Insuring Data Risks: Problems and Solutions

Mamanazarov Sardor Shukhratovich
Tashkent State University of Law
sardormamanazarov@gmail.com
ORCID: 0009-0004-5855-6498

Abstract

The proliferation of valuable data assets and connectivity in the digital economy has been accompanied by intensifying cyber risks. However, systemic constraints including data ambiguities, legal uncertainty, and misaligned incentives have severely limited advancement of cyber insurance coverage relative to rising enterprise protection needs. This research provides a comprehensive analysis of key bottlenecks inhibiting cyber data risk insurability. It examines constraints stemming from historical data deficiencies, risk modeling complexities, opaque controls, and fragmented regulatory regimes. The study also evaluates internal challenges faced by insurers in advancing policies like claims ambiguities, talent gaps, and reliance on primitive actuarial techniques. It further proposes targeted legal, risk management and public-private partnership enhancements that can expand viable transfer of cyber data risks. These include graduated security frameworks, transparent data exchanges, resilience incentives, risk pooling structures and international cooperation. With balanced reforms, cyber insurance can systematically enable enterprises to secure data assets commensurate with their rising economic and societal value.

Keywords: Cyber Insurance, Data Risks, Cybersecurity, Risk Management, Resilience, Insurance Regulation, Risk Modeling

I. Introduction

The exponential growth of data generation and collection around the world has led to immense economic benefits, but also created novel systemic risks related to data security, integrity, and privacy. Recent years have witnessed an alarming rise in the frequency and impact of cyber incidents targeting organizational and consumer data assets globally. According to emerging loss trends, the average total cost of a data breach has risen to $4.35 million in 2021, representing a nearly 13% year-over-year increase. Experts have attributed these cost escalations to factors like more stringent data protection regulations, the shift to remote work during the pandemic, and the increasing sophistication of threat actors.[1]

[1] Khatamjonova, G. (2023). Xalqaro Xususiy Huquqda Erk Muxtoriyati (Party Autonomy) Prinsipining Konseptual Rivojlanishi. *International Journal of Law and Policy*, 1(2). https://doi.org/10.59022/ijlp.35

While traditional cyber insurance policies cover certain first and third party costs from security incidents, underwriters have been conservative in embracing new data risks like those stemming from artificial intelligence systems, cryptocurrencies, smart cities, and systemic data supply chain compromises. The absence of robust historical actuarial data regarding advanced persistent threats, coupled with ambiguities in emerging legal liability frameworks for data-related harms, have made reliable risk modeling and pricing difficult. Consequently, many organizations today are left exposed to potentially catastrophic data risks falling in the gaps between new digital realities and legacy insurance coverage constructs.[2]

This research seeks to provide a comprehensive analysis of the key technological, regulatory, and insurance market structure challenges inhibiting adequate transfer of intensifying data risks. It aims to illuminate the constraints on insurers in closing existing coverage gaps, while also evaluating possible legal, risk management, and public-private partnership enhancements needed to enable expanded cyber data risk protection globally. The study strives to synthesize perspectives across stakeholders encompassing cyber underwriters, brokers, lawyers, technologists, regulators, and enterprise risk managers to develop a systemic roadmap for strengthening the cyber insurance ecosystem.[3]

II. Methodology

This study employs a mixed methods approach encompassing both qualitative and quantitative analyses to holistically examine the insurability challenges associated with advancing data risks in the digital era. The qualitative research entails an extensive review of cyber insurance policy documents across both affirmative and non-affirmative covers focused on analyzing exclusions, limitations, and conditionality's that could inhibit claims payments after incidents. Particular attention is devoted to evaluating coverage provisions related to data restoration, network business interruption, cyber extortion, media liability, crisis management, and legal liability which represent critical costs during response and recovery phases.[4]

Beyond insurance agreements, the qualitative study also examines relevant case law, regulatory directives, legislative acts, industry risk management frameworks, and cybersecurity technical standards. For instance, analysis of legal

[2] Yulduz , A. (2023). Dealing with the Challenge of Climate Change within the Legal Framework of the WTO. *International Journal of Law and Policy*, 1(2). https://doi.org/10.59022/ijlp.31

[3] Ergashev, M. (2023). Global Transfer of Bitcoins from One Party to Another. *International Journal of Law and Policy*, 1(2). https://doi.org/10.59022/ijlp.34

[4] Allah Rakha, N. (2023). Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices. *International Journal of Law and Policy*, 1(3). https://doi.org/10.59022/ijlp.43

liability precedents will illuminate gaps in jurisprudence addressing harms like ransomware attacks, systemic data supply chain compromises, and failures of AI systems. Evaluating cybersecurity policy and legal environments across key countries like the United States, China, the United Kingdom, Japan, and members of the European Union facilitates identification of jurisdictional inconsistencies that hinder advancement of cyber insurance recoverability constructs.[5]

To provide empirical grounding, the research also leverages insurance industry data on cyber premiums, losses, and claims rejection rates across segments like healthcare, retail, manufacturing, financial services, and critical infrastructure. Statistical analysis of longitudinal loss trends enables assessment of aggregations in interconnected portfolios which poses systemic solvency risks for carriers. The quantitative component also entails distributional analysis of cyber insurance penetration and density rates across firm revenue and sectoral categories. This facilitates evidence-based conclusions regarding current coverage adequacies vis-à-vis intensifying cyber risk landscapes organizations face.[6]

