The University of Tehran Press

Journal of

Social Business

Home Page: https://jsbu.ut.ac.ir/

Online ISSN:

Creating Cyber Insurance Market in Iran, The Institutional Role of Government and its Impact on Enterprises

Jaber Abdi[1] | Reza Kalantari[2*]

1. ICT Security Research Faculty, Iran Telecommunication Research Center, Tehran, Iran. Email: Ja.abdi17@gmail.com
2. Corresponding Author, ICT Security Research Faculty, Iran Telecommunication Research Center, Tehran, Iran. Email: kalantar@itrc.ac.ir

ARTICLE INFO

Article type:
Research Article

Article History:
Received August 11, 2024
Revised August 23, 2024
Accepted September 07, 2024
Published online September 22, 2024

Keywords:
Cyber insurance,
Cyber risk,Enterprises,
Institutions,
Government.

ABSTRACT

Cyber attacks can have severe and damaging consequences on businesses, governments and individuals, resulting in financial losses, harm to reputation and disruptions to essential infrastructure. As the digital landscape evolves and cyber threats escalate, the need for more robust cyber risk management strategies has led to the expansion of the cyber insurance market as a vital defense against the threats. Cyber insurance not only acts as a stand-alone risk control measure but also impacts other risk management practices. The growth of this market benefits the overall insurance industry and enhances its market penetration. However, despite the cyber insurance market becoming a primary method for managing cyber risk in many countries over the past thirty years, various businesses in Iran lack access to such a market. This study aims to explore the reasons behind the absence of a cyber insurance market in the Iran's economy. By reviewing the literature on market failures in economics and proposing a conceptual model for the cyber insurance market, the findings suggest that the high relative level of cyber risk and excessive transaction costs pose significant obstacles to establishing this market in Iran. It is recommended to create a platform named the Cyber Insurance Market Guide, focused on designing and implementing government institutional policies to foster the development of the cyber insurance market.

Cite this article: Abdi, J. & Kalantari, R. (2024). Creating Cyber Insurance Market in Iran, The Institutional Role of Government and its Impact on Enterprises. *Journal of Social Business*. 1 (1), 93-113.

 Publisher: The University of Tehran Press.

انتشارات دانشگاه تهران

نشریهٔ کسب و کار اجتماعی

سایت نشریه: https://jsbu.ut.ac.ir/

شاپا الکترونیکی:

ایجاد بازار بیمهٔ سایبری در ایران؛ نقش نهادی دولت و تأثیرات آن بر کسب‌وکارها

جابر عبدی[۱] | رضا کلانتری[۲*]

۱. پژوهشکده امنیت فاوا، تهران، ایران. رایانامه: Ja.abdi17@gmail.com

۲. نویسنده مسئول، پژوهشکده امنیت فاوا، تهران، ایران. رایانامه: kalantar@itrc.ac.ir

اطلاعات مقاله

نوع مقاله:
پژوهشی

تاریخ‌های مقاله:
تاریخ دریافت: ۱۴۰۳/۰۵/۲۱
تاریخ بازنگری: ۱۴۰۳/۰۶/۰۲
تاریخ پذیرش: ۱۴۰۳/۰۶/۱۷
تاریخ انتشار: ۱۴۰۳/۰۷/۰۱

کلیدواژه:
بیمهٔ سایبری،
دولت،
ریسک سایبری،
کسب‌وکارها،
نهادها.

چکیده

حمله‌های سایبری می‌توانند اثرهای جدی و مخربی بر کسب‌وکارها، دولت‌ها و افراد داشته باشند و سبب خسارات مالی، آسیب به اعتبار و اختلال در زیرساخت‌های حیاتی شوند. پویایی و تحول در فضای دیجیتال، افزایش تهدیدهای سایبری و نیاز به رویکردهای مؤثرتر در مدیریت ریسک سایبری، بازار بیمهٔ سایبری را به‌منزلهٔ یک گام کلیدی در برابر تهدیدهای سایبری، گسترش داده است. بیمهٔ سایبری افزون‌بر نقش مستقل در کنترل ریسک، بر دیگر روش‌های مدیریت ریسک نیز تأثیرگذار است. توسعهٔ این بازار همچنین موجب رونق صنعت بیمه و افزایش ضریب نفوذ آن می‌شود. اگرچه در بسیاری از کشورها بازار بیمهٔ سایبری به یکی از روش‌های اصلی مدیریت ریسک حوزهٔ سایبر در سه دههٔ اخیر تبدیل شده است، کسب‌وکارهای مختلف در ایران، از داشتن چنین بازاری بی‌بهره بوده‌اند. این پژوهش در پی پاسخ به چرایی شکل نگرفتن بازار بیمهٔ سایبری در اقتصاد ایران است. با بررسی ادبیات حوزهٔ شکست بازارها در علم اقتصاد و ارائهٔ مدل مفهومی از بازار بیمهٔ سایبر، یافته‌های ما نشان می‌دهد که بالا بودن سطح نسبی ریسک سایبری و هزینهٔ بالای مبادله، مهم‌ترین موانع ایجاد بازار بیمهٔ سایبری در ایران است. پیشنهاد ما ایجاد سکویی با عنوان راهنمای بازار بیمهٔ سایبری با هدف طراحی و اجرای سیاست‌های نهادی دولت برای توسعهٔ بازار بیمهٔ سایبری است.

استناد: عبدی، جابر و کلانتری، رضا (۱۴۰۳). ایجاد بازار بیمهٔ سایبری در ایران؛ نقش نهادی دولت و تأثیرات آن بر کسب‌وکارها. *کسب و کار اجتماعی*، ۱ (۱) ۹۳-۱۱۳ .

ناشر: مؤسسه انتشارات دانشگاه تهران.

۱. مقدمه

جامعهٔ مدرن به‌طور روزافزون به خدمات فناوری اطلاعاتی وابسته می‌شود. امروزه خدمات فناوری اطلاعات همهٔ جنبه‌های فعالیت‌های بشری را از کار تا تفریح و از بخش خصوصی تا بخش عمومی تحت تأثیر قرار می‌دهد. زمانی که این خدمات به هر دلیلی مانند اشتباه‌های غیرعمدی یا حمله‌های شرورانه متوقف شود، پیامدهای آن به‌سرعت احساس شده و اثرهای آن از طریق زنجیره‌های تأمین یکپارچه و فرایندهای تعاملی کسب‌وکار، در سراسر جهان مشهود می‌شود. از این منظر، خدمات فناوری اطلاعات در حال تبدیل به یکی از زیرساخت‌های حیاتی کشورها همچون جاده‌ها، برق، آب شرب و خدمات مالی هستند. از این‌رو، تحقیقات زیادی به‌منظور جلوگیری از قطعی خدمات فناوری اطلاعات و تضمین پایداری کسب‌وکارها انجام می‌گیرد. در ابتدا عمده‌ترین عامل توقف خدمات فناوری اطلاعات، سخت‌افزارهای رایانه‌ای بودند، اما از دههٔ ۱۹۸۰ به بعد، خطاهای مدیریتی، انسانی و نرم‌افزاری سهم بزرگی در ایجاد این خاموشی‌ها داشتند (Gordon & Loeb, 2018). با ظهور سرویس‌های مبتنی بر خدمات سایبری و ابرمحاسبات، تلاش‌های زیادی برای بررسی بهینه‌سازی کیفیت خدمات در این محیط‌ها، از جمله یادگیری از حوادث گذشته به‌منظور ارائهٔ بهترین خدمات صورت گرفته است (Kieninger et al., 2013). از منظر مهندسی قابلیت اطمینان سنتی، مدیریت ریسک قطعی خدمات فناوری اطلاعات شامل مطالعهٔ توزیع آماری قطعی‌های فناوری اطلاعات و اهمیت فناوری در رفع آن است (Franke, 2014). با این‌حال، با درک این موضوع که نمی‌توان تنها با ابزارهای فنی از تمام تهدیدها، نقص‌ها و قطعی‌های امنیتی و فناوری اطلاعات جلوگیری کرد، مدیریت ریسک مالی از طریق بیمهٔ سایبری به نوعی سیاست مکمل تبدیل شده است.

سابقهٔ بیمهٔ سایبری به دههٔ ۱۹۹۰ میلادی بازمی‌گردد، زمانی که سازمان‌ها نیاز به پوشش در برابر خطرهای سایبری را به‌منزلهٔ یکی از روش‌های مدیریت ریسک سایبری درک کردند. رشد اینترنت و افزایش فراوانی و شدت حمله‌های سایبری، رشد محصولات بیمهٔ سایبری را تشویق کرده است. در سال ۲۰۲۲، هزینه‌های جرایم سایبری در جهان حدود ۸/۴ تریلیون دلار برآورد شده است که با افزایش چشمگیری روبه‌رو بوده است. برای مثال، در سال ۲۰۱۵ هزینه‌های جرایم سایبری جهانی حدود ۳ تریلیون دلار برآورد شده بود (IBM Security, 2022). بیمهٔ سایبری که بیمه مسئولیت سایبری نیز شناخته می‌شود، نوعی بیمه است که پوششی را برای خسارت‌های مربوط به حمله‌های سایبری، نقض امنیت داده‌ها و سایر تهدیدهای سایبری فراهم می‌کند. نسخه‌های ابتدایی بیمهٔ سایبری اغلب بر هزینه‌های پاسخ به نفوذ به داده‌ها و ارسال هشدار[1] متمرکز بودند و در ادامه دامنهٔ پوشش آن به اخلال در کسب‌وکار، آسیب به شهرت و جرایم نظارتی[2] گسترش یافته است. براساس آخرین داده‌ها، ارزش بازار بیمهٔ سایبری در جهان در سال ۲۰۲۲ حدود ۷/۸ میلیارد دلار برآورد شده است. کارشناسان این صنعت پیش‌بینی می‌کنند که این بازار با نرخ رشد سالانهٔ تقریبی ۲۰ درصد از سال ۲۰۲۳ تا ۲۰۳۰ رشد کند و در پایان این دهه به بیش از ۲۸ میلیارد دلار برسد (Reports and Data, 2022).

بیمه‌نامه‌های سنتی از اصطلاحاتی استفاده می‌کنند که آسیب فیزیکی و اموال مشهود را به هم مرتبط می‌کند و خسارت ناشی از اموال غیر فیزیکی نامشهود (مانند از دست دادن داده‌ها) را لحاظ نمی‌کنند. درحالی که بیمه‌گزاران تمایل به پوشش بیمه در کسب‌وکار اینترنتی دارند، بیمه‌گرها به‌طور مداوم بر حذف خسارت‌های سایبری از پوشش بیمه‌ای اصرار دارند و به‌طور فزاینده‌ای خطرهای الکترونیکی را از پوشش بیمه‌ای سنتی کنار می‌گذارند. ناکافی بودن بیمه‌های سنتی برای مقابله با تهدیدهای جدید در دنیای سایبری، نیاز به محصولات بیمه‌ای جدید را که به‌طور خاص برای پوشش خطرهای جدید دنیای اینترنت طراحی شده‌اند آشکار می‌کند. این مهم نیازمند شناسایی چارچوب نهادی و فنی است تا به بازیگران اصلی، یعنی شرکت‌های بیمه‌گر و بیمه‌گزاران انگیزهٔ کافی برای ورود به بازار بیمهٔ سایبری بدهد. از این‌رو هدف این پژوهش، تحلیل چرایی شکل نگرفتن بازار بیمهٔ سایبری در ایران و اثرهای آن بر کسب‌وکارها و بررسی نقش دولت در ایجاد بستر نهادی مناسب برای ایجاد این بازار است.

در بخش دوم ابتدا پیشینهٔ پژوهشی حوزهٔ بیمه و اهمیت بیمهٔ سایبری برای کسب‌وکارها مرور شده و سپس پیشینهٔ پژوهشی

1. Notification
2. Regulatory penalties

علم اقتصاد در عوامل ایجاد ناکارایی در بازار و ویژگی‌های بازار بیمهٔ سایبری بررسی می‌شود. در بخش سوم با ارائهٔ مدلی مفهومی از بازار بیمهٔ سایبری، علت شکل نگرفتن این بازار بررسی خواهد شد. در بخش چهارم با استفاده از نتایج بخش دوم و تحلیل محتوایی- آماری از داده‌های کتابخانه‌ای، نقش نهادی دولت در ایجاد بازار بیمهٔ سایبری ارزیابی شده و در انتها نتیجه‌گیری ارائه می‌شود.

۲. پیشینهٔ پژوهش و مبانی نظری

به‌طور کلی روش‌های مدیریت ریسک را می‌توان به چهار روش خودداری[1]، انتقال[2]، کاهش[3] و پذیرش[4] تقسیم کرد. هر بنگاه در واکنش به ریسک‌های متفاوت، بسته به نیاز و صلاحدید خود از یک یا همهٔ این روش‌ها استفاده می‌کند. خودداری به روش‌هایی اشاره دارد که مانع بروز حادثه می‌شوند. خرید بیمه نوعی انتقال ریسک به بازیگر سوم یعنی شرکت‌های بیمه است و در رویکرد کاهش، با مدیریت حادثه از عوارض و خسارت ناشی از آن کاسته می‌شود. گاهی ممکن است خسارت برخی از حوادث کمتر از هزینهٔ واکنش در برابر آن باشد، از این‌رو بنگاه‌ها آن را می‌پذیرند (Hillson, 2020).

