Mirko Cobović
Sveučilište u Slavonskom Brodu
Ulica 108. brigade ZNG 36,
35 000 Slavonski Brod
mcobovic@unisb.hr

Pregledni rad

EKONOMSKA DIMENZIJA KIBERNETIČKE OTPORNOSTI: PREGLED UTJECAJA DIREKTIVE NIS2 NA INVESTICIJSKE STRATEGIJE I TRŽIŠNU DINAMIKU

Sažetak

Eskalacija malicioznih kibernetičkih aktivnosti i tržišni neuspjesi u samoregulaciji privatnog sektora potaknuli su donošenje Direktive NIS2, čiji ekonomski utjecaj nadilazi puku pravnu usklađenost. Ovaj rad analizira ekonomske mehanizme Direktive s fokusom na investicijske strategije i dinamiku lanca opskrbe. Metodološki pristup temelji se na sintezi teorijske literature o ekonomici sigurnosti te analizi sekundarnih kvantitativnih podataka globalnih industrijskih izvješća. Rezultati istraživanja potvrđuju da NIS2 transformira kibernetičku sigurnost iz varijabilnog tehničkog u fiksni regulatorni trošak, potičući ex-ante ulaganja neovisno o razini prijetnje. Nadalje, analiza otkriva asimetričan rast transakcijskih troškova uslijed prelaska s relacijskog na verificirano povjerenje, što rezultira fenomenom „bijega u kvalitetu" i tržišnom konsolidacijom. Zaključno, rad pokazuje da novi regulatorni okvir postavlja visoke ulazne barijere za male i srednje poduzetnike, čineći sigurnosnu usklađenost ne samo zakonskom obvezom, već temeljnim preduvjetom za ekonomski opstanak i sudjelovanje u modernim lancima vrijednosti, posebice u kontekstu manjih tržišta poput hrvatskog.

Ključne riječi: NIS2 direktiva, ekonomika kibernetičke sigurnosti, transakcijski troškovi, lanac opskrbe, investicijske strategije

1. UVOD

Eskalacija malicioznih kibernetičkih aktivnosti predstavlja jedan od najbrže rastućih sistemskih rizika za globalno gospodarstvo. Prema procjenama *Cybersecurity Ventures*, ekonomski teret ovih incidenata na globalnoj razini mogao bi dosegnuti 10,5 bilijuna dolara godišnje do 2025. godine (Morgan, 2020). Iako je digitalizacija pokretač napretka, novija istraživanja naglašavaju da visokokvalitetan razvoj digitalne ekonomije mora biti praćen robusnim sigurnosnim okvirima kako bi bio održiv (He et al., 2024).

U tom kontekstu, analize pokazuju da praćenje indikatora održivosti i upravljanja (ESG) postaje imperativ i za ekonomske subjekte na zapadnom Balkanu, pri čemu sigurnosni aspekti igraju sve važniju ulogu u ocjeni ukupnih performansi (Lukić, 2024). Unatoč tome, tradicionalni pristup ulaganju u informacijsku sigurnost u poslovnom sektoru često je bio reaktivan, vođen logikom minimalne nužnosti.

Ovaj raskorak između eksponencijalnog rasta prijetnji i razine ulaganja u ekonomskoj se teoriji definira kao tržišni neuspjeh (market failure) (Yu, H. et al., 2024)). Privatni subjekti često podcjenjuju rizik ili očekuju da će troškove incidenata snositi treće strane. Kao odgovor na nedovoljnu otpornost tržišta, Europska unija usvojila je Direktivu (EU) 2022/2555 (NIS2). Važnost ovog regulatornog zaokreta potvrđuju

i novija istraživanja u regionalnom kontekstu (Ravlić i Unukić, 2025), koja ističu da kibernetička sigurnost više nije izolirano tehničko pitanje, već temelj jačanja institucionalne i geopolitičke otpornosti gospodarstva.

Cilj ovog rada je analizirati ekonomske mehanizme NIS2 direktive. Rad ne teži prikupljanju primarnih podataka, već kroz sintezu postojeće literature i sekundarnih podataka testira dvije temeljne hipoteze, uz kritički osvrt na specifičnosti tržišta:

H1: Direktiva NIS2 mijenja funkciju troškova poduzeća pretvarajući kibernetičku sigurnost iz varijabilnog tehničkog troška u fiksni regulatorni trošak, što rezultira povećanjem ex-ante ulaganja neovisno o stvarnoj razini tehničke prijetnje.

