Journal of
Information System and Technology Auditing

Research Paper

A Systemic Analysis of Barriers to Cyber Insurance Adoption by Businesses: A Delphi–DEMATEL Approach[1]

Ali Sibevei[2], Mostafa Niazy[3] and Reza Morshedzadeh[4]

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 1, No. 2, Autumn & Winter 2025 - 2026
pp. 54-61

Received: 2025.12.29
Revised: 2026.01.21
Accepted: 2026.02.24

1. Introduction

The rapid escalation of cyber threats has fundamentally reshaped the global risk landscape faced by businesses. Cyberattacks now impose substantial financial, operational, and reputational losses across virtually all industries. Recent global estimates project that the annual economic cost of cybercrime will reach approximately USD 10.5 trillion by 2025, positioning cyber risk among the most severe global economic threats. Consequently, cyber risk has consistently ranked as the top concern in global risk outlooks published by major insurers and reinsurers over recent years. Cyber insurance has emerged as one of the primary financial risk transfer mechanisms to manage these risks. However, despite the sharp increase in cyber exposure, the adoption of cyber insurance remains uneven and, in many emerging and institutionally constrained

[1] https://doi.org/10.22034/JISTA. 2026.569359.1078
[1] Presented Paper on the 21st International Conference on Management
[2] Assistant Professor, Faculty of Agriculture Economics, University of Torbat Heydarieh, Torbat Heydarieh, Iran .(Corresponding Author). Email: alisibevei@torbath.ac.ir
[3] M.Sc., Faculty of Industrial Engineering and Management, Shahrood University of Technology, Shahrood, Iran. Email: niazyi.mfinancial@gmail.com
[4] M.Sc., Faculty of Industrial Engineering and Management, Shahrood University of Technology, Shahrood, Iran. Email: morshedzade.r@gmail.com

markets, notably limited. This imbalance between rising cyber risk and sluggish insurance uptake suggests the presence of deep-rooted structural and institutional barriers. Iran represents a particularly salient case of this paradox. Iranian businesses have become increasingly dependent on digital infrastructures and have experienced several high-profile cyber incidents, especially in technology-intensive and critical service sectors. Despite these developments, the domestic cyber insurance market remains underdeveloped, with very low penetration rates and limited product diversity. Although initial attempts to introduce cyber insurance products date back to the late 2010s, the market has yet to reach operational maturity. Recent large-scale cyber incidents resulting in substantial financial losses have further highlighted the gap between cyber exposure and insurance-based risk transfer.

Importantly, the persistence of this gap indicates that limited adoption cannot be explained solely by insufficient risk awareness or lack of demand at the firm level. Rather, cyber insurance adoption appears to be constrained by a complex system of interacting barriers related to data availability, underwriting practices, reinsurance capacity, contractual ambiguity, regulatory alignment, institutional governance, and behavioral concerns. Understanding these interdependencies is critical for designing effective policy and market interventions.

2. MATERIALS AND METHODS

This study adopts an applied mixed-methods research design with a systems-oriented analytical perspective. In the qualitative phase, a comprehensive review of academic literature, industry reports, insurer publications, and regulatory documents was conducted to identify barriers to cyber insurance adoption. This review resulted in an initial list of fifteen barriers encompassing contractual, actuarial, market, behavioral, and institutional dimensions. To validate and contextualize these barriers for the Iranian market, the Delphi method was employed. A panel of five experts with strategic-level experience in the insurance industry and familiarity with cybersecurity issues was convened. Through two iterative Delphi

rounds, panelists evaluated the relevance, clarity, and contextual applicability of each identified barrier. Based on expert feedback, redundant or marginal factors were eliminated, and the final set of barriers was refined to ten key dimensions. Notably, two barriers specific to the Iranian context were emphasized: firms' concerns regarding the disclosure of sensitive cyber incident information and sanctions-induced limitations on access to international reinsurance and technical expertise. In the quantitative phase, the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method was applied to analyze causal relationships among the ten finalized barriers. Experts provided pairwise evaluations of the degree to which each barrier influences the others using a five-point scale. Individual judgment matrices were aggregated and normalized to construct a total relation matrix. From this matrix, four key indicators were calculated for each barrier: influence (D), dependence (R), prominence (D+R), and net causal role (D−R). These indicators enabled the identification of causal drivers, dependent factors, and the overall structure of interactions within the barrier system.

3. RESULTS AND DISCUSSION

The DEMATEL analysis reveals a highly structured and hierarchical system of barriers to cyber insurance adoption. Among all factors, the insufficiency and low quality of cyber incident and loss data emerged as the most prominent barrier, exhibiting the highest D+R value. This finding indicates that data-related deficiencies occupy a central position in the system, simultaneously influencing and being influenced by multiple other barriers. Several barriers were identified as primary causal drivers with positive D−R values. These include limited participation of governmental and security institutions in supporting the cyber insurance market, inadequate reinsurance capacity, ambiguity in coverage boundaries, particularly concerning war-related and state-attributed cyber incidents, regulatory and standards misalignment between insurance and cybersecurity domains, sanctions-related constraints on international cooperation, and firms' concerns over the disclosure of sensitive technical and organizational information following cyber incidents. In contrast, barriers such as misalignment between

insurance coverage design and firms' cybersecurity architectures, challenges associated with correlated and cascading cyber losses, and weaknesses in post-incident services (including incident response, recovery assistance, and claims handling) were identified as predominantly downstream and dependent factors. These barriers materialize at the insurer–insured interface and are largely shaped by upstream institutional, data, and capacity constraints. The causal network further highlights reinforcing feedback loops that inhibit market maturation. For example, weak data infrastructures lead to conservative underwriting practices, which in turn result in narrow coverage terms and high premiums. Reduced adoption then limits data generation, reinforcing the original data scarcity. This systemic perspective demonstrates that many commonly cited obstacles are symptoms rather than root causes. Compared to prior studies, the relatively lower prominence of behavioral biases suggests that, in the Iranian context, adoption challenges are driven less by managerial misperceptions and more by structural and institutional constraints. The findings also underscore the importance of context-specific factors. Concerns over information disclosure reflect broader political, legal, and governance considerations, while sanctions fundamentally shape reinsurance access, pricing dynamics, and product credibility. These factors should therefore be treated as integral components of the cyber insurance adoption system.

4. CONCLUSION

By integrating Delphi-based expert consensus with DEMATEL causal analysis, this study provides a systemic and context-sensitive understanding of the barriers to cyber insurance adoption in Iran. The results demonstrate that sluggish adoption is primarily rooted in upstream data, institutional, regulatory, and reinsurance constraints rather than isolated firm-level behavior. Addressing these structural drivers through coordinated policy, regulatory, and market interventions is essential for fostering a resilient and credible cyber insurance ecosystem. The study contributes to the literature by moving beyond linear explanations and highlighting causal interdependencies among barriers, while also offering actionable insights for policymakers, regulators, and insurers operating in institutionally constrained environments. Future research may

extend this framework by embedding the identified causal structure into system dynamics models and evaluating alternative policy scenarios as empirical loss data become more available.

Keywords: Cyber Insurance, Systems Approach, DEMATEL, Delphi Method

JEL classification: *G22*, *G28*, *C44*, *D81*

References

Adriko, R., & Nurse, J. R. (2024a). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. *Information & Computer Security*, *32*(5), 691-710. https://doi.org/10.1108/ICS-01-2024-0025

Adriko, R., & Nurse, J. R. (2024b). Does cyber insurance promote cyber security best practice? an analysis based on insurance application forms. *Digital Threats: Research and Practice*, *5*(3), 1-39. https://doi.org/10.1145/3676283

Allianz, S.E. (2025). *Allianz Risk Barometer 2025: Identifying the major business risks for 2025*. Allianz Global Corporate & Specialty. Retrieved February 23, 2026, from https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity Risks and Incidents Disclosure: A Literature Review. *Accounting Perspectives*, *24*(3), 605-667. https://doi.org/10.1111/1911-3838.12411

AXA. (2025). AXA Future Risks Report 2025. Retrieved February 23, 2026, from https://www.axa.com/en/news/future-risks-report?tab=future-risks-report-2025

Bace, B., Dubois, E., & Tatar, U. (2024). Resilience against Catastrophic Cyber Incidents: A Multistakeholder Analysis of Cyber Insurance. *Electronics*, *13*(14), 2768. https://doi.org/10.3390/electronics13142768

Ballestra, L. V., D'Amato, V., Fersini, P., Forte, S., & Greco, F. (2024). Pricing Cyber Insurance: A Geospatial Statistical Approach. *Applied Stochastic Models in Business and Industry*, *40*(5), 1365-1376. https://doi.org/10.1002/asmb.2891

Banerjee, S., & Das, S. (2024). Analyzing the Critical Challenges of Cyber Insurance Market: A Fuzzy DEMATEL Approach. *In Proceedings of the International Conference on Industrial Engineering and Operations Management.* https://doi.org/10.46254/EU07.20240258

Bardopoulos, J. (2025). Cyber-insurance pricing models. *British Actuarial Journal*, *30*, e6. https://doi.org/10.1017/S1357321724000205

Boonen, T. J., Feng, Y., & Tong, Z. (2025). Cybersecurity investments and cyber insurance purchases in a non-cooperative game. *ASTIN Bulletin: The Journal of the IAA*, *55*(2), 426-448. https://doi.org/10.1017/asb.2024.40

Carannante, M., & Mazzoccoli, A. (2025). An Analytical Review of Cyber Risk Management by Insurance Companies: A Mathematical Perspective. *Risks*, *13*(8), 144. https://doi.org/10.3390/risks13080144