Together, the multi-pronged qualitative and quantitative analyses will provide a comprehensive perspective on limitations in today's data risk protection safety nets. The research synthesizes insights from legal, technical, and insurance vantage points to propose targeted reforms that balance the objectives of expanding insurability while also maintaining stable insurance economics. Recommended enhancements account for constraints stemming from profitability pressures, controls fragmentation, information asymmetries, and misaligned incentives between cyber insurers and their policyholders.[7]

III. Results

A. Insuring Data Risks: Problems and Solutions

1. Insurmountability challenges for advancing data risk protection

The intensifying frequency and severity of cyber incidents targeting organizational data assets has highlighted systemic limitations in transferring such emerging risks through conventional insurance constructs. Constraints stemming from historical data deficiencies, legal uncertainty, risk modeling complexities, information asymmetries, and misaligned incentives have severely inhibited

[5] Allah Rakha, N. (2023). Exploring the Role of Block-chain Technology in Strengthening International Legal Guarantees for Investment Activity. *International Journal of Law and Policy*, 1(3). https://doi.org/10.59022/ijlp.37

[6] Utegenov Ongarbay Dariyabayevichc. (2023). A Comprehensive Analysis of Ecological Law in the Cyber Era. *International Journal of Law and Policy*, 1(4). https://doi.org/10.59022/ijlp.58

[7] Xudaybergenov, A. (2023). Toward Legal Recognition of Artificial Intelligence Proposals for Limited Subject of law Status. *International Journal of Law and Policy*, 1(4). https://doi.org/10.59022/ijlp.55

underwriting profitability for new age data exposures. Consequently, multiple challenges have arisen in expanding insurability to match the widening protection needs of entities increasingly threatened by cyber-attacks on their sensitive information, networks, and connected technologies.[8]

2. Absence of historical actuarial data for novel exposures

Unlike traditional property and casualty risks, the fundamentally new and rapidly advancing nature of cyber data hazards has meant absence of robust historical claims experience data to facilitate pricing and reserving decisions by insurers. For instance, nascent technologies like Internet of Things, artificial intelligence, cryptocurrencies, and quantum computing lack longitudinal loss observations which are prerequisite inputs for actuaries to quantify event likelihoods, severities, and correlations. The clandestine and asymmetric nature of cyber-attacks has also limited forensic visibility into causative factors underlying major breaches, impeding detailed risk Differentiation. The resulting uncertainty has necessitated heavy dependence on subjective expert judgment for cyber risk assessments, leading to volatility in premiums amidst evolving threat landscapes. Such constraints have dampened underwriter confidence in achieving profitable economics over the long-term for data risk covers.[9]

3. Ambiguity in legal liability frameworks

The absence of well-established legal liability precedents and statutory guidelines addressing data security harms has further discouraged insurer capacity for new data risk categories. For instance, jurisprudence remains inconsistent globally in determining organizational duties for preventing different cyber-incidents and also calculating resultant damages eligible for victim compensation. Key questions on issues like liability caps, minimum security standards, and accountability thresholds for aggregated or inherited risks within digital ecosystems continue to lack definitive guidance through case laws or regulations in most countries. Such legal uncertainty regarding evolving cyber data harm liabilities has constrained insurers' ability to reliably model maximum loss exposures. It has also increased potentials of litigation against carriers attempting to deny questionable claims after incidents. The resulting profitability concerns

[8] Ruslan, S. (2023). Challenges and Opportunities for Legal Practice and the Legal Profession in the Cyber Age. *International Journal of Law and Policy*, 1(4). https://doi.org/10.59022/ijlp.59

[9] AllahRakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, 16(2), 23-54.

have constrained advancement of cyber risk solutions for emergent data vulnerabilities.[10]

4. Complexity in modeling systemic risks

The increasing interconnections between entities and technologies in modern digital environments has exponentially amplified systemic contagion and cascading implications from cyber-attacks on particular data assets. However, the complexity in modeling butterfly effects and risk correlations across IT networks, cloud service dependencies, and automated software ecosystems poses significant challenges for underwriters. Actuarial techniques traditionally relied upon to quantify aggregation risks for natural catastrophes, financial crises, and other systemic loss events remain primitive when it comes to cyber data exposures. Difficulties in tracing causations across incidents and lack of shared historical data further impedes insurers' ability to simulate sufficient stress test scenarios to capture systemic data breach risks. Consequently, major global cyber events entailing billions in economic costs like the 2017 NotPetya and the 2020 SolarWinds attacks highlighted catastrophic protection gaps even for organizations with seemingly adequate cyber.[11]