از سوی دیگر گاهی دولت‌ها با هدف حفاظت از منافع عمومی و مقابله با شکست بازار، از طریق الزام به رعایت استانداردها، قوانین و مقررات به مداخله می‌پردازند (Bannister & Connolly, 2018). برای مثال، دولت ممکن است حداقل استانداردهای ایمنی را برای محصولات، ساختمان‌ها یا وسایل نقلیه اعمال کند تا ریسک را کاهش دهد. در مقابل، بیمه یک روش بازاری است که در آن افراد و کسب‌وکارها با پرداخت حق بیمه، ریسک‌های مالی خود را به شرکت‌های بیمه منتقل می‌کنند و این شرکت‌ها با ادغام ریسک بیمه‌گزاران مختلف، ریسک کلی را متنوع و کاهش می‌دهند (Vaughan & Vaughan, 2014). برتری روش‌های مبتنی بر عملکرد بازاری آن است که بازیگران اصلی با داشتن اطلاعات کامل‌تر تصمیم‌هایی کاراتر خواهند گرفت. باید به این نکته توجه کرد که استانداردها و مقررات می‌توانند بازار بیمه را با ایجاد یک خط پایه از روش‌های مدیریت ریسک تقویت کنند، ولی از سوی دیگر ممکن است سبب بروز محدودیت در انعطاف‌پذیری و نوآوری در یک سیستم مبتنی بر بازار شوند (Harrington & Niehaus, 2019).

بیمهٔ سایبری اغلب نوعی سازوکار انتقال ریسک معرفی می‌شود، ولی به دو دلیل بر دیگر روش‌های مدیریت ریسک تأثیرگذار است. نخست اینکه از اولین اقدامات پس از بروز حادثه، اطلاع‌رسانی به مشتریان بیمه است. این اقدام در قالب «خدمات پاسخ اولیه» شناخته می‌شود که در بازارهای توسعه‌یافته توسط شرکت‌های روابط عمومی انجام می‌پذیرد. این خدمت از طرف شرکت‌های بیمه‌ای ارائه می‌شود، ولی برای بیمه‌گزاران نیز بااهمیت است. آنها نیازمند اطمینان از ارسال هشدارهای اولیه به مشتریانشان در مورد احتمال بروز حادثهٔ سایبری هستند. این موضوع خود برای بیمه‌گزاران به‌عنوان ریسک عمل می‌کند که سبب می‌شود آنها افزون‌بر سازوکار انتقال اصلی بیمه، مواردی از پذیرش و کاهش را نیز به سبد روش‌های مدیریت ریسک خود اضافه کنند. دوم اینکه، شرکت‌های بیمه، برای مشتریان خود حداقل‌هایی از افشای اطلاعات و امنیت IT را تعیین می‌کنند و از ابزار پذیره‌نویسی در رد یا پذیرش مشتریان و نیز سیاست قیمتگذاری با ارائهٔ تخفیف‌های مختلف، در جهت هدایت آنها به‌سوی ایجاد امنیت بیشتر استفاده می‌کنند. در نتیجه خرید بیمهٔ سایبری می‌تواند همراه با جنبه‌هایی از خودداری و کاهش باشد (Kshetri, 2017).

با توجه به افزایش چشمگیر حمله‌های سایبری، به‌ویژه در سال‌های اخیر، نیاز به بیمهٔ سایبری بیش از پیش احساس می‌شود. برای مثال، گزارش هزینهٔ نقض داده‌ها در سال ۲۰۲۳ نشان می‌دهد که هزینهٔ متوسط نقض در داده‌ها به ۴/۴۵ میلیون دلار رسیده است که این رقم در مقایسه با سال‌های گذشته به‌طور چشمگیری افزایش یافته است (IBM, 2023). بیمهٔ سایبری می‌تواند هزینه‌های ناشی از این حوادث را پوشش دهد و به کسب‌وکارها کمک کند تا بدون نگرانی از بار مالی ناشی از حمله‌های، به فعالیت‌های خود ادامه دهند. همچنین، این نوع بیمه به بنگاه‌ها امکان می‌دهد که با افزایش اعتماد مشتریان و

1. Avoidance
2. Transfer
3. Mitigation
4. Acceptance

بهبود امنیت اطلاعات، به تقویت موقعیت رقابتی خود بپردازند. از این‌رو بیمهٔ سایبری برای کسب‌وکارها ابزاری حیاتی در مدیریت ریسک مرتبط با حمله‌های سایبری و نقض‌های اطلاعاتی شناخته می‌شود.

مطالعات مرتبط با بیمهٔ سایبری را می‌توان به دو گروه تقسیم کرد. گروه اول مطالعاتی است که شکل‌گیری بازار بیمهٔ سایبری را که به‌دلیل ماهیت پیچیده و همبستگی زیاد مشتریان، ناتوانی بیمه‌گرها در ارزیابی سطح امنیت سایبری و قیمت زیاد بیمه‌نامه به‌دلیل ناتوانی شرکت‌های بیمه در پیش‌بینی خسارت‌های ثانویه مانند خسارت به شهرت، ناممکن می‌دانند. ولی گروه دوم با رویکرد تشویقی به این بازار نگاه می‌کنند به‌طوری که بیمهٔ سایبری به سرمایه‌گذاری بیشتر در بهبود امنیت سایبری می‌انجامد و همچنین حق بیمه‌ها هم قابل تخمین هستند (Frank, 2017). باینر[1] و همکاران (۲۰۱۵) اشاره می‌کنند که مشکلاتی که در ادبیات برای ایجاد بازار بیمهٔ سایبر مطرح شده است شامل وجود همبستگی بین خسارت‌ها، نبود داده‌های تاریخی و نامتقارنی بالای اطلاعات است.

۲. ۱. چه زمانی بازار برای یک محصول شکل نمی‌گیرد؟

بازار مفهومی بنیادی در علم اقتصاد است که تعامل بین خریداران و فروشندگان کالاها و خدمات را نشان می‌دهد. بازار محلی است که نیروهای عرضه و تقاضا با هم به تلاقی می‌رسند و قیمت و مقدار مبادلهٔ یک کالا را تعیین می‌کنند. بازار نقش حیاتی در تخصیص کارآمد منابع دارد، زیرا به تولیدکنندگان امکان می‌دهد که تقاضا برای محصولات خود را ارزیابی کنند و به مصرف‌کنندگان امکان می‌دهد که تصمیم‌های خرید را آگاهانه اتخاذ کنند. از طریق سازوکار قیمت، بازار، تصمیم‌های میلیون‌ها فعال اقتصادی را هماهنگ و تولید، توزیع و مصرف کالاها و خدمات را هدایت می‌کند. بازار به‌عنوان ستون فقرات اقتصاد سرمایه‌داری عمل می‌کند و محرک نوآوری، رقابت و استفادهٔ کارآمد از منابع کمیاب برای پاسخگویی به نیازها و تمایلات جامعه است. با این‌حال، در مواردی ممکن است بازارها ایجاد نشوند یا به بیان دیگر با شکست بازار[2] مواجه باشیم. در این شرایط، بازار قادر به تخصیص بهینهٔ منابع نیست و شاید مداخلهٔ دولت، برای بهبود شرایط لازم باشد (Mankiw, 2020). شکست بازار هنگامی رخ می‌دهد که انگیزه‌های خصوصی با منافع جامعه همسو نباشند یا با شفاف نبودن اطلاعات روبه‌رو باشیم.

یکی از عوامل کلیدی ناکارآمدی بازار، «ماهیت خود بازار» است. هنگامی که یک شرکت یا گروهی از شرکت‌ها، سهم کافی در بازار برای تأثیرگذاری بر قیمت‌ها، مقدار و کیفیت کالا یا اطلاعات مهم در اختیار داشته باشند، دارای قدرت بازاری هستند. شرکت‌ها از این قدرت برای حداکثرسازی سود به‌جای بهبود کارایی استفاده می‌کنند. بازارهای متمرکز مانند بازار انحصاری، انحصار کامل خرید، انحصار چندجانبهٔ فروش و انحصار چندجانبهٔ خرید نمونه‌هایی از این شکل از ناکارآمدی بازار هستند (NSW, 2017). عامل مهم دیگر، «ماهیت کالا یا خدمات» مورد معامله است. برخی از کالاها و خدمات ویژگی‌هایی دارند که سبب تأمین ناکافی یا بیش از حد نسبت به سطح بهینه می‌شود. کالاهای عمومی که تفکیک‌ناپذیر و غیررقابتی هستند، اغلب به‌طور ناکافی تأمین می‌شوند، زیرا مشکلات هماهنگی[3] سبب دشواری در تأمین کافی آنها می‌شود. دفاع ملی نمونهٔ کلاسیک یک کالای عمومی است؛ مانند زمانی که سیستم دفاع ملی در کشور، به همهٔ شهروندان آن کشور منفعت می‌رساند، صرف نظر از اینکه به‌صورت فردی، هزینه‌ای برای آن پرداخت کرده باشند یا نه. همچنین ویژگی تفکیک‌ناپذیری، امکان کنار گذاشتن افراد از بهره‌مندی از آن را منتفی می‌کند (NSW,2017).

پیامدهای خارجی[4] به شرایطی اشاره دارد که در آن هزینه‌ها یا منافع حاصل از تولید یا مصرف، به‌طور کامل در قیمت‌های بازاری منعکس نمی‌شود و به شکست بازار می‌انجامد (Varian, 2019). آلودگی هوا یکی از پیامدهای خارجی منفی است. تولید یک کارخانه ممکن است آلاینده‌هایی را به هوا منتشر کند که به سلامت ساکنان نزدیک به آن آسیب برساند. با این‌حال، این خسارت در قیمت بازاری محصول تولیدی کارخانه منعکس نمی‌شود. در این وضعیت، تولید کارخانه بیشتر از سطح بهینهٔ همراه با کنترل انتشار آلودگی است که یک نمونه از شکست بازار در تخصیص بهینهٔ منابع به شمار می‌رود (NSW, 2017).

1. Biener
2. Market failure
3. Coordination problems
4. Externality

در تشخیص کارایی بازار، *در دسترس بودن و کیفیت اطلاعات* در بازار نیز عامل کلیدی است. زمانی که اطلاعات ناکافی یا نامتقارن باشد، ناکارایی به صورت‌های مختلف بروز می‌کند. نخست، نامتقارنی اطلاعات که به زمانی اشاره دارد که یک طرف از مبادله، با داشتن اطلاعات بیشتر نسبت به طرف مقابل، از آن به نفع خود استفاده می‌کند. انتخاب نامساعد[۱] یکی از مشکلات ناشی از اطلاعات نامتقارن است. دوم شکست اطلاعاتی[۲] است که طرف‌های بازار در کشف یا دریافت اطلاعات با شکست مواجه می‌شوند. این موضوع می‌تواند به‌شکل کمبود اطلاعات، ناآگاهی، شکست هماهنگی یا قراردادهای ناقص ظاهر شود (NSW,2017).

شکست بازار، در حالت حدی می‌تواند به حذف کامل بازار یک کالا یا خدمت منجر شود. در واقع اگر قدرت بازاری، ویژگی‌های کالای عمومی و نقص یا نامتقارنی در اطلاعات در سطح بالایی باشد، با افزایش ناکارایی و کاهش منفعت حاصل از مبادله، به‌تدریج بازار مربوطه حذف می‌شود. با درک عوامل مختلف ناکارایی در بازار، سیاستگذاران می‌توانند مداخلات هدفمندتری را برای هدایت بازارها برای همسو کردن بهتر انگیزه‌های خصوصی با منافع جامعه و بهبود کارایی اقتصادی طراحی کنند.

۲. ۲. بازار بیمهٔ سایبری

بازار بیمهٔ سایبری می‌تواند تأثیرهای چشمگیری بر کسب‌وکارها و صنعت بیمه داشته باشد. این نوع بیمه به شرکت‌ها کمک می‌کند تا ریسک‌های مرتبط با حمله‌های سایبری و نقض‌های اطلاعاتی را شناسایی و مدیریت کنند و همچنین ایجاد اعتماد در میان مشتریان و شرکای تجاری را تسهیل می‌کند. در صورت وقوع حملهٔ سایبری، بیمهٔ سایبری می‌تواند هزینه‌های مرتبط به پاسخ به حادثه و دعاوی قانونی را پوشش دهد که سبب ادامهٔ فعالیت بدون نگرانی از بار مالی ناشی از این حمله‌ها به کسب‌وکارها می‌شود. افزون‌بر این، همان‌طور که اشاره شد توجه بیشتر به بیمهٔ سایبری به بهبود روش‌های مدیریت ریسک و ارتقای زیرساخت‌های امنیتی در سازمان‌ها منجر می‌شود (Deloitte, 2022; Zhao et al., 2023).

از سوی دیگر، با گسترش بازار بیمهٔ سایبری، شرکت‌های بیمه به توسعهٔ محصولات جدید می‌پردازند و این موضوع موجب رونق بازار بیمه و افزایش ضریب نفوذ آن می‌شود. کسب‌وکارهای کوچک و متوسط که قبلاً به بیمه توجه نداشتند، به‌دلیل نیاز به حفاظت از داده‌های خود، به خرید بیمهٔ سایبری روی می‌آورند. این روند به افزایش آگاهی عمومی دربارهٔ اهمیت بیمه و امنیت سایبری کمک می‌کند و در نهایت سبب ایجاد فرهنگ بیمه‌ای قوی‌تر در میان افراد جامعه می‌شود (Miller, 2023; KPMG, 2023).