Cimbru, I., Wagner, J., & Zeier Röschmann, A. (2025). On IoT-enabled risk prevention and insurance: A systematic literature review. *Risk Management and Insurance Review*. https://doi.org/10.1111/rmir.70025

Clemente, G. P., Cornaro, A., & Belvedere, S. (2025). Pricing Cyber Risk Insurance Coverages by Means of Epidemic Models and Network Theory. *Variance*, *18*. https://variancejournal.org/article/74729-pricing-cyber-risk-insurance-coverages-by-means-of-epidemic-models-and-network-theory

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Materne, S., & Murphy, F. (2024). Enhancing cyber insurance strategies: exploring reinsurance and alternative risk transfer approaches. *Journal of Cybersecurity*, *10*(1), tyae027. https://doi.org/10.1093/cybsec/tyae027

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. Computers & Security, 142, 103886. https://doi.org/10.1016/j.cose.2024.103886

Cybersecurity Ventures. (2025). *Cyberwarfare in the C-Suite 2025*. Retrieved February 23, 2026, from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/?hl=en-US

Eling, M., & Jung, K. (2025). Optimism bias and its impact on cyber risk management decisions. *Risk Sciences*, *1*, 100001. https://doi.org/10.1016/j.risk.2024.100001

Fattahi Zafarghandi, S. (2023). A comparative study of cyber insurance laws. *Proceedings of the 1st International Conference on Law, Management, Educational Sciences, Psychology, and Educational Planning Management.* https://civilica.com/doc/1877044 (in Persian)

Gómez, Y., Branley-Bell, D., Briggs, P., & Vila, J. (2025). Cyberinsurance adoption strategies and security of online behaviour: an experimental study. *Behaviour & Information Technology*, *44*(6), 1169-1182. https://doi.org/10.1080/0144929X.2025.2467891

Hamid, N. H. A. A., Mokhtar, M., Abd Manan, W. K. A. W., & Hashim, H. (2025). Exploring Critical Success Factors in Compliance-Driven Cyber Insurance within Malaysian Organizations: A COBIT 5 enabler approach. *Environment-Behaviour Proceedings Journal*, *10*(SI31), 77-84. https://doi.org/10.21834/e-bpj.v10iSI31.6936

Harel, Y., & Carmeli, A. (2025). A strategic cybersecurity oversight framework: a board's imperative. *Journal of Cybersecurity*, *11*(1), tyaf021. https://doi.org/10.1093/cybsec/tyaf021

Hasanpour, M., & Oloukhani, N. (2021). Identification and prioritization of challenges facing cyber insurance in Iran. *Proceedings of the 28th Insurance and Development Conference*. https://civilica.com/doc/1390777 (in Persian)

He, Q., Faure, M., & Chen, C. Y. (2025). Insuring the "uninsurable" cyberwarfare: rethinking war exclusions in cyber policies and the role of insurance in global

cybersecurity governance. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 1-32. https://doi.org/10.1057/s41288-025-00346-3

Hui, W., Hui, K. L., & Yue, W. T. (2024). Cyber Insurance and Post-Breach Services: A Normative Analysis. *Service Science*, *16*(2), 124-141. https://doi.org/10.1287/serv.2021.0120

Jain, R., Hrle, T., & Woods, D. W. (2025). Insurance versus digital harm: a content analysis of home and cyber insurance policies in the USA and UK. *Journal of Cybersecurity*, *11*(1), tyae031. https://doi.org/10.1093/cybsec/tyae031

Joshi, C., Slapničar, S., Yang, J., & Ko, R. K. (2025). Contrasting the optimal resource allocation to cybersecurity controls and cyber insurance using prospect theory versus expected utility theory. *Computers & Security*, *154*, 104450. https://doi.org/10.1016/j.cose.2025.104450

Lefèvre, C., Tamturk, M., Utev, S., & Carenzo, M. (2024). Cyber Risk in Insurance: A Quantum Modeling. *Risks*, *12*(5), 83. https://doi.org/10.3390/risks12050083

Li, Y., Wang, X., Zhao, P., & Hu, T. (2025). Cyber breach risk modeling for insurance: capturing temporal and cross-group dependence. *Annals of Actuarial Science*, 1-25. https://doi.org/10.1017/S1748499525100109

Mott, G., Turner, S., Nurse, J. R., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security*, *128*, 103162. https://doi.org/10.1016/j.cose.2023.103162

Muktadir-Al-Mukit, D., & Ali, M. H. (2025). The dynamics of stock market responses following the cyber-attacks news: Evidence from event study. *Information Systems Frontiers*, 1-18. https://doi.org/10.1007/s10796-025-10639-6

Nobitex. (2025). *Nobitex hack: CEO answers users' questions* [Web page]. Retrieved February 23, 2026, from https://nobitex.ir/mag/nobitex-hack/

Piralou, M., Danakhoo, H., & Ameri Siahuei, H. (2025). Challenges of cyber insurance. *Proceedings of the 5th International Conference on Advanced Research in Management and Humanities*. https://civilica.com/doc/2325794 (in Persian)

Puteri, N. K., Kusnadi, F., & Kristiani, F. (2025). Cybersecurity Insurance Modeling Using Archimedean Copulas. *Science & Technology Asia*, 177-188. https://doi.10.14456/scitechasia.2025.11

Sadeghi, A., & Asghari Eskouei, M. R. (2021). A review of risk estimation models in cyber insurance. Proceedings of the 28th Insurance and Development Conference. https://civilica.com/doc/1390872 (in Persian)

Schütz, F., Rampold, F., Kalisch, A., & Masuch, K. (2023). Consumer cyber insurance as risk transfer: a coverage analysis. *Procedia Computer Science*, *219*, 521-528. https://doi.org/10.1016/j.procs.2023.01.320

Skeoch, H. R., & Ioannidis, C. (2024). The barriers to sustainable risk transfer in the cyber-insurance market. *Journal of Cybersecurity*, *10*(1), tyae003. https://doi.org/10.1093/cybsec/tyae003

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, *22*(3), 737-748. https://doi.org/10.1007/s10207-023-00660-8

Woods, D. W., & Wolff, J. (2025). A history of cyber risk transfer. *Journal of Cybersecurity*, *11*(1), tyae028. https://doi.org/10.1093/cybsec/tyae028

World Bank. (2025). *GDP (current US$) – China [NY.GDP.MKTP.CD]*. World Development Indicators. Retrieved from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CN

Zhao, A. P., Fei, F. X., & Alhazmi, M. (2024). Cyber Insurance for Energy Economic Risks. *Smart Cities (2624-6511)*, *7*(4). https://doi.org/10.3390/smartcities7040081

Zhao, A. P., Gu, C., Bao, Z., Cheng, X., & Alhazmi, M. (2025). Optimizing Cyber Insurance and Defense for Multi-Energy Systems Under False Data Injections. *IET Renewable Power Generation*, *19*(1), e70011. https://doi.org/10.1049/rpg2.70011

COPYRIGHTS

This license allows others to download the works and share them with others as long as they credit them, but they can't change them in any way or use them commercially.

نشریه علمی
حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن علمی حسابرسی فناوری اطلاعات ایران

مقالهٔ پژوهشی

بررسی سیستمی موانع پذیرش بیمه سایبری توسط کسب‌وکارها با رویکرد دلفی ـ دیمتل[1]

علی سیبویه*[2]، مصطفی نیازی[3] و رضا مرشدزاده[4]

نشریه علمی حسابرسی سیستم‌ها و فناوری اطلاعات
انجمن حسابرسی فناوری اطلاعات ایران
سال اول، پیاپی ۲، پاییز و زمستان ۱۴۰۴
صص ۱۹۹ - ۲۱۹

تاریخ دریافت: ۱۴۰۴/۱۰/۰۸
تاریخ بازنگری: ۱۴۰۴/۱۱/۰۱
تاریخ پذیرش: ۱۴۰۴/۱۲/۰۵

چکیده

با وجود شدّت و گسترش تهدیدات سایبری، پذیرش بیمه سایبری در ایران کند است. این پژوهش با رویکردی سیستمی، به شناسایی موانع پذیرش و ترسیم روابط علّی میان آن‌ها می‌پردازد. مطالعه از نظر هدف، کاربردی و از نظر ماهیت، ترکیبی (کیفی-کمّی) است. ابتدا با مرور نظام‌مند ادبیات، ۱۵ مانع بالقوه استخراج شد؛ سپس در روش دلفی فهرست موانع توسط خبرگان به ۱۰ مانع کلیدی تقلیل یافت. در بخش کمّی، با استفاده از دیمتل و قضاوت‌های زوجی خبرگان، شاخص‌های محاسبه و شبکه علّی-معلولی ترسیم گردید. یافته‌ها نشان می‌دهد کفایت و کیفیت داده‌های رخداد/خسارت هسته اصلی شبکه موانع است و به‌شدت از عوامل بالادستی مثل سطح مشارکت نهادی و حاکمیتی، ظرفیت بازار اتکایی، شفافیت حدود پوشش (به‌ویژه در مورد جنگ) و ناهماهنگی‌های مقرراتی و استانداردی تأثیر می‌پذیرد. در این میان، دو مانع بومی ریسک ادراک‌شده افشای اطلاعات و قیود تحریمی بر دسترسی فنی و اتکایی چهره خاص بازار ایران را شکل داده و موانع رفتاری و عملیاتی در سطح کسب‌وکارها و بیمه‌گران را تشدید می‌کنند. بر اساس نقشه علّی—بازخوردی، پژوهش بسته‌ای سیاستی با سه محور «داده و شفافیت کنترل‌شده»، «هم‌راستاسازی مقررات و استانداردها» و «تقویت ظرفیت مالی و اتکایی» همراه با بازطراحی پوشش‌ها، هم‌ترازی با کنترل‌های دفاعی و بهبود خدمات پسارخداد برای افزایش اعتماد و پذیرش بیمه سایبری پیشنهاد می‌کند.

