث (برون‌سپاری) به‌دلیل مهارت و تخصص بیشتر اشخاص ثالث و مقرون به صرفه بودن آن است. دیگر ترکیب رایج مدیریت ریسک، انتقال ریسک‌های خاص از طریق تضمین محصول یا قرارداد خدمت است. اگرچه در این مقاله ما بر بیمه اینترنت تمرکز می‌کنیم، اما باید درنظرداشت که بیمه اینترنت تنها یکی از چند گزینه تکمیلی مدیریت ریسک است هرچند که اهمیت این گزینه در حال افزایش است.

پذیرش رویکرد مدیریت ریسک در بسیاری از صنایع رواج یافته است. البته حفاظت نسبی است و ریسک‌ها باتوجه به اولویت‌های طرف‌های درگیر و همچنین روابط و تأثیرات ناشی از محیط خاص، باید مدیریت شوند. این رویکرد با رویکرد رایج چندین ساله در صنعت فناوری اطلاعات که ایمنی را مطلق می‌دانست و براساس آن باید [به‌طور مطلق] از ریسک‌ها اجتناب می‌شد، متفاوت است. برمبنای این رویکرد، متخصصین کامپیوتر بر روی توسعه تکنولوژی برای حل مشکلات امنیتی اینترنت کار می‌کردند. اما امروزه این رویکرد و طرز فکر با فهم این مسئله که امنیت کامل و مطلق، غیرممکن و بسیار گران است، تدریجاً در حال تغییر به این رویکرد است که سطحی از ایمنی که برای انجام امور عادی لازم است، کافی بوده و مابقی ریسک را که نمی‌توان کاهش داد از طریق پوشش بیمه‌ای می‌توان انتقال داد.

با ادغام دو دیدگاه بیمه‌گران و افراد/ سازمان‌ها با یکدیگر، منطق اولیه تجارت بیمه اینترنت به این شرح خواهد بود:

– ازآنجایی‌که اتصال اینترنتی، آسیب‌پذیری سازمان‌ها را در برابر خسارت افزایش می‌دهد، سازمان‌ها با بهره‌گیری از بیمه اینترنت به‌عنوان یک گزینه به همراه دیگر گزینه‌های مدیریت ریسک درصدد اداره این نوع ریسک هستند.

– بیمه‌گران اینترنت با مغتنم شمردن فرصت سودبردن از بیمه اینترنت، ضمن ارائه بیمه‌نامه‌هایی، به‌طور هم‌زمان استانداردها را برای بیمه‌پذیری توسعه می‌بخشند. بیمه‌گران با درنظرگرفتن عرضه و تقاضا و برای تعیین دامنه حق‌بیمه‌ها در پوشش‌های مختلف، به‌گونه‌ای که برای آنها سوددهی داشته باشد، به‌سمت یافتن بهترین شیوه‌های سنجش سوق داده می‌شوند.

– سازمان‌هایی که ریسک را با استفاده از بیمه اینترنت مدیریت می‌کنند، انگیزه‌های اقتصادی قوی برای کاهش ریسک از راه‌های ملموس(به‌عنوان‌مثال با به‌کارگیری بهترین تکنیک‌ها و ابزار جهت تأمین امنیت) دارند. انگیزه‌های اقتصادی دو شکل اصلی دارد:

- حق‌بیمه پایین‌تر (تخفیف‌ها) در قبال حفاظت امنیتی بهتر؛
- بازرسی‌های مالی که افراد و سازمان‌ها را ملزم می‌سازد ثابت کنند از منابع شبکه ایشان حفاظت می‌کنند (که این بخشی از وظایف محوله به عوامل اجرایی در بیشتر سازمان‌های تجاری است).

– نتیجه نهایی انگیزه‌های اقتصادی بیمه‌گران اینترنت و افراد/سازمان‌ها، یک راه‌حل مبتنی‌بر بازار است. بیمه‌گران

اینترنت به دنبال استفاده از فرصت‌های سودآوری هستند که از نرخ‌گذاری دقیق بیمه اینترنت حاصل می‌شود و افراد و سازمان‌ها به دنبال ممانعت از خسارت‌های بالقوه‌اند.

پیچیدگی‌های بیشتری فراتر از این منطق اولیه تجارت وجود دارد که برای تکمیل بحث به‌طورخلاصه به آنها اشاره می‌کنیم. به‌عنوان‌مثال، این منطق بر رقابتی‌بودن ساختار بازار استوار است، دیگر ساختارهای بازار (انحصاری، انحصار چند جانبه) ممکن است این وضعیت را تغییر دهد. همچنین ازآنجاکه امنیت اینترنتی امری به هم وابسته است، افراد و سازمان‌ها ممکن است در تأمین امنیت، کمتر سرمایه‌گذاری کنند تا از سرمایه‌گذاری دیگران بهره‌برداری کنند (سواری مجانی)[1] و نیز ازآنجایی‌که اطلاعات در مورد میزان تأمین امنیتی غالباً فقط برای افراد و سازمان‌ها شناخته شده است، ممکن است بیمه‌گران مجبور به تصمیم‌گیری در شرایط غیرقطعی شوند. در ادامه، به دو مقوله اخیر (عوامل خارجی[2] و عدم‌تقارن اطلاعات[3]) پرداخته می‌شود.

۲. توسعه بیمه اینترنت

۲-۱. بیمه‌نامه‌های سنتی

به‌طور سنتی شرکت‌ها برای پوشش خسارات در این حوزه بر چند بیمه‌نامه تکیه می‌کنند:

- بیمه‌نامه‌های اشخاص در حوزه کسب‌وکار برای پوشش خسارت‌های وارده به شخص اول (بیمه‌گذار)؛
- بیمه‌نامه‌های توقف در کار[4]؛
- بیمه‌نامه‌های مسئولیت عمومی یا بیمه‌نامه‌های چتری مسئولیت[5] (برای پوشش مسئولیت خسارات به اشخاص ثالث)
- بیمه‌نامه‌های خطا و اشتباه[6] (پوشش برای کارکنان شرکت).

این بیمه‌نامه‌های سنتی برای پوشش خطرات سنتی آتش‌سوزی، سیل و دیگر قوای قهریه (نیروهای طبیعی) طراحی شده است. ازآنجایی‌که این بیمه‌نامه‌ها قبل از ظهور اینترنت مرسوم بوده‌اند، ریسک‌های اینترنتی جدید را پوشش نمی‌دهند. همین امر منجربه دعاوی قضایی پرهزینه بین بیمه‌گران و بیمه‌گذاران شده است؛ دراین‌میان بیمه‌گران، بر طراحی استثنائات سخت‌تری تأکید دارند؛ آنها همچنین برای جلوگیری از تحت شمول قرار گرفتن خسارات اینترنتی، بیمه‌نامه‌های جدیدی را ارائه می‌دهند. به‌عنوان‌مثال از آنجا که اموال و دارایی‌های اینترنتی الزاماً شکل فیزیکی ندارند، حمله به آنها ممکن است منجربه خسارت فیزیکی نشود. ازاین‌رو مناقشات زیادی بین بیمه‌گران و شرکت‌ها بر سر این موضوع در گرفته است که منظور از «دارایی ملموس» و «خسارت فیزیکی» مورد نظر در متن بیمه‌نامه‌های سنتی چیست. در دعوای قضایی شرکت ریتیل سیستمز علیه شرکت‌های بیمه‌ای سی.ان.ای[7]، حکم دادگاه این بود که ازآنجایی‌که داده‌ها ارزش دائمی داشته و با ماهیت مادیِ (ملموس) نوارهای مغناطیسی درآمیخته است، لذا نوارها و داده‌های کامپیوتری تحت بیمه‌نامه مسئولیت عمومی، دارایی ملموس محسوب می‌شوند. همچنین، در دعوای قضایی شرکت بیمه مسئولیت و تضمین آمریکا علیه شرکت اینگرام مایکرو[8]، حکم دادگاه آریزونا این بود که خسارت برنامه‌نویسی در حافظه[9] کامپیوتر، خسارت یا زیان فیزیکی محسوب می‌شود. در دعوای قضایی شرکت بیمه سنتنیال و شرکت اپلاید هلث کر[10] نیز، در مناقشه پردازش داده‌های معیوب و نقص سیستم که به لطمه به داده‌ها منجر شده بود، دادگاه به نفع بیمه‌گذار رأی داد. اما در دعاوی قضایی دیگری همچون لاکر ام‌اف‌جی. علیه شرکت بیمه هوم[11]، عکس این مسئله اتفاق افتاده است. همچنین در دعوای قضایی شرکت پیپل تلفن علیه شرکت بیمه آتش‌سوزی هارتفورد[12]، حکم دادگاه