چند ویژگی بازار بیمهٔ سایبری را از بقیهٔ بازارهای بیمه متمایز می‌کند. نخست تنوع و گستردگی ریسک‌های مرتبط با فضای سایبر است. حمله‌های سایبری می‌توانند از مسیرهای مختلفی از جمله دسترسی غیرمجاز به سیستم‌ها و شبکه‌ها، سرقت اطلاعات، تخریب سرویس‌ها و برنامه‌ها و تزریق نرم‌افزارهای مخرب رخ دهند. پوشش این میزان از ریسک، نیازمند بازار بیمهٔ انعطاف‌پذیری است که توانایی واکنش فعال در برابر تهدیدهای مختلف را داشته باشد (Böhme & Moore, 2012). دوم، پویایی و تغییرپذیری زیاد آن است. با توجه به رشد روزافزون ظهور فناوری‌ها و استفادهٔ گسترده از اینترنت، تهدیدهای سایبری نیز به‌طور مداوم در حال تکامل و تغییرند. به همین دلیل، بازار بیمهٔ سایبری باید توانایی سازگاری با این تغییرها و پاسخگویی پویا و به هنگام در برابر تهدیدهای جدید را داشته باشد. بیمه‌های سنتی از پیچیدگی و تغییرپذیری کمتری برخوردارند (Doherty & Fulford, 2017). برای مثال در بیمهٔ سیل و زلزله، منبع بروز ریسک تغییر نمی‌کند، ولی همزمان با پیشرفت فناوری، استانداردهای شرکت‌های بیمه برای مشتریان ارتقا می‌یابد.

سوم، سرایت‌پذیری زیاد ریسک سایبری است. حادثهٔ سایبری می‌تواند از طریق شبکه‌های انتقال اطلاعات یا با تخریب زنجیرهٔ تأمین صنعت، از یک نقطه به بخش‌های دیگر انتقال و به‌صورت زنجیره‌ای گسترش یابد. این موضوع حساسیت چگونگی ارزیابی و تخمین خسارت را در بیمه‌های سایبری افزایش می‌دهد. به‌طور کلی، در هر موضوع بیمه‌ای امکان انتقال ریسک و بروز

---

۱. انتخاب نامساعد زمانی رخ می‌دهد که معامله‌گران با ویژگی‌های خاص (مانند ریسک زیاد یا کیفیت کم) به‌دلیل عدم دسترسی طرف دیگر به اطلاعات کافی، وارد بازار می‌شوند. در نتیجه، این شرایط می‌تواند به کاهش کیفیت کالاها یا خدمات و در نهایت به ناکارآمدی بازار منجر شود.

2. Information failure

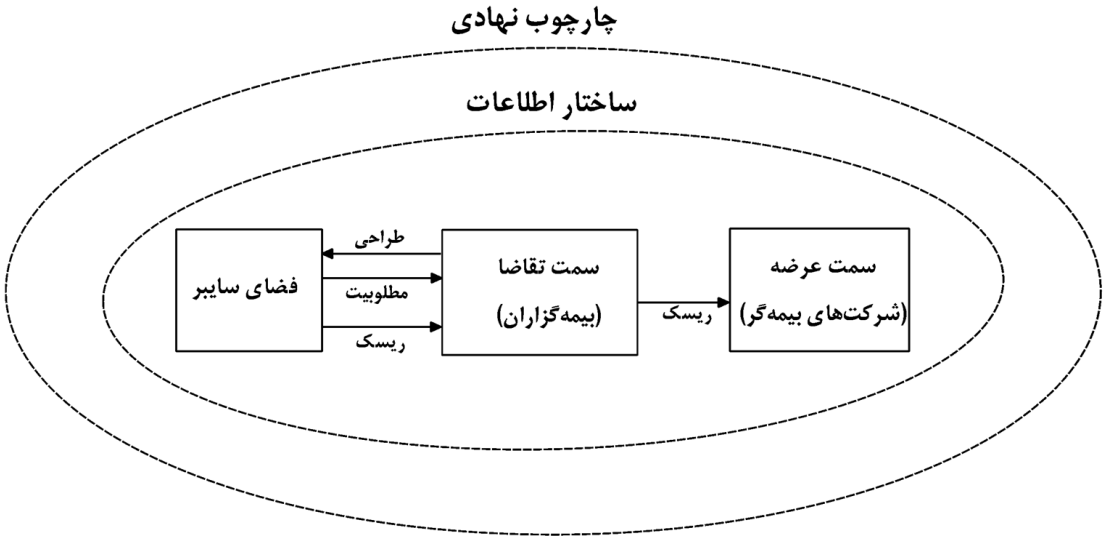
اثرهای زنجیره‌ای وجود دارد، ولی در حوادث سایبری به‌دلیل ماهیت پیوستهٔ شبکهٔ اطلاعات و سرعت انتقال، این ویژگی از شدت بیشتری برخوردار است (Kak & Goyal, 2020). برای مثال، یک حادثهٔ رانندگی ممکن است تأثیری مستقیم بر سایر بخش‌های یک سازمان نداشته باشد، مگر اینکه در زنجیرهٔ تأمین یا عملکرد سازمان اثرهای جانبی ایجاد کند.

با توجه به اینکه بیمهٔ سایبری، نوعی کالای خصوصی است و اثر پیامدهای خارجی هم در این بازار وجود ندارد و از سوی دیگر به‌دلیل شکل نگرفتن این بازار در کشور، قدرت بازاری نیز وجود ندارد، در نتیجه عامل اصلی ناکارایی براساس ادبیات رایج حوزهٔ شکست بازارها نقص یا نامتقارنی اطلاعات است. با توجه به وجود تنوع، تغییرپذیری و سرایت‌پذیری زیاد ریسک سایبری، حساسیت عوامل ایجاد ناکارایی در بازار بیمهٔ سایبری بیشتر است. نقص یا نامتقارنی اطلاعات به خطاهایی در ارزیابی ریسک و خسارت‌ها می‌انجامد که می‌تواند نتایج منفی بزرگ‌تری داشته باشد. نبودن بازار بیمهٔ سایبری در ایران نشان می‌دهد که عوامل ناکارایی در این بازار به حدی است که ایجاد چنین بازاری را ناممکن می‌کند.

در ادامه سعی می‌کنیم با ارائهٔ مدل مفهومی از بازار بیمهٔ سایبری، علت نبود این بازار در ایران را افزون‌بر عامل نقص یا نامتقارنی اطلاعات، در دو عامل بالا بودن ریسک سایبری و هزینهٔ مبادله جست‌وجو کنیم.

۳. مدل مفهومی بازار بیمهٔ سایبری

بازار بیمهٔ سایبری از بازیگرانی تشکیل شده است که در بستری که معمار آن دولت است به فعالیت و مبادله مشغول‌اند. با شناخت این بازیگران و درک نقش و چگونگی ارتباط بین آنها می‌توان به راه حل‌هایی برای اصلاح و بهبود کارایی در این بازار رسید. این موضوع خود، به افزایش پوشش و حمایت افراد و سازمان‌ها در برابر خطرهای سایبری کمک خواهد کرد.



شکل ۱. مدل مفهومی بازار بیمهٔ سایبری (اقتباس از بوهم و شوارتز[1]، ۲۰۱۰)

مدل مفهومی ارائه‌شده در شکل ۱ نشان‌دهندهٔ جایگاه و چگونگی ارتباط بازیگران اصلی در بازار بیمهٔ سایبری است. بازیگران اصلی در هر بازاری که در آن دولت مداخله مستقیم ندارد، شامل عرضه‌کننده (فروشنده) و تقاضاکننده (خریدار) است. سمت تقاضا در بازار بیمهٔ سایبری، بیمه‌گزاران یا مشتریان بیمهٔ سایبری هستند که به‌عنوان کارگزاران اقتصادی، افزون‌بر اینکه طراحی فضای سایبر را بر عهده دارند از آن مطلوبیت و در عین‌حال ریسک دریافت می‌کنند. بیمه‌گزاران با خرید بیمه، بخشی از این ریسک را به شرکت‌های بیمه منتقل می‌کنند. در سمت عرضه، شرکت‌های بیمهٔ سایبری قرار دارند که با ارزیابی ریسک، تعیین حق بیمه و پوشش‌های بیمه‌ای و عرضهٔ محصولات بیمهٔ سایبری در پی حداکثر کردن سود خود هستند.

1. Böhme & Schwartz

همچنین این مدل نشان می‌دهد که در یک بستر اطلاعاتی، شرکت‌های بیمه و بیمه‌گزاران با یکدیگر و همچنین با فضای سایبری ارتباط دارند. سطح اطلاعات هر بازیگر در شکل‌گیری ذهنیت و تابع تصمیم آن نقش اساسی دارد. در سطوح اطلاعات بالاتر و متقارن‌تر، هزینهٔ جمع‌آوری اطلاعات کمتر و تخصیص منابع از کارایی بیشتری برخوردار است. در نهایت همهٔ این عوامل در یک چارچوب نهادی قرار دارند. نهادها به‌عنوان تعیین‌کنندهٔ قواعد بازی اجتماعی با تنظیم‌گری، نقش مهمی در شکل‌دهی رفتار و تعاملات افراد و سازمان‌ها در محیط‌های مختلف دارند. از منظر اقتصاد هزینهٔ مبادله که زیرمجموعهٔ مکتب اقتصاد نهادگرای جدید است، هدف از ایجاد نهادها، حداقل‌سازی هزینه‌های انتظاری سازماندهی مبادلات است.

مدل مفهومی سادهٔ بالا امکان می‌دهد که عوامل ناکارایی در بازار بیمهٔ سایبری در ایران را در بخش‌های مختلف بازار بیمهٔ سایبری شناسایی و ارزیابی کنیم. برای این منظور بر سه جریان تأثیرگذار بر عملکرد بازیگران در بازار شامل جریان ریسک، جریان اطلاعات و جریان هزینهٔ مبادله تمرکز می‌کنیم.

۳. ۱. جریان ریسک

قیمت‌ها در بازارهای رقابتی به‌عنوان سیگنالی در جهت تخصیص بهینهٔ منابع عمل می‌کنند. در بازار بیمه افزون‌بر قدرت انحصاری و فناوری، مجموعهٔ دیگری از عوامل خاص صنعت بیمه شامل ریسک، ارزش بیمه‌شده، سابقهٔ بیمه‌ای و دیگر ویژگی‌های بیمه‌گزار نیز در تعیین قیمت حق بیمه‌ها مؤثرند. هر کدام از این عوامل می‌تواند به‌طور مستقل یا در ترکیب با یکدیگر تأثیرگذار باشد. ارزیابی ریسک مشتری بیمه، شرط لازم تعیین حق بیمه است. برای مثال، بیمهٔ خودرو براساس منطقهٔ جغرافیایی و ریسک بروز سرقت ممکن است با قیمت‌های متفاوتی عرضه شود. ارزش بیمه‌شده، به انتخاب سطح پوشش بیمه‌ای برای محصول بستگی دارد. افرادی که از سابقهٔ بیمه‌ای مثبت برخوردارند و خسارت بزرگی گزارش نکرده‌اند، می‌توانند از تخفیف‌های مختلف استفاده کنند. عوامل فردی مانند سن، جنسیت و وضعیت تأهل نیز ممکن است در قیمتگذاری تأثیرگذار باشند.

به‌دلیل طبیعت در حال تغییر تهدیدهای سایبری و نبود داده‌های تاریخی، قیمتگذاری بیمهٔ سایبری با چالش‌هایی مواجه است. ادبیات حوزهٔ بیمهٔ سایبری نشان می‌دهد که شرکت‌های بیمه از روش‌های مختلفی برای شناسایی، جمع‌آوری اطلاعات و قیمتگذاری حق بیمه‌ها استفاده می‌کنند. پژوهش رومنسکی[1] و همکاران (۲۰۱۸) در بازار بیمهٔ سایبری آمریکا نشان می‌دهد که شرکت‌های بیمه از روش‌هایی چون استفاده از گزارش‌های منتشرشده یا روش‌های معمول در دیگر شرکت‌ها، حدس زدن، قیمتگذاری رقابتی، استفاده از مدل‌های قیمتگذاری و همچنین قیمتگذاری براساس دیگر انواع بیمه برای قیمتگذاری بیمهٔ سایبری استفاده می‌کنند. در همهٔ این روش‌ها به‌طور مستقیم یا غیرمستقیم، سطح ریسک بیمه‌گزاران ارزیابی می‌شود. شرکت‌های بیمه حداقل‌هایی از وجود استاندارد در کنترل ریسک سایبری را برای مشتریان خود در نظر می‌گیرند و از بیمهٔ مشتریان پرریسک خودداری می‌کنند. از سوی دیگر در سمت تقاضا نیز ممکن است محدودیت وجود داشته باشد؛ به این ترتیب که با افزایش ریسک، قیمت پیشنهادی بیمه‌گر برای ارائهٔ خدمت بیمه افزایش می‌یابد و در نتیجه ممکن است بیمه‌گزاران قادر به خرید این بیمه‌نامه‌ها نباشند.

به این ترتیب با توجه به اهمیت و جایگاه ریسک در محاسبهٔ حق بیمه، با افزایش ریسک، بخشی از تقاضا شامل مشتریانی که استانداردهای امنیتی را رعایت نمی‌کنند و نیز مشتریان دارای سطوح درآمدی پایین‌تر از بازار بیمه حذف می‌شوند. این کاهش تقاضا در بازار بیمه، همگرایی ریسک[2] را با مشکل روبه‌رو می‌کند. همگرایی ریسک مفهومی اساسی در شکل‌گیری بازار بیمهٔ پایدار است. به این ترتیب که شرکت‌های بیمه با ایجاد مجموعه‌ای متنوع از ریسک افراد مختلف، به مدیریت و توزیع ریسک می‌پردازند و در نتیجه از یک‌سو با کاهش قیمت حق بیمه، مشتریان کم‌درآمدتر برای خرید بیمه تشویق می‌شوند و از سوی دیگر امکان مدیریت بروز خسارت‌های زیاد ناشی از برخی حوادث فراهم می‌شود (Gatzert & Schmeiser, 2012). از این‌رو وجود ریسک زیاد در بازار بیمه، می‌تواند شکل‌گیری و پایداری آن را با مشکل روبه‌رو کند. همچنین این مشکل تشدید می‌شود اگر مشتریان پردرآمدتر، از ریسک بیشتری نیز برخوردار باشند.[3]

1. Romanosky
2. Risk pooling

۳. مشابه انتخاب نامساعد مشتریان پر ریسک در بازار بیمه به دلیل اطلاعات نامتقارن.