5. Limited transparency into cyber controls

The largely intangible nature of data assets and their security has meant customer cyber risk profiles perceived by underwriters during policy issuance often diverge from actual risk levels leading to incidents down the road. Unlike physical property risks, constant changes to enterprise IT environments and governance frameworks make it difficult for insurers to monitor ongoing efficacy of cybersecurity controls within policyholders' systems. Current cyber insurance processes also rely heavily upon self-reported controls questionnaires which can suffer from subjectivity and disclosures gaps due to confidentiality concerns or misaligned customer incentives. Resulting information asymmetries and adverse selection risks contribute to carriers struggling to accurately price policies ex-ante relative to actual cyber risk levels. This necessitates conservative underwriting to protect profit margins amidst opaque cyber data environments at customers.[12]

6. Gaps in cybersecurity compliance certifications

[10] Ubaydullayeva, A. (2023). Artificial Intelligence and Intellectual Property: Navigating the Complexities of Cyber Law. International Journal of Law and Policy, 1(4). https://doi.org/10.59022/ijlp.57

[11] Ollanazarova Mamura Muzaffarovna. (2023). Analyzing the Legal Labyrinth: Current Trends in Genetic Research and Their Legal Perspectives. *International Journal of Law and Policy*, 1(5). https://doi.org/10.59022/ijlp.84

[12] Muxammadiyev Sindorbek Bobirjon o'g'li. (2023). Complexities of International Arbitrator Liability: A Comparative Analysis and the Case for Qualified Immunity. *International Journal of Law and Policy*, 1(5). https://doi.org/10.59022/ijlp.46

While risk-based premiums tied to auditable cybersecurity frameworks can partly help overcome limited transparency challenges, inconsistencies in existing compliance certification regimes also constrain underwriting progress. Except select sectors like finance and healthcare, most industries currently lack mandated baseline cybersecurity standards and supervision processes globally. Voluntary frameworks like ISO 27001, NIST CSF, and CSA STAR provide useful but fragmented guidance focused on limited control dimensions. And certification schemes like SOC 2 and the European Data Protection Seal remain young with variable assessment rigor and adoption outside niche sectors so far. Such gaps in standardized cybersecurity benchmarks hinder insurers' ability to assess relative risk levels across customers and reward improved controls through coverage terms. It thereby restricts advancement of affirmative and graduated cyber insurance solutions.[13]

7. Financial constraints for potential victims

The significant upfront investments needed to assess, implement, and sustain adequate cybersecurity protections remain out of reach for many small and mid-sized organizations which nonetheless face similar data breach risks like larger entities. At the same time, the considerable costs involved in post-incident responses including legal liability settlements, regulatory fines, technical recovery, and reputational damage repairs also often exceed the limited balance sheet capacities of smaller firms. However, current market dynamics disincentivize insurers from offering comprehensive and affordable cyber covers for such customers due to concerns about moral hazard risks exacerbating claims costs. The resulting protection gaps leave such organizations highly vulnerable to even survive existential data security events. Their residual exposures also contribute to the aggregations risks in insurers' portfolios.[14]

8. Low incentives for proactive cyber risk management

The pricing dynamics in the cyber insurance market today focuses overwhelmingly on indicators like company sizes, revenues, and past breach incidents when assessing customers' risk levels. However, this fails to provide sufficient differentiation for policyholders' widely varying internal cybersecurity maturity. There are limited incentives or credit for organizations proactively minimizing risks through measures like vulnerability testing, IT infrastructure upgrades, and employee training which could significantly reduce insurers' loss

[13] Allah Rakha, N. (2023). The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. *International Journal of Law and Policy*, 1(1). https://doi.org/10.59022/ijlp.23

[14] Allah Rakha, N. (2023). Artificial Intelligence strategy of the Uzbekistan: Policy framework, Preferences, and challenges. *International Journal of Law and Policy*, 1(1). https://doi.org/10.59022/ijlp.27

exposures. As a result, many enterprises just seek to transfer residual risk through insurance rather than prioritizing continuous cyber risk reduction - creating moral hazard costs for underwriters. The lack of partnerships between carriers and policyholders in cyber risk mitigation thereby remains a key barrier to growth in cyber insurance protections.[15]

9. Reluctance sharing confidential data

Organizations are often justifiably reluctant in providing detailed forensics on previous breaches or complete network architectures to external parties including cyber insurers during policy procurement, due to concerns over reputation, liability, and further data security risks from potential confidential data leakage. However, such disclosures constraints significantly impede underwriters' ability to accurately evaluate customers' cyber risk postures and exposures. It necessitates them to depend on limited self-reported controls details and generic sectoral risk assumptions flowing insufficient risk segmentation granularity in pricing. The resulting adverse selection risks require insurers to utilize conservative underwriting standards to protect profitability, thereby hindering access to adequate and affordable cyber data risk transfer solutions for many customers.[16]

10. Jurisdictional inconsistencies in liability awards

Current legal landscapes related to cybersecurity duties, liabilities, and victim compensation remain highly fragmented across different countries globally. Local laws, regulations, case law precedents, and sectoral compliance mandates leading to material inconsistencies in interpreting organizational accountability and awarding damages after major data breaches. For instance, privacy violation penalties in Europe GDPR framework can go up to 4% of global revenues while the US healthcare sector sees significantly higher legal settlements under HIPAA regulations compared to other industries for compromised personal health data. Such jurisdictional variabilities in liability outcomes significantly complicates reliable estimation of the cyber claims costs distributions and maximum possible exposures for global insurance carriers. It thereby necessitates localization