1. Free Riding
2. Externalities
3. Information Asymmetry
4. Business Interruption
5. Commercial General Liability (CGL) or Umbrella Liability Insurance Policies

پوشش چتری مسئولیت یا پوشش مازاد مسئولیت (Excess Liability)، زمانی که خسارت از حد بیمه‌نامه فراتر رود، پوشش مازادی فراهم می‌آورد. به‌عنوان‌مثال اگر بیمه‌نامه مسئولیت عمومی، پوششی در حد یک میلیون دلار فراهم کند و خسارت ۱/۵ میلیون دلار باشد، پوشش چتری، مازاد ۰/۵ میلیون دلاری را پوشش می‌دهد. (مترجم)

6. Errors and Omissions Insurance

7. Retails Systems, Inc. v. CNA Insurance Companies
8. American Guarantee & Liability Insurance Co. v. Ingram Micro
9. RAM
10. Centennial Insurance Co. v. Applied Health Care Systems
11. Lucker Mfg. v. Home Insurance
12. Peoples Telephone Co

ایالتی فلوریدا این بود که شماره‌های سریال الکترونیکی و شماره‌های شناسه تلفن همراه، دارایی ملموس محسوب نمی‌شود.

علاوه‌براین مشکلات، مسئله دیگر آن است که درحالی‌که بیشتر بیمه‌نامه‌های مسئولیت عمومی پوشش جهانی ندارند، ولی بسیاری از آسیب‌های خسارت‌های اینترنتی، جنبه بین‌المللی دارند. اگر در بیمه‌نامه یک شرکت، پوشش دادن ریسک تصریح شده باشد، معلوم نیست که [این پوشش] جرم‌های بین‌المللی را شامل می‌شود یا نه. نتیجه آنکه نقص و ناتوانی بیمه سنتی در رابطه با خطرات اینترنتی جدید، نیاز به طراحی و ارائه بیمه‌نامه‌هایی را به‌وجود آورده است که ریسک‌های اینترنتی جدید را نیز تحت پوشش قرار دهد.

۲-۲. ظهور اولین بیمه‌نامه‌های هکر

اگر چه پوشش تخصصی برای جلوگیری از جرائم کامپیوتری برای اولین بار در اواخر دهه ۱۹۷۰ به‌وجود آمد، اما این بیمه‌نامه‌ها شاخه‌ای از بیمه سنتی جرائم برای بانکداری الکترونیک بودند که عمدتاً برای پوشش ریسک امکان دستیابیِ فیزیکی افراد خارجی به سیستم‌های کامپیوتری طراحی شدند. در اواخر دهه ۱۹۹۰ بیمه‌نامه هکر برای اولین بار طراحی شد. نخستین بیمه‌نامه معروف هکر توسط شرکت‌های فناوری و با همکاری شرکت‌های بیمه‌ای به‌منظور ارائه خدمات فناوری و بیمه شخص اول به مشتریان عرضه شد تا از تکنولوژی‌های شرکت‌های فناوری حمایت کند یا یک راه‌حل جامع مدیریت کامل ریسک را برای شرکت‌های متقاضی فراهم کند.

به‌دلیل جدید و ناشناخته‌بودن این بخش، شرکت‌های بیمه‌ای فعالیت خود را با پوشش‌های کوچک آغاز نمودند. بنابراین انجمن بین‌المللی امنیت کامپیوتری[1] که اولین گروهی بود که به ارائه بیمه هکر به‌عنوان نوعی تضمین برای معتبربودن خدماتش اقدام کرد، فعالیت خود را فقط با حداکثر پوشش ۲۵۰۰۰۰ دلار در سال آغاز نمود.

علاوه‌براین، تقریباً تمام این اولین بیمه‌نامه‌های هکر فقط خسارت شرکت خصوصی بیمه‌گذار (شخص اول) را پوشش می‌داد. جدول ۱ چگونگی شروع فعالیت اولین

1. International Computer Security Association (ICSA)

جدول ۱. پوشش‌های اولیه بیمه هکر

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

بیمه هکر از پوشش‌های ساده و کم در مقابل خسارت حملات هکرها تا بیمه‌نامه‌های متنوع هکر را نشان می‌دهد.

۳-۲. وقایع سببی: افزایش ریسک‌ها و سازگاری با قوانین

اگرچه قبل از یازدهم سپتامبر ۲۰۰۱ حوادث اینترنتی بسیاری وجود داشت، اما بعد از آن حادثه بود که درک و تصور از ریسک و نگرش به آن به طرز قابل توجهی تغییر یافت. سه مورد از جدی‌ترین حملات کرم‌های اینترنتی در طول سه ماه حول‌وحوش یازدهم سپتامبر ۲۰۰۱به وقوع پیوست (کد رد[1] در جولای ۲۰۰۱، نیمدا[2] در سپتامبر ۲۰۰۱، و کلز[3] در اکتبر ۲۰۰۱). کرم اینترنتی اسلمر[4] نیز در ژانویه ۲۰۰۳ منتشر شد. البته قبل از یازدهم سپتامبر ۲۰۰۱ و در فوریه ۲۰۰۰ نیز یک سری حملات هماهنگ داس[5] بر ضد شرکت‌های بزرگ آمریکایی طرح‌ریزی شد. این حملات نه تنها مانع ارائه خدمات پنج وب‌سایت از ده وب‌سایت معروف اینترنتی به مشتریان گردید بلکه سرعت

1. Code Red
2. Nimda

3. Klez
4. Slammer
5. Denial-of-Service (DoS)

حملات داس، منابع کامپیوتر را برای کاربران غیرقابل استفاده می‌کند. اگرچه ابزارهای اجرا، انگیزه‌ها و اهداف حملات داس ممکن است متنوع باشد اما عموماً شامل تلاش‌های هم‌جهت از جانب فرد یا افرادی است برای جلوگیری از فعالیت یک سایت به‌صورت کارا یا از کار انداختن آن به‌صورت موقت یا نامحدود. این افراد عموماً سایت‌هایی را هدف‌گذاری می‌کنند که ارائه‌کننده خدمات به افراد زیادی باشد، نظیر بانک‌ها و... (مترجم)

اینترنت را هم کاهش داد (کی‌نوت سیستمز[1] تخمین زد که در عملکرد ۴۰ وب‌سایت دیگر که مورد حمله واقع نشده بودند، ۶۰٪ تنزل ایجاد گردید).

علاوه‌بر اینها، هکرها حملاتی به سیستم‌های تشخیص هویت، نفوذ به کامپیوترها، تخریب و اختلال در شبکه‌ها، سرقت شناسه، اسم رمز و دیگر اطلاعات مهم نیز داشته‌اند. تحقیقات نشان می‌دهد که ۹۰٪ شرکت‌های تجاری و دولتی نفوذهای امنیتی را کشف کرده‌اند، ۷۵٪ این شرکت‌های تجاری دچار زیان مالی گردیده، ۳۴٪ سازمان‌ها اذعان می‌دارند درصورتی‌که سیستم‌هایشان در معرض خطر قرار گیرد، توانایی کافی برای شناسایی خطرات را ندارند و ۳۳٪ نیز به عدم‌توانایی برای مقابله با این خطرات اذعان کرده‌اند. در حقیقت، کراکرها[2] (هکرها) نه تنها به شرکت‌های تجاری حمله کردند و وارد سیستم‌های آنها شدند، بلکه حتی به سیستم شرکت‌های دولتی مهم مانند سنای امریکا، اف.بی.آی، سازمان فضانوردی (ناسا) و وزارت دفاع نیز نفوذ کردند. ویروس لاو باگ[3] در سال ۲۰۰۰، ۲۰ کشور و ۴۵ میلیون کاربر را آلوده کرد و بالغ بر ۸/۷۵ میلیارد دلار به بهره‌وری (کاهش بهره‌وری محاسبه شده به دلار) و نرم‌افزارها خسارت وارد آورد. ریسک‌های اینترنتی طی سال‌های ۲۰۰۳ -۲۰۰۰، به وضوح افزایش یافته که این افزایش، موجب افزایش نیاز افراد و سازمان‌ها برای مدیریت این‌گونه ریسک‌ها شده است.