H2: Mehanizmi nadzora lanca opskrbe propisani Direktivom NIS2 dovode do asimetričnog rasta transakcijskih troškova, što uzrokuje tržišnu konsolidaciju i podiže ulazne barijere za male i srednje poduzetnike (MSP).

2. SINTEZA DOSADAŠNJIH ISTRAŽIVANJA

Dosadašnja literatura o ekonomici kibernetičke sigurnosti može se kvalitativno kategorizirati u tri dominantna teorijska pravca: neoklasični pristup racionalnog izbora, bihevioralna ekonomija sigurnosti i institucionalna teorija usklađenosti.

2.1. Granice racionalnog izbora i kratkovidnost tržišta

Rana istraživanja, predvođena radom Gordona i Loeba (2002), temeljila su se na pretpostavci da su menadžeri racionalni ekonomski agenti. Njihov model sugerira da poslovni subjekt treba ulagati u sigurnost sve dok je granična korist veća od graničnog troška (MK > MT).Međutim, kvalitativna analiza novijih studija (npr. Moore, 2010) ukazuje na to da ovaj model u praksi zakaže zbog fenomena kratkovidnosti (myopia). Recentna istraživanja dodatno potvrđuju ovu složenost kroz dvije dimenzije. Prvo, analiza troškovnih i sigurnosnih aspekata nadzornih sustava ukazuje na to da tehnička implementacija nosi specifične financijske terete koji zahtijevaju preciznu evaluaciju unutar operativnih troškova (Cobović, 2023a). Drugo, u širem kontekstu digitalne transformacije, menadžerski izazovi se usložnjavaju te zahtijevaju nove, holističke modele odlučivanja koji nadilaze jednostavnu cost-benefit analizu i promatraju sigurnost kao stratešku nužnost, a ne samo tehničku opciju (Cobović, 2023b). U nedostatku regulatornog okvira, tržišni modeli sustavno podcjenjuju vjerojatnost pojave ekstremnih scenarija (tail risk (Melina, Sukono et al., 2023) koji nose ne srazmjerno velike negativne posljedice. Novija literatura u ovaj diskurs uvodi koncept "regulatorne točke preokreta" (Regulatory Tipping Point (Armstrong, 2016)). Za razliku od velikih sustava koji mogu amortizirati fiksne troškove sigurnosti kroz ekonomiju razmjera, za mikro poduzetnike točka u kojoj granični trošak usklađenosti premašuje graničnu korist poslovanja nastupa znatno ranije. U tom trenutku, racionalan ekonomski izbor za manje subjekte nije ulaganje, već izlazak s tržišta ili prelazak u sivu zonu (shadow IT (Raković, L. et al., 2020)), što predstavlja negativnu eksternaliju regulative.

2.2. Institucionalna teorija i regulatorni izomorfizam

Primjenom institucionalne teorije (DiMaggio & Powell, 1983), istraživači analiziraju kako regulativa ne djeluje samo kroz kazne, već kroz prisilni izomorfizam. Poslovni subjekti ne ulažu u sigurnost samo radi zaštite podataka, već radi legitimiteta. Kada regulativa poput NIS2 definira standard, poslovni subjekti ga kopiraju kako bi signalizirale tržištu da su pouzdane.

Tablica 1. Sinteza ključnih ekonomskih teorija u kontekstu NIS2 direktive

Teorijski pristup	Ključni autori	Osnovna premisa	Implikacija za NIS2 Direktivu
Neoklasična ekonomija	Gordon & Loeb (2002)	Poslovni subjekti ulažu do točke MK = MT.	NIS2 umjetno povećava trošak incidenta (kazne), prisiljavajući višu točku ravnoteže ulaganja (podloga za H1).
Ekonomika poticaja	Anderson (2001)	Sigurnost ovisi o tome tko snosi trošak neuspjeha.	Članak 20. (odgovornost uprave) rješava problem moralnog hazarda prebacivanjem rizika na donositelje odluka.
Institucionalna teorija	DiMaggio & Powell (1983)	Poslovni subjekti kopiraju prakse radi legitimiteta.	NIS2 dovodi do standardizacije sigurnosnih praksi kroz prisilni izomorfizam.
Asimetrija informacija	Akerlof (1970); Böhme (2010)	Kupci ne mogu procijeniti sigurnost proizvoda.	Obvezno izvještavanje i certifikacija smanjuju asimetriju i omogućuju diferencijaciju na tržištu (podloga za H2).