[15] Babaev Isa. (2023). Integrating System Analysis, Information Management, and Decision-Making: Legal Perspectives and Challenges. *International Journal of Law and Policy*, 1(5). https://doi.org/10.59022/ijlp.85

[16] Laylo, K. (2023). The Impact of AI and Information Technologies on Islamic Charity (Zakat): Modern Solutions for Efficient Distribution. *International Journal of Law and Policy*, 1(5). https://doi.org/10.59022/ijlp.83

constraints on underwritten cyber insurance limits provided in respective markets to avoid catastrophic losses.[17]

11.Lack of cyber underwriting expertise

The profound technical complexities and rapidly evolving nature of cyber risk landscapes have greatly limited the availability of insurance talent with adequate expertise to perform advanced data risk modeling, underwriting, and claims handling. The niche nature of the exposures and confidentiality constraints has also hindered detailed sharing of historical breaches data further dampening opportunities for actuaries to hone skills through on-the-job learning or classroom trainings. High turnover rates for existing cyber underwriters attracted to new startups or technology vendors have further depleted incumbents' internal talent pools and loss data repositories further. Without concerted public-private investments in cyber insurance knowledge ecosystems, the talent bottlenecks are likely to persist as a key barrier to growth in risk-based underwriting capacities across the industry.[18]

12.Insurer limitations in closing coverage gaps

While systemic constraints like data ambiguities and legal uncertainties have dampened underwriter risk appetites, insurers also face internal challenges in their ability to close emerging cyber data protection gaps. Factors including limited loss assessment capabilities, risk aggregation issues, reinsurance dependencies, and channel incentive misalignments have further contributed to gaps between intensifying enterprise cyber risks and coverages currently offered in the market. A holistic examination of cyber insurance dynamics must synthesize both external ecosystem bottlenecks and internal carrier capability constraints to identify solutions for expanding data risk insurability.[19]

13.Constraints on breach loss assessments

A key prerequisite for insurers in paying out claims is precise estimation of covered losses suffered by the policyholder organization from a cyber-attack. However, accurately attributing impacted business income across integrated systems, untangling event causation sequences across incidents, and isolating insured peril factors from broader management failures often proves complex for

[17] Bayzakova Diana Bakhtiyorovna. (2023). Legal Regulation of Foreign Investment Regime in the Oil and Gas Sector of Uzbekistan. *International Journal of Law and Policy*, 1(6). https://doi.org/10.59022/ijlp.99

[18] Bekmirzaeva, U. (2023). The Evolution of Investment Standards: A Comparative Analysis of the New Edition of the Law of the Republic of Uzbekistan on Investments and Investment Activity. *International Journal of Law and Policy*, 1(6). https://doi.org/10.59022/ijlp.97

[19] Sharopov, R. (2023). Behavioral Law and Antitrust Legislation in the Agro-Industrial Complex: Interconnection, Challenges, and Solutions. *International Journal of Law and Policy*, 1(6). https://doi.org/10.59022/ijlp.98

cyber-attacks. Data integrity challenges also arise in validating compromised records volumes when determining costs like customer notification expenses and legal liability exposures after large-scale breaches. Such ambiguities in quantifying covered cyber incident damages increase disputes between policyholders and carriers leading to delays or claim denials that exacerbate protection gaps even for entities with active cyber insurance covers.[20]

14.Premium controls and risk appetite limitations

As profit-driven entities, insurers have to maintain disciplined risk appetites and underwriting standards aligned to their loss assessment capabilities, capital buffers, and reinsurance availabilities regardless of wider market dynamics. However, the absence of mandated cybersecurity baselines and intensifying regulatory pressures constrains carriers' ability to raise premiums adequately relative to deteriorating cyber risk landscapes and inflating breach costs. Resulting constraints on underwriting capacities increase exclusions and conditionalities within cyber policies, magnifying gaps in coverages relative to enterprise cyber risk spectrums. Without balanced public-private partnerships to enhance safety nets, such insurer constraints will persist as barriers to insurability expansion.[21]

15.Cyber risk interconnections and aggregations

The highly interconnected digital ecosystems in modern economies greatly magnify systemic contagion and cascading implications from cyber-attacks focused on particular high-value data targets. However, most insurers have limited visibility into the dependencies and risk correlations across their policyholders to reliably estimate aggregations potential. The predominant firm-level underwriting techniques also fail to model or price risks flowing across interconnected entities. The resulting exposure underestimations became evident in the wide-scale business interruptions and losses triggered across sectors by systemic hacks like NotPetya, Colonial Pipeline and SolarWinds even when individual companies had cyber coverage.[22]

IV. Discussion

A. Addressing such Data Contagion Risks Necessitates Fundamentally New Cyber Risk Pooling and Diversification Approaches.