هم‌زمان با افزایش ریسک حملات اینترنتی، در رابطه با استفاده قانونی از اطلاعات الکترونیکی و حفظ آنها مقرراتی تدوین شد. بسیاری از این قوانین در پاسخ به نیاز برای استانداردهای به‌روزشده در رابطه با اطلاعات کامپیوتری به‌وجودآمدند و سپس با حوادث گسترده کلاهبرداری شرکتی (انرون و ورلدکام)[4] توسعه یافتند. جدول ۲ خلاصه‌ای از قوانین و مقررات مربوط‌به کاربرد و ذخیره اطلاعات را ارائه می‌کند. قانون ساربنز - اکسلی[5]، هیپا[6]، قانون گرام - لیچ - بلایلی[7] و قوانین دیگر، الزام می‌کند که اطلاعات مالی، اطلاعات بیماران و دیگر اطلاعات مربوط به مشتری باید در شرایط مطمئن و امن نگهداری شود.

جریمه عدم‌انجام این اقدام، شامل مجازات‌های شرکتی، مدنی و جزایی علاوه‌بر پاسخ‌گویی به مقامات عالی‌رتبه است. برای انجام این تکالیف، مدیریت ریسک هم به شکل کاهش ریسک و هم به شکل بیمه ضروری است. در مجموع برای شرکت‌هایی که تحت شمول این قوانین هستند، استانداردهای بالاتری تعریف شده است. البته صاحب‌نظران ابراز می‌دارند، دیگر شرکت‌ها که صریحاً با قوانین موجود در جدول ۲ تحت شمول قرار نگرفته‌اند براساس عرف عمومی، مسئول حفاظت از اطلاعاتی هستند که در اختیار دارند.

ترکیب افزایش ریسک و الزامات سازگاری با قوانین در نمودار ۱ نمایش داده شده است. محصولات بیمه‌ای که به‌طورخاص برای اینترنت طراحی شده‌اند از محصولات اولیه و ناقص قبل از یازدهم سپتامبر ۲۰۰۱ به بیمه‌نامه‌های پیچیده‌تر بلوغ پیدا کرد. اگر چه متغیرهای تأثیرگذار زیادی در این امر دخیل‌اند، اما اعتقاد بر این است که افزایش ریسک و الزامات سازگاری، دو عامل اصلی تأثیرگذار بر توسعه بیمه اینترنت است.

1. Keynote Systems
2. Crackers
3. Love Bug Virus
4. Enron and Worldcom
5. Sarbanes-Oxley Act
6. HIPAA
7. Gramm-Leach-Bliley Act

جدول ۲. قوانین فدرال و ایالتی مربوط به اطلاعات الکترونیکی

قانون	توضیح
Health Insurance Portability and Accountability Act (HIPAA) (1996)	این قانون رازداری و امانتداری اطلاعات بیمار و دیگر اطلاعات پزشکی را الزام می‌کند و به عرضه‌کنندگان خدمات درمانی تکلیف می‌کند که از اطلاعات نگهداری‌شده حفاظت کنند.
SEC 17a-3 and 17a-4 (revised 2002)	مؤسسات مالی را ملزم می‌کند که مکاتبات مشتریان و تمام اطلاعات الکترونیکی را برای بازرسی با حفظ امانت نگهداری کنند.
Gramm-Leach-Bliley Act (1999)	این قانون مؤسسات مالی را ملزم می‌کند که سیاست‌هایشان را جهت حفظ اطلاعات محرمانه مشتریان اعلام کرده و ضمن تضمین رازداری و امانتداری از دسترسی بدون مجوز به اطلاعات جلوگیری نمایند.
Sarbanes-Oxley Act (2002)	این قانون با ملزم‌کردن شرکت‌ها به رعایت صحت و دقت در اطلاعات مالی، دقت و قابل اعتمادبودن این اطلاعات را تضمین می‌کند.
California State Law SB 1386 (2002)	این قانون تمام نمایندگی‌ها و شرکت‌های ایالتی که اطلاعات مشتریان را نگهداری می‌کنند را ملزم می‌کند که نفوذهای امنیتی را سریعاً اطلاع دهند.

نمودار ۱. حوادث اینترنتی و قوانین مربوط و محصولات بیمه اینترنت

۴-۲. برخی انواع پیشرفته‌تر بیمه‌نامه اینترنت

برخی از نمونه‌های جدید بیمه‌نامه‌های اینترنت شامل نت‌ادونتج[1] گروه بین‌المللی آمریکایی[2]، بیمه‌نامه جامع الکترونیک لویدز لندن[3]، بیمه‌نامه‌های اینشور تراست دات‌کام[4]، جی. اچ. مارش و مک‌لنان[5]، شروود[6]، سی. ان. ای.[7] و زوریخ نورث آمریکا[8] است. حق‌بیمه‌ها بسته به نوع پوشش و میزان آن از ۵۰۰۰ تا ۶۰۰۰۰ دلار برای ۱۰۰۰۰۰۰ دلار پوشش بیمه‌ای (یا از ۰/۵٪ تا ۶٪) متغیر است.

از جدول ۳ این‌گونه می‌توان نتیجه‌گیری کرد که بیمه‌نامه‌های جدید اینترنت در مقایسه با بیمه‌نامه‌های اولیه هکر، بسیار پیشرفته‌تر هستند. بر خلاف بیمه‌نامه‌های اولیه هکر که بر خسارات شخص اول تکیه می‌کرد، بیمه‌نامه‌های اینترنت جدید، هم خسارات اشخاص اول و هم خسارات اشخاص ثالث را پوشش می‌دهد؛ ضمن اینکه پوشش بالاتری را نیز ارائه می‌کند. پوشش شخص اول نوعاً شامل تخریب یا واردشدن خسارت به دارایی‌های اطلاعاتی، توقف در کار اینترنت، سرقت اینترنتی، خسارت ناشی از حملات داس و حتی اختلاس‌های الکترونیکی است. پوشش شخص ثالث ادعاهای خساراتی مربوط‌به محتوای اینترنتی، امنیت اینترنتی و خطاها و اشکالات فناوری و همچنین هزینه‌های دفاعی را شامل می‌شود.

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

جدول ۳. خلاصه بیمه‌نامه‌های اینترنتی اخیر

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

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

جدول ۴ مثالی را نشان می‌دهد که بیمه‌گران اینترنت چگونه برای به‌دست‌گرفتن بخش‌های مختلف بازار، بیمه‌نامه‌های متفاوت طراحی می‌کنند. در جدول ۴ مشاهده می‌کنیم که AIG برای به‌دست‌گرفتن بخش‌های مختلف بازار با نیازهای بیمه‌ای متفاوت، انواع مختلفی از بیمه‌نامه‌های اینترنت را ارائه کرده است؛ به‌عنوان‌مثال، برخی بیمه‌نامه‌ها، بعضی از ریسک‌های خاص را پوشش می‌دهند (مانند زیان یا خسارت مربوط‌به نقض حقوق انحصاری یا اسرار تجاری)، که دیگر بیمه‌نامه‌ها [این موارد را] استثنا کرده‌اند.

جدول ۴. محصولات مختلف بیمه اینترنت شرکت AIG که نشان‌دهنده استراتژی متنوع کردن محصول است

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

شرکت‌هایی که بیمه‌نامه‌های جدید اینترنت را خریداری کرده‌اند از بین مزایای آن این چند نمونه را بر می‌شمارند:

- احساس امنیت به خاطر انتقال ریسک به بیمه‌گر؛
- توانایی اقدام سریع در برابر خطر؛
- مراقبت (نظارت) مداوم توسط متخصصین؛
- ارائه پوشش لازم و مناسب، چرا که بیمه سنتی پوشش و تأمین کافی در برابر ریسک‌های الکترونیکی فراهم نمی‌کرد. دراین‌زمینه، برآوردهای فعلی صنعت بیمه نیز نشان‌دهنده تقاضای فزاینده برای محصولات بیمه اینترنت است.

۳. بیمه‌گران اینترنت چگونه مسائل پیش روی توسعه پوشش‌ها را حل کردند؟

در توسعه بیمه اینترنت از بیمه‌نامه‌های سنتی به بیمه‌نامه‌های اولیه هکر و تا شکل کنونی آن، بیمه‌گران اینترنت چندین مسئله مهم برای بررسی و حل پیش رو داشتند. در این بخش این مسائل و راه‌حل‌های بیمه‌گران اینترنت برای پرداختن به آنها را بررسی می‌کنیم.