واژه‌های کلیدی: *بیمه سایبری، رویکرد سیستمی، دیمتل، روش دلفی.*

طبقه‌بندی موضوعی: *G22, G28, C44, D81*

---

[1] https://doi.org/10.22034/JISTA.2026.569359.1078

۱. مقاله ارائه‌شده دربیست و یکمین کنفرانس بین‌المللی مدیریت

۲. استادیار، دانشکده کشاورزی، دانشگاه تربت حیدریه، تربت حیدریه، ایران. (نویسنده مسئول). Email: alisibevei@torbath.ac.ir

۳. کارشناسی ارشد، دانشکده مهندسی صنایع و مدیریت، دانشگاه صنعتی شاهرود، شاهرود، ایران. Email: niazy.mfinancial@gmail.com

۴. کارشناسی ارشد، دانشکده مهندسی صنایع و مدیریت، دانشگاه صنعتی شاهرود، شاهرود، ایران. Email: morshedzade.r@gmail.com

مقدمه

بر اساس تازه‌ترین گزارش شرکت سایبرسکیوریتی ونچرز[1] (۲۰۲۵)، پیش‌بینی می‌شود هزینه جرایم سایبری در سطح جهانی تا سال ۲۰۲۵ به ۱۰.۵ تریلیون دلار در سال برسد؛ رقمی نزدیک به نصف تولید ناخالص داخلی چین، دوّمین اقتصاد بزرگ جهان که نشان‌دهنده شدت فزاینده تهدیدات دیجیتال برای نظام‌های اقتصادی است (بانک جهانی، ۲۰۲۵). هم‌زمان، گزارش‌های بارومتر ریسک آلیانز[2] (۲۰۲۵) و گزارش ریسک‌های آینده آکسا[3] (۲۰۲۵) نشان می‌دهند که ریسک سایبری برای چهارمین سال متوالی در صدر تهدیدات جهانی قرار گرفته و بیش از ۳۸ درصد از پاسخ‌دهندگان، آن را مهم‌ترین خطر برای سال ۲۰۲۵ دانسته‌اند. این ریسک در اروپا، قاره‌های آمریکا، آفریقا و خاورمیانه و در صنایعی چون خدمات مالی، فنّاوری، مخابرات و تولید به‌عنوان تهدید نخست شناخته شده است. به‌ویژه، در گزارش آکسا آمده است که ۷۱ درصد از متخصصان و ۷۰ درصد از مردم خود را در برابر حملات سایبری آسیب‌پذیر می‌دانند، در حالی‌که ۸۰ درصد از خبرگان معتقدند نهادهای عمومی آمادگی کافی برای مقابله با این خطر را ندارند.

در چنین شرایطی، گنجاندن امنیت سایبری در سطوح استراتژی و حاکمیت شرکتی برای بقای بلندمدت و مزیّت رقابتی در چشم‌اندازِ کسب‌وکاریِ امروز که روزبه‌روز دیجیتالی‌تر می‌شود، امری ضروری است (هارل و کارملی[4]، ۲۰۲۵) و بیمه سایبری به عنوان یکی از ابزارهای انتقال ریسک سایبری بایستی به‌مثابه جزئی از راهبرد سازمان دیده شود (وودز و ولف[5]، ۲۰۲۵). بیمه سایبری در سطح جهانی، سازوکاری قراردادی برای جبران زیان‌های ناشی از رخدادهای امنیتیِ دیجیتال است که معمولاً در دو سبدِ مکمل ارائه می‌شود؛ پوششِ شخصِ اوّل[6] برای زیان‌های مستقیمِ بنگاه، از جمله هزینه‌های پاسخ و فارنزیک[7]، بازیابی داده/سامانه، وقفه در کسب‌وکار و اخاذی؛ و پوششِ شخصِ ثالث[8] برای مسئولیت‌های حقوقی در برابر دیگران، از

---

[1] Cybersecurity Ventures
[2] Allianz Risk Barometer
[3] AXA Future Risks
[4] Harel & Carmeli
[5] Woods & Wolff
[6] First-party
[7] هزینه فارنزیک (Forensic Cost) یا هزینه کارشناسی فارنزیک: به هزینه‌های بررسی تخصصی برای کشف تقلب، تخلف یا علت یک رویداد می‌گویند.
[8] Third-party

دعاوی نقض داده و حریم خصوصی تا هزینه‌های دفاع و پرداخت غرامت به ذی‌نفعان را شامل می‌شود. این دوگانه بسته‌های پوشش، هسته استانداردِ صورت‌بندی محصولات را می‌سازد (هه و همکاران[1]، ۲۰۲۵؛ تسوهو و همکاران[2]، ۲۰۲۳).

با گسترش وابستگی اقتصاد و خدمات به زیرساخت‌های دیجیتال، تهدیدات سایبری در ایران نیز به یکی از دغدغه‌های اصلی کسب‌وکارها تبدیل شده است. با وجود رشد فنّاوری و تحول دیجیتال، بازار بیمه سایبری هنوز در کشور به طور عام شکل نگرفته و ضریب نفوذ آن بسیار پایین است. نخستین طرح بیمه سایبری توسط بیمه ملت در سال ۱۳۹۹ ارائه شد، هرچند هنوز به‌طور کامل وارد مرحله اجرایی نشده است. با این حال، در سال‌های اخیر، زمزمه‌هایی از ارائه خدمات مشابه توسط برخی شرکت‌های بیمه‌ای دیگر به گوش می‌رسد و به‌نظر می‌آید که بازار بیمه سایبری در ایران به‌تدریج در حال شکل‌گیری است (حسن‌پور و اولوخانی، ۱۴۰۰). در سال ۱۴۰۴، حمله سایبری به صرافی ارز دیجیتال نوبیتکس و از دست رفتن ۹۰ تا ۱۰۰ میلیون دلار از دارایی‌های رمزارزی آن، بار دیگر نشان داد که حتی کسب‌وکارهای فنّاورمحور نیز در برابر تهدیدات پیچیده سایبری آسیب‌پذیرند (نوبیتکس، ۱۴۰۴).

پذیرش بیمه سایبری و کاهش ریسک سایبری، حاصل برهم‌کنش شبکه‌ای از متغیرها و عوامل است. به عنوان مثال، یکی از اهرم‌های تسهیل کارکرد بازار و به‌تبع آن گسترش پوشش بیمه سایبری، افشای به‌موقع و شفّاف رخدادهاست که با کاهش عدم‌تقارن اطلاعاتی به بهبود ارزیابی و قیمت‌گذاری کمک می‌کند (امانی و همکاران[3]، ۲۰۲۵)؛ با این‌حال، افشا می‌تواند از کانال تبعات اعتباری/بازاری، ریسک تجاری و فشار کوتاه‌مدت بر سودآوری را افزایش دهد (موکتادیر-المکیت و علی[4]، ۲۰۲۵)؛ در نتیجه، احتیاطِ کسب‌وکارها در قبال خرید بیمه سایبری قابل دفاع است؛ زیرا تصمیم نهایی تحت تأثیرِ مجموعه‌ای از موانع به‌هم‌پیوسته قرار دارد و این برهم‌کنشی در عمل با اصطکاک‌های اجرایی و ادراکی روبه‌رو می‌شود و آهنگ پذیرش را کند می‌کند. ازاین‌رو، پرسش اصلی این پژوهش آن است که " چه عواملی مانع پذیرش بیمه سایبری توسط کسب‌وکارها هستند و این عوامل چگونه در قالب یک نظام علّی و بازخوردی بر یکدیگر

[1] He et al.
[2] Tsohou et al.
[3] Amani et al.
[4] Muktadir-Al-Mukit & Ali

اثر می‌گذارند؟". پژوهش حاضر با اتخاذ رویکرد سیستمی و تحلیلی، در پی شناسایی و تبیین روابط میان موانع کلیدی بازار بیمه سایبری است تا درکی جامع از پویایی‌های این عوامل و مسیرهای بهبود اعتماد و پذیرش بیمه سایبری در کشور ارائه دهد.