به‌منظور ارزیابی تأثیر ریسک بر تقاضای بیمه، شاخص ریسک را همراه با سطح درآمد در نظر می‌گیریم. هرچه نسبت سطح ریسک به سطح درآمد بیمه‌گزار کمتر باشد، توانایی بیمه‌گزار در خرید بیمه افزایش می‌یابد. به بیان دیگر هرچه ریسک کمتر یا درآمد بیشتر باشد بیمه بیشتری خریداری می‌شود. پژوهش‌ها، شواهدی از تأثیر مثبت افزایش سطح درآمد بر بازار بیمه را نشان می‌دهد. گزارش چشم‌انداز جهانی امنیت سایبری[1] (۲۰۲۴) نشان می‌دهد که در سال ۲۰۲۲، ۷۴/۵۵ درصد از سازمان‌های پردرآمد از بیمه‌نامهٔ سایبری استفاده می‌کنند، درحالی که این رقم برای سازمان‌های کم‌درآمد تنها ۲۴/۶۲ درصد بوده است (Global Cybersecurity Outlook, 2024). از این‌رو شناسایی مسیر احتمالی حرکت ریسک در اقتصاد از اهمیت زیادی برخوردار است. همچنین پژوهش‌ها نشان می‌دهد که همبستگی بین رشد اقتصادی و ضریب نفوذ بیمه مثبت است و افزایش درآمد، به افزایش تقاضا برای محصولات بیمه و در نتیجه افزایش ضریب نفوذ بیمه در کشورها می‌انجامد (Alhassan & Biekpe, 2016).

از این‌رو شاخص نسبت ریسک به درآمد سرانه را نماینده‌ای برای قدرت خرید بیمه در نظر می‌گیریم و سعی می‌کنیم ارتباط این شاخص با ضریب نفوذ بیمه را بررسی کنیم. این شاخص مشابه شاخص قابلیت دسترسی[2] است که به‌طور معمول برای مسکن استفاده می‌شود.[3] برای این منظور از شاخص راهنمای ریسک کشوری بین‌المللی ICRG[4] به‌عنوان جانشینی برای ریسک در معرض افراد استفاده می‌کنیم. شاخص ICRG ابزاری پرکاربرد برای ارزیابی و مقایسهٔ ریسک‌های سیاسی[5]، اقتصادی[6] و مالی[7] بین کشورهای جهان است که توسط گروه PRS[8] تولید و منتشر می‌شود. این شاخص به‌طور گسترده توسط سرمایه‌گذاران، کسب‌وکارها و سیاستگذاران برای ارزیابی ریسک‌ها و فرصت‌های بالقوه مرتبط با کشورهای مختلف استفاده می‌شود. شاخص ICRG معیاری کمّی و عینی از ریسک کشورها در سه بخش ریسک سیاسی، اقتصادی و مالی را به‌دست می‌دهد که هر یک از این بخش‌ها نیز از زیرشاخص‌هایی تشکیل شده و در مقیاس ۰ تا ۱۰۰ امتیازدهی شده است که در آن ۱۰۰ کمترین ریسک را نشان می‌دهد. امتیاز کلی ریسک کشور به‌عنوان میانگین وزنی این سه زیرشاخص محاسبه می‌شود (www.PRS.com).

شکل ۲، ارتباط بین شاخص قدرت خرید بیمه و شاخص ضریب نفوذ بیمه را برای ۳۰ کشور عضو در سازمان توسعه و همکاری‌های اقتصادی OECD[9] نشان می‌دهد. با افزایش نسبت ریسک به درآمد، به‌طور متوسط ضریب نفوذ بیمه برای این گروه از کشورها[10] کاهش می‌یابد. یعنی با افزایش نسبت ریسک به درآمد، توانایی خرید بیمه‌گزاران کاهش می‌یابد و آنها بیمهٔ کمتری خریداری می‌کنند. به این ترتیب فراتر از آنچه در پژوهش‌های اقتصادی دربارهٔ دلایل بروز ناکارایی و شکست بازارها مطرح شده است، در بازار بیمه، یکی از دلایل شکست بازار، می‌تواند سطح بالای ریسک نسبی باشد.

شکل ۳ نشان می‌دهد که ریسک یا حادثهٔ سایبری چه مسیری را تا رسیدن به بازار بیمهٔ سایبری طی می‌کند. چنانچه منبع حادثهٔ سایبری از درون مجموعه بنگاه باشد یا خارج از آن، نخستین سد در برابر آن، زیرساخت امنیت سایبری یک کشور است. زیرساخت امنیت سایبری شامل قوانین و مقررات و تجهیزات فنی مرتبط با شبکهٔ امنیت سایبری کشور است.

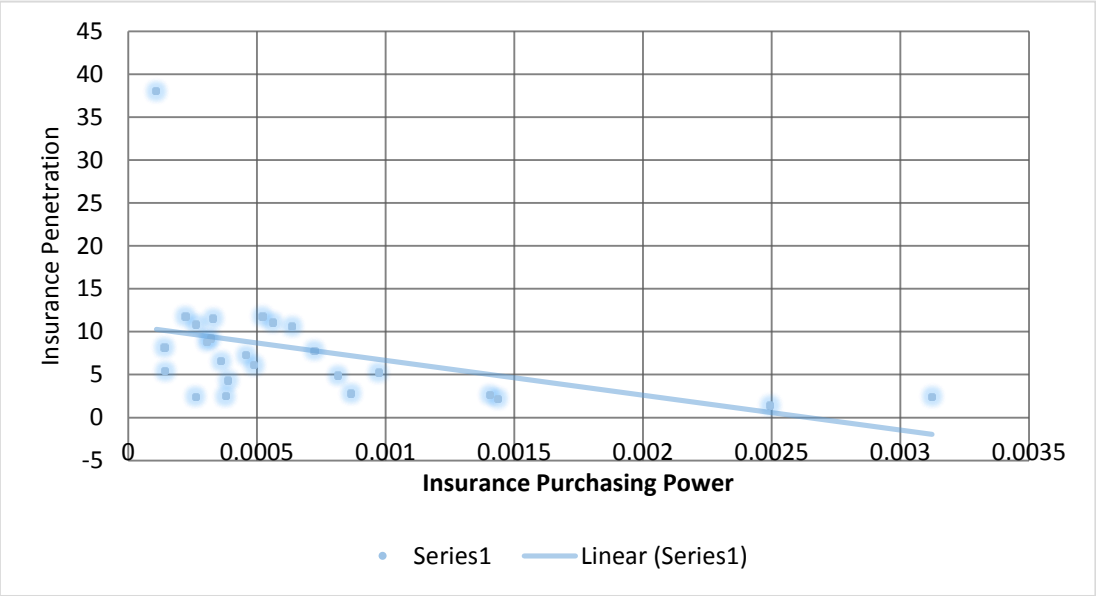
در مرحلهٔ دوم، هر بنگاه با ایجاد سپر امنیت داخلی، در برابر ریسک‌های احتمالی واکنش نشان می‌دهد. بسته به مقیاس تولید

---

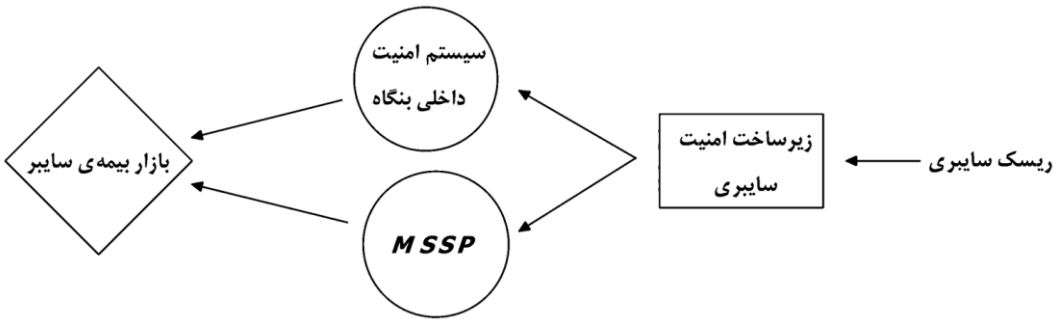
1. Global Cybersecurity Outlook
2. Affordability Index
۳. یکی از انواع آن، شاخص قابلیت دسترسی مسکن مرکب است که ماهانه توسط انجمن متخصصان املاک آمریکا منتشر می‌شود. این شاخص درآمد خانوار میانی را نسبت به درآمد لازم برای خرید یک خانه با قیمت متوسط اندازه گیری می کند (انجمن ملی املاک، ۲۰۲۲).
4. International Country Risk Gide
۵. رتبه‌بندی ریسک سیاسی عواملی مانند ثبات دولت، شرایط اجتماعی- اقتصادی، پروفایل سرمایه‌گذاری، تعارض‌های داخلی و خارجی، فساد، حضور نظامی در سیاست، تنش‌های مذهبی، قانون و نظم، تنش‌های قومی و پاسخگویی دموکراتیک را ارزیابی می‌کند.
۶. رتبه‌بندی ریسک اقتصادی، نقاط قوت و ضعف اقتصادی یک کشور از جمله رشد تولید ناخالص داخلی، تورم، تراز بودجه، تراز حساب جاری و ثبات نرخ ارز را ارزیابی می‌کند.
۷. رتبه‌بندی ریسک مالی، توانایی یک کشور در پرداخت تعهدات مالی خود را بررسی می‌کند و به عواملی مانند بدهی خارجی، خدمت بدهی خارجی، حساب جاری، نقدینگی خالص بین‌المللی و ثبات نرخ ارز می‌پردازد.
8. PRS (Political Risk Services) یک شرکت خصوصی متخصص در تحلیل ریسک سیاسی است.
9. Organization for Economic Co-operation and Development
۱۰. ۱۷ کشور که با توجه به داده‌های در دسترس برای شاخص‌های جرم سایبری، ضریب نفوذ بیمه و درآمد سرانه انتخاب شده‌اند.

و درآمد بنگاه، هر بنگاه با تحلیل هزینه– فایده در مورد برون‌سپاری سیستم امنیت داخلی خود به شرکت‌های ارائه‌دهندهٔ خدمات امنیت سایبری مدیریت‌شده MSSP[1] تصمیم می‌گیرد. MSSP شرکت‌های خدمات تخصصی فناوری اطلاعات هستند که بر امنیت سایبری تمرکز دارند و به کسب‌وکارها کمک می‌کنند تا از خود در برابر تهدیدهای سایبری محافظت کنند، اقدامات امنیتی خود را افزایش دهند و با سهولت و تخصص بیشتر در چشم‌انداز پیچیدهٔ امنیت اطلاعات حرکت کنند. روش‌های خودداری، کاهش و پذیرش در مدیریت ریسک تحت این مرحله انجام می‌گیرد.

در مرحلهٔ سوم و آخر بنگاه می‌تواند با خرید بیمه، ریسک باقی‌مانده را به شرکت‌های بیمهٔ سایبری انتقال دهد. به این ترتیب، بیمهٔ سایبری اغلب برای پوشش فاصلهٔ بین تعهدات MSSP (در صورت برون‌سپاری امنیت سایبری) و خسارت واردشده به بیمه‌گزاران استفاده می‌شود.



شکل ۲. ارتباط بین قدرت خرید بیمه و ضریب نفوذ بیمه در بین کشورهای OECD (منبع: یافته‌های تحقیق)

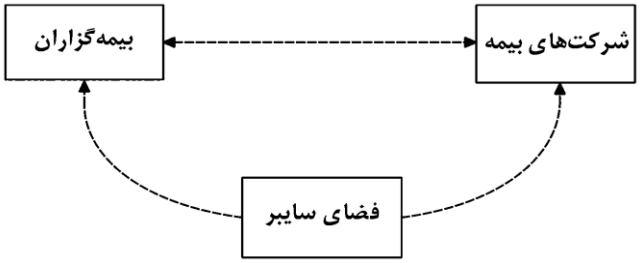


شکل ۳. جریان ریسک سایبری در اقتصاد (منبع: یافته‌های تحقیق)

۳. ۲. جریان اطلاعات

جریان اطلاعات در بازار بیمهٔ سایبری شامل اطلاعات مرتبط با ارزیابی ریسک، تحلیل امنیت سایبری، داده‌های آماری مرتبط با حادثه و خسارت سایبری و اطلاعات مرتبط با قراردادهای بیمه می‌شود. جریان اطلاعات در بازار بیمهٔ سایبری نقش اساسی در تحلیل و ارزیابی ریسک‌های مختلف، ارائه مشاوره‌های بیمه‌ای و مدیریت مطالبات دارد. شکل ۴ نشان می‌دهد که اطلاعات در بازار بیمهٔ سایبری در چه مسیر و جهتی جریان دارد.