۳-۱. انتخاب نامساعد

در یک دنیای ایده‌آل، طرفین قرارداد در رابطه با قرارداد و تصمیماتشان اطلاعات کامل دارند. اما در دنیای واقعی در بسیاری از موارد، ممکن است یکی از طرفین در

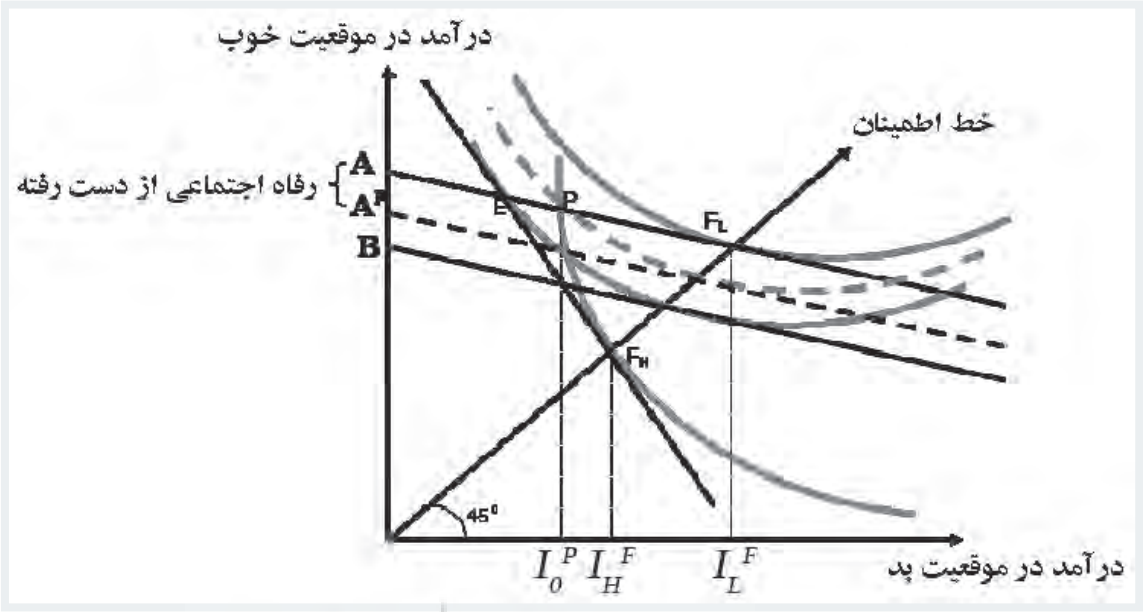
مـورد ماهیت محصول مورد توافـق، اطلاعات کمتری در اختیار داشـته باشـد. در قراردادهای بیمه‌ای این مشکلات زمانی بروز می‌کند که بیمه‌گر نسبت‌به اینکه متقاضی بیمه، دارای ریسک بالاست یا پایین، بی‌اطلاع باشد. ازآنجایی که متقاضی خود می‌داند که ریسـک بالا یـا پایین دارد ولی بیمه‌گر نمی‌داند، یک عدم‌تقارن اطلاعاتی بین آنها وجود دارد که این همان چیزی اسـت که در ادبیات اقتصادی به مسئله انتخاب نامساعد معروف است. زمانی که این وضعیت ظاهر می‌شود، طبق تئوری‌ها بیمه‌گران دو نوع قرارداد بیمه عرضه خواهند کرد: قرارداد با حق بیمه پایین و پوشش کم برای شـرکت‌هایی(بیمه‌گذارانی) که ریسک پایین دارند، و قرارداد با حق‌بیمه بالا و پوشـش بیشتر برای شرکت‌هایی که ریسـک بالا دارند. در حالت تعادلی شـرکت‌هایی که ریسـک بالا دارند قراردادی را انتخاب می‌کنند که دارای پوشش بیمه‌ای کاملی باشـد. درحالی‌که شرکت‌هایی که ریسـک پایین دارند قراردادی که فقط پوشش جزئی دارد را بـر می‌گزینند. یعنی در اینجا شـرکت‌های با ریسـک پایین لطمه می‌بینند، چرا که شـرکت‌هایی که ریسک بالا دارند پوشش کامل را به‌دسـت‌آورده‌اند، اما شرکت‌های با ریسـک پایین این پوشـش را ندارند و ازآنجایی که این شـرکت‌ها نمی‌تواننـد به‌طور کامل بیمه شـوند، لذا اولین راه‌حل بهتر[1] حاصل نشـده است و فقط دومین راه‌حلِ بهتر (یعنی بهترین راه‌حل، تحت شرایط محدودیت اطلاعاتی) دسـت‌یافتنی بوده و حاصل شـده اسـت. بنابراین مسـئله انتخاب نامسـاعد به کاهش رفاه اجتماعی می‌انجامد. رفاه ازدسـت‌رفته ناشی از انتخاب نامساعد را می‌توان، براساس ادبیات تجارت بین‌الملل در مورد سـنجش رفاه اجتماعی، به واحد پولی محاسبه نمود.

در اینجا نمودار ۲ را برای نشـان‌دادن محاسـبه این رفاه ازدسـت‌رفته به‌کارمی‌بریم. فاصله عمودی مربوط‌به نقطه تقاطعِ خط بودجه (خط بودجه مماس با منحنی بی‌تفاوتی) و محور عمودی، ارزش بازاری درآمد اسـت که به‌عنوان معیاری بـرای رفاه به‌کارمی‌رود. با مقایسـه ارزش بازاری درآمـد در حالـت بهترین راه‌حـل با بیمـه اینترنت کامل با حالتـی که اطلاعات نامتقـارن از میزان رفـاه اجتماعی می‌کاهـد، می‌توانیـم رفاه ازدسـت‌رفته اجتماعی ناشـی از مشـکل اطلاعـات نامتقـارن را به واحد پولـی برآورد کنیم. اگـر در اقتصاد دو نوع بیمه‌گذار (با ریسـک بالا و ریسـک پایین) وجود داشته باشـد و بیمه‌گر نتواند این دو نوع بیمه‌گذار را از هم تشـخیص دهد، بیمه‌گر قرارداد F_H (قـرارداد بیمه کامـل) را به متقاضیانی که ریسـک بالایی دارنـد، ارائه می‌کند امـا نمی‌تواند F_L (بیمـه کامل) را به متقاضیانی که ریسـک پایین دارند، ارائه کند. چرا که در صورت ارائه F_L، متقاضیانی که ریسـک بـالا دارند برای معرفی خود به‌عنوان متقاضیانِ دارای ریسک پایین، انگیزه پیدا خواهند نمود و پوشـش F_L را خریداری می‌کنند. این بدان معناسـت که راه‌حل تعادلی باید به گونه‌ای باشد که نه شرکت‌هایی که ریسک بالا دارند انگیزه‌ای برای معرفی خود به‌عنوان شرکت‌هایِ دارای ریسک پایین داشته باشند و نه شـرکت‌هایی که ریسـک پایین دارند خـود را مانند شـرکت‌هایی که ریسک بالا دارند، معرفی کنند. می‌دانیم که این امر با ارائه دو نوع قرارداد (بیمه‌نامه) توسط بیمه‌گر محقق می‌شـود: قرارداد با حق‌بیمه بالا و پوشش بیشتر F_H، که شـرکت‌هایی که ریسک بالایی دارند آن را خریداری می‌کننـد و قرارداد بـا حق‌بیمه پایین و پوشـش کم P که شـرکت‌هایی که ریسـک پایینی دارنـد آن را خریداری می‌کنند.

بنابرایـن تحت شـرایط اطلاعـات نامتقـارن، بهترین راه‌حـل اول (یعنی قرارداد بیمه کامـل F_L برای متقاضیانی که ریسـک پاییـن دارند و قـرارداد بیمه کامـل F_H برای متقاضیانی که ریسـک بالا دارند) دسـت‌نیافتنی است. به جـای آن فقط دومیـن راه‌حل بهتر (جایی کـه بیمه‌گران پوشـش بیمه‌ای جزیـی P به متقاضیانی که ریسـک پایین دارند و پوشـش کامل بیمه‌ای F_H به متقاضیانی که ریسک بالا دارند ارائه می‌کنند) قابل اجراسـت. بنابراین در نتیجه عدم‌توانایـی برخـی شـرکت‌ها (یعنی شـرکت‌هایی که ریسـک پایین دارند) برای کامل بیمه‌شدن، رفاه اجتماعی

1. First Best Solution

نمودار۲. رفاه اجتماعی ازدست‌رفته ناشی از انتخاب نامساعد



کاهش می‌یابد. این رفاه اجتماعی ازدست‌رفته ناشی از مشکل انتخاب نامساعد را می‌توان محاسبه نمود (نمودار ۲، $A-A^P$).