مبانی نظری و توسعه فرضیه‌ها

بر اساس شرایطی که مقدمه از شدت‌یافتن ریسک و کندی پذیرش بیمه سایبری نشان می‌دهد موانع پذیرش حاصل برآیند لایه‌هایی درهم‌تنیده است که از متن قرارداد و سازوکارهای بیم‌سنجی تا پویایی شبکه‌ای تهدیدات، رفتار تصمیم‌گیران و نهایتاً حکمرانی و رگولاتوری امتداد می‌یابد. روایت از جایی آغاز می‌شود که بیمه‌گر باید نخست مرز تعهدات خود را بشناسد؛ درست همان‌جا که ابهام در حدود پوشش، به‌ویژه هنگامی که حمله به دولت‌ها منتسب می‌شود یا رنگ‌وبوی «جنگ سایبری» می‌گیرد، خطرات حقوقی و سیاسی را بالا می‌برد و تصمیم برای پذیرش ریسک را پرهزینه می‌سازد (کرمر و همکاران[1]، ۲۰۲۴). تجربه بازارهای مختلف نیز تصدیق می‌کند هرقدر زبان قرارداد شفاف‌تر و همسان‌سازی شروط دقیق‌تر باشد، میل به خرید و امکان ظرفیت‌سازی افزایش می‌یابد (جین و همکاران[2]، ۲۰۲۵). همین منطق، تلاش‌های نو برای بازنگری استثنائات به‌ویژه استثنای جنگ را توضیح می‌دهد؛ تلاشی که هدفش کاستن از نااطمینانی قراردادی و تقویت نقش بیمه در حکمرانی امنیت سایبری است (هه و همکاران، ۲۰۲۵). اما حتی بیرون از متن قرارداد، اگر زنجیره انتقال ریسک به بیمه‌گران اتکایی کارآمد نباشد و عدم‌تقارن اطلاعاتیِ بیمه‌گر و بیمه‌گذار تداوم یابد، هزینه پوشش بالا می‌رود و ظرفیت بازار محدود می‌شود (کرمر و همکاران، ۲۰۲۴). کمی جلوتر، بیمه‌گر در عرصه برآورد و قیمت‌گذاری ریسک با کمبود و ناهمگونی داده‌های رخداد روبه‌رو می‌شود؛ معضلی که تعیین حق‌بیمه منصفانه و پایدار را دشوار می‌کند و مدل‌ها را در معرض عدم‌قطعیت قرار می‌دهد (بالسترا و همکاران[3]، ۲۰۲۴). پاسخ ادبیات نظری روشن است: مدل‌های قیمت‌گذاری باید با داده‌های تجربی و معیارهای منسجم سنجش ریسک سایبری بازبینی و تنظیم شوند تا عدم‌قطعیت

[1] Cremer et al.
[2] Jain et al.
[3] Ballestra et al.

و قضاوت‌های حدسی در پذیره‌نویسی به حداقل برسد (بردوپولوس[1]، ۲۰۲۵؛ آدریکو و نرس[2]، ۲۰۲۴ب). همین‌جا چالش‌های اجرایی فرا می‌رسند: از دقت ارزیابی متقاضی در پذیره‌نویسی تا سازوکار عادلانه و به‌موقعِ جبران خسارت؛ گره‌هایی که اگر سفت بمانند، چرخه اعتماد را کند کرده و انگیزه ورود یا ماندن در بازار را می‌کاهند (پیرالو و همکاران، ۱۴۰۴).

اما ماهیت ریسک سایبری فقط در کمیت‌های ایستا خلاصه نمی‌شود؛ تهدیدات روی شبکه‌ای از پیوندها می‌لغزند و همچون فرآیندهای سرایتی، از گره‌های بحرانی نیرو می‌گیرند. همین وابستگی ساختاری است که هم‌بستگی خسارت‌ها را بالا می‌برد و پیش‌بینی را دشوارتر می‌سازد (پوتری و همکاران[3]، ۲۰۲۵؛ کلیمنته و همکاران[4]، ۲۰۲۵). وقتی زمان نیز وارد ماجرا شود، وابستگی‌های بین‌گروهی و زمانی شکل قرارداد را عوض می‌کنند و بیمه‌گر را به طراحی‌های حساس‌تر نسبت به توالی رخدادها فرامی‌خوانند (لی و همکاران[5]، ۲۰۲۵). حتی برخی رویکردها برای مواجهه با این عدم‌قطعیت، به مدل‌سازی کوانتومی متوسل می‌شوند تا تنوع و جهش‌های رفتاری ریسک بهتر نمایش یابد (لفور و همکاران[6]، ۲۰۲۴). در کنار این‌ها، تغییرات فنّاورانه سریع از هوش مصنوعی تا رایانش کوانتومی می‌تواند توزیع‌های ریسک را ناپایدار کند و اتکاپذیری الگوهای سنتی را کاهش دهد؛ به‌گونه‌ای که ایستایی مفروضات اکچوئری مخدوش و پارامترهای کلیدی مدل به‌طور مستمر ناپایدار می‌شوند (اسکیوچ و یوانیدیس[7]، ۲۰۲۴).

در سطح بازار، موج‌های پرهزینه رخدادهای بزرگ فشار را بر توانگری مالی شرکت‌ها می‌افزایند؛ نتیجه معمولاً افزایش نرخ‌ها، محدودسازی پوشش‌ها و تعمیق شکاف بیمه‌ای است (بیس و همکاران[8]، ۲۰۲۴). هم‌زمان خیزش باج‌افزار، استانداردهای پذیرش را سخت‌گیرانه‌تر کرده است: احراز هویت چندمرحله‌ای، تفکیک شبکه و سایر کنترل‌های پیشینی هرچند برای مدیریت ریسک ضروری‌اند اما هزینه و پیچیدگی آن‌ها بیمه‌پذیری برخی صنایع، به‌ویژه سلامت

[1] Bardopoulos
[2] Adriko & Nurse
[3] Puteri et al.
[4] Clemente et al.
[5] Li et al.
[6] Lefèvre et al.
[7] Skeoch & Ioannidis
[8] Bace et al.

و آموزش، را دشوار می‌سازد (مات و همکاران[1]، ۲۰۲۳). سوی تقاضا نیز آرام نیست: تصمیم‌گیران گاه با خوش‌بینی بیش‌ازحد نسبت به سطح امنیت خود یا با زیان‌گریزی در تصمیم‌های مالی، احتمال حادثه را کمتر از واقع می‌بینند و از خرید بیمه فاصله می‌گیرند؛ و گاه پس از خرید، با اتکا به پوشش مالی، سرمایه‌گذاری امنیتی را کاهش داده و خطر رفتار غیر اخلاقی را تقویت می‌کنند رفتارهایی که پیامدهای مستقیم اکچوئری و کنترلی برای بیمه‌گر دارند (ایلینگ و یونگ[2]، ۲۰۲۵؛ جوشی و همکاران[3]، ۲۰۲۵؛ کارانانته و مازوکولی[4]، ۲۰۲۵). این تصویر در کسب‌وکارهای کوچک و متوسط تندتر است: محدودیت مالی، زبان مبهم قراردادها و فقدان داده دقیق، تصمیم‌گیری را پرهزینه می‌کند؛ و حتی در سطح خردِ مصرف‌کننده، فقدان زبان روشن و درک مشترک، اعتماد عمومی را محدود نگه می‌دارد (آدریکو و نرس، ۲۰۲۴ الف؛ شوتس و همکاران[5]، ۲۰۲۳). در نقطه مقابل، کیفیت خدمات پسارخداد (حادثه‌یابی، بازیابی و راهبری ادعا) و سطح آگاهی ذی‌نفعان، محرک‌های مهم پذیرش‌اند (هوی و همکاران[6]، ۲۰۲۴؛ ژائو و همکاران[7]، ۲۰۲۴؛ گومز و همکاران[8]، ۲۰۲۵).

با وجود این اصطکاک‌ها، مسیرهایی برای هموارسازی پیشِ روست. هرجا بیمه با اقدامات پیشگیرانه فنّاورانه هم‌نشین می‌شود از اینترنت اشیا تا برنامه‌های هوش مصنوعی و کاربردهای آن مانند تئوری بازی، سیستم‌های توصیه‌گر، بینایی ماشین و یادگیری ماشین هم ریسک مورد انتظار فرو می‌نشیند و هم انگیزه خرید شکل می‌گیرد (چیمبرو و همکاران[9]، ۲۰۲۵؛ صادقی و اصغری اسکویی، ۱۴۰۰). اما ادبیات یک هشدار به همراه دارد: کارایی پایدار زمانی پدیدار می‌شود که سیاست‌های بیمه‌ای با تدابیر دفاعی هماهنگ و هم‌تکاملی طراحی شوند؛ اتکای صرف به بیمه بی‌آن‌که مسئولیت‌پذیری امنیتی نهادینه شود پاسخی ناقص است (بونن و همکاران[10]، ۲۰۲۵؛ ژائو و همکاران، ۲۰۲۵). از این نقطه، نگاه به سطح نهادی و رگولاتوری ضروری است: هرجا مقررات، استانداردهای امنیتی و سیاست‌های نظارتی هم‌راستا باشند،

[1] Mott et al.
[2] Eling & Jung
[3] Joshi et al.
[4] Carannante & Mazzoccoli
[5] Schütz et al.
[6] Hui et al.
[7] Zhao et al.
[8] Gómez et al.
[9] Cimbru et al.
[10] Boonen et al.

اصطکاک‌های ورود و بقا در بازار کمتر می‌شود (حمید و همکاران، ۲۰۲۵). تجربه صنعت نیز نشان می‌دهد که تصمیم‌های امروزِ بیمه‌گر و تنظیم‌گر بر شانه یادگیری‌های دیروز ایستاده است؛ تاریخی از آزمون‌وخطا که به‌تدریج زبان محصولات و ظرفیت‌سازی را شکل داده است (وودز و ولف، ۲۰۲۵). در کشورها، تفاوت‌های فرهنگی، فنّاورانه و اقتصادی ایجاب می‌کند چارچوب‌های حقوقی، اقتضایی طراحی شوند و از تجربه دیگران برای کاستن از ریسک‌های حقوقی و عملیاتی و تسهیل پذیرش بهره گرفته شود (فتاحی زفرقندی، ۱۴۰۲).