1. Managed Security Service Provider



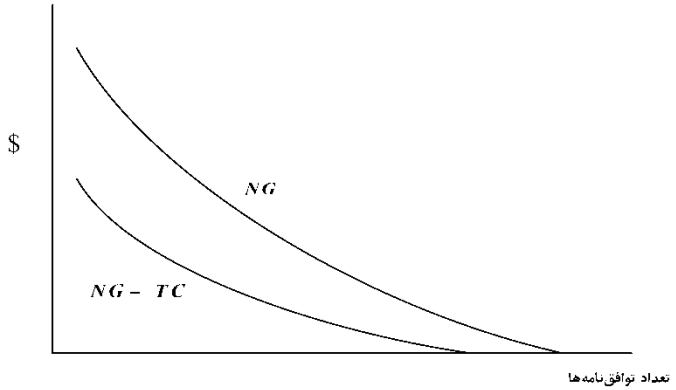
شکل ٤. جریان انتقال اطلاعات در بازار بیمهٔ سایبری (منبع: یافته‌های تحقیق)

شرکت‌های بیمه با تحلیل ریسک و آسیب‌پذیری موجود در فضای سایبری، قراردادهای بیمه پیشنهادی خود را به مشتریان (بیمه‌گزاران) ارائه می‌دهند. بیمه‌گزاران نیز با توجه به نیازهای امنیتی خود و بیمه‌نامهٔ پیشنهادی از سوی شرکت‌های بیمه، در مورد خرید بیمهٔ سایبری تصمیم می‌گیرند. وجود اطلاعات ناقص و نامتقارن بازیگران اصلی نسبت به یکدیگر و نسبت به فضای سایبر، با افزایش هزینهٔ مبادله، فرایند مذاکره برای رسیدن به یک توافق را سخت‌تر می‌کند. در عوض هرچه فضای اطلاعاتی گسترده‌تر و شفاف‌تر باشد امکان رسیدن به توافق با کارایی بیشتر افزایش می‌یابد. همچنین نبود اطلاعات شفاف از عوامل اصلی ایجاد رانت و انحصار است که به قیمتگذاری انحصاری و ناکارایی منجر می‌شود.

۳. ۳. جریان هزینهٔ مبادله

تحقق هر مبادله‌ای، مستلزم تحمل هزینه است؛ به‌طوری‌که گستردگی مبادله و بنابراین گستردگی منافع حاصل از مبادله وابسته به هزینه‌های مبادله است (رنانی[1]، ۱۹۹۷). یک انتقاد بزرگ به اقتصاد نئوکلاسیک آن است که هزینهٔ مبادله را برابر با صفر در نظر می‌گیرد. «هزینهٔ مبادله، هزینه‌ای است که به فرد، گروه یا سازمان، برای کنترل رفتار و نظارت بر مبادله در زمانی که با دیگران معامله اقتصادی انجام می‌دهند تحمیل می‌شود» (عاقلی و همکاران، ۲۰۱۷).

هزینهٔ مبادله بر تصمیم فعالان اقتصادی برای ورود به مذاکره برای رسیدن به توافق و مبادله اثر می‌گذارد. به‌طوری که اگر هزینهٔ مبادلهٔ پیش‌بینی‌شده بیشتر از آوردهٔ پیش‌بینی‌شدهٔ حاصل از مبادله باشد طرفین مبادله تمایلی برای ورود به میز مذاکره نخواهند داشت (عبدی و همکاران، ۲۰۲۲). شکل ۵، تأثیر هزینهٔ مبادله بر حجم مبادلات اقتصادی را نشان می‌دهد. محور افقی تعداد توافق‌نامه‌ها و محور عمودی آوردهٔ خالص NG[2] (منافع منهای هزینه) حاصل از توافق را نشان می‌دهد. توافق‌نامه‌ها انجام می‌پذیرد تا جایی که دیگر آوردهٔ خالص مثبت نباشد. با وجود هزینهٔ مبادله[3]TC، آوردهٔ خالص کاهش و منحنی به پایین منتقل شده و در نتیجه از تعداد توافق‌نامه‌ها کاسته می‌شود.



شکل ۵. تأثیر هزینهٔ مبادله بر تعداد توافق‌ها (مک‌کان، ۲۰۰۴)

1. Renani
2. Net gains
3. Transaction costs

از این‌رو در این پژوهش، هزینهٔ مبادله مفهوم دیگری است که در توضیح شکست بازار مورد تأکید است. هزینهٔ مبادله به‌تنهایی بخشی از عوامل بروز ناکارایی مطرح‌شده در ادبیات را شامل می‌شود. کاهش هزینهٔ مبادله از یک‌سو سبب کاهش پیامدهای خارجی می‌شود و از سوی دیگر با افزایش تعداد مبادلات و ورود بنگاه‌های بیشتر به بازار، به کاهش قدرت بازاری و انحصار می‌انجامد. همچنین کاهش هزینهٔ مبادلهٔ ناشی از نقص یا نامتقارن بودن اطلاعات، از مشکلات مرتبط به آن یعنی انتخاب نامساعد، مخاطره اخلاقی، مشکلات نماینده- صاحب، و عدم افشا می‌کاهد. تودوروا[1] (۲۰۱۶) نشان می‌دهد که ناکارایی بازارها که دلیل توسعه‌نیافتگی در کشورهای در حال توسعه است در هزینهٔ بالای مبادله ریشه دارد.

هزینهٔ مبادله در بازار بیمهٔ سایبری مشابه دیگر بازارها شامل زمان صرف‌شده برای جمع‌آوری اطلاعات، مذاکره و نظارت بر اجرای قرارداد است و به عواملی چون فناوری، سطح افشای اطلاعات، کیفیت نهادی و درآمد وابسته است. در ادامه به بررسی هر یک از این عوامل می‌پردازیم.

۱. فناوری: در پژوهش‌های اقتصادی، مقصود از فناوری، روش تولید کالا یا خدمت است. بهبود فناوری به تولید محصولاتی با قیمت کمتر یا کیفیت بهتر می‌انجامد. همچنین در اثر پیشرفت فناوری به روش‌ها و ابزارهای نوینی دست می‌یابیم که سبب صرفه‌جویی در زمان و هزینهٔ مبادله خواهد شد. برای مثال استفاده از دستگاه‌های هوشمند برای پایش استانداردهای امنیتی یا استفاده از فناوری‌های ارتباطی جدید مانند رسانه‌های اجتماعی[2] برای تنظیم زمان و برگزاری جلسهٔ مذاکره به کاهش هزینهٔ مبادله می‌انجامد.

۲. کیفیت نهادی: در پژوهش‌های اقتصاد نهادگرا بر نقش نهادهای فرهنگی اجتماعی، سیاسی، حقوقی و اقتصادی تأکید می‌شود. نهادها می‌توانند با تغییر قواعد، اقتصاد را به‌سمت کارایی سوق دهند. زیرا تصمیم‌های کارگزاران اقتصادی براساس ادراک ذهنی[3] متأثر از نهادهای رسمی (نظام اجرایی، قانونگذاری و قضایی و نیز قواعد و قوانین رسمی کشور) و نهادهای غیررسمی (قواعد غیررسمی، آداب و رسوم و هنجارهای اجتماعی و فرهنگی) شکل می‌گیرد (North, 1999). «از دید اقتصاد هزینهٔ مبادله که زیرمجموعهٔ اقتصاد نهادگرای جدید است، نهادها مشتمل بر سازمان‌ها به‌وسیلهٔ تنظیم ویژگی‌های مبادله با ساختارهای سازماندهی متفاوت در پی حداقل‌سازی هزینه‌های انتظاری سازماندهی در طی دوران مبادله هستند» (شکوهی، ۲۰۱۵). هرچه محیط مبادله از کیفیت نهادی بیشتری برخوردار باشد زمان و هزینهٔ کمتری برای تضمین پیش‌بینی‌ها و اجرای قرارداد صرف می‌شود.

۳. سطح افشای اطلاعات: همان‌طور که اشاره شد مبادلهٔ بیمه به مانند هر مبادلهٔ دیگری نیازمند کسب اطلاعات است. افشای اطلاعات از سوی بیمه‌گزار، بیمه‌گر و نیز انتشار اطلاعات از فضای سایبر، افزون‌بر اینکه با شفافیت اطلاعات به افزایش رقابت می‌انجامد، با کاهش هزینهٔ مبادله امکان رسیدن به توافقی با کارایی بیشتر را افزایش می‌دهد.

٤. درآمد: هرچه درآمد بازیگران بیشتر باشد، هزینه فرصت مذاکره و چانه‌زنی بیشتر است. به این ترتیب با افزایش درآمد، هزینهٔ مبادله بیشتر می‌شود و ممکن است بسیاری از قراردادهای بیمه محقق نشود.

۴. یافته‌ها؛ نقش نهادی دولت در شکل‌گیری بازار بیمهٔ سایبری

نهادها در اقتصاد، سازوکارهایی از قوانین، قواعد، مقررات، فرهنگ، سنت و ساختارهای اجتماعی شناخته می‌شوند که تعیین‌کنندهٔ قواعد بازی در جامعه هستند. دولت، قوهٔ قضایی، سیاستمداران، سازمان‌های بین‌المللی، سازمان‌های غیرانتفاعی از مهم‌ترین نهادهایی هستند که رفتار کارگزاران اقتصادی را در جامعه شکل می‌دهند. در این بین دولت در جایگاه ابرنهاد، به‌طور مستقیم با ابداع و اجرای قوانین، ارائهٔ خدمات عمومی، حفظ نظم و امنیت و نیز به‌طور غیرمستقیم از طریق وضع مقررات برای نهادهای دیگر، نقشی اساسی در اقتصاد به عهده دارد.

در بخش قبل بررسی جریان‌های اصلی مؤثر در بازار بیمهٔ سایبری، امکان رصد و بررسی عوامل اصلی مؤثر بر کارایی را

1. Todorova
2. Social media
3. Subjective perceptions

به‌دست داده است. از این‌رو می‌توان نقش نهادی دولت برای ایجاد بازار بیمهٔ سایبری در اقتصاد ایران را تنظیم‌گری اقتصاد با هدف کاهش ریسک سایبری و کاهش هزینهٔ مبادله در نظر گرفت.

۴. ۱. کاهش ریسک سایبری

همان‌طور که اشاره شد یکی از عوامل شکست بازار در بازار بیمه، سطح ریسک زیاد مشتریان بیمه است. از این‌رو برای شکل‌گیری بازار بیمهٔ سایبری، یکی از مهم‌ترین اقدامات کاهش ریسک برای کاهش قیمت بیمه‌نامه‌هاست تا هم شرکت‌های بیمه تمایل به ارائهٔ محصول بیمهٔ سایبری و هم بیمه‌گزاران توانایی خرید آن را داشته باشند. بررسی مسیر حرکت جریان ریسک تا مرحلهٔ رسیدن به بازار بیمهٔ سایبری در شکل ۳ نشان می‌دهد که سطح کیفیت نرم‌افزاری و سخت‌افزاری زیرساخت امنیت سایبری و همچنین سطح امنیت داخلی بنگاه و نیز کیفیت شرکت‌های MSSP، تعیین‌کنندهٔ آن است که حق بیمهٔ محصولات بیمهٔ سایبری در چه سطحی از ریسک سایبری قیمتگذاری می‌شود.

سطح سلامت و امنیت سایبری در یک اقتصاد را با شاخص‌های مختلفی از جمله شاخص امنیت سایبری جهانی[1] GCI اندازه‌گیری می‌شود. GCI یک مرجع قابل اعتماد برای ارزیابی تعهد کشورها به امنیت سایبری در سطح جهانی است. ازآنجا که امنیت سایبری گسترهٔ بزرگی را شامل می‌شود، سطح توسعه یا مشارکت هر کشور براساس پنج رکن شامل اقدامات قانونی، اقدامات فنی، اقدامات سازمانی، توانمندسازی و همکاری ارزیابی می‌شود. اقدامات قانونی به موجودیت و پیاده‌سازی چارچوب‌ها و مقررات قانونی مربوط به امنیت سایبری در یک کشور می‌پردازد. قوانین مرتبط با جرایم سایبری، حفاظت داده‌ها، حریم خصوصی و ... از جمله آن هستند. بخش اقدامات فنی، بر تأمین و آماده‌سازی زیرساخت‌های فنی مانند شبکه‌ها، سیستم‌ها و نرم‌افزارهای امن، همچنین ظرفیت پاسخ به حوادث و جرم‌شناسی دیجیتال تمرکز دارد. اقدامات سازمانی به ارزیابی بخش‌ها و سازمان‌های مسئول امنیت سایبری در داخل کشور می‌پردازد و ساختار استراتژی‌های ملی امنیت سایبری، نقش نهادهای مختلف و سازوکارهای هماهنگی موجود را بررسی می‌کند. بخش دیگر از شاخص GCI، توانمندسازی است که در آن تلاش‌های یک کشور را برای افزایش توانایی‌های امنیت سایبری در میان نیروی کار و افراد جامعه را ارزیابی می‌کند. این تلاش‌ها می‌تواند شامل برنامه‌های آموزشی، کمپین‌های آگاهی، فعالیت‌های آموزش به‌منظور ارتقای مهارت‌های امنیت سایبری باشد. آخرین مورد بر سطح همکاری بین‌المللی و منطقه‌ای یک کشور در حوزه امنیت سایبری تمرکز دارد که شامل همکاری با دیگر کشورها از طریق فرایندهای اشتراک‌گذاری اطلاعات، مشارکت در فعالیت‌های امنیت سایبری و همکاری با سازمان‌های بین‌المللی است.

براساس داده‌های موجود از GCI مشاهدهٔ روند وضعیت ایران و نیز مقایسهٔ آن با دیگر کشورها می‌تواند تصویری از سطح امنیت سایبری کشور را ارائه دهد.