حل مشکل انتخاب نامساعد مستلزم آن است که بیمه‌گران اینترنت، متقاضیان را ملزم به پذیرش ارزیابی‌های دقیق، کامل و گسترده از ریسک نمایند. بیمه‌گران اینترنت، امنیت متقاضی را به‌عنوان پیش‌نیازی برای ارائه پوشش، از طریق هزاران فعالیت مبتنی‌بر بررسی درون سایت و خارج سایت به‌منظور بررسی آسیب‌پذیری‌های متقاضی، ارزیابی می‌کنند.

ارزیابی ریسک با تکمیل فرم درخواست و پرسش‌نامه مفصل توسط متقاضی آغاز می‌شود که برخی از این پرسش‌نامه‌ها شامل ۲۵۰ پرسش بوده (شامل پرسش‌هایی در رابطه با عواملی همچون بودجه فناوری، زیرساخت امنیتی، برنامه‌های ضد ویروس، فرآیندهای آزمایشی و امنیتی و برون‌سپاری) و برای ارزیابی ریسک‌های امنیتی و حفاظت اینترنتی به‌کارمی‌رود. پرسش‌های عمومی، شامل اطلاعاتی در رابطه با این موارد است:

– کد طبقه‌بندی استاندارد صنعتی[1] متقاضی؛

1. Standard Industrial Classification (SIC)

– سایت‌های اینترنتی که برای بیمه پیشنهاد شده‌اند، که این مورد شامل تعداد صفحات، مشتریان/کاربران، و تعداد مشاهدات صفحات است؛

– درآمد و فروش سالیانه شامل درآمد کسب‌شده از فعالیت‌های اینترنتی؛

– بودجه فناوری اطلاعات و درصد تخصیص‌یافته آن برای امنیت؛

– نوع فعالیت‌های انجام‌شده اینترنتی(مانند ایمیل و جستجوی شبکه، تولید و تلفیق فعالیت‌های داخلی، تجارت الکترونیک، شبکه مجازی خصوصی[2]، خدمات هاستینگ[3] شخص ثالث، مشاوره و ...).

سؤالات اختصاصی‌تر در مورد بیمه‌گری، شامل اطلاعاتی در رابطه با این موارد است:

– متن (محتوا): آیا متقاضی بیمه، محتوای وب‌سایتش را کنترل می‌کند؛ آیا وکیل باصلاحیت در رابطه با دارایی معنوی[4] و یا بیمه‌نامه مکتوبی جهت رفع موارد بحث‌انگیز دارد؛

2. Virtual Private Network (VPN)
3. Hosting Services
هاستینگ (میزبانی وب) در اصل تخصیص‌دادن مقداری فضا بر روی شبکه جهانی اینترنت با شرایط و ضوابط خاص است. (مترجم)
4. Intellectual Property

- نوع خدمات حرفه‌ای که ارائه می‌شود:

آیا خدمات متقاضی بیمه شامل سیستم‌های آنالیز (تجزیه‌وتحلیل)، انتشار، مشاوره، خدمات حرفه‌ای تکنولوژی، پردازش داده‌ها، چت‌روم[1] و ... است؛ آیا متقاضی، نرم‌افزار یا سخت‌افزار می‌فروشد یا به نرم‌افزار و سخت‌افزار مجوز می‌دهد؛

- امنیت شبکه: آیا شرکت دارای بیمه‌نامه‌هایی در رابطه با امنیت فناوری اطلاعات، اطلاعات محرمانه اشخاص و استفاده مجاز از ایمیل/اینترنت است؛ آیا کارکنان از اقدامات تنبیهی ممکن برای تخلفات و سوءاستفاده‌ها آگاهی دارند؛ آیا ارزیابی‌های امنیتی برای شخص ثالث یا آزمایش نفوذ انجام شده است؛ آیا پیشنهادات و توصیه‌های بیمه‌گر که اهمیت بالایی دارند، عملی شده است.

متقاضی علاوه‌بر سایر موارد باید مواردی نظیر بیمه‌نامه مکتوب شرکت در خصوص امنیت فناوری اطلاعات، بیمه‌نامه مکتوب برای حذف موارد مجرمانه و متخلفانه، کپی ارزیابی کنترل‌های امنیتی فناوری اطلاعات و نتایج آزمایش نفوذ، سوابق شغلی کارکنان بلندپایه از جمله مدیر فناوری اطلاعات و صورت‌های مالی حسابرسی‌شده را ضمیمه کند. سرانجام فرم درخواست باید قوانینی را ذکر کند که به متقاضی یادآوری کند که ارائه اطلاعات نادرست از روی عمد در بسیاری از موارد جرم محسوب می‌شود. این امر انگیزه‌ای را برای متقاضی به‌وجودمی‌آورد که نوع ریسک را به قیمت بازداشت یا زندانی شدن، نادرست ارائه نکند.

بعد از بررسی فرم مفصل درخواست متقاضی، بیمه‌گران بررسی فیزیکی و تکنیکی از بالا به پایین از ایمنی، شبکه‌ها و رویه‌ها انجام می‌دهند. ارزیابی ریسک در این مرحله با بررسی این موارد شروع می‌شود:

- امنیت فیزیکی: (شامل اینکه تجهیزات کجا قرار گرفته‌اند، آیا تجهیزات در چند طبقه یک ساختمان قرار دارند، آیا تجهیزات در فضای شرکت قرار گرفته یا در خارج آن و ...)؛

- نمودار شبکه: (که نشان‌دهنده موقعیت سیستم‌های عامل، ابزارهای کنترل از راه دور، محل قرار گرفتن مسیریاب‌ها[2]، دیواره‌های آتش[3]، وب، سرورهای پایگاه داده و ایمیل است؛ اینکه کدام سیستم‌ها در فضای اجاره‌ای از شرکت ارائه‌دهنده اینترنت[4] قرار گرفته؛ هر آی.پی[5] و هر دستگاه کجا قرار گرفته؛ و اینکه آیا درایو هارد یا فضای سرور اجاره‌ای است)؛

- توصیف فعالیت‌های شبکه: (مانند لیست آدرس‌های آی.پی؛ لیست تجهیزات کنترلی مانند سوئیچ‌ها، هابها[6]، مسیریاب‌ها، دیواره‌های آتش؛ سیستم‌های عامل شامل پراکسی سرورها، اسکنرهای(جستجوگرهای) مشکلات امنیتی، نرم‌افزار ضد ویروس، نگهداری کامپیوتر از راه دور، پروتکل‌های داده ابر کامپیوتر، تونلینگ دیواره‌های آتش، ارتباطات بی‌سیم و ...).

سپس بازدیدهای فیزیکی به‌عمل‌می‌آید که شامل بازدید در مورد کارکنان متقاضی و شیوه‌های استخدام آنها، بررسی امنیت فیزیکی، ارزیابی عکس‌العمل سریع، بهبود در بلایا، برنامه‌های آموزشی ایمنی و همچنین ارزیابی فنی آسیب‌پذیری خارجی شبکه، جستجوهای آسیب‌پذیری، سوییپ‌های دیجیتالی[7]، مراقبت از شبکه در برابر کاربران مغرض داخلی و خارجی و بازدید از دیواره‌های آتش، مسیریاب‌ها و پیکربندی شبکه است. این نتایج، تجزیه‌وتحلیل شده و به‌منظور تضمین شبکه‌ای ایمن‌تر لیستی از پیشنهادات و توصیه‌ها برای ارتقا و ثبات فراهم می‌شود.

این مکانیسمی است که بیمه‌گران اینترنت برای کار در مورد مسئله انتخاب نامساعد به‌کارمی‌برند. ارزیابی امنیتی دقیق و موشکافانه قبلی[8] به بیمه‌گران این اجازه را می‌دهد تا بتوانند بین متقاضیان با ریسک بالا و متقاضیان با ریسک پایین تفاوت قائل شوند. با بهره‌گیری از مکانیسم

1. Chatroom

2. Routers
3. Firewalls
فایروال، نرم‌افزار/سخت‌افزار ایمن‌ساز است (مترجم).
4. Internet Service Provider (ISP)
5. Internet Protocol
6. Hubs
7. Digital Sweeps نوعی ویراشگر صوتی (مترجم)
8. Ex Ante

هوشمند بررسی ایمنی متقاضیان، بیمه‌گران قادر خواهند بود از شکست بازار که از انتخاب نامساعد ناشی می‌شود جلوگیری کرده و مانع ازدست‌رفتن رفاه اجتماعی شوند که ناشی از مسئله اطلاعات نامتقارن است. علاوه‌براین چنین مکانیسمی مستقیماً برای شرکت‌هایی که ریسک پایین دارند، نفع دارد چرا که بررسی‌های امنیتی، آنها را قادر می‌سازد تا خود را از شرکت‌هایی که ریسک بالا دارند، متمایز سازند. با توانایی بیمه‌گران برای تفکیک و تفاوت قائل‌شدن بین انواع ریسک‌های متقاضیان، دیگر متقاضیانی که ریسک بالا دارند نمی‌توانند خود را دارای ریسک پایین معرفی کنند و در نتیجه رفاه اجتماعی مربوط‌به این مسئله از دست نمی‌رود.