در جمع‌بندی این روایت، قطعات پازل پژوهش‌های پیشین کنار هم تصویری روشن می‌سازند: ابهام‌های قراردادی و حدود پوشش، دشواری‌های ارزیابی ریسک تحت محدودیت داده و هم‌بستگی خسارت‌ها، پویایی شبکه‌ای و ناپایداری توزیع‌های ریسک، فشارهای بازار و سخت‌گیری‌های پذیره‌نویسی، رفتارهای شناختی و خطر اخلاقی، شکاف‌های آگاهی و خدمات پسارخداد و ضرورت طراحیِ هم‌تکاملیِ بسته‌های دفاع و بیمه در پرتو حکمرانی اقتضایی. در کنار این شواهد، تنها یک مطالعه هم‌روش با رویکرد دیمتل فازی چالش‌های بازار را واکاوی کرده و بر اثرات آبشاریِ ریسک‌های هم‌بسته و نقش مشارکت فعال مدیران ارشد امنیت اطلاعات در کارآمدی اکوسیستم تأکید دارد، اما از منظر شرکت‌های بیمه سامان نیافته است (بانرجی و داس[1]، ۲۰۲۴). با این‌همه، هنوز چارچوبی نظام‌مند برای آشکارسازی شبکه علّیِ این موانع به‌ویژه در بافت ایران به‌قدر کافی بسط نیافته است؛ ازهمین‌رو، پژوهش حاضر با تکیه بر اجماع خبرگان و به‌کارگیری دیمتل می‌کوشد نقشه جهت‌دار روابط را ترسیم کند، موانع را بر حسب برجستگی و نقش علت–معلول تفکیک کند و مسیرهای مداخله اولویت‌دار برای ارتقای پذیرش را پیشنهاد دهد؛ و این، دقیقاً همان پلی است که متن را از پیشینه به روش‌شناسی عبور می‌دهد.

روش‌شناسی پژوهش

این پژوهش از نظر هدف، کاربردی و از نظر ماهیت، ترکیبی (کیفی–کمی) است. فرآیند انجام پژوهش در سه گام اصلی و به‌صورت پیوسته طراحی و اجرا شد. در گام نخست، با هدف شناسایی و استخراج دقیق موانع مؤثر بر پذیرش بیمه سایبری توسط کسب‌وکارها، مجموعه‌ای

[1] Banerjee & Das

از پژوهش‌های معتبر در حوزه بیمه سایبری و مدیریت ریسک‌های فنّاورانه بررسی و گزاره‌های مرتبط با موانع پذیرش استخراج می‌شود. داده‌های استخراج‌شده در روش دلفی طی چند مرحله پالایش، مقایسه و تلفیق می‌شوند تا موارد مشابه ادغام و موارد متمایز حفظ شوند. در نهایت، موانع شناسایی‌شده در قالب عوامل اصلی مرتبط سازمان‌دهی می‌گردند و این فهرست به‌عنوان ورودی مرحله دوّم پژوهش مورد استفاده قرار می‌گیرد. در مرحله دوم، با هدف اعتبارسنجی و بومی‌سازی یافته‌های نظری، فهرست اولیه موانع در یک پنل خبرگی بازبینی شد تا درباره کفایت عناوین، ادغام موارد هم‌پوشان و افزودن موارد ضروری اجماع حاصل شود. جامعه آماری این مرحله به‌صورت نمونه‌گیری هدفمند انتخاب می‌شوند و شامل پنج نفر از خبرگان صنعت بیمه هستند که هم‌زمان با مسائل امنیت سایبری آشنایی داشته و در سطح راهبردی در صنعت بیمه نقش‌آفرین بودند. در مرحله نهایی، به‌منظور تحلیل روابط میان موانع و شناسایی عوامل علّی و معلولی، روش دیمتل و نرم‌افزارهای اِکسِل[1] و مَتلَب[2] مورد استفاده قرار می‌گیرد. برای این منظور، پرسشنامه زوجی دیمتل طراحی می‌گردد که در آن، هر خبره بر اساس مقیاس عددی متعارف دیمتل (مثلاً ۰،۱،۲،۳،۴) میزان تأثیر هر عامل بر سایر عوامل را ارزیابی می‌نماید تا درجه اثرگذاری و اثرپذیری برای هر مانع محاسبه و شبکه علّی-معلولی ترسیم شود. نتایج در بخش یافته‌های پژوهش به تفصیل بیان شده است.

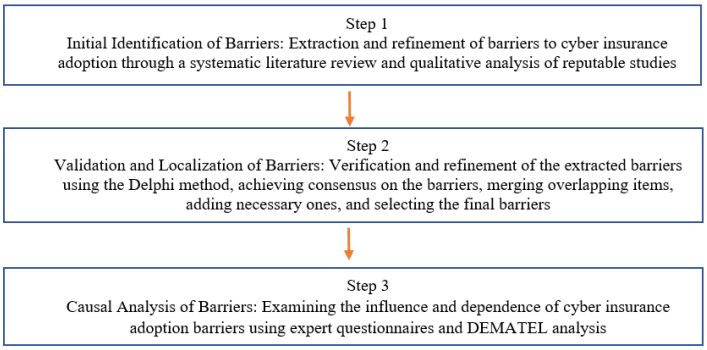

Figure 1. Research Process

شکل ۱. فرآیند پژوهش

[1] Excel
[2] MATLAB

یافته‌های پژوهش

در این بخش، نتایج تجربی پژوهش با تمرکز بر موانع پذیرش بیمه سایبری توسط کسب‌وکارها ارائه می‌شود. بر مبنای راهبرد ترکیبی پژوهش، ابتدا داده‌های گردآوری‌شده تشریح می‌گردد، سپس برونداد تحلیل کیفی و فرآیند نهایی‌سازی موانع با استفاده از نظر خبرگان و روش دلفی گزارش می‌شود و در نهایت، نتایج تحلیل علّی–ساختاری موانع با بهره‌گیری از روش دیمتل تبیین می‌گردد. تمرکز اصلی این فصل بر تبیین این نکته است که کدام موانع از دید بیمه‌گر برجسته‌ترند و چگونه در قالب یک شبکه علّی و بازخوردی بر یکدیگر اثر می‌گذارند.

نتایج شناسایی اولیه موانع

در گام نخست، به‌منظور صورت‌بندی اولیه مسئله پژوهش، ادبیات نظری و اسناد تخصصی مرتبط با بیمه سایبری به‌صورت نظام‌مند مرور شد. برآیند این مرحله، استخراج فهرستی از ۱۵ مانع بالقوه بود که در پژوهش حاضر با کدهای "R_1" تا "R_{15}" نشان داده می‌شوند. این موانع بر اساس صورت‌بندی نظریِ مطالعات پیشین و گزارش‌های صنعت بیمه، ابعاد مختلفی از چالش‌های قراردادی، فنی–اکچوئری، ساختار بازار، رفتار بیمه‌گذاران و محیط نهادی را پوشش می‌دهند.

فهرست موانع استخراج‌شده از ادبیات به همراه کد، عنوان مانع و منابع مربوطه در جدول۱ ارائه شده است.

جدول زیر از فهرست اولیه ادبیات، تصویری نسبتاً جامع از موانع بالقوه پذیرش بیمه سایبری ارائه می‌کند؛ با این حال، این فهرست در آغاز صرفاً مبتنی بر شواهد نظری و تجربیات بین‌المللی است و به‌خودی‌خود تضمین نمی‌کند که همهٔ این موانع در بافت ایران از دید فعالان صنعت بیمه، «محوری» یا «متمایز» تلقی شوند. از این‌رو، در مرحله بعد، فهرست پانزده‌گانه به‌عنوان ورودی روش دلفی مطرح شد و هر یک از موانع از حیث ارتباط با شرایط بازار ایران، میزان اهمیت نسبی و هم‌پوشانی مفهومی با سایر موارد مورد ارزیابی قرار گرفت.

جدول ۱. استخراج موانع

Table 1. Extraction of Barriers

References	Barriers	Code
Cremer et al., 2024; Jain et al., 2025; He et al., 2025	Coverage transparency and governance of exclusions (especially war exclusion)	R_1
Adriko & Nurse, 2024b; Ballestra et al., 2024	Adequacy and quality of incident/loss data	R_2
Berdopoulos, 2025; Lefèvre et al., 2024; Skeoch & Ioannidis, 2024	Model risk and structural instability of loss distributions	R_3
Cremer et al., 2024	Capacity and efficiency of the reinsurance market	R_4
Cremer et al., 2024	Insurer–insured information asymmetry	R_5
Puteri et al., 2025; Clemente et al., 2025	Interdependence and contagion of cyber risk	R_6
Li et al., 2025	Temporal dependencies and structural changes	R_7
Bece et al., 2024; Mott et al., 2023	Cybersecurity prerequisites (underwriting controls)	R_8
Eling & Jung, 2025; Joshi et al., 2025	Managerial cognitive biases (optimism, loss aversion)	R_9
Carannante & Mazzoccoli, 2025	Moral hazard post-purchase (reduced security efforts)	R_{10}
Adriko & Nurse, 2024a; Schütz et al., 2023	Policy readability and consumer insurance literacy	R_{11}
Hui et al., 2024; Zhao et al., 2024; Gómez et al., 2025	Post-incident service quality and awareness programs	R_{12}
Boonen et al., 2025; Zhao et al., 2025; Cimbru et al., 2025; Sadeghi & Eskouei, 2021	Defense–insurance co-design (aligning coverage with controls)	R_{13}
Hamid et al., 2025; Woods & Wolff, 2025; Fattahi Zafarghandi, 2023	Alignment of regulations and standards	R_{14}
Banerjee & Das, 2024	Governance and involvement of security organizations	R_{15}

نتایج اعتبارسنجی و بومی‌سازی موانع

بر اساس جمع‌بندی نظرات خبرگان، بخشی از موانع به‌عنوان عوامل فرعی یا پیامدی تشخیص داده شدند و از فهرست اصلی کنار گذاشته شدند در مقابل، خبرگان بر وجود دو مانع مهم تأکید کردند که در فهرست اولیه ادبیات به‌صورت مستقل منعکس نشده بودند و متناسب با شرایط فعلی بازار بیمه و محیط نهادی ایران، نقشی متمایز در تبیین پذیرش بیمه سایبری دارند. این دو مانع جدید با کدهای "R_{16}" و"R_{17}" به فهرست افزوده شد و به تأیید همگان در دورِ دوّم دلفی قرار گرفت.