Izradio autor

3. NIS2 KAO REGULATORNI KOREKTIV TRŽIŠTA

Direktiva NIS2 ekonomski djeluje kao intervencija kojom se internaliziraju eksternalije identificirane u literaturi.

3.1. Internalizacija troškova rizika

Kroz članak 21., NIS2 propisuje obvezne mjere upravljanja rizicima. Ekonomski gledano, ovo pretvara kibernetičku sigurnost iz varijabilnog troška u fiksni trošak poslovanja. Svaki subjekt koji želi sudjelovati na tržištu mora platiti ulaznicu u obliku usklađenosti. Ova regulatorna transformacija troška predstavlja temeljni mehanizam na kojem počiva hipoteza H1.

3.2. Smanjenje asimetrije informacija

Tržište pati od asimetrije informacija jer kupci teško procjenjuju sigurnost dobavljača ("Tržište limuna"). NIS2 uvodi stroge obveze izvještavanja (članak 23.), čime se povećava transparentnost. To smanjuje transakcijske troškove provjere za kupce, ali istovremeno povećava troškove za dobavljače. Ovaj mehanizam stvara rizik od tržišne koncentracije, gdje samo subjekti s dovoljno kapitala mogu signalizirati svoju sigurnosnu kvalitetu.

4. UTJECAJ NA INVESTICIJSKE STRATEGIJE

Implementacija NIS2 direktive dovodi do redefiniranja funkcije troškova i koristi. Analiza recentnih empirijskih istraživanja potvrđuje ove trendove i pruža dokaze za prvu hipotezu.

Prilikom interpretacije podataka u Tablici 2, nužno je zadržati metodološki oprez. Podaci potječu od ponuđača sigurnosnih rješenja (*vendors*) koji mogu imati komercijalni interes u naglašavanju rizika (Vendor Bias). Iako apsolutne novčane projekcije gubitaka mogu biti precijenjene, relativni trendovi i promjene u alokaciji budžeta, koji su fokus ovog rada, ostaju validan indikator promjene tržišnog sentimenta.

Tablica 2: Pregled ključnih kvantitativnih istraživanja relevantnih za NIS2 direktivu

Istraživanje (Izvor)	Uzorak i Godina	Ključni Kvantitativni Nalazi	Ekonomska Implikacija za NIS2
PwC Global Digital Trust Insights	N=3.800+ (2024.)	79% poslovnih subjekata povećava budžet. Poslovni subjekti s velikim incidentima ulažu 15-20% više.	Potvrđuje tezu da regulativa postaje primarni pokretač alokacije kapitala (podrška H1).
BlueVoyant: Supply Chain Defense	N=2.100 (2023.)	Broj nadziranih dobavljača porastao s 1.013 na 4.242. 29% poslovnih subjekata prekida suradnju zbog sigurnosti.	Ukazuje na drastičan porast transakcijskih troškova nadzora i rizik isključenja s tržišta (podrška H2).
IBM Security: Cost of a Data Breach	N=553 (2023.)	Prosječan trošak proboja: 4,45 mil. USD. Plan odgovora štedi 1,49 mil. USD.	Dokazuje ekonomsku isplativost mjera iz članka 21. (IR planovi) kroz konkretne uštede.

Izradio autor

4.1. Uloga sankcija i rast budžeta

Kazne propisane člankom 34. (do 10 milijuna eura ili 2% prometa) mijenjaju izračun povrata na investiciju (ROSI). Istraživanje PwC Global Digital Trust Insights 2024 pruža robustan dokaz za potvrdu hipoteze H1. Podatak da 79% organizacija planira povećanje budžeta, pri čemu se regulativa navodi kao ključni pokretač, sugerira da tržište internalizira trošak usklađivanja. Posebno je značajno da organizacije potaknute strahom od regulatornih posljedica ulažu dodatna sredstva, čime se potvrđuje da NIS2 potiče ex-ante ulaganja neovisno o trenutnoj tehničkoj prijetnji.