۲-۳. مخاطرات اخلاقی[1]

دومین مشکل عمده‌ای که بیمه‌گران در ارائه پوشش بیمه‌ای باید مدنظر قرار دهند، مسئله مخاطرات اخلاقی است. این مسئله زمانی بروز می‌کند که شرکت‌های بیمه‌گذار، خود تعمداً باعث بروز خسارت شوند یا برای جلوگیری از وقوع خسارت اقدامات لازم را انجام ندهند؛ به‌عنوان‌مثال زمانی که شرکت‌ها تحت پوشش بیمه‌ای هستند در انجام کارهای امنیتی تعلل و سستی ورزند. بنابراین ممکن است این شرکت‌ها در زیرساخت‌های امنیتی سرمایه‌گذاری نکنند یا برای حفظ یا ارتقای سطح امنیتی موجود انگیزه نداشته باشند.

تفاوت بین مسئله مخاطرات اخلاقی و مسئله انتخاب نامساعد در دو مقوله هزینه‌ها و ساختار انگیزشی آنهاست. حل مسئله انتخاب نامساعد مستلزم صرف هزینه‌های سرمایه‌گذاری در زیرساخت‌های لازم برای تصمیم‌گیری در مورد تعیین نوع ریسک متقاضیان بالقوه‌ای است که ممکن است لازم نباشد دائماً بازنگری شوند. در مقابل مسئله مخاطرات اخلاقی، سرمایه‌گذاری در زیرساخت‌هایی را می‌طلبد تا بر متقاضیانی که لازم است به طور مستمر مورد بررسی قرار گیرند، نظارت شود. ازطرف‌دیگر، درحالی‌که مسئله انتخاب نامساعد به بررسی انگیزه بیمه‌گذاران با ریسک بالا در مورد پنهان‌کردن اطلاعات در مورد نوع ریسکشان به بیمه‌گر می‌پردازد (به همین دلیل است که در علم اقتصاد، مسئله انتخاب نامساعد به مسئله اطلاعات پنهان[2] نیز معروف است)، مسئله مخاطرات اخلاقی به انگیزه بیمه‌گذاران برای تعلل و کوتاهی در اقداماتشان می‌پردازد (به همین دلیل است که در علم اقتصاد مسئله مخاطرات اخلاقی، مسئله اقدامات پنهان[3] نیز نامیده می‌شود). در ادبیات اقتصاد بیمه‌ای، یک روش معروف برای بیمه‌گران برای حل مسئله مخاطرات اخلاقی وجود دارد و آن مشاهده سطح مراقبت بیمه‌گذار جهت ممانعت از خسارت و مرتبط ساختن مبلغ حق‌بیمه به این سطح مراقبت است. بدین‌ترتیب، وجود بیمه با چنین خصوصیتی می‌تواند سطح مراقبت از خود، توسط بیمه‌گذار را افزایش دهد.

میزان ایمنی را به‌طورکامل می‌توان قبل از توافق و امضای قرارداد و بعد از آن (طی دوره اعتبار پوشش) مشاهده نمود، به‌طوری‌که وجود بیمه اینترنت باعث افزایش میزان مخارج شرکت‌های بیمه‌گذار برای مراقبت از خود به شکلی منطقی، کاهش حق‌بیمه را به دنبال دارد، که این امر باعث افزایش سطوح امنیت فناوری اطلاعات در جامعه می‌شود. بنابراین ارزیابی‌های مفصل ریسک که توسط بیمه‌گران جهت ارائه پوشش بیمه اینترنت انجام می‌شود، برای شناسایی نوع ریسک بیمه‌گذار (و در نتیجه حل مسئله انتخاب نامساعد) و همچنین مرتبط ساختن طبقه‌بندی ریسک به مشوق‌های حق‌بیمه‌ای (برای حل مسئله مخاطرات اخلاقی) کاربرد دارد.

در بررسی شیوه عمل رایج صنعت بیمه و همچنین بررسی چند ویژگی بیمه‌نامه‌های اینترنت، می‌توان دریافت که بیمه‌گران با گنجاندن چند مکانیسم در قراردادهای بیمه اینترنت می‌توانند مسئله مخاطرات اخلاقی را حل کنند. بیمه‌گران اینترنت با وضع حق‌بیمه براساس طبقه‌بندی‌های ریسک، متقاضیان را به پذیرش ارزیابی امنیتی قبل از انعقاد قرارداد ملزم می‌کنند. از نگاه بیمه‌گران اینترنت، شرکت‌هایی که سطح حفاظت الکترونیکی پایین و

1. Moral Hazard

2. Hidden Information Problem
3. Hidden Action Problem

تجـارت آنلاین بالا دارند یا دارای تجـارت یا نوع کار با مقررات زیاد و همچنین در معرض جریمه‌های بالا هسـتند (نظیـر شـرکت‌های مالی)، شـرکت‌های با ریسـک بالا تلقی می‌شـوند. بنابراین یک بیمه‌گر اینترنت باید شرکت متقاضی را برحسـب یکـی از چندین طبقه‌بندی ریسـک طبقه‌بندی کند و حق‌بیمه را با ایمنی شـرکت مرتبط سازد و به شرکت‌هایی که پروسـه‌های ایمن‌تری دارند تخفیف بیشتری دهد. شـرکت بیمه اینشوردات‌کام[1] متقاضیانش را بین ۱ تا ۳۰، طبقه‌بندی می‌کند؛ به‌عنوان‌مثال شرکت اینترنتی جدیدی کـه معامـلات کارت اعتباری نـدارد به‌گونه‌ای متفاوت با شـرکت آمازون[2] طبقه‌بندی می‌شـود. همچنین بیمه‌گـران بـر فرآیندهای امنیتـی شـرکت، ایمنی دیگر شرکای فناوری شرکت، جوایزی برای ارائه اطلاعاتی که منجربه جلب (دسـتگیری) هکرها شـود و مخارج جبرانی بـرای فعالیت‌های مدیریـت بحران پس از نفـوذ، نظارت می‌کنند. به‌عنوان نمونه، شرکت سیف‌آنلاین[3] یک قراردادِ ارزیابی ریسک تکنولوژی با شرکت‌هایی نظیر آی.بی.ام.[4] و دیگر شـرکت‌ها منعقد کرده اسـت. شـرکت مارش[5] با شرکتِ سیستم‌های امنیت اینترنت[6] شریک است و شرکای تکنولوژیکـی AIG عبارت‌انـد از IBM، شـرکت امنیتی آر.اس.ای.[7] و شرکت گلوبال اینتگریتی[8].

همچنیـن بیمه‌گران اینترنت بعـد از انعقاد قرارداد بیمه، بررسی‌هایی در مورد زیرسـاخت‌های اطلاعاتی بیمه‌گذار در اشکال زیر انجام می‌دهند:

– به‌عنوان بخشی از بررسی‌های منظم سالیانه بیمه‌گران؛

– به‌عنوان مقدمه‌ای برای تصمیم‌گیری در مورد ادامه و یا اصلاح پوشش بیمه‌ای؛

– در خلال بررسی خسارت یا ادعای خسارت.

شـروط مختلف دیگری که در بیمه‌نامه‌های استاندارد جهت اجتناب از مسـئله مخاطرات اخلاقی گنجانده‌شـده در جدول ۵ آمده اسـت. **نخسـت**، بیمه‌گران در قرارداد قید می‌کنند که در صورتی که خسـارت، ناشـی از قصور بیمه‌گذار در حفظ سـطحی از امنیـت برابر یا بهتر از آنچه باشد که در شروع قرارداد بیمه‌نامه وجود داشت؛ بیمه‌گران تعهدی در قبال آن ندارند. این به معنی مشوقی برای داشتن امنیت بهتر است؛ زیرا همچنان که در بیمه‌نامه تصریح شده در صورتی که شـرکت‌های بیمه‌گـذار در انجام اقدامات لازم برای حفظ و بهبود امنیتشان کوتاهی کنند برای جبران خسـارات این‌چنینی نمی‌توانند ادعای دریافت خسـارت نمایند. بنابراین بیمه‌نامه جامع الکترونیکی در پوشـش‌های مختلفش همیشه شامل این بند است: «به شرط آنکه شرکت بیمه‌گذار همیشـه سطوح امنیتی سیسـتم را برابر یا بهتر از سطح موجود در زمان شروع این بیمه‌نامه حفظ کند».