فهرست نهایی موانع مورد تأیید خبرگان، پس از دورِ دوّم دلفی در جدول(۲) به نمایش گذاشته شده است.

جدول۲. موانع نهایی

Table 2. Final Barriers

Barriers	Code
Ambiguity in cyber insurance coverage and exclusions (especially war and governmental actions)	R_1
Low quality and insufficient adequacy of cyber incident and loss data	R_2
Higher premiums and restrictive terms due to limited reinsurance support	R_4
Coverage limitations due to cascading and simultaneous cyberattacks across firms	R_6
Weak support and ancillary services of cyber insurance (training, incident response, claims handling)	R_{12}
Misalignment of cyber insurance coverage with business needs, processes, and security architecture	R_{13}
Low involvement of security and governmental institutions in supporting and developing the cyber insurance market	R_{14}
Regulatory and standardization constraints and misalignments in cyber insurance	R_{15}
Firms' concerns about disclosure of sensitive technical information and organizational/governmental consequences of incident reporting	R_{16}
Impact of sanctions and restricted access to international technical and reinsurance partners on coverage design and credibility	R_{17}

در ادامه، با تکیه بر این فهرست نهایی ده‌گانه به‌عنوان مجموعه موانع اصلی، ساختار علّی بین موانع با استفاده از روش دیمتل تحلیل می‌شود که نتایج آن در قسمت بعد گزارش می‌شود.

نتایج تحلیل روابط علّی موانع

در این بخش، بر مبنای فهرست نهایی ده‌گانهٔ موانع پذیرش بیمه سایبری، چارچوب علّی-ساختاری روابط میان این موانع با بهره‌گیری از روش دیمتل بررسی شده است. همان‌گونه که در بخش روش‌شناسی توضیح داده شد، برای تشکیل ماتریس روابط مستقیم، از خبرگان خواسته شد که تأثیر هر مانع بر سایر موانع را بر روی مقیاس ۰ تا ۴ (از "بدون تأثیر" تا "تأثیر بسیار زیاد") ارزیابی کنند. ماتریس‌های به‌دست‌آمده از پنج خبره به‌صورت میانگین‌گیری تجمیع شد و پس از نرمال‌سازی، ماتریس روابط کل محاسبه گردید. بر این اساس، برای هر مانع، مجموع سطری ماتریس روابط کل به‌عنوان شاخص تأثیرگذاری (D)، مجموع ستونی به‌عنوان شاخص تأثیرپذیری (R) و در ادامه، شاخص‌های D+R (اهمیت/برجستگی) و D−R (نقش علّی/معلولی) استخراج شد.

جدول(۳) مقادیر نهایی این شاخص‌ها را برای ده مانع پژوهش نشان می‌دهد. در این جدول، ستون D+R میزان درگیر بودن هر مانع در شبکه روابط (اهمیت ساختاری) و ستون D−R جهت غالب تأثیر را مشخص می‌کند؛ به‌گونه‌ای که مقادیر مثبت D−R نشان‌دهندهٔ عوامل علّی و مقادیر منفی آن نمایانگر عوامل پیامدی هستند.

جدول۳. نتایج شاخص‌های دیمتل برای موانع

Table 3. DEMATEL Indicator Results for Barriers

D-R	D+R	R	D	Barriers	Code
1.80	9.20	3.70	5.50	Low quality and insufficient adequacy of cyber incident and loss data	R_2
2.80	8.80	3.00	5.80	Low involvement of security and governmental institutions in supporting and developing the cyber insurance market	R_{14}
1.20	8.80	3.80	5.00	Higher premiums and restrictive terms due to limited reinsurance support	R_4
0.80	8.60	3.90	4.70	Ambiguity in cyber insurance coverage and exclusions (especially war and governmental actions)	R_1
1.40	8.20	3.40	4.80	Regulatory and standardization constraints	R_{15}

D-R	D+R	R	D	Barriers	Code
				and misalignments in cyber insurance	
-1.10	8.10	4.60	3.50	Misalignment of cyber insurance coverage with business needs, processes, and security architecture	R_{13}
-1.40	8.00	4.70	3.30	Coverage limitations due to cascading and simultaneous cyberattacks across firms	R_6
-1.20	7.60	4.40	3.20	Weak support and ancillary services of cyber insurance (training, incident response, claims handling)	R_{12}
1.70	7.50	2.90	4.60	Impact of sanctions and restricted access to international technical and reinsurance partners on coverage design and credibility	R_{17}
0.80	7.40	3.30	4.10	Firms' concerns about disclosure of sensitive technical information and organizational/governmental consequences of incident reporting	R_{16}

همان‌گونه که در جدول شاخص‌های دیمتل مشاهده می‌شود، در بین موانع مورد بررسی، کیفیت پایین و کفایت ناکافی داده‌های رخداد و خسارت سایبری (R_2)، با بالاترین مقدار D+R(۹،۲۰) در مرکز شبکه روابط قرار دارد و از بیشترین اهمیت ساختاری برخوردار است؛ به این معنا که هم بر سایر موانع به‌طور معناداری اثر می‌گذارد و هم از آن‌ها تأثیر می‌پذیرد. پس از آن، مشارکت پایین نهادهای امنیتی و حاکمیتی در حمایت و توسعه بازار بیمه سایبری (R_{14})، افزایش قیمت و محدود شدن شرایط به‌دلیل کمبود حمایت بیمه‌گران اتکایی (R_4)، ابهام در پوشش و استثناهای بیمه سایبری (R_1) و محدودیت‌ها و ناهماهنگی‌های مقرراتی و استانداردی (R_{15}) در رده‌های بعدی قرار گرفته‌اند؛ این نتایج نشان می‌دهد که موانع مرتبط با زیرساخت داده‌ای، محیط نهادی-حاکمیتی و ظرفیت اتکایی، هسته اصلی ساختار علّی موانع پذیرش را شکل می‌دهند و در صورت مداخله، بیشترین پتانسیل برای ایجاد تغییر در کل نظام را دارند. در

مقابل، موانعی مانند عدم تطابق پوشش با نیازها و ساختار امنیتی بنگاه‌ها (R_{13})، محدود شدن پوشش در اثر حملات زنجیره‌ای (R_6) و ضعف پشتیبانی و خدمات همراه بیمه سایبری (R_{12})، مقادیر پایین‌تری از D+R را دارند و بیشتر در لایه‌های پایین‌دست و نزدیک به سطح تعامل با بیمه‌گذاران قرار می‌گیرند.

بررسی مقادیر D−R نیز تصویر روشنی از نقش علّی-معلولی هر مانع ارائه می‌کند. مقادیر مثبت و نسبتاً بالای D−R برای R_{14}، R_2، R_{17}، R_{15}، R_4، R_1 و R_{16} نشان می‌دهد که این موانع عمدتاً در زمرهٔ عوامل علّی و بالادستی قرار می‌گیرند؛ یعنی ابتدا ضعف مشارکت نهادهای امنیتی و حاکمیتی، فقدان داده‌های قابل اتکا، محدودیت‌های ناشی از تحریم‌ها، ناهماهنگی‌های مقرراتی، کمبود حمایت اتکایی، ابهام در حدود تعهدات و نیز نگرانی بنگاه‌ها از افشای اطلاعات حساس، ساختاری پرریسک و نامطمئن برای توسعه بیمه سایبری ایجاد می‌کند. در چنین بستری، به‌صورت پیامدی، موانعی نظیر عدم تطابق پوشش با نیازها (R_{13})، محدود شدن پوشش در مواجهه با ریسک‌های زنجیره‌ای (R_6) و ضعف خدمات همراه (R_{12}) با مقادیر منفیD−R، به‌عنوان عوامل معلولی و پایین‌دستی ظاهر می‌شوند و خود را در قالب محصول، دامنه پوشش و تجربه خدماتی بیمه‌گذاران نشان می‌دهند.

به‌طور خلاصه، نتایج دیمتل تأیید می‌کند که بخش مهمی از مشکلات مشاهده‌شده در سطح پذیرش بیمه سایبری توسط کسب‌وکارها، ریشه در موانع ساختاری‌تر داده‌ای، نهادی، اتکایی و حاکمیتی دارد. در گام بعد، بر اساس همین نتایج، شبکه علّی-بازخوردی روابط بین موانع ترسیم می‌شود تا زنجیره‌های اصلی اثرگذاری مشخص و مبنایی برای پیشنهادهای سیاستی و مدیریتی فراهم گردد.

بر مبنای نتایج دیمتل، برای تبیین ساختار درونی موانع، شبکه علّی-بازخوردی روابط میان ۱۰ مانع نهایی ترسیم شد (شکل ۲). در این شبکه، هر مانع به‌صورت یک گره مستقل نمایش یافته و تنها روابطی نشان داده شده‌اند که شدت آن‌ها در ماتریس روابط کل از آستانه تعیین‌شده فراتر رفته است. الگوی حاصل نشان می‌دهد که موانع نهادی، داده‌ای و قراردادیِ بالادست نظیر ضعف داده‌های خسارت، مشارکت ناکافی نهادهای امنیتی و حاکمیتی، محدودیت‌های اتکایی و مقرراتی و ابهام در حدود پوشش، عمدتاً در نقش عوامل محرک عمل می‌کنند و به‌صورت

زنجیره‌ای به موانع پایین‌دستِ مرتبط با طراحی محصول و تجربه خدمات (مانند عدم تطابق پوشش، محدود شدن دامنه تعهد و ضعف خدمات همراه) سرریز می‌شوند.