جدول ۱. مقایسهٔ ایران با کشورهای ترکیه و آمریکا در شاخص امنیت سایبری جهانی (رتبهٔ ۱ بهترین و امتیاز ۱۰۰ در شاخص بیانگر بیشترین مشارکت است)[2]

امارات متحدهٔ عربی		آمریکا		ترکیه		ایران		سال گردآوری داده
رتبه جهانی	شاخص GCI	رتبهٔ جهانی	شاخص GCI	رتبهٔ جهانی	شاخص GCI	رتبهٔ جهانی	شاخص GCI	
۱۷	۳۵/۰	۱	۸۲/۰	۷	۶۵/۰	۱۹	۲۹/۰	۲۰۱۳–۲۰۱۴
۴۷	۵۷/۰	۲	۹۲/۰	۴۳	۵۸/۰	۵۹	۴۹/۰	۲۰۱۶
۳۳	۸۱/۰	۲	۹۳/۰	۲۰	۸۵/۰	۶۰	۶۴/۰	۲۰۱۷–۲۰۱۸
۵	۹۸/۰۶	۱	۱۰۰	۱۱	۹۷/۰۵	۵۴	۸۱/۰۶	۲۰۲۰
الگوسازی	۱۰۰	الگوسازی	۱۰۰	الگوسازی	۱۰۰	نوپا	۶۵,۹۷	۲۰۲۳–۲۰۲۴

1. Global Cybersecurity Index (GCI)

۲. شاخص امنیت سایبری جهانی از سال ۲۰۱۵ تا ۲۰۲۴ در قالب پنج گزارش انتشار یافته است. رتبه‌بندی کشورها در گزارش ۲۰۲۴ در قالب جدید تحت عنوان پنج ردیف عملکردی شامل ۱. الگوسازی (Role-modelling) (نمرهٔ ۹۵ تا ۱۰۰)، ۲. پیشرفت (Advancing) (امتیاز ۸۵ تا ۹۵)، ۳. نوپا (Establishing) (امتیاز ۵۵ تا ۸۵)، ۴. در حال تحول (Evolving) (امتیاز ۲۰ تا ۵۵)، ۵. در حال ساخت (Building) (امتیاز ۰ تا ۲۰).

جدول ۱ نشان می‌دهد که در سال‌های اخیر وضعیت ایران در شاخص امنیت سایبری جهانی بهبود یافته است، ولی همچنان رتبهٔ ایران در مقایسه با کشوری مانند ترکیه تفاوت زیادی دارد. این موضوع بیانگر حرکت و پیشرفت جهانی در ارتقای استانداردها و روش‌های ایجاد امنیت سایبری همگام با پیشرفت فناوری است و اهمیت استفاده از فرصت‌های برآمده از ارتباط و تعامل با اقتصاد بین‌الملل را خاطرنشان می‌کند.

همچنین به‌تازگی شاخصی با عنوان «شاخص جرایم سایبری جهانی» معرفی شده است. این شاخص با استفاده از نظرسنجی از کارشناسان جرایم سایبری در سراسر جهان در مورد جرایم سایبری مورد نظر[۱]، مهم‌ترین مراکز[۲] جرایم سایبری را در سطح ملی شناسایی می‌کند. براساس این شاخص، ایران در بین ۲۰ کشور اول با بیشترین جرایم سایبری در سال ۲۰۲۳ قرار دارد (بروس[۳] و همکاران، ۲۰۲۴).

در این بین نقش دولت‌ها برای کاهش ریسک سایبری افزون‌بر سرمایه‌گذاری در ایجاد و بهبود زیرساخت‌های سخت‌افزاری، استفاده از روش‌ها و ابزارهای نهادی است که در ادامه براساس ادبیات نظری و تجربهٔ کشورها به آنها اشاره می‌شود.

۱. قوانین و مقررات: دولت می‌تواند قوانین و مقرراتی را تصویب کند که استانداردهای حداقلی از امنیت سایبری برای سازمان‌ها، به‌ویژه مجموعه‌های مرتبط با بهره‌برداری از زیرساخت‌های حیاتی و استفاده از اطلاعات حساس را تعیین کند. این مقررات می‌توانند اجرای تدابیر امنیتی خاصی را الزامی کنند و ضامن رعایت بهترین شیوه‌ها برای مقابله با تهدیدهای سایبری باشند. در برخی کشورها این قوانین با عنوان قانون امنیت سایبری[۴] شناخته می‌شود. مجوزنامهٔ عمومی حفاظت داده‌های اتحادیهٔ اروپا (GDPR[۵]) الزامات سختی را برای سازمان‌های مرتبط با داده‌های شخصی تعیین می‌کند. این قانون، مقررات حقوقی را برای کسب‌وکارهای فعال در اتحادیهٔ اروپا با هدف حفاظت از اطلاعات شخصی و اجرای تدابیر امنیتی مناسب تعیین می‌کند (European Union, 2016).

۲. همکاری و اشتراک اطلاعات: دولت‌ها می‌توانند همکاری بین نهادهای زیرمجموعه و شرکای مختلف مانند کسب‌وکارها، متخصصان امنیت سایبری و نهادهای اجرایی قانونی را تسهیل کنند. ترویج اشتراک اطلاعات دربارهٔ تهدیدها، ضعف‌ها و بهترین شیوه‌های ایجاد امنیت سایبری، می‌تواند به سازمان‌ها در جست‌وجوی روش‌های دفاعی پیشرفته و بهبود راهبردهای مقابله کمک کند. نمونه‌ای از این سیاست، برنامهٔ تبادل خودکار نشانگرها (AIS[۶]) مربوط به وزارت امور داخلی ایالات متحدهٔ آمریکا (DHS[۷]) است که امکان تبادل نشانگرهای تهدید سایبری بین دولت و نهادهای بخش خصوصی را فراهم می‌کند. این برنامه به اشتراک‌گذاری اطلاعات در زمان مناسب[۸] برای افزایش توانایی جمعی در تشخیص و پاسخ به تهدیدهای سایبری کمک می‌کند (DHS, 2015).

۳. حمایت مالی و مشوق‌ها: دولت می‌تواند با تخصیص منابع مالی و ایجاد مشوق‌های مالی، سازمان‌ها و کسب‌وکارها را به سرمایه‌گذاری در ایجاد تدابیر امنیتی قوی‌تر تشویق کند. این مشوق‌ها می‌تواند شامل اعطای گرنت‌ها، معافیت‌های مالیاتی یا حمایت‌هایی برای پیاده‌سازی فناوری‌های نوین امنیت سایبری، انجام دوره‌ای ارزیابی ریسک و آموزش کارکنان در زمینهٔ آگاهی امنیت سایبری باشد. این حمایت‌های مالی به‌ویژه برای کسب‌وکارهای کوچک و متوسط، به ارتقای امنیت سایبری می‌انجامد. برنامهٔ

---

۱. شامل: ۱- محصولات/خدمات فنی (مانند کدنویسی بدافزار، دسترسی به شبکه‌های آلوده، تولید ابزارها)؛
۲- حمله‌های باجگیری (مانند حمله‌های انکار سرویس، باج‌افزار)؛
۳- سرقت داده و هویت (مانند هک، فیشینگ، نقض حساب‌ها، کلاهبرداری با کارت‌های اعتباری)؛
۴- کلاهبرداری (مانند کلاهبرداری با پیش‌پرداخت، کلاهبرداری ایمیل تجاری، کلاهبرداری در حراج‌های آنلاین)؛
۵- خارج کردن پول و پولشویی (مانند کلاهبرداری با کارت‌های اعتباری، مجرمان پول‌شو، پلتفرم‌های ارز مجازی غیرقانونی).

2. Hotspots
3. Bruce
4. Cyber Safety Act
5. General Data Protection Regulation
6. Automated Indicator Sharing
7. Department of Homeland Security
8. Real-time information sharing

دولت استرالیا با نام برنامهٔ امنیت سایبری کسب‌وکارهای کوچک، گرنت‌هایی به ارزش ۲۱۰۰ دلار استرالیا به کسب‌وکارهای کوچک برای ارزیابی امنیت سایبری و اجرای روش‌های بهبود امنیت سایبری اختصاص می‌دهد. هدف از این برنامه کمک به کسب‌وکارهای کوچک برای ارتقای توانمندی‌های سایبری است (Australian Cyber Security Centre, 2023).

٤. آموزش متخصصان سایبری: حوزهٔ امنیت سایبری و بیمهٔ سایبری نیازمند افراد متخصص در حوزهٔ سایبر هستند. سازمان‌ها باید با یک واسطه یا متخصص بیمهٔ سایبری[1] برای انتخاب مناسبی از پوشش بیمه مشورت کنند. متخصص بیمهٔ سایبری کسی است که از شناخت کافی از صنعت، کسب‌وکار و ریسک‌های امنیت سایبری برخوردار است. همچنین متخصصان سایبری در بازار بیمهٔ سایبری به‌عنوان کارآگاهان سایبری[2] نقش اساسی در شناسایی منبع وقوع حادثه و ارزیابی خسارت دارند. کارآگاهان سایبری پس از بروز رخداد سایبری می‌توانند منبع و وسعت خسارت را شناسایی کنند (ITU-T, 2021). دولت‌ها می‌توانند در برنامه‌های آموزشی و توسعهٔ نیروی کاری سایبری سرمایه‌گذاری کنند. با ترویج امنیت سایبری به‌عنوان یک مسیر شغلی، ارائهٔ فرصت‌های آموزشی و حمایت از مؤسسات دانشگاهی ارائه‌دهندهٔ برنامه‌های امنیت سایبری، دولت می‌توان به ایجاد نیروی کار ماهر برای مقابله با تهدیدهای سایبری در حال تحول کمک کرد. برنامهٔ ملی امنیت سایبری انگلستان (NCSC[3]) مجموعه‌ای از فعالیت‌های آموزشی از جمله برنامهٔ CyberFirst را ارائه می‌دهد. این برنامه شامل دوره‌های تابستانی، آموزشگاه‌ها و بورس‌های آموزشی با هدف تربیت نسل بعدی از متخصصان امنیت سایبری است (NCSC, 2023).

٥. پاسخ به حوادث و بازیابی[4]: دولت‌ها می‌توانند منابع مالی و فرایندهایی را برای واکنش به حوادث سایبری و نیز بازیابی منابع ازدست‌رفته تخصیص دهند. این می‌تواند شامل تشکیل گروه‌های ویژه برای واکنش به حوادث سایبری، تعیین دستورالعمل‌هایی برای گزارش‌دهی و مدیریت حوادث سایبری و ارائهٔ کمک به سازمان‌های درگیر با هدف کاهش خسارت ناشی از حملات باشد. برای مثال، گروه واکنش سریع رایانه‌ای سنگاپور با نام SingCERT که زیر نظر سازمان امنیت سایبری سنگاپور (CSA[5]) اداره می‌شود، با هدف واکنش به حوادث سایبری، خدمات پاسخ به حوادث را به سازمان‌ها در سنگاپور ارائه می‌دهد. SingCERT در پردازش حوادث، اجرای تحقیقات و راهنمایی برای کاهش تأثیر حوادث سایبری به سازمان‌ها کمک می‌کند (CSA, 2024).

٦. همکاری بین‌المللی: تهدیدهای سایبری[6] اغلب از مرزهای ملی عبور می‌کنند. از این‌رو دولت‌ها باید در برنامه‌های بین‌المللی برای مقابله با خطرهای سایبری نقش ایفا کنند. چنین برنامه‌هایی شامل به اشتراک‌گذاری اطلاعات با کشورهای دیگر، مشارکت در فعالیت‌های بین‌المللی در حوزهٔ امنیت سایبری و همکاری در توسعهٔ استانداردها و قوانین بین‌المللی برای دفاع سایبری است. نمونه‌ای مهم از این همکاری‌های بین‌المللی، موافقت‌نامهٔ بوداپست است که با عنوان موافقت‌نامه اتحادیهٔ اروپا دربارهٔ جرم سایبری نیز شناخته می‌شود. این موافقت‌نامه، تفاهم‌نامه‌ای بین‌المللی با هدف ایجاد هماهنگی در قوانین جرم سایبری و تسهیل همکاری بین کشورهاست. این موافقت‌نامه چارچوبی برای کمک حقوقی متقابل، استرداد مجرم[7] و اشتراک اطلاعات در تحقیقات جرایم سایبری فراهم می‌کند (European Union, 2001).

۷. رونق بازار MSSP: جریان ریسک سایبری پس از عبور از زیرساخت‌های فنی و نهادی سایبری، به مرحله‌ای می‌رسد که هر بنگاه باید با توجه به ویژگی‌های کسب‌وکار خود، در زمینهٔ مدیریت و کنترل ریسک در معرض، تحت مدیریت داخلی بنگاه یا برون‌سپاری به شرکت‌های MSSP تصمیم بگیرد. از این‌رو اغلب بیمهٔ سایبری به‌عنوان پوششی برای فاصلهٔ بین تعهدات MSSP و خسارت واردشده به بیمه‌گزاران شناخته می‌شود (Kumar & Singh, 2019).

1. Cyber insurance expert
2. Cyber detector
3. National Cyber Security Centre
4. Recovery
5. Cyber Security Agency
6. Cyber treats
7. Extradition

اهمیت شرکت‌های MSSP در ارائهٔ خدمات امنیت سایبری به شکل تخصصی است که به افزایش کارایی می‌انجامد. به بیان دیگر بیمه‌گزاران سایبری می‌توانند امنیت سایبری را با هزینهٔ کمتر فراهم آورند و در نتیجه با کاهش سطح ریسک، شرکت‌های بیشتری به بازار بیمهٔ سایبری وارد می‌شوند. از سوی دیگر شرکت‌های بیمه نیز حاضر به پذیرش مشتریان بیشتری خواهند شد (Fraser & Simkins, 2016). از این‌رو باید گفت بین بازارها همبستگی وجود دارد و رونق بازار بیمهٔ سایبری به رونق بازار شرکت‌های MSSP وابسته است.