1. Reliance on reinsurance support

[20] Abduvalieva Mumtozkhan Asilbekovna. (2023). Comparative Analysis of International Standards for the Protection of Persons with Disabilities and National Legal Norms. *International Journal of Law and Policy*, 1(6). https://doi.org/10.59022/ijlp.96

[21] Gulyamov, S., & Raimberdiyev, S. (2023). Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*, 1(7). https://doi.org/10.59022/ijlp.119

[22] AllahRakha, N. (2023). Legal Challenges for International Fintech Startups. *International Journal of Law and Policy*, 1(8). https://doi.org/10.59022/ijlp.148

Most insurers aim to transfer portions of their concentrated cyber risk exposures to secure capacitive and economic stability through reinsurance markets. However, ambiguities in cyber data and systemic risk models also constrain the risk appetites of reinsurers to back untested exposures at competitive costs. Their support is also contingent on primary carriers implementing sufficient underwriting controls.[23]

2. Industry fragmentation and risk pooling barriers

The cyber insurance sector today remains highly fragmented with the top 10 carriers accounting for less than 60% of the global market share. The absence of centralized data repositories and risk analytics capabilities makes most insurers dependent on their own experience which remains limited compared to aggregate industry loss footprints. Such fragmented risk visibility and modeling capabilities reduce insurers' ability to diversify exposures through risk pooling and hinders advancement of policies tailored to distinct customer segments. It also allows adverse selection risks to manifest when high-risk entities are able to circumvent controls by moving across different underwriters.[24]

3. Channel incentive misalignments on cyber insurance

While insurers aim for cyber risk reduction and resilient underwriting, channels like brokers and agents are still incentivized predominantly to maximize policy sales which may not align with enhanced customer cybersecurity. Gaps also exist between chief information security officers seeking security advances and chief financial officers focused on securing budget efficiencies. Such misalignments contribute to continued reactive purchasing of cyber policies for residual risk transfer rather than proactive risk reduction. It necessitates public-private collaborations to create ecosystems wherein cyber insurers become trusted partners to their policyholders rather than just vendors of protection products.[25]

4. Dependence on reactive security signals in underwriting

Currently, most cyber underwriting reliance heavily on indicators like past breach incidents, total data stores, and revenue sizes to categorize customers into risk segments. However, markers of policyholders' forward-looking security postures like controls efficacy improvements, vulnerability management, and cyber

[23] Ahmadjonov, M. (2023). Anti-Corruption and Compliance Control: Legal Literacy among Lawyers and Law Students. *International Journal of Law and Policy*, 1(8). https://doi.org/10.59022/ijlp.145

[24] Abdikhakimov, I. (2023). Jurisdiction over Transnational Quantum Networks. *International Journal of Law and Policy*, 1(8). https://doi.org/10.59022/ijlp.147

[25] AllahRakha, N. (2024). Rethinking Digital Borders to Address Jurisdiction and Governance in the Global Digital Economy. *International Journal of Law and Policy*, 2(1). https://doi.org/10.59022/ijlp.124

hygiene rarely factor into pricing models. This limits the value insurers can provide in strengthening cyber resilience. It also hampers risk reflection, as entities with similar histories but widely differing control frameworks are treated homogenously in underwriting assessments. Tight partnerships to allow underwriters continuous visibility into clients' changing risk exposure levels are critical to advancing cyber insurance protections.[26]

5. Coverage constraints for emergent technology risks

While cyber risks from emerging technologies like cryptocurrencies, Internet-of-Things, and augmented reality platforms are rising, insurers have been constrained in developing dedicated solutions to adequately transfer such exposures. Challenges like the anonymity and irreversibility of blockchain transactions, systemic risks of coordinated edge device hacks, and liability ambiguities for failures in AI systems have made reliable underwriting difficult. However, abrupt regulatory shifts like the EU AI Act necessitate urgent enhancements in insurability frameworks to foster innovation in such technologies responsibly. Constructive public-private dialogues to balance risk management and tech advancement objectives are vital to manage uncertainties.[27]

6. Advancing legal & risk management frameworks

While systemic constraints have contributed to cyber insurability gaps, constructive evolution of risk management and regulatory regimes can help strengthen the overall data protection ecosystem. A collaborative approach is needed between public and private sector stakeholders to implement targeted reforms that motivate proactive security while also enabling viable risk transfer solutions.[28]

7. Stratify controls standards tied to liability caps

An internationally coordinated public-private initiative can establish graduated cybersecurity frameworks tuned to different industry contexts with embedded liability caps tied to certified tiers of controls efficacy, resilience testing, and executive accountability. Such frameworks can mandate baseline data security standards for organizations based on risk profiles while capping liabilities for certified firms meeting advanced control requirements. This balances the objectives of improving protections and providing legal certainty for entities

[26] Ubaydullaeva, A. (2024). Rights to Digital Databases. *International Journal of Law and Policy*, 2(1). https://doi.org/10.59022/ijlp.151

[27] Cupi, D. (2024). The Role of the Albanian Media as Mediator and Creator of Collective Memory. *International Journal of Law and Policy*, 2(1). https://doi.org/10.59022/ijlp.146

[28] Murodullaev, D. (2024). Problems of Application of Termination of Employment Contract due to Circumstances beyond the Control of the Parties . *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.155

proactively managing risks. Indexed liability caps also offer insurers a reliable mechanism to model maximum exposures at underwriting.[29]