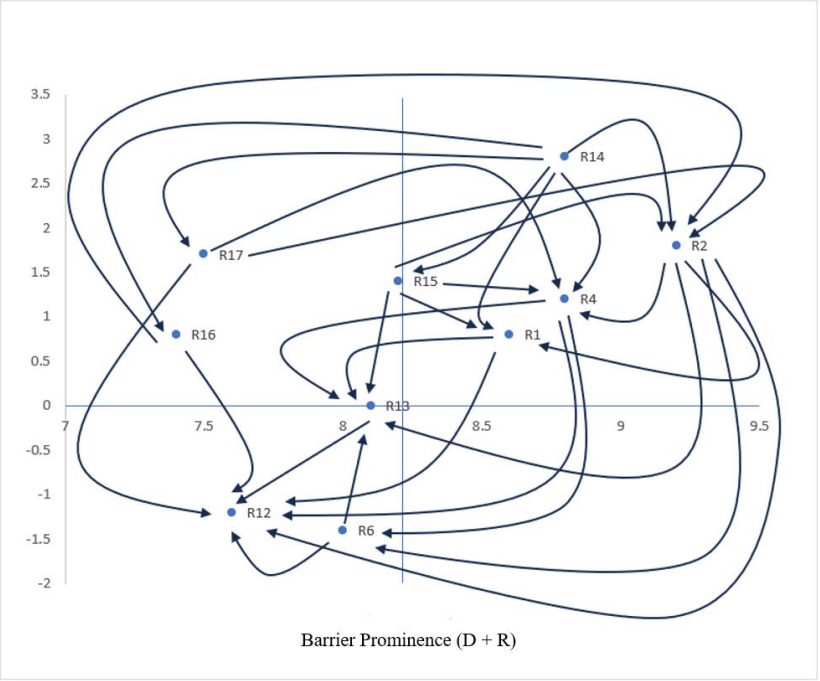

Figure 2. Cause–Effect Diagram

شکل ۲. نقشه علّی-بازخوردی

بحث و نتیجه‌گیری

در پرتو نتایج این پژوهش، می‌توان روشن‌تر به پرسش آغازین بازگشت که چرا با وجود آن‌که ریسک سایبری در گزارش‌های جهانی به‌عنوان یکی از مهم‌ترین تهدیدهای اقتصادی و کسب‌وکاری شناخته می‌شود، بازار بیمه سایبری در ایران همچنان کم‌عمق باقی مانده است. ترکیب مرور نظام‌مند ادبیات، پنل دلفی و تحلیل علّی با دیمتل نشان داد این کندی بیش از آن‌که ناشی از بی‌میلی ساده کسب‌وکارها باشد، محصول شبکه‌ای از موانع ساختاری و نهادی است؛

به‌گونه‌ای که از میان ۱۵ مانع اولیه، ۱۰ مانع کلیدی برگزیده شد که هم تجربه جهانی و هم اقتضائات بومی را منعکس می‌کنند. در این شبکه، کیفیت و کفایت داده‌های رخداد و خسارت (R_2)با بالاترین D+R در مرکز قرار گرفت و همراه با مشارکت پایین نهادهای امنیتی/حاکمیتی (R_{14})، محدودیت ظرفیت اتکایی (R_4)، ابهام در حدود پوشش و استثنائات جنگ (R_1) و ناهماهنگی مقرراتی (R_{15})، گره‌های بالادست و مداخله‌پذیر را شکل داد؛ درحالی‌که عدم‌تطابق پوشش با نیازها و ساختار امنیتی (R_{13})، محدودیت پوشش در حملات زنجیره‌ای (R_6) و ضعف خدمات پسارخداد (R_{12}) بیشتر به‌عنوان پیامد این فشارهای بالادستی ظاهر شدند.

مقایسه این نقشه با ادبیات نشان می‌دهد برجسته‌شدن ابهام قراردادی و استثنائات پرریسک (R_1)با یافته‌های کرمر و همکاران (۲۰۲۴)، جین و همکاران (۲۰۲۵) و هه و همکاران (۲۰۲۵) هم‌راستاست که نااطمینانی قراردادی را محرک افزایش ریسک حقوقی و کاهش تمایل به عرضه می‌دانند. قرار گرفتن R_2 در مرکز شبکه نیز شواهد تجربی تازه‌ای در تأیید نتایج بالسترا و همکاران (۲۰۲۴)، بردوپولوس (۲۰۲۵) و آدریکو و نرس (۲۰۲۴ب) است که کم‌بسندگی و ناهمگونی داده‌ها و خوشه‌ای‌بودن خسارت‌ها را چالش اصلی قیمت‌گذاری پایدار می‌شمرند؛ همان‌طور که نقش R_4، R_6 و R_7 با تصویر شبکه‌ای و سرایتی ریسک سایبری در آثار بیس و همکاران (۲۰۲۴)، مات و همکاران (۲۰۲۳)، پوتری (۲۰۲۵) و کلیمنته و لی (۲۰۲۵) سازگار است. در مقابل، وزن کمتر موانع رفتاری نسبت به تأکید آثار ایلینگ و یونگ (۲۰۲۵)، جوشی (۲۰۲۵) و کارانانته و مازوکولی (۲۰۲۵) نشان می‌دهد از منظر خبرگان، کانون مسئله بیش از آن‌که در سطح سوگیری‌های فردی باشد، در سطوح داده، مقررات، اتکایی و محیط نهادی قرار دارد. نوآوری مهم پژوهش، برجسته‌کردن دو مانع بومی ریسک ادراک‌شده افشای رخداد و اطلاعات حساس (R_{16}) و قیود ناشی از تحریم‌ها بر دسترسی به شرکای فنی و اتکایی بین‌المللی (R_{17})است که بُعد حاکمیتی–سیاسیِ خاص بازار ایران را به‌عنوان گره‌های علّی بالادست وارد نقشه موانع می‌کند.

بر پایه این خوانش شبکه‌ای، راهبرد توسعه بیمه سایبری می‌تواند حول سه محور بازطراحی شود: (۱) «داده و شفافیتِ کنترل‌شده» از طریق زیرساخت ملی ثبت و اشتراک‌گذاری خسارت، چارچوب‌های افشای ایمن و استانداردسازی شاخص‌های ریسک؛ (۲) «حکمرانی و تنظیم‌گری»

با هم‌راستاسازی مقررات بیمه‌ای و استانداردهای امنیت سایبری، بازنگری استثنائات پرریسک و تقویت نقش نهادهای امنیتی و حاکمیتی در پشتیبانی بازار؛ و (۳) «ظرفیت مالی و اتکایی» با تنوع‌بخشی شرکای اتکایی، تقویت ظرفیت‌های داخلی/منطقه‌ای توزیع ریسک و مدیریت آثار تحریم. در چنین بستری، بازطراحی پوشش‌ها متناسب با ساختار امنیتی بنگاه‌ها، سرمایه‌گذاری بر خدمات پسارخداد و توسعه بسته‌های مشترک «دفاع–بیمه» می‌تواند R_{13} و R_{12} را از عوامل بازدارنده به فرصت‌های تقویت اعتماد و تمایز رقابتی بدل کند. برای پژوهش‌های آتی، پیشنهاد می‌شود نقشه علّی به‌دست‌آمده با استفاده از مدل‌های پویایی سیستم و داده‌های واقعی خسارت سایبری، در قالب سناریوهای سیاستی مشخص (مانند بازنگری استثنائات، مشوق‌های افشا و تقویت ظرفیت اتکایی) شبیه‌سازی و ارزیابی شود. همچنین اجرای طرح‌های آزمایشی در صنایع منتخب و مقایسه تطبیقی با کشورهایی دارای محدودیت‌های نهادی و تحریمی مشابه، می‌تواند اعتبار بیرونی یافته‌ها و کارآمدی آن‌ها را در طراحی «برنامه ملی توسعه بیمه سایبری» به‌طور عینی محک بزند.

ملاحظات اخلاقی

حامی مالی: مقاله حامی مالی ندارد.

مشارکت نویسندگان: تمام نویسندگان در آماده‌سازی مقاله مشارکت داشته‌اند.

تعارض منافع: بنا بر اظهار نویسندگان در این مقاله هیچ‌گونه تعارض منافعی وجود ندارد.

تعهد کپی‌رایت: طبق تعهد نویسندگان حق کپی‌رایت رعایت شده‌است.