4.2. Ekonomska isplativost mjera

Dok NIS2 nameće troškove, podaci iz izvješća IBM Cost of a Data Breach 2023 pružaju argument za ekonomsku korist. Direktiva zahtijeva planove za odgovor na incidente. IBM-ovi podaci pokazuju da organizacije s takvim timovima bilježe prosječni trošak incidenta manji za 33,4%. Ovo dodatno osnažuje ekonomsku racionalnost iza hipoteze H1 – ulaganje u usklađenost dugoročno štiti vrijednost poslovnog subjekta.

5. TRŽIŠNA DINAMIKA I UČINCI NA LANAC OPSKRBE

Kako bi se testirala druga hipoteza o promjeni tržišne strukture, provedena je kvalitativna analiza ključnih tržišnih dimenzija prikazana u Tablici 3.

Tablica 3: Kvalitativna analiza utjecaja NIS2 na tržišnu dinamiku i strukturu lanca opskrbe

Tržišna dimenzija	Status Ex-Ante (Prije NIS2)	Mehanizam transformacije (NIS2)	Status Ex-Post (Nakon NIS2)	Ekonomska implikacija
Priroda povjerenja	Relacijsko povjerenje: Temelji se na reputaciji.	Članak 21. (Sigurnost lanca opskrbe): Zakonska obveza provjere.	Verificirano povjerenje: Temelji se na revizijama..	Eksponencijalni rast transakcijskih troškova provjere i nadzora.
Ulazne barijere za MSP	Niske: Konkurencija cijenom. Sigurnost je opcija.	Prelazak rizika: Klijenti prenose zahtjeve na dobavljače.	Visoke: Sigurnosna usklađenost postaje licenca za rad.	Tržišna konsolidacija: Eliminacija manjih igrača bez kapitala za usklađivanje.
Informacijska asimetrija	Visoka: Kupac ne razlikuje siguran softver od nesigurnog.	Signaliziranje: Usklađenost postaje tržišni signal.	Smanjena: Transparentnost omogućuje diferencijaciju.	Premija na cijenu: Sigurnost postaje konkurentska prednost.

Izradio autor

5.1. Kaskadni prijenos troškova i konsolidacija

Kvalitativna promjena povjerenja (Tablica 3) ima svoje kvantitativne posljedice koje direktno podupiru hipotezu H2. Izvješće poslovnog subjekta BlueVoyant (2023) pokazuje četverostruki porast broja nadziranih dobavljača (na 4.242 u 2023.), što potvrđuje tezu o rastu transakcijskih troškova.

S makroekonomskog aspekta, podatak da je 29% organizacija prekinulo suradnju s dobavljačima isključivo zbog sigurnosnih razloga pruža snažan dokaz za drugi dio hipoteze H2. Ovdje dolazi do fenomena bijega u kvalitetu (Flight to Quality), gdje veliki obveznici (Essential entities) smanjuju broj dobavljača kako bi smanjili površinu napada i administrativni teret nadzora, konsolidirajući tržište oko većih igrača.

5.2. Specifičnosti utjecaja na hrvatsko gospodarstvo

Primjena ovih globalnih trendova na hrvatsko tržište, kojim dominiraju mikro i mali poduzetnici (preko 99% subjekata), sugerira potencijalne strukturne poremećaje. Budući da NIS2 kroz lanac opskrbe indirektno obvezuje i manje subjekte koji nisu direktni obveznici, hrvatski MSP sektor suočava se s nerazmjernim troškovima.

Za razliku od razvijenih tržišta, u Hrvatskoj postoji rizik od stvaranja oligopola na strani ponude sigurnosnih usluga. Nagli porast potražnje za uslugama usklađivanja (konzultanti, *CISO-as-a-Service*, tehnička rješenja), uz ograničenu ponudu stručnjaka, dovodi do rasta cijena usluga (inflacija cijena usluga). To dodatno podiže ulazne barijere za MSP-ove, potvrđujući hipotezu H2 u lokalnom kontekstu s pojačanim intenzitetom.

6. ZAKLJUČAK

Ekonomska analiza Direktive NIS2 pokazuje da se ne radi samo o pravnom aktu, već o snažnom instrumentu ekonomske politike koji fundamentalno mijenja tržišno ponašanje. Na temelju sintetizirane literature i empirijskih podataka, moguće je potvrditi obje postavljene hipoteze, uz važne ograde vezane uz strukturu tržišta.