در نمونـه بیمه‌نامه وب‌نت[9] شـرطی مشـابه را می‌توان یافت: «شـما (بیمه‌گذار) موافق هستید که حفاظت سیستم کامپیوتـری و دارایی‌های اطلاعاتی تجـارت الکترونیک و ارتباطـات تجـارت الکترونیکی‌تـان را در سـطحی یا استانداردی که وجود داشـته و ارائه گردیده است، حفظ نمایید».

دوم، بیمه‌گران همچنیـن صریحاً اظهار می‌کنند که به شـرکت‌هایی که از تهیه نسخه پشـتیبان برای فایل‌هایشان امتناع می‌کنند، پوششی ارائه نمی‌کنند. بیمه‌گران اینترنت، به‌صورت اجماعی با استثناکردن خسارت یا ادعای خسارت شـرکت‌هایی که از تهیه نسخه پشـتیبان برای فایل‌هایشان امتنـاع می‌کنند، به شـرکت‌های بیمه‌گذار ایـن انگیزه را می‌دهنـد که به طور منظـم از فایل‌های الکترونیکی‌شـان نسـخه پشـتیبان تهیه کنند. **سـوم**، زمانی که تخلفی اتفاق افتاد، بیمه‌گران شـرکت‌های بیمه‌گذار را به انجام اقدامات لازم جهت کاهش خسارت تشویق می‌کنند؛ به‌عنوان‌مثال، در بیمه‌نامـه جامـع الکترونیک لویدز، تصریح شـده که هزینه‌هایـی کـه بیمه‌گـذار در اسـتفاده از خدمات واحد اطلاعات ریسـک بیمه‌گر بـرای کاهش میزان خسـارت متحمل می‌شود، تحت عنوان خسارت شخص اول پوشش

1. Insuredotocom.com
2. Amazon.com
3. Safeonline
4. IBM
5. Marsh
6. Internet Security Systems (ISS)
7. RSA Security
8. Global Integrity Corporation
9. Web Net

جدول ۵. استثنائات بیمه‌نامه‌های اینترنتی اخیر که مسئله مخاطرات اخلاقی را حل کرده‌اند

استثنائات	بیمه‌نامه نت‌ادونتج	بیمه‌نامه جامع الکترونیکی	بیمه‌نامه وب‌نت
امتناع از تهیه نسخه پشتیبان فایل‌ها	✓	✓	✓
امتناع از انجام اقدامات معقول جهت حفظ یا بهبود امنیت	✓	✓	✓
اعمال متقلبانه، نادرست و مجرمانه بیمه‌گذار	✓	✓	✓
استهلاک طبیعی و عادی دارایی‌های اطلاعاتی بیمه‌گذار	✓	✓	✓
ادعاهای خسارت خارج از مسئولیت طرف‌های درگیر	✓	✓	✓
دیگر شروط مربوطه			
سهم‌های نگهداری	✓	✓	✓
حدود مسئولیت	✓	✓	✓
جوایز کشف مجرمان/هزینه تفحص‌ها(بررسی‌ها)	✓		✓
[هزینه] خدمات واحد اطلاعات ریسک برای کاهش خسارت شخص اول		✓	
بازدید منظم/سالیانه از امکانات بیمه‌گذار	✓	✓	✓

داده می‌شود. ازطرف‌دیگر، پوشش نت‌ادونتج شرکت بیمه AIG، به‌عنوان بخشی از پوشش شخص اول، وجوه (جوایز) اعطایی به افرادی که اطلاعاتی ارائه می‌دهند که این اطلاعات منجربه محکومیت مجرمان اینترنتی شود را تحت پوشش قرار می‌دهد، درحالی‌که بیمه‌نامه وب‌نت تصریح می‌کند که هزینه تفحص‌های(بررسی‌های) بیمه‌گذار را پوشش می‌دهد. همچنین، وب‌نت بیمه‌گذار را ملزم می‌کند که «در صورت نقض قانون، مراتب را به پلیس اطلاع داده» و «فوراً تمام اقدامات لازم برای محدودکردن یا کاهش خسارت و هزینه‌های دفاعی را به‌عمل آورد». بیمه‌نامه جامع الکترونیک همچنین در تحت پوشش قراردادن خسارات شخص اول که ناشی از کپی، ثبت و ضبط یا سرقت اسرار تجاری بیمه‌گذار باشد، بیمه‌گذار را ملزم می‌کند که اقدامات لازم برای جلوگیری را به‌عمل آورد.

جدول ۶. استثنائاتی که نشان‌دهندهٔ وجود صرفه‌های جانبی در بیمه‌نامه‌های جدید اینترنتی است

استثنائات	بیمه‌نامه نت‌ادونتج	بیمه‌نامه جامع الکترونیک	بیمه‌نامه وب‌نت
عدم‌توانایی استفاده از برنامه‌های نرم‌افزاری یا اجرانشدن آنها	✓	✓	✓
نقص الکتریکی یا ارتباط راه دور	✓	✓	✓

درصورتی‌که نظارت کامل بر سطح ایمنی شرکت بیمه‌گذار ممکن نباشد، برای حل مسئله مخاطرات اخلاقی، مکانیسم‌های تشویقی دیگری در بیمه‌نامه‌های استاندارد اینترنت گنجانده شده است؛ به‌عنوان‌مثال، محدودیت‌های مسئولیت و سهم نگهداری[1] به‌گونه‌ای طراحی و گنجانده شده که بیمه‌گذار مانند یک بیمه‌گر مشترک[2] باشد که در جلوگیری از وقوع خسارت ذی‌نفع باشد. مثلاً بیمه‌گذار، اولین خسارت‌ها[3] (سهم نگهداری) را پوشش می‌دهد و بیمه فقط مازاد بر این حد (که در بیمه‌نامه نیز تصریح شده است) را پوشش می‌دهد. ذکر این نکته لازم است که سهم‌های نگهداری عموماً برای هر خسارتی به‌کارمی‌رود. دیگر شروطی که برای حل مسئله مخاطرات اخلاقی درنظرگرفته‌شده‌اند، استثنائاتی از پوشش خسارات است که در نتیجه انجام اقدامات متقلبانه (فریبکارانه) و نادرست بیمه‌گذار باشد، همچنین خسارات ناشی از مسئولیت طرف‌های تجاری بیمه‌گذار مستثنا شده است. بنابراین براساس سطح احتیاط اعمال‌شده توسط بیمه‌گذار، بیمه‌گران اینترنت می‌توانند میزان حق‌بیمه را برمبنای سرمایه‌گذاری شرکت بیمه‌گذار در اقدامات امنیتی تعیین نمایند، که منجربه ایجاد انگیزه‌های بازارمحور در تجارت الکترونیک جهت افزایش امنیت اطلاعاتی می‌شود.

۳-۳. دیگر مسائل پیش‌رو

در مقوله امنیت اینترنتی به‌دلیل وابستگی‌های ناشی از ارتباطات فراوان، صرفه‌های جانبی[4] ایجاد می‌گردد. امنیت سیستم‌های کامپیوتری به‌گونه‌ای به‌هم وابسته است که یک حادثه در یک سیستم ممکن است بر همه سیستم‌های مشابه تأثیر بگذارد حتی اگر آن سیستم‌ها تحت کنترل ناظر اجرایی دیگری باشند. بنابراین اگر کد مخربی از طریق یک دستگاه معیوب به سیستم نفوذ کند، می‌تواند از این دستگاه به‌عنوان سکوی پرتابی برای حملات بعدی استفاده کند؛ به‌عنوان‌مثال اگر شخص یا شرکتی از نرم‌افزار آنتی ویروس استفاده نکند، درصورتی‌که سیستم آلوده شود ممکن است سیستم‌های دیگر را که تحت کنترل ناظر اجرایی دیگری می‌باشند نیز آلوده کند. به‌دلیل این پدیده، یعنی به‌صورتِ جمعی در معرضِ ریسکِ اینترنتی‌بودن، مسئله مهم در عرضه پوشش بیمه اینترنتی، امکان بالقوه وقوع حادثه در یک سیستم است به‌گونه‌ای که هم‌زمان خساراتی به بیمه‌گذاران زیادی وارد آورد. بیمه‌گران از چندین مکانیسم که برای کاهش معضل ریسک‌های به‌هم وابسته طراحی شده است، استفاده می‌کنند. همان‌طورکه در جدول ۶ نشان داده شده است، ممکن است بیمه‌گران جهت حفاظت خودشان از پرداخت خسارت‌های بزرگِ ناشی از ریسک‌های به‌هم وابسته، برخی حوادث را از پوشش استثنا کنند. به‌عنوان‌مثال، یک استثنای رایج به خسارت‌های ناشی از نقص تجهیزات الکتریکی و وسایل ارتباط از راه دور مربوط می‌شود. این استثنائات برای حمایت از بیمه‌گران از یک ریسک که منجربه خسارت

1. Retentions
2. Coinsurer
3. First Losses
4. Externality

در مقیاس وسیع می‌شود، گنجانده شده است.