منابع

پیرالو، محمد؛ داناخو، حسن؛ عامری سیاهویی، حمید. (۱۴۰۴). چالش‌های بیمه سایبری. *پنجمین کنفرانس بین‌المللی تحقیقات پیشرفته در مدیریت و علوم انسانی*. https://civilica.com/doc/2325794

حسن پور، مجید؛ اولوخانی، نفیسه. (۱۴۰۰). شناسایی و اولویت‌بندی چالش‌های پیش روی بیمه سایبری در ایران. *بیست و هشتمین همایش بیمه و توسعه*. https://civilica.com/doc/1390777

صادقی، علی؛ اصغری اسکویی، محمدرضا. (۱۴۰۰). بررسی مدل‌های تخمین ریسک در بیمه سایبری. *بیست و هشتمین همایش بیمه و توسعه*. https://civilica.com/doc/1390872

فتاحی زفرقندی، س. (۱۴۰۲). بررسی تطبیقی قوانین بیمه سایبری. *اولین کنفرانس بین المللی حقوق، مدیریت، علوم تربیتی، روانشناسی و مدیریت برنامه‌ریزی آموزشی*. https://civilica.com/doc/1877044

نوبیتکس. (۱۴۰۴). *هک نوبیتکس: پاسخ به سؤالات کاربران از زبان مدیرعامل*. در ۲۵ تیر ۱۴۰۴، بازیابی‌شده از https://nobitex.ir/mag/nobitex-hack/

References

Adriko, R., & Nurse, J. R. (2024a). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. *Information & Computer Security*, *32*(5), 691-710. https://doi.org/10.1108/ICS-01-2024-0025

Adriko, R., & Nurse, J. R. (2024b). Does cyber insurance promote cyber security best practice? an analysis based on insurance application forms. *Digital Threats: Research and Practice*, *5*(3), 1-39. https://doi.org/10.1145/3676283

Allianz, S.E. (2025). *Allianz Risk Barometer 2025: Identifying the major business risks for 2025*. Allianz Global Corporate & Specialty. Retrieved February 23, 2026, from https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity Risks and Incidents Disclosure: A Literature Review. *Accounting Perspectives*, *24*(3), 605-667. https://doi.org/10.1111/1911-3838.12411

AXA. (2025). AXA Future Risks Report 2025. Retrieved February 23, 2026, from https://www.axa.com/en/news/future-risks-report?tab=future-risks-report-2025

Bace, B., Dubois, E., & Tatar, U. (2024). Resilience against Catastrophic Cyber Incidents: A Multistakeholder Analysis of Cyber Insurance. *Electronics*, *13*(14), 2768. https://doi.org/10.3390/electronics13142768

Ballestra, L. V., D'Amato, V., Fersini, P., Forte, S., & Greco, F. (2024). Pricing Cyber Insurance: A Geospatial Statistical Approach. *Applied Stochastic Models in Business and Industry*, *40*(5), 1365-1376. https://doi.org/10.1002/asmb.2891

Banerjee, S., & Das, S. (2024). Analyzing the Critical Challenges of Cyber Insurance Market: A Fuzzy DEMATEL Approach. *In Proceedings of the International Conference on Industrial Engineering and Operations Management*. https://doi.org/10.46254/EU07.20240258

Bardopoulos, J. (2025). Cyber-insurance pricing models. *British Actuarial Journal*, *30*, e6. https://doi.org/10.1017/S1357321724000205

Boonen, T. J., Feng, Y., & Tong, Z. (2025). Cybersecurity investments and cyber insurance purchases in a non-cooperative game. *ASTIN Bulletin: The Journal of the IAA*, *55*(2), 426-448. https://doi.org/10.1017/asb.2024.40

Carannante, M., & Mazzoccoli, A. (2025). An Analytical Review of Cyber Risk Management by Insurance Companies: A Mathematical Perspective. *Risks*, *13*(8), 144. https://doi.org/10.3390/risks13080144

Cimbru, I., Wagner, J., & Zeier Röschmann, A. (2025). On IoT-enabled risk prevention and insurance: A systematic literature review. *Risk Management and Insurance Review*. https://doi.org/10.1111/rmir.70025

Clemente, G. P., Cornaro, A., & Belvedere, S. (2025). Pricing Cyber Risk Insurance Coverages by Means of Epidemic Models and Network Theory. *Variance*, *18*. https://variancejournal.org/article/74729-pricing-cyber-risk-insurance-coverages-by-means-of-epidemic-models-and-network-theory

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Materne, S., & Murphy, F. (2024). Enhancing cyber insurance strategies: exploring reinsurance and alternative risk transfer approaches. *Journal of Cybersecurity*, *10*(1), tyae027. https://doi.org/10.1093/cybsec/tyae027

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. Computers & Security, 142, 103886. https://doi.org/10.1016/j.cose.2024.103886

Cybersecurity Ventures. (2025). *Cyberwarfare in the C-Suite 2025*. Retrieved February 23, 2026, from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/?hl=en-US

Eling, M., & Jung, K. (2025). Optimism bias and its impact on cyber risk management decisions. *Risk Sciences*, *1*, 100001. https://doi.org/10.1016/j.risk.2024.100001

Fattahi Zafarghandi, S. (2023). A comparative study of cyber insurance laws. *Proceedings of the 1st International Conference on Law, Management, Educational Sciences, Psychology, and Educational Planning Management.* https://civilica.com/doc/1877044 (in Persian)

Gómez, Y., Branley-Bell, D., Briggs, P., & Vila, J. (2025). Cyberinsurance adoption strategies and security of online behaviour: an experimental study. *Behaviour & Information Technology*, *44*(6), 1169-1182. https://doi.org/10.1080/0144929X.2025.2467891

Hamid, N. H. A. A., Mokhtar, M., Abd Manan, W. K. A. W., & Hashim, H. (2025). Exploring Critical Success Factors in Compliance-Driven Cyber Insurance within Malaysian Organizations: A COBIT 5 enabler approach. *Environment-Behaviour Proceedings Journal*, *10*(SI31), 77-84. https://doi.org/10.21834/e-bpj.v10iSI31.6936

Harel, Y., & Carmeli, A. (2025). A strategic cybersecurity oversight framework: a board's imperative. *Journal of Cybersecurity*, *11*(1), tyaf021. https://doi.org/10.1093/cybsec/tyaf021

Hasanpour, M., & Oloukhani, N. (2021). Identification and prioritization of challenges facing cyber insurance in Iran. *Proceedings of the 28th Insurance and Development Conference*. https://civilica.com/doc/1390777 (in Persian)

He, Q., Faure, M., & Chen, C. Y. (2025). Insuring the "uninsurable" cyberwarfare: rethinking war exclusions in cyber policies and the role of insurance in global cybersecurity governance. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 1-32. https://doi.org/10.1057/s41288-025-00346-3

Hui, W., Hui, K. L., & Yue, W. T. (2024). Cyber Insurance and Post-Breach Services: A Normative Analysis. *Service Science*, *16*(2), 124-141. https://doi.org/10.1287/serv.2021.0120

Jain, R., Hrle, T., & Woods, D. W. (2025). Insurance versus digital harm: a content analysis of home and cyber insurance policies in the USA and UK. *Journal of Cybersecurity*, *11*(1), tyae031. https://doi.org/10.1093/cybsec/tyae031

Joshi, C., Slapničar, S., Yang, J., & Ko, R. K. (2025). Contrasting the optimal resource allocation to cybersecurity controls and cyber insurance using prospect theory versus expected utility theory. *Computers & Security*, *154*, 104450. https://doi.org/10.1016/j.cose.2025.104450

Lefèvre, C., Tamturk, M., Utev, S., & Carenzo, M. (2024). Cyber Risk in Insurance: A Quantum Modeling. *Risks*, *12*(5), 83. https://doi.org/10.3390/risks12050083

Li, Y., Wang, X., Zhao, P., & Hu, T. (2025). Cyber breach risk modeling for insurance: capturing temporal and cross-group dependence. *Annals of Actuarial Science*, 1-25. https://doi.org/10.1017/S1748499525100109

Mott, G., Turner, S., Nurse, J. R., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security*, *128*, 103162. https://doi.org/10.1016/j.cose.2023.103162

Muktadir-Al-Mukit, D., & Ali, M. H. (2025). The dynamics of stock market responses following the cyber-attacks news: Evidence from event study. *Information Systems Frontiers*, 1-18. https://doi.org/10.1007/s10796-025-10639-6

Nobitex. (2025). *Nobitex hack: CEO answers users' questions* [Web page]. Retrieved February 23, 2026, from https://nobitex.ir/mag/nobitex-hack/

Piralou, M., Danakhoo, H., & Ameri Siahuei, H. (2025). Challenges of cyber insurance. *Proceedings of the 5th International Conference on Advanced Research in Management and Humanities*. https://civilica.com/doc/2325794 (in Persian)

Puteri, N. K., Kusnadi, F., & Kristiani, F. (2025). Cybersecurity Insurance Modeling Using Archimedean Copulas. *Science & Technology Asia*, 177-188. https://doi.10.14456/scitechasia.2025.11

Sadeghi, A., & Asghari Eskouei, M. R. (2021). A review of risk estimation models in cyber insurance. Proceedings of the 28th Insurance and Development Conference. https://civilica.com/doc/1390872 (in Persian)

Schütz, F., Rampold, F., Kalisch, A., & Masuch, K. (2023). Consumer cyber insurance as risk transfer: a coverage analysis. *Procedia Computer Science*, *219*, 521-528. https://doi.org/10.1016/j.procs.2023.01.320

Skeoch, H. R., & Ioannidis, C. (2024). The barriers to sustainable risk transfer in the cyber-insurance market. *Journal of Cybersecurity*, *10*(1), tyae003. https://doi.org/10.1093/cybsec/tyae003

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. *International*

Journal of Information Security, *22*(3), 737-748. https://doi.org/10.1007/s10207-023-00660-8

Woods, D. W., & Wolff, J. (2025). A history of cyber risk transfer. *Journal of Cybersecurity*, *11*(1), tyae028. https://doi.org/10.1093/cybsec/tyae028

World Bank. (2025). *GDP (current US$) – China [NY.GDP.MKTP.CD]*. World Development Indicators. Retrieved from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CN

Zhao, A. P., Fei, F. X., & Alhazmi, M. (2024). Cyber Insurance for Energy Economic Risks. *Smart Cities (2624-6511)*, *7*(4). https://doi.org/10.3390/smartcities7040081

Zhao, A. P., Gu, C., Bao, Z., Cheng, X., & Alhazmi, M. (2025). Optimizing Cyber Insurance and Defense for Multi-Energy Systems Under False Data Injections. *IET Renewable Power Generation*, *19*(1), e70011. https://doi.org/10.1049/rpg2.70011

COPYRIGHTS

This license allows others to download the works and share them with others as long as they credit them, but they can’t change them in any way or use them commercially.