8. Mandate disclosures for priority sectors

Regulations can mandate expedited and detailed disclosures of cyber incidents as well as periodic transparency reports on security protocols effectiveness for public and private firms in critical infrastructure sectors. Clean information sharing channels with trusted government agencies can be reciprocated through intelligence warnings, sans legal penalties. Such transparency frameworks targeted to priority sectors with systemic risks can aid better loss analytics by insurers while also improving oversight of cyber hygiene. Policymakers must however adopt strong confidentiality safeguards and liability shields to secure buy-in from enterprises.[30]

9. Develop cyber risk data exchanges

Industry associations can establish anonymized pools of historical incident data enriched with cyber control efficacy signals and technology audit benchmarks. Structured data taxonomies and consistent reporting templates will be key to enhancing model value. Strict access controls for participants like accredited insurers, reinsurers, brokers and vetted third-party cyber auditors can be instituted, alongside multiparty confidentiality agreements. Such credible cyber risk data exchanges can significantly improve loss model reliability while also providing technology benchmarking visibility for enterprises.[31]

10. Incentivize cyber resilience certification

Governments can subsidize adoption of advanced cyber resilience and infrastructure stress testing certification schemes aligned to established technical standards like the Cyber Resilience Review process. Cost offsets for small businesses to undertake virtual CISO-led reviews, penetration testing, cyber range simulations etc can be tied to mandatory public disclosures to create transparency market signals incentivizing tech robustness. Such resilience certifications can

[29] Soyipov, K. (2024). Features of Termination of an Employment Contract at the Initiative of the Employer: Uzbekistan's Case. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.153

[30] Karimjonov, M. (2024). A Disciplinary Responsibility by the New Labor Legislation of the Republic of Uzbekistan. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.158

[31] AllahRakha, N. (2024). Transformation of Crimes (Cybercrimes) in Digital Age. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.156

inform graduated pricing and accumulated risk management by insurers for enterprises going beyond barebones compliance.[32]

11.Promote data integrity validation techniques

Industry consortiums can design blockchains, distributed ledgers and immutable data stores for multi-party recording of sensitive transactions, data transfers and system access logs across public-private ecosystems. Consensus-based integrity validations will enhance forensic visibility and attribution for cyber-attacks. It will also enable reliable data damage quantification for insurers post incidents. Anonymized metadata can be shared securely with cyber insurers to aid analytics. Policymakers will need to reform dated record retention and liability rules to enable adoption.[33]

12.Standardize cybersecurity legal expertise

Associations of cyber insurers, attorneys, forensic investigators and technology auditors can institute standardized professional education programs, certifications, ethical codes, and continuing expertise mandates. Such accreditation frameworks can accelerate capacity building for global cybersecurity jurisprudence, contracts, and evidence management. It will foster professional standards needed for modern cyber litigation and insurance claims assessments. Public-private centers of excellence can also be set up to train investigators and prosecutors on pursuing cybercrime.[34]

13.Distinguish state-sponsored threat liability

International public-private taskforces consisting of law enforcement, intelligence, and industry experts should aim to formulate precise definitions and tests for distinguishing cyber-attacks with nation-state backing versus criminal threats. A high evidentiary standard like beyond reasonable doubt should be set for any exclusions from cyber policies, along with mandatory conciliation before disputes. This will balance underwriting viability with policyholder protection against arbitrary cyberwar attribution by insurers after commonplace incidents.[35]

14.Foster cyber risk pooling and diversification

---

[32] Ismoilov, S. (2024). What is the Importance of Entering into a Non-Compete Agreement?. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.159

[33] Rakhimov, M. (2024). The Principles of the Classical Theory of Labor Law. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.157

[34] AllahRakha, Naeem, Modernizing Criminal and Evidence Laws to Facilitate Tourism in Pakistan. Available at *SSRN*: https://ssrn.com/abstract=4707544 or http://dx.doi.org/10.2139/ssrn.4707544

[35] Bakhramova, M. (2024). Harmonization of the Legal Framework for Online Arbitration. *International Journal of Law and Policy*, 2(2). https://doi.org/10.59022/ijlp.154

Policymakers should assess models like the US Terrorism Risk Insurance Program which created a public-private risk pool along with a temporary government reinsurance backstop to expand insurability for a systemic and ambiguous emerging threat category. Similar national cyber risk diversification structures can help build out cyber insurance capacity until private reinsurance markets mature. Mandatory cross-border participation can also aid global stability. Such pooling mechanisms can be funded through levies on firms based on revenues, cyber maturity levels and criticality.[36]

15.Explore cyber reinsurance treaties

Global associations of insurers and reinsurers should explore feasibility of pandemic-style systemic risk treaties for catastrophic cyber-attacks or threat scenarios like cyber BI events or infrastructure grid failures impacting interconnected economies. Pooled buffer capital reserves can be maintained in special purpose vehicles domiciled neutral jurisdictions, invested safely to sustain claims. Pre-agreed thresholds and trigger tests will need to be formulated through open industry dialogues. While complex, such multi-country solidarity mechanisms are vital to improving cyber resilience safety nets.[37]

Conclusion

The proliferation of data generation and connectivity in the digital economy has been accompanied by systemic risks from cyber-attacks targeting organizational information assets, technologies, and network interactions. However, examination of the cyber insurance sector that has emerged to transfer such risks highlights significant constraints in expanding protection to match intensifying enterprise exposures. Limitations including ambiguities in new age risks like AI and cryptocurrencies, legal uncertainty regarding evolving cyber harms, opacity of policyholders' controls, systemic contagion across interconnected entities, and misalignments of incentives have severely inhibited underwriting profitability and capacity for comprehensive cyber data risk transfer solutions.