مشکل دیگر در عرضه بیمه اینترنت، عدم‌وجود استاندارد بیمه‌گری است. ازآنجاکه ریسک‌های اینترنتی پیچیده‌اند، ارزیابی ایمنیِ شرکت ممکن است هزاران دلار هزینه در بر داشته باشد. به‌عنوان نمونه، ارزیابی امنیتی شرکت آلفا تراست[1] که اینشور تراست[2] آن را بیمه کرده است ۲۰۰۰۰ دلار هزینه داشته، همچنین ارزیابی امنیتی مارش ۲۵۰۰۰دلار هزینه در بر داشته است. با درک این مطلب که بررسی مفصل و از بالا تا پایین ممکن است برای خریداران پوشش مشکل باشد، برخی بیمه‌گران روش‌های صدور بیمه‌نامه را تسهیل کرده‌اند. مثلاً اینشوردات‌کام[3] یک پرسش‌نامه به‌صورت آنلاین عرضه کرده، درحالی‌که AIG فرآیند صدور سه مرحله‌ای بیمه‌نامه را برگزیده است که شامل این موارد است:

– درخواست آنلاین؛

– ارزیابی آنلاین که بر مبنای پرسش‌نامه و سنجشِ از راه دور ایمنی شرکت انجام می‌شود؛

– ارزیابی‌های فیزیکی.

برخلاف بیمه سنتی در دیگر حوزه‌ها که اطلاعات ده‌ها سال در آنها موجود است، داده‌های آماری اندکی برای شرکت‌های بیمه‌ای که به دنبال کاهش ریسک‌های اینترنتی هستند، وجود دارد. به‌دلیل اینکه بیمه‌گران برای برآورد ریسک احتمالی و تعیین حق‌بیمه بر پیش‌بینی‌ها تکیه می‌کنند، نبود داده‌های آماری برای ریسک‌های اینترنتی، تعیین حق‌بیمه را بسیار مشکل می‌کند. واضح است که جهت برآورد دقیق‌تر ریسک‌ها، روش‌های سنجش ریسک باید توسعه یابد. یک گام صحیح می‌تواند همکاری نزدیک‌تر کارگزاران بیمه با عرضه‌کنندگان خدمات امنیت اینترنتی باشد. اقدام دیگر اصلاح و تعدیل مقررات و استانداردسازی پوشش‌های مربوط‌به کامپیوتر با کمک انجمن ملی قانون‌گذاران بیمه‌ای[4] بوده که سازمانی خصوصی و غیرانتفاعی از قانون‌گذاران بیمه‌ای است.

۴. خلاصه و نتیجه‌گیری

بیمه اینترنت ابزاری مهم برای امنیت اینترنتی در دو سطح مختلف است:

– بیمه اینترنت، انگیزه‌های اقتصادی بیمه‌گران و اشخاص/ سازمان‌ها را برای مدیریت ریسک‌ها به‌منظور کسب سود همسو می‌کند.

– مجموع نفع شخصی موجود در یک بازار بیمه اینترنت، منجر به افزایش رفاه اجتماعی می‌شود.

در این مقاله یک مطالعه تاریخی و با هدف دنبال‌کردن تکامل بیمه اینترنت از شکل بیمه‌نامه‌های سنتی به بیمه‌نامه‌های اولیه ریسک اینترنتی و سپس به محصولات جامع کنونی انجام گرفت. نتیجه اینکه صنعت بیمه اینترنت از شکل بیمه‌نامه‌های اولیه هکر که عمدتاً بیمه‌های شخص اول را با پوشش‌های کم ارائه می‌کرد به شکل بیمه‌نامه‌های پیچیده‌تر و متنوع‌تر که بیمه شخص اول و شخص ثالث را با پوشش‌های بالاتری ارائه می‌دهد، بلوغ یافته است.

همچنین مشخص گردید که شرکت‌های بیمه اینترنت قادرند با مسائل پیش‌رو دست و پنجه نرم کنند. به‌عنوان‌مثال، بیمه‌گران با طبقه‌بندی دقیق و موشکافانه میزان ریسک بیمه‌گذار، به مسئله انتخاب نامساعد و مخاطرات اخلاقی پرداختند و تکالیفی در خصوص ایمنی که از بیمه‌گذار انتظار می‌رود را در بیمه‌نامه‌ها گنجاندند. در این مقاله روشی برای محاسبه رفاه اجتماعی ازدست‌رفته ارائه گردید، رفاهی که با حل مسائلی همچون انتخاب نامساعد می‌توان مانع ازدست‌رفتن آن شد.

نتیجه آن که محصولات و پوشش‌های مختلف بیمه اینترنت، اینترنت را محیطی امن‌تر می‌سازد زیرا بیمه‌گران اینترنت با ارائه مشوق‌های اقتصادی، شرکت‌ها را ترغیب به حداقل‌کردن خسارت نموده و افراد/سازمان‌ها به‌طور روزافزون، به دنبال بیمه اینترنت در راستای منافع شخصی خود هستند. بیمه‌گران می‌توانند اطلاعاتشان را در مورد ریسک‌ها بیشتر کنند، آسیب‌پذیری‌های سیستم‌ها را شناسایی کنند، از بیمه‌گذار بخواهند که حسابرسی‌های

1. AlphaTrust Corp
2. Insuretrust
3. Insuredotcom.com
4. National Association of Insurance Commissioners (NAIC)

قبلـی را بپذیرند و راهبردهای کنش‌گرایانه[1] پیشـگیری از خسـارت را برگزینند. این موارد شـبیه همان چیزی است که در دیگر صنایع اتفـاق افتاده، مثلاً بیمه منجربه افزایش ایمنی در پیشگیری از آتش‌سوزی، حوادث هواپیما، بویلر و آسانسـور گردید. علاوه‌بر گزینه تبعیت از قانون فدرال برای حفاظت از زیرساخت‌های شبکه‌ای، یارانه‌های فدرال گزینه دیگری برای ترغیب شـرکت‌ها بـه خریداری بیمه اینترنت است (نظیر آنچه قوانین و دستورالعمل‌های انجمن ملی قانون‌گذاران بیمه‌ای در حوزه‌هایی نظیر بیمه درمان و حوادث، و مداخله دولت در حوادث سـیل و نیروگاه‌های هسته‌ای ایجاد کرد).

متأسفانه تغییر در اقدامات مدیریت ریسک غالباً مستلزم وقوع حوادث بزرگ اسـت. پیشـتر در این مقاله به حادثه یازدهم سـپتامبر ۲۰۰۱ به‌عنوان چنین حادثه‌ای اشـاره شد. آتش‌سـوزی سـال ۱۹۱۱ کارخانه تراینگل شرت‌ویست[2] شـهر نیویورک در زمره چنین حوادث هولناکی است که به تقویت و نهادینه‌شـدن حفاظت در برابر آتش‌سـوزی و بیمه آتش‌سـوزی در ایالات متحده انجامید. ممکن اسـت حادثه‌ای اینترنتی با چنین مقیاسی قبل از اینکه بیمه اینترنت نفوذش را به سطوح بالاتر افزایش دهد، روی دهد اما اینکه چه وقت چنین اتفاقی می‌افتد معلوم نیست.

منبع:

Majuca, R P, Yurcik, W &, Kesan, J P 2006, 'The Evolution of Cyberinsurance', *Department of Economics; National Center for Supercomputing Applications (NCSA)*, College of Law, University of Illinois at Urbana-Champaign.

1. Pro-active
2. Triangle Shirtwaist Factory