شرکت‌های MSSP، در ارتقای وضعیت امنیت سایبری کسب‌وکارها، به‌ویژه شرکت‌های کوچک و متوسط SME[1] که اغلب از منابع و تخصص لازم برای مدیریت تهدیدهای امنیتی پیچیده برخوردار نیستند نقشی مهم دارند. این شرکت‌ها گسترهٔ وسیعی از خدمات امنیت سایبری شامل تشخیص تهدیدها و پاسخ به حوادث، مدیریت آسیب‌پذیری و پایش انطباق را ارائه می‌دهند (Baker & Wallace, 2007). بازار جهانی MSSP رشد چشمگیری را تجربه می‌کند، به‌طوری که MarketsandMarkets برآورد می‌کند این بازار تا سال ۲۰۲۵ به ۵۲/۳ میلیارد دلار خواهد رسید که این رشد تحت تأثیر افزایش اعتماد به خدمات امنیتی ابری و نیاز به توانایی‌های پیشرفته در تشخیص تهدیدهاست (MarketsandMarkets, 2020). در سراسر جهان دولت‌ها، اهمیت وجود MSSP در تقویت اکوسیستم امنیت سایبری را درک کرده و اقدامات مختلفی را برای تشویق استفاده از آنها اجرا کرده‌اند. برای مثال، در اتحادیهٔ اروپا، دستورالعمل شبکه و امنیت اطلاعات NIS[2] استفاده از MSSP را برای اپراتورهای زیرساخت حیاتی الزامی کرده است (European Union, 2016). همچنین در ایالات متحده، برنامهٔ گواهینامهٔ بلوغ امنیت سایبری (CMMC[3]) پیمانکاران دفاعی را ملزم به همکاری با شرکت‌های MSSP دارای گواهینامه برای تأمین الزامات امنیتی کرده است (U.S. Department of Defense. 2020).

دولت می‌تواند برای حمایت و ارتقای بازار شرکت‌های MSSP سیاست‌هایی را مدنظر قرار دهد. نخست، دولت می‌تواند استانداردها و الزامات پایهٔ امنیت سایبری را تعیین کند، به‌طوری که با پایبندی سازمان‌ها به آن، برای خدمات MSSP تقاضا ایجاد شود. برای مثال، دولت می‌تواند کنترل‌های امنیتی خاصی را اجباری کند یا سازمان‌ها را به ارزیابی ریسک شخص ثالث ملزم سازد تا به همکاری با شرکت‌های MSSP هدایت شوند (Eling & Schnell, 2016).

همچنین دولت می‌تواند مشوق‌ها و حمایت‌هایی را در نظر گیرد. این مشوق‌ها می‌تواند شامل معافیت‌های مالیاتی و تسهیلات مالی باشد. تسهیل تبادل اطلاعات بین شرکت‌های MSSP و ارائهٔ اطلاعات تهدیدهای سایبری، سیاست دیگری است که دولت‌ها می‌توانند در پیش گیرند (Bandyopadhyay, 2009). افزون‌بر این، دولت می‌تواند در فرایند اعطای گواهی و اعتبارسنجی MSSP نقش داشته باشد. با تعیین استانداردها و فرایند تأیید، دولت می‌تواند با کمک به سازمان‌ها برای شناسایی شرکت‌های معتبر MSSP، اعتماد به بازار را افزایش دهد (Fruhlinger, 2019). دولت همچنین ممکن است برنامه‌های آموزشی MSSP را تأمین مالی کند تا استخدام متخصصان امنیت سایبری در این شرکت‌ها گسترش یابد.

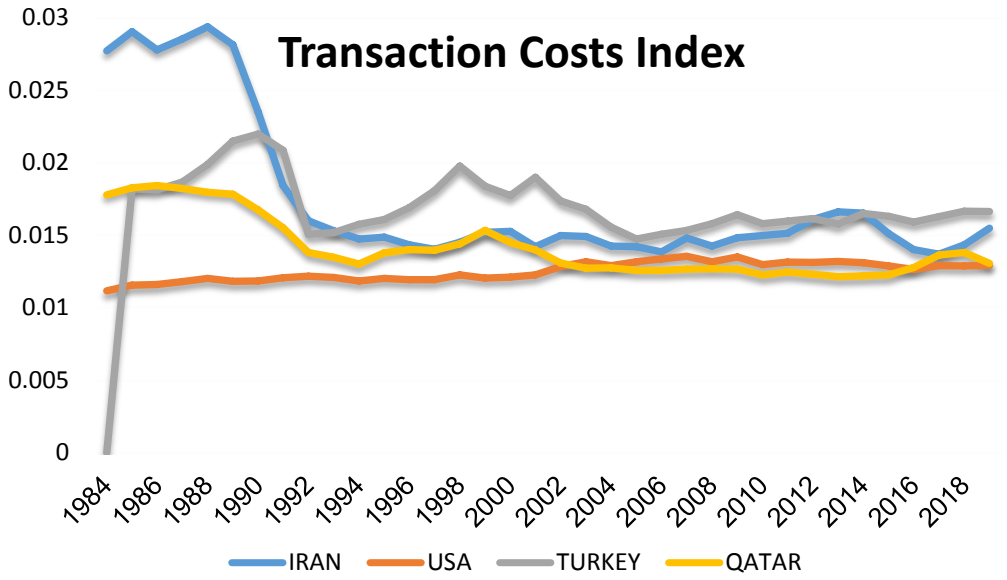
۴. ۲. کاهش هزینهٔ مبادله

خریداران و فروشندگان در بازار بیمهٔ سایبری به مانند دیگر بازارها، برای مبادله متحمل هزینه‌هایی در جست‌وجوی اطلاعات، مذاکره و نظارت بر اجرای قرارداد می‌شوند. هزینهٔ مبادله، دیگر عامل بروز ناکارایی در بازار بیمهٔ سایبری است. در یک سطح درآمد و ریسک مشخص، با کاهش هزینهٔ مبادله، افراد بیشتری وارد بازار بیمهٔ سایبری خواهند شد و محصولات بیمه‌ای بیشتری مبادله می‌شود.

ازآنجا که هزینهٔ مبادله در فرایند تولید و قیمت لحاظ نمی‌شود، نوعی متغیر پنهان است. از این‌رو برای محاسبهٔ آن می‌توان از شاخص‌های جانشین از جمله شاخص راهنمای ریسک کشوری بین‌المللی ICRG استفاده کرد. با توجه به اینکه ریسک بیانگر عدم اطمینان به آینده است، با افزایش ریسک، هزینهٔ مبادلهٔ افزایش می‌یابد. از این‌رو می‌توان معکوس این شاخص را معیاری

1. Medium-sized enterprises
2. Network and Information Security
3. Cybersecurity Maturity Model Certification

برای ارزیابی هزینهٔ مبادله در نظر گرفت (عاقلی و همکاران، ۲۰۱۷). نمودار زیر وضعیت ایران در مقایسه با برخی دیگر از کشورها را نشان می‌دهد.



شکل ٦. مقایسهٔ شاخص هزینهٔ مبادلهٔ ایران با کشورهای آمریکا، قطر و ترکیه (منبع: محاسبات تحقیق).

شکل ۶ نشان می‌دهد که هزینهٔ مبادله در اقتصاد ایران در مقایسه با کشوری مانند آمریکا همواره بیشتر است. از مهم‌ترین دلایل این موضوع باید به جنگ، تنش سیاسی با دیگر کشورها و وضع تحریم‌های مختلف علیه ایران اشاره کرد. همین‌طور که مشاهده می‌شود هزینهٔ مبادله در اقتصاد ایران در سال‌های جنگ با عراق (۱۹۸۸-۱۹۸۰) و نیز پس از وضع تحریم‌های سازمان ملل در سال ۲۰۱۱، با تکانهٔ بالایی روبه‌رو شد.

نقش نهادی دولت در کنترل هزینهٔ مبادله را می‌توان از طریق اثرگذاری بر بهبود کیفیت نهادی جامعه، پیشرفت فناوری و افزایش افشای اطلاعات جست‌وجو کرد.

۱. بهبود کیفیت نهادی جامعه: بستر نهادی جامعه از بخش‌های مختلفی تشکیل شده است که هر مذاکره یا قراردادی را تحت تأثیر قرار می‌دهد. به‌طور کلی کارگزاران اقتصادی همواره تحت تأثیر نااطمینانی‌های ناشی از ریسک‌های سیاسی-اجتماعی مانند ثبات دولت[1]، درگیری‌های داخلی و خارجی[2]، نظم و قانون[3] و ... و ریسک‌های اقتصادی و مالی مانند ریسک ثبات نرخ ارز[4]، نرخ تورم سالانه، تراز بودجه به تولید ناخالص داخلی و ... تصمیم‌گیری می‌کنند. همان‌گونه که مکتب اقتصاد نهادگرای جدید بر آن تأکید دارد طراحی و انتخاب سیاست برای هر موضوعی باید براساس ویژگی‌های فیزیکی و نهادی انجام پذیرد. در پاسخ به این پرسش که آیا دولت‌ها می‌توانند بر همهٔ عوامل نهادی تأثیرگذار باشند باید گفت تغییر برخی از این عوامل به‌سختی و در بلندمدت رخ می‌دهد. برای مثال افزایش اعتماد یا سرمایه اجتماعی که بخشی از فرهنگ یک ملت است یا سیستم قانونی کارا، به‌راحتی و در کوتاه‌مدت امکان‌پذیر نخواهد بود. عوامل نهادی دیگری از جمله کاهش لابی و رانت، اصلاح ساختار بازارها، تعیین حقوق مالکیت، ترتیب و زمان‌بندی مناسب برای مداخلات سیاستی[5] و میانجی‌گری‌ها[6] وجود دارد که دولت‌ها می‌توانند با نوآوری‌های نهادی[7] در جهت اصلاح یا بهبود آنها اقدام کنند (McCann, 2013؛ عبدی و همکاران، ۲۰۲۲).

1. Government Stability
2. Internal and External Conflict
3. Low and Order
4. Risk Point for Exchange Rate Stability
5. Appropriate Sequencing and Timing of Policy Interventions
6. Intermediaries
7. Institutional Innovation

نقش نهادی دولت فراهم آوردن بستر نهادی مناسب برای ورود بازیگران اصلی (به‌طور مثال بیمه‌گر و بیمه‌گزار) به مذاکره و انجام مبادلهٔ بازاری است. هرچه چارچوب نهادی کشور ضعیف‌تر باشد، باید هزینهٔ بیشتری صرف کرد تا تضمینی برای صحت پیش‌بینی‌ها باشد. دولت‌ها می‌توانند با نوآوری‌های نهادی از هزینهٔ مبادلهٔ مرتبط با مذاکره، قرارداد و اجرای آن بکاهند تا بازیگران اصلی به‌سوی توافق ترغیب شوند. برای مثال هرچه کارآمدی قوانین شامل کیفیت و ثبات قوانین ضعیف‌تر باشد، زمان بیشتری لازم خواهد بود تا افراد بر سر مفاد قرارداد به تفاهم برسند. وظیفهٔ دولت‌ها ابداع قوانینی است که شفاف، حداقلی و با پایداری حداکثری باشد. همچنین دولت‌ها می‌توانند با ابداع «الگوهای قراردادی» در بخش‌های مختلف اقتصادی به تسریع فزایندهٔ مذاکره کمک کنند. برای مثال ارائهٔ مدل‌های فنی ارزیابی ریسک و نمونه قراردادهای بیمه، به شرکت‌های بیمه و کسب‌وکارها کمک می‌کند تا با خطای کمتر ریسک در معرض را محاسبه و در زمان کمتری به توافق برسند. همچنین در هر سیستم قضایی، هرچه فرایند دادرسی طولانی‌تر و ناکارآمدتر باشد افراد به شرایطی که نیازمند مراجعه به دادگاه است حساسیت بیشتری خواهند داشت و از این‌رو از ابتدا سعی می‌کنند با صرف زمان بیشتر، بندهای قرارداد را شفاف‌تر و مؤثرتر تنظیم کنند؛ دولت باید با بهبود نظام قضایی از سطح این نااطمینانی‌ها بکاهد (دادگر، ۲۰۰۷؛ عبدی و همکاران، ۲۰۲۲).

۲. افشای اطلاعات: اهمیت افشا و اشتراک‌گذاری اطلاعات در موضوع بیمهٔ سایبری در آن است که افزون‌بر ریسک سایبری، هزینهٔ مبادله را نیز کاهش می‌دهد. از این‌رو دولت‌ها باید سیاست‌هایی در زمینهٔ ترغیب و تشویق کسب‌وکارها و سازمان‌ها به افشای اطلاعات سایبری اتخاذ کنند. عبدی (۱۴۰۲) در مورد افشای اطلاعات زیست‌محیطی بنگاه‌ها، نتیجه می‌گیرد که دولت می‌تواند نقش نهادی خود را در هدایت بنگاه‌ها به افشای اطلاعات از دو مسیر انجام دهد. نخست، ایجاد یا تقویت نهادهایی برای نظارت بر عملکرد بنگاه‌ها و انتشار گزارش از عملکرد آنها به جامعه؛ به این ترتیب بنگاه‌ها برای حفظ یا افزایش شهرت خود ملزم به افشای بیشتر اطلاعات خواهند شد. این نهادها می‌توانند از نهادهایی همچون سازمان محیط زیست یا از سازمان‌های مردم‌نهاد[1] و حتی رسانه‌ها باشند. دوم، دولت می‌تواند از ابزارهایی مانند یارانه‌ها یا معافیت‌های مالیاتی برای تشویق بنگاه‌ها به افشای اطلاعات استفاده کرده و نیز با قانونگذاری برای تهدید به مداخله، بنگاه‌ها را وادار به افشای اطلاعات کند. از این ابزارها می‌توان برای هدایت بنگاه‌ها و سازمان‌ها به افشای اطلاعات سایبری نیز استفاده کرد. می‌توان یکی از وظایف نهاد ناظر سایبری را انتشار گزارش‌های دوره‌ای از تهدیدها و وضعیت امنیت سایبری بنگاه‌ها و سازمان‌ها قرار داد. همچنین دولت می‌تواند با هدف ایجاد انگیزه، برای منتشرکنندگان اطلاعات حوادث سایبری، تخفیف‌های مالیاتی در نظر گیرد.