Hipoteza H1 je potvrđena analizom investicijskih trendova (PwC) koji pokazuju da "compliance" postaje primarni motivator budžetiranja. NIS2 uspješno pretvara kibernetičku sigurnost u fiksni regulatorni trošak, čime se eliminira diskrecijsko pravo menadžera da "štede na sigurnosti" i osigurava stabilnija ex-ante alokacija resursa.

Hipoteza H2 je potvrđena analizom dinamike lanca opskrbe. Analiza ukazuje na to da sigurnost postaje "luksuzno dobro" dostupno primarno većim tržišnim igračima. Prijelaz s relacijskog na verificirano povjerenje drastično je povećao transakcijske troškove. Ovo stvara asimetričan pritisak na male i srednje poduzetnike, posebno u ekonomijama poput hrvatske, što neminovno vodi ka konsolidaciji tržišta i podizanju ulaznih barijera.

Ovaj rad podliježe ograničenjima vezanim uz sekundarnu prirodu podataka koji često potječu od ponuđača sigurnosnih rješenja, čime postoji rizik od pristranosti. Također, stvarni dugoročni učinci na profitabilnost tek se trebaju manifestirati.

Za buduća istraživanja, ključno je provesti empirijsku validaciju u nacionalnom kontekstu (anketiranje hrvatskih poslovnih subjekata nakon implementacije ZKS-a), analizu točke preokreta (Break-even analysis) kako bi se utvrdilo gdje se nalazi financijska granica isplativosti usklađivanja za mikro-poduzetnike u odnosu na rizik gubitka ugovora, teLongitudinalnu analizu učinkovitosti kako bi se potvrdilo rezultiraju li povećana ulaganja stvarnim smanjenjem incidenata.

Za hrvatske poslovne subjekte i zakonodavce, ovi nalazi impliciraju da usklađenost s NIS2 više nije samo pravna obveza, već preduvjet za ekonomski opstanak u modernim lancima vrijednosti.

LITERATURA

1. Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, Volume 84, Issue 3, August 1970, Pages 488–500, https://doi.org/10.2307/1879431
2. Amstrong, P. (2016). Financial Technology: The Regulatory Tipping Points , https://www.esma.europa.eu/sites/default/files/library/2016-1420_financial_technology_the_regulatory_tipping_points_by_patrick_armstrong_0.pdf
3. Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. *ACSAC Proceedings*.
4. BlueVoyant. (2023). The State of Supply Chain Defense: Annual Global Insights Report New Orleans, LA, USA, pp. 358-365, doi: 10.1109/ACSAC.2001.991552.
5. Cobović, M. (2023). Cost and Security Aspects of the System for Monitoring and Managing Things Over the Internet. *Tehnički vjesnik*, 30(2), 486-491. https://doi.org/10.17559/TV-20220914230921
6. Cobović, M. (2022). Eksternalizacija elemenata poslovnih procesa poslovnih subjekata u Republici Hrvatskoj. Marsonia: časopis za društvena i humanistička istraživanja, 1 (1), 35-48. Preuzeto s https://hrcak.srce.hr/281838
7. DiMaggio, Paul & Powell, Walter. (2000). 'The Iron Cage Revisited: Isomorphism in Organizational Fields'. American Sociological Review. 48. 147-160. 10.2307/2095101.
8. Europski parlament i Vijeće. (2022). Direktiva (EU) 2022/2555 (NIS 2). *Službeni list Europske unije*.
9. Gordon, Lawrence & Loeb, Martin. (2002). The Economics of Information Security Investment. ACM Trans. Inf. Syst. Secur.. 5. 438-457. 10.1145/581271.581274.
10. He, Y., Song, J., & Ouyang, W. (2024). Digital Economy, Entrepreneurship, and High-Quality Development of the Manufacturing Industry. *Tehnički vjesnik*, 31(3), 851-863, https://doi.org/10.17559/TV-20231121001135
11. IBM Security. (2023). Cost of a Data Breach Report 2023. *Ponemon Institute & IBM*.
12. Lukić, R. (2024). Analysis of ESG Performance Indicators of Western Balkan Countries. *Marsonia*, 3(1), