231. THE ECONOMICS OF CYBERSECURITY: BALANCING INVESTMENT AND SYSTEMIC RISK

Budko A. V.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Yeliseyeva V. A. – Senior Lecturer, Master of Arts

This paper explores the intersection of cybersecurity and modern economic theory. The study analyzes the Investment Paradox using the Gordon-Loeb model, emphasizing that cybersecurity is not merely a technical expense but a strategic capital investment. Furthermore, it addresses the systemic risks posed to global financial stability and the growing labor market gap in the IT security sector. The purpose of this work is to demonstrate how rational economic actors balance the costs of defense against the catastrophic risks of digital insecurity.

In the third decade of the 21st century, the global economy has become inseparable from information technology. As enterprises shift operations to the cloud and rely on big data, a new economic challenge has emerged: the management of cyber risk. Cybersecurity is no longer just a technical necessity; it is a critical economic variable. For a modern organization, the question is not whether an attack will occur, but what volume of resources should be allocated to mitigate the inevitable financial impact. To understand the economics of cybersecurity, an analysis of the cost of failure must first be conducted.

When a data breach occurs, the financial consequences are rarely limited to a single moment. According to recent industry research, the average global cost of a breach has reached $4.45 million [1]. This figure represents a combination of direct financial losses, such as the immediate theft of funds and the cost of forensic investigations, as well as indirect long-term costs. These hidden expenses include regulatory fines, legal fees, and devastating reputational damage that often leads to a significant drop in stock prices and customer trust.

Building on the analysis of costs, a primary issue for IT managers and economists is the Investment Paradox. If an enterprise spends too little, it risks losing its entire value to a breach; however, if investment is excessive, the cost of protection may exceed the value of the assets being protected. This dilemma is governed by the law of diminishing returns, which dictates that achieving 100 % security is mathematically and economically impossible. The most influential framework for addressing this problem is the Gordon-Loeb Model [2]. This model suggests that a rational firm should generally spend only a small fraction of the expected loss from a cyberattack on prevention. Specifically, the model demonstrates that the optimal level of investment is often less than 37 % of the potential loss, as spending beyond this point becomes inefficient. Thus, the goal of a rational economic actor is to identify the equilibrium where the cost of a breach and the cost of prevention are perfectly balanced.

However, while individual entities focus on internal budgets, the integration of global finance creates what is defined as systemic risk. Because modern banks and supply chains are deeply interconnected through shared cloud providers and payment gateways, a single vulnerability in widely used software can freeze global trade. The International Monetary Fund has warned that the financial sector is uniquely vulnerable to this domino effect [3]. A large-scale cyberattack on a major financial institution could trigger a liquidity crisis similar to the 2008 financial crash, but driven by code rather than subprime loans. Unlike traditional economic crises, a cyber-recession can occur within minutes, leaving regulators with almost no time to react, which elevates cybersecurity to the matter of national security and macroeconomic stability.

The final economic hurdle in this field is the significant gap in the labor market. The demand for cybersecurity professionals has created a massive imbalance in human capital. Industry studies indicate that there is a global shortage of approximately 4 million experts [4]. This shortage leads to significant wage inflation, making it difficult for smaller firms or government institutions to afford high-level protection. This talent gap effectively acts as a tax on digital transformation, slowing down the adoption of new technologies because organizations cannot adequately secure them. As noted in broader economic outlooks, this creates a cyber-resilience gap between wealthy corporations and the rest of the economy [5].

In conclusion, the economics of cybersecurity is a complex balancing act between investment, risk, and resilience. As demonstrated by the cost analyses and the Gordon-Loeb model, technology alone cannot solve the problem of insecurity. The future of the digital economy depends on how trust is valued and how systemic vulnerabilities are managed. For the global economy to remain stable, cybersecurity must be treated not as an optional IT expense, but as a strategic capital investment that ensures long-term economic survival in an increasingly volatile digital landscape.

Building on the structural challenges of the labor market, the economics of cybersecurity is further complicated by information asymmetry. In this digital arms race, the marginal cost for an attacker to find a single vulnerability is significantly lower than the marginal cost for a defender to protect every possible entry point [6]. This imbalance creates a market failure where offensive capabilities scale more efficiently than defensive ones. To mitigate this, a robust market for cyber insurance has emerged as a primary tool for risk

transfer. However, this introduces the moral hazard problem: policyholders might inadvertently lower internal security standards, assuming the insurer will absorb the financial shock [7].

Furthermore, the role of insurance companies is evolving into that of a private regulator. By setting high security standards as a prerequisite for coverage, insurers are effectively mandating a baseline of cyber hygiene across the global economy [8]. Yet, even with insurance, data from the past year shows that the ransomware economy continues to drain billions from productive sectors into the shadow economy, acting as a global drain on GDP [9]. Ultimately, as the gap between cyber-resilient super-firms and vulnerable small businesses widens, the stability of the digital ecosystem depends on a shift from individual defense to collective, state-backed economic resilience [10].

Furthermore, the rise of systemic risks and the complexities of the cyber insurance market demonstrate that individual corporate defense is no longer sufficient. The attacker's advantage fueled by information asymmetry ensures that the digital arms race remains a permanent feature of the modern economy. Ultimately, achieving a secure digital future requires more than just improved software; it demands a shift in economic policy where cyber-resilience is treated as a critical public good, essential for maintaining the integrity of global trade and national security.

Final observations indicate that the economics of cybersecurity has evolved from a niche technical concern into a fundamental pillar of global financial stability. As analyzed, the financial impact of a breach extends far beyond immediate losses, encompassing long-term reputational and regulatory costs that can threaten the existence of a commercial enterprise. While the Gordon-Loeb Model provides a rational mathematical framework for optimizing investment, the persistent Investment Paradox and the global labor shortage of 4 million experts continue to create a resilience gap across the private sector.

Ultimately, the transition from fragmented defensive protocols to a cohesive economic framework marks a critical evolution in the digital age. This analysis underscores that cybersecurity is no longer a peripheral technical concern but a core determinant of macro-financial equilibrium. As evidenced by the synthesis of the Gordon-Loeb Model and the inherent information asymmetries of the digital arms race, the traditional reliance on linear investment is insufficient to counter the exponential nature of systemic threats. The persistence of the resilience gap and the global deficit in human capital necessitate a paradigm shift: moving away from reactive risk mitigation toward the construction of a proactive, state-backed economic architecture.

Furthermore, the escalating complexity of interconnected supply chains suggests that the marginal utility of isolated defense is rapidly diminishing in the face of unpredictable cyber events. For the global financial infrastructure to survive this era of digital entropy, the valuation of trust must be quantified as a measurable asset that reflects an enterprise's true exposure to cyber-shocks. This requires a fundamental recalibration of corporate governance, where cyber-resilience is redefined as a transnational public good, essential for ensuring trust and stability in global trade. Consequently, future economic stability will depend not on the illusory goal of absolute protection, but on the ability of the global ecosystem to maintain institutional continuity within an increasingly volatile and non-linear digital landscape. Such a transformation demands that policymakers and market actors alike move beyond the "Investment Paradox" to treat digital integrity as the primary strategic capital. n this context, capital allocation frameworks must evolve to integrate probabilistic risk modeling that captures systemic cyber interdependencies rather than isolated vulnerabilities. Only by internalizing these externalities can institutions align incentives toward collective resilience instead of fragmented security postures. In this paradigm, the capacity to absorb, adapt, and rapidly recover from cyber disruptions will become the defining metric of competitive advantage in the digital economy. Ultimately, the endurance of the global financial system will hinge on its collective ability to institutionalize trust as a dynamic, continuously reinforced property rather than a static assumption.

References:

1. Cost of a Data Breach Report 2023 / IBM Security. — 2023. — URL: https://www.ibm.com/reports/data-breach (date of access: 15.03.2024).

2. Gordon, L. A. The Economics of Information Security Investment / L. A. Gordon, M. P. Loeb // ACM Transactions on Information and System Security. — 2002. — Vol. 5, № 4. — P. 438–457.

3. Global Financial Stability Report: Cyber Risk / International Monetary Fund. — Washington: IMF, 2024. — 120 p.

4. Cybersecurity Workforce Study: Looking Deeper into the Talent Gap / ISC2. — 2023. — URL: https://www.isc2.org/research (date of access: 15.03.2024).

5. Global Cybersecurity Outlook 2024 / World Economic Forum. — Geneva: World Economic Forum, 2024. — 45 p.

6. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. — 3rd ed. — Indianapolis: Wiley, 2020. — 1232 p.

7. The Global Cyber Risk Report: Bridging the Gap in Insurance and Resilience / Marsh McLennan. — 2024. — URL: https://www.marshmclennan.com/insights/publications (date of access: 15.03.2024).

8. Enhancing the Digital Security of Critical Activities / OECD. — Paris: OECD Publishing, 2023. — 80 p.

9. Data Breach Investigations Report (DBIR) 2025 / Verizon. — 2025. — URL: https://www.verizon.com/business/resources/reports/dbir/ (date of access: 15.03.2024).

10. World Economic Forum. Global Cybersecurity Outlook 2024 / World Economic Forum. — Geneva: WEF, 2024. — 40 p.