At the same time, internal constraints like claims assessment challenges, dependence on primitive actuarial models, capital limitations, and fragmented data access have also hampered insurers' ability to keep pace with rapid risk advancements. Public-private collaborations are imperative to implement targeted legal and risk management reforms that can expand cyber insurability while also

[36] Saidakhror, G. (2024). The Impact of Artificial Intelligence on Higher Education and the Economics of Information Technology. *International Journal of Law and Policy*, 2(3), 1–6. https://doi.org/10.59022/ijlp.125

[37] Mamanazarov, S. (2024). Intellectual Property Theories as Applied to Big Data. *International Journal of Law and Policy*, 1(7). https://doi.org/10.59022/ijlp.164

maintaining stable insurance economics. Introducing graduated frameworks that mandate minimum controls for organizations based on risk profiles while capping liability for proactive adopters can incentivize cyber resilience. Focused transparency mandates for critical infrastructure sectors, development of anonymized cyber risk data exchanges, and certification of cybersecurity legal expertise will also foster more accurate underwriting and claims assessments.

Exploring innovative risk pooling structures akin to terrorism insurance programs can enable diversification of ambiguity laden systemic cyber risk concentrations currently constrained by individual insurers' balance sheet and data limitations. And international initiatives to formulate precise definitions and evidentiary thresholds for narrow cyberwar exclusions are needed to prevent disputes over arbitrary attribution of state sponsorship to commonplace attacks. Of course, care must be taken to ensure regulatory interventions balance prescriptiveness with flexibility for insurer innovation. And public backstops or subsidies should only temporarily fill critical gaps rather than clouding market discipline. But thoughtful cooperation to enhance cyber protection ecosystems will be vital as the global economy enters an era of unprecedented data interconnections and vulnerabilities.

This research study provided a detailed analysis of key bottlenecks inhibiting advancement of cyber data risk insurability and examined potential legal, policy, governance, and partnership interventions that can systematically address the constraints. Significant opportunities exist for synergistic capacity building across insurers, regulators, enterprises, technology vendors and research institutions to enable adequate risk transfer solutions commensurate with the growing role of data as an economic asset requiring robust security. The proposed roadmap encompassing graduated control standards, transparent data exchanges, proactive resilience incentives, enhanced forensics, risk pooling structures and international cooperation provides constructive pathways. Of course, further actuarial, empirical, and experimental research will be essential to refine approaches balancing risk management and innovation within unique jurisdictional and industrial realities across the world.

But collective action is clearly needed to reform outdated paradigms and enable expanded insurability for enterprises seeking security commensurate with the valuable data entrusted to them by customers, regulators and partners. This study also reiterates that managing cyber data risks fundamentally necessitates a shared responsibility paradigm. Insurers must strengthen partnerships with policyholders to reward proactive protection, regulators must mandate baseline controls without stifling markets, and enterprises must invest in resilience rather than just insurance. With collaborative action, cyber risk protection frameworks can keep pace with the exponential advancement of data as a strategic economic

asset and public trust pillar of the digital transformation era.

References

Khatamjonova, G. (2023). Xalqaro Xususiy Huquqda Erk Muxtoriyati (Party Autonomy) Prinsipining Konseptual Rivojlanishi. *International Journal of Law and Policy*, *1*(2). https://doi.org/10.59022/ijlp.35

Yulduz , A. (2023). Dealing with the Challenge of Climate Change within the Legal Framework of the WTO. *International Journal of Law and Policy*, *1*(2). https://doi.org/10.59022/ijlp.31

Ergashev, M. (2023). Global Transfer of Bitcoins from One Party to Another. *International Journal of Law and Policy*, *1*(2). https://doi.org/10.59022/ijlp.34

Allah Rakha, N. (2023). Ensuring Cyber-security in Remote Workforce: Legal Implications and International Best Practices. *International Journal of Law and Policy*, *1*(3). https://doi.org/10.59022/ijlp.43

Allah Rakha, N. (2023). Exploring the Role of Block-chain Technology in Strengthening International Legal Guarantees for Investment Activity. *International Journal of Law and Policy*, *1*(3). https://doi.org/10.59022/ijlp.37

Utegenov Ongarbay Dariyabayevichc. (2023). A Comprehensive Analysis of Ecological Law in the Cyber Era. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.58

Xudaybergenov, A. (2023). Toward Legal Recognition of Artificial Intelligence Proposals for Limited Subject of law Status. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.55

Ruslan, S. (2023). Challenges and Opportunities for Legal Practice and the Legal Profession in the Cyber Age. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.59

AllahRakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, *16*(2), 23-54.

Ubaydullayeva, A. (2023). Artificial Intelligence and Intellectual Property: Navigating the Complexities of Cyber Law. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.57

Ollanazarova Mamura Muzaffarovna. (2023). Analyzing the Legal Labyrinth: Current Trends in Genetic Research and Their Legal Perspectives. *International Journal of Law and Policy*, *1*(5). https://doi.org/10.59022/ijlp.84

Muxammadiyev Sindorbek Bobirjon o'g'li. (2023). Complexities of International Arbitrator Liability: A Comparative Analysis and the Case for Qualified Immunity. *International Journal of Law and Policy*, *1*(5). https://doi.org/10.59022/ijlp.46

Allah Rakha, N. (2023). The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.23

Allah Rakha, N. (2023). Artificial Intelligence strategy of the Uzbekistan: Policy framework, Preferences, and challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.27

Babaev Isa. (2023). Integrating System Analysis, Information Management, and Decision-Making: Legal Perspectives and Challenges. *International Journal of Law and Policy*, *1*(5).

https://doi.org/10.59022/ijlp.85

Laylo, K. (2023). The Impact of AI and Information Technologies on Islamic Charity (Zakat): Modern Solutions for Efficient Distribution. *International Journal of Law and Policy*, *1*(5). https://doi.org/10.59022/ijlp.83

Bayzakova Diana Bakhtiyorovna. (2023). Legal Regulation of Foreign Investment Regime in the Oil and Gas Sector of Uzbekistan. *International Journal of Law and Policy*, *1*(6). https://doi.org/10.59022/ijlp.99

Bekmirzaeva, U. (2023). The Evolution of Investment Standards: A Comparative Analysis of the New Edition of the Law of the Republic of Uzbekistan on Investments and Investment Activity. *International Journal of Law and Policy*, *1*(6). https://doi.org/10.59022/ijlp.97

Sharopov, R. (2023). Behavioral Law and Antitrust Legislation in the Agro-Industrial Complex: Interconnection, Challenges, and Solutions. *International Journal of Law and Policy*, *1*(6). https://doi.org/10.59022/ijlp.98

Abduvalieva Mumtozkhan Asilbekovna. (2023). Comparative Analysis of International Standards for the Protection of Persons with Disabilities and National Legal Norms. *International Journal of Law and Policy*, *1*(6). https://doi.org/10.59022/ijlp.96

Gulyamov, S., & Raimberdiyev, S. (2023). Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*, *1*(7). https://doi.org/10.59022/ijlp.119

AllahRakha, N. (2023). Legal Challenges for International Fintech Startups. *International Journal of Law and Policy*, *1*(8). https://doi.org/10.59022/ijlp.148

Ahmadjonov, M. (2023). Anti-Corruption and Compliance Control: Legal Literacy among Lawyers and Law Students. *International Journal of Law and Policy*, *1*(8). https://doi.org/10.59022/ijlp.145

Abdikhakimov, I. (2023). Jurisdiction over Transnational Quantum Networks. *International Journal of Law and Policy*, *1*(8). https://doi.org/10.59022/ijlp.147

AllahRakha, N. (2024). Rethinking Digital Borders to Address Jurisdiction and Governance in the Global Digital Economy. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.124

Ubaydullaeva, A. (2024). Rights to Digital Databases. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.151

Cupi, D. (2024). The Role of the Albanian Media as Mediator and Creator of Collective Memory. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.146

Murodullaev, D. (2024). Problems of Application of Termination of Employment Contract due to Circumstances beyond the Control of the Parties . *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.155

Soyipov, K. (2024). Features of Termination of an Employment Contract at the Initiative of the Employer: Uzbekistan's Case. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.153

Karimjonov, M. (2024). A Disciplinary Responsibility by the New Labor Legislation of the Republic of Uzbekistan. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.158

AllahRakha, N. (2024). Transformation of Crimes (Cybercrimes) in Digital Age. *International*

Journal of Law and Policy, *2*(2). https://doi.org/10.59022/ijlp.156

Ismoilov, S. (2024). What is the Importance of Entering into a Non-Compete Agreement?. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.159

Rakhimov, M. (2024). The Principles of the Classical Theory of Labor Law. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.157

AllahRakha, Naeem, Modernizing Criminal and Evidence Laws to Facilitate Tourism in Pakistan. Available at SSRN: https://ssrn.com/abstract=4707544 or http://dx.doi.org/10.2139/ssrn.4707544

Bakhramova, M. (2024). Harmonization of the Legal Framework for Online Arbitration. *International Journal of Law and Policy*, *2*(2). https://doi.org/10.59022/ijlp.154

Saidakhror, G. (2024). The Impact of Artificial Intelligence on Higher Education and the Economics of Information Technology. *International Journal of Law and Policy*, *2*(3), 1–6. https://doi.org/10.59022/ijlp.125

Odilov, J. (2024). Digital Use of Artificial Intelligence in Public Administration. *International Journal of Law and Policy*, *2*(3), 7–15. https://doi.org/10.59022/ijlp.161

AllahRakha, N. (2024). Legal Procedure for Investigation under the Criminal Code of Uzbekistan. *International Journal of Law and Policy*, *2*(3). https://doi.org/10.59022/ijlp.160

Mamanazarov, S. (2024). Intellectual Property Theories as Applied to Big Data. *International Journal of Law and Policy*, *1*(7). https://doi.org/10.59022/ijlp.164