۳. پیشرفت فناوری: پیشرفت فناوری به کاهش هزینه‌های مبادله می‌انجامد. زیرا فناوری امکان ایجاد روش‌هایی با صرف هزینه و زمان کمتر برای مبادلات را فراهم می‌کند. با استفاده از فناوری‌های پیشرفته مانند اینترنت، سامانه‌های پرداخت الکترونیکی، اتوماسیون و هوش مصنوعی، فرایندهای انجام مبادله سریع‌تر و کارآمدتر می‌شود که کاهش هزینه‌ها و بهبود کارایی در فعالیت‌های مبادلاتی را در پی خواهد داشت. دولت‌ها نقش اساسی در پیشرفت فناوری دارند؛ از جمله ۱. تعیین سیاست‌ها و راهبردهای مناسب برای توسعهٔ فناوری و افزایش تولید؛ ۲. ایجاد زیرساخت‌های فنی و فرهنگی شامل ارتقای زیرساخت‌های شهری، توسعهٔ مهارت‌های فنی و ارتقای فرهنگ نوآوری که امکان پذیرش و انتقال فناوری‌های نوین را افزایش می‌دهد؛ ۳. سرمایه‌گذاری در تحقیق و توسعه از طریق تأمین و تخصیص منابع به تحقیقات پیشرفته و ایجاد همکاری‌های انتقال فناوری که به پیشرفت علوم پایه می‌انجامد؛ ۴. استانداردهایی که اهمیت زیادی در تشویق به نوآوری، افزایش رقابت و تنظیم بازارها دارند (Fenwick, 2017 ؛World Bank, 2019 ؛ Foray, 2011).

5. نتیجه‌گیری؛ ایجاد سکوی راهنمای بازار بیمهٔ سایبری

حمله‌های سایبری ممکن است پیامدهای مخربی برای کسب‌وکارها، دولت‌ها و افراد داشته باشند و سبب خسارات مالی، آسیب به اعتبار و اختلال در زیرساخت‌های حیاتی شوند. با افزایش تهدیدهای سایبری در سال‌های اخیر، بیمهٔ سایبری اهمیت فزاینده‌ای پیدا کرده است. این بیمه به کسب‌وکارها کمک می‌کند تا ریسک‌های مرتبط با حمله‌های سایبری و نقض‌های اطلاعاتی را

1. NJO: Non-Governmental Organization

مدیریت کنند و اعتماد مشتریان را افزایش دهند. در صورت وقوع حمله، بیمهٔ سایبری هزینه‌های پاسخ به حادثه و دعاوی قانونی را پوشش می‌دهد و به کسب‌وکارها امکان می‌دهد که بدون نگرانی از بار مالی ناشی از این حوادث به فعالیت خود ادامه دهند. همچنین افزایش توجه به بیمهٔ سایبری به بهبود روش‌های مدیریت ریسک و ارتقای امنیت در سازمان‌ها منجر می‌شود. گسترش این بازار سبب رونق صنعت بیمه و افزایش ضریب نفوذ آن نیز می‌شود، به‌ویژه در میان کسب‌وکارهای کوچک و متوسط که به‌دنبال حفاظت از داده‌های خود هستند.

در این پژوهش سعی کردیم تا با بررسی ادبیات علم اقتصاد، به چرایی نبود بازار بیمهٔ سایبری در ایران بپردازیم. از این منظر با ارائهٔ مدل مفهومی از بازار بیمهٔ سایبری، دو عامل ریسک سایبری نسبی بالا و هزینهٔ مبادلهٔ بالا را به‌عنوان دلایل شکل نگرفتن این بازار در ایران شناسایی و معرفی کردیم. سطح ریسک سایبری بالا به همراه درآمد نسبی پایین بنگاه‌ها، یکی از عواملی است که مانع از ایجاد تقاضا برای بیمهٔ سایبری و شکل‌گیری بازار خواهد شد. بررسی شاخص‌های بین‌المللی نشان می‌دهد که متأسفانه ایران از جمله کشورهای با بیشترین سطح ریسک سایبری است و علی‌رغم بهبود امنیت سایبری در ایران در سال‌های اخیر، ولی همچنان از قافلهٔ پیشرفت جهانی در ارتقای روش‌های امنیت سایبری عقب هستیم. هزینهٔ مبادلهٔ بالا از منفعت خالص حاصل از مبادله می‌کاهد و سبب می‌شود تا طرفین مبادله، رغبت کمتری برای ورود به مذاکره برای توافق داشته باشند. از این‌رو هزینهٔ مبادله عامل مهمی در بروز ناکارایی در هر بازاری از جمله بیمهٔ سایبری با توجه به حساسیت و پیچیدگی خاص آن است. سطح شاخص هزینهٔ مبادله در ایران در سال‌هایی که درگیر جنگ، تنش سیاسی و تحریم بوده‌ایم روند افزایشی داشته است. این موضوع اهمیت ایجاد ثبات در روابط خارجی را خاطرنشان می‌کند.

نقش دولت برای ایجاد و تقویت این بازار طراحی و اجرای سیاست‌هایی با هدف کاهش ریسک سایبری، کاهش هزینهٔ مبادله است. پیشنهاد ما ایجاد سکوی «راهنمای بازار بیمهٔ سایبری» با هدف ایجاد شفافیت و رقابت و کاهش هزینهٔ مبادله در بازار بیمهٔ سایبری است. این زیرساخت می‌تواند چند کارکرد اصلی داشته باشد: نخست، جمع‌آوری داده‌های مرتبط با حوادث سایبری و مخاطرات بیمه‌گزاران و شرکت‌های بیمه و ارائهٔ آنها در قالب اطلاعات به‌روز با هدف افزایش سطح اطلاعات؛ دوم، رتبه‌بندی کسب‌وکارها با هدف تشویق به انتشار بیشتر اطلاعات حوادث سایبری؛ سوم، ارائهٔ مدل‌های فنی مناسب و به‌روز برای ارزیابی ریسک در معرض سایبری کسب‌وکارها با هدف کاهش هزینهٔ مبادله؛ چهارم، معرفی و آموزش بهترین شیوه‌های ایجاد امنیت سایبری و نیز رتبه‌بندی شرکت‌های MSSP؛ پنجم، تربیت و آموزش متخصصان و کارآگاهان حوزهٔ سایبری با هدف کاهش خطا در فرایند ارزیابی ریسک و نیز تخمین خسارت.

References

Abdi, J., Taghinejadimran, & Abbasinejad. (2022). Revisiting the Coase theorem with positive transaction costs: An approach to examine the role of government in facilitating market exchanges. *Journal of Economic Research*, 57(3), 505-531 (In Persian).

Agheli L, Sahabi B, Solhkhah N. (2017). The Impact of Transaction Cost on Financial Development in Selected OPEC Members. *The Economic Research*, 17(1), 95-120 (In Persian).

Alhassan, A.L., & Biekpe, N. (2016). Insurance market development and economic growth. *International Journal of Social Economics*, 43(3), 321-339.

Australian Government, Australian Cyber Security Centre. (2023). Cyber Security Small Business Program. https://www.cyber.gov.au/acsc/view-all-content/programs-and-initiatives/cyber-security-small-business-program.

Baker, W., & Wallace, L. (2007). Is Information Security Under Control? *Proceedings of the 2007 ACM SIGMIS CPR Conference on Computer Personnel Research*.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. Communications of the ACM, 52(11), 68-73.

Bannister, F., & Connolly, R. (2018). Risk Management and Governance: A Practical Guide*International Journal of Information Management*, 38(1), 236-244.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*, 131-158.

Böhme, R., & Moore, T. (2012). The Blockchain and Cyber Insurance: A New Paradigm, *Proceedings of the 2012 Workshop on the Economics of Information Security*.

Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: towards a unifying framework. In *WEIS*.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *Plos one*, 19(4), e0297312.

Council of Europe. (2001). Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Cyber Security Agency of Singapore. (2024). SingCERT. https://www.csa.gov.sg/singcert

Dadgar. (2007). The role of the Coase theorem and transaction costs in recent economic developments. *Scientific Journal of Economic Studies and Policies*, (11), 89-114 (In Persian).

Deloitte. (2022). *Cyber insurance: What you need to know*.

Doherty, N.F., & Fulford, H. (2017). Cyber Insurance: The Role of Insurance in Managing Cyber Risk. *The Journal of Risk Finance*, 18(5), 513-528.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?. The Journal of Risk Finance.

European Commission. (2016). General Data Protection Regulation (GDPR). https://ec.europa.eu/info/law/law-topic/data-protection_en.

European Commission. (2021). Solvency II. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/insurance-and-pensions/risk-management-and-supervision-insurance-companies-solvency-ii_en.

European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

Fenwick, M. (2018). *May States Regulate Innovation Under Federal Law? A Proposed Framework for State Patent Policy.*

Foray, D. (2011). *The economics of knowledge*. MIT Press.

Franke, U., Holm, H., König, J. (2014). The distribution of time to recovery of enterprise IT services. IEEE T Reliab; 63(4):858–67. http://dx.doi.org/10.1109/TR.2014.2336051.

Franke, U. (2017). The cyber insurance market in Sweden. *Computers and Security*, 68, 130-144.

Fraser, J., & Simkins, B. (2016). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. John Wiley and Sons.

Fruhlinger, J. (2019). What is a managed security service provider (MSSP)? A vital resource for security. CSO Online. Retrieved from https://www.csoonline.com/article/2122440/managed-security-service-provider-definition-and-solutions.html.

Gatzert, N., & Schmeiser, H. (2012). The merits of pooling claims revisited. *The Journal of Risk Finance*, 13(3), 184-198.

Gordon, L.A., & Loeb, M.P. (2018). The Economics of Cybersecurity: Evidence from the Field. *Journal of Cybersecurity*, 4(1), 1-14.

Harrington, S.E., & Niehaus, G.R. (2019). *Risk management and insurance* (2nd ed.). McGraw-Hill Education.

Hillson, D. (2020). The risk management of projects: A strategic approach to managing risk. *International Journal of Project Management*, 38(8), 429-439. https://doi.org/10.1016/j.ijproman.2020.06.006

IBM Security. (2022). 2022 Cost of a Data Breach Report. https://www.ibm.com/reports/data-breach
IBM. (2023). Cost of a Data Breach Report 2023.
ITU-T. (2021). Cyber insurance acquisition guidelines (ITU-T Recommendation X.1061). International Telecommunication Union.
Kak, A., & Goyal, P. (2020). Emerging Trends in Cyber Insurance: A Review. *Journal of Cybersecurity and Privacy*, 1(2), 123-139.
Kieninger, A., Straeten, D., Kimbrough, S., Schmitz, B., & Satzger, G. (2013). Leveraging service incident analytics to determine cost-optimal service offers.
KPMG. (2023). *Cyber insurance: A growing necessity*.
Kshetri, N. (2017). Cybersecurity and Cyber Insurance: An Overview. *Journal of Business Research*, 70, 353-365.
Kumar, S., & Singh, S. (2019). Managed Security Services Providers: A Comprehensive Overview. *International Journal of Information Security*, 18(1), 51-67.
Mankiw, N.G. (2020). Principles of economics (8th ed.). Cengage Learning.
MarketsandMarkets. (2020). Managed Security Services Market with COVID-19 Impact Analysis by Service Type, Organization Size, Vertical, and Region - Global Forecast to 2025. Retrieved from https://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-1251.html.
McCann, L. (2004). Induced institutional innovation and transaction costs: The case of the Australian National Native Title Tribunal. *Review of Social Economy*, 62(1), 67-82.
McCann, L. (2013). Transaction costs and environmental policy design. *Ecological Economics*, *88*, 253-262.
Miller, A. (2023). The evolving landscape of cyber insurance. *Risk Management Journal*, 12(4), 45-59.
Mohammad, R.S. (2014). Governance Transactions Costs in National Iranian Oil Company. *Iranian Energy Economics Research*, 4(3), 117-168 (In Persian).
National Cyber Security Centre. (2023). CyberFirst overview. https://www.ncsc.gov.uk/cyberfirst/overview.
North, D.C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge University Press.
Williamson, O. E. (1985). *The Economic Institutions of Capitalism*. Free Press.
NSW Department of Industry. (2017). Market failure guide: A guide to categorising market failures for government policy development and evaluation. State of New South Wales. https://www.opengov.nsw.gov.au/publications/17004
Renani, M. (1997). *Market or non-market*. Tehran: Management and Planning Organization Publications (In Persian).
Reports and Data. (2022). Cyber Insurance Market Size to Reach $28.6 Billion by 2030 | CAGR: 20.1%. https://www.reportsanddata.com/report-detail/cyber-insurance-market.
Todorova, T. (2016). Transaction costs, market failures and economic development. *Journal of Advanced Research in Law and Economics (JARLE)*, *7*(17), 678-684.
U.S. Department of Defense. (2020). Cybersecurity Maturity Model Certification (CMMC). Retrieved from https://www.acq.osd.mil/cmmc/.
U.S. Department of Homeland Security. (2015). Automated Indicator Sharing (AIS). https://www.dhs.gov/automated-indicator-sharing.
Varian, H. R. (2019). *Intermediate microeconomics: A modern approach* (9th ed.). W. W. Norton and Company.
Vaughan, E. J., & Vaughan, T. M. (2014). *Fundamentals of risk and insurance* (11th ed.). Wiley.
World Bank. (2019). *World Development Report 2019: The Changing Nature of Work*.
Zhao, Y., Wang, J., & Li, X. (2023). The role of cyber insurance in improving cybersecurity posture. *Journal of Cybersecurity*, 5(1), 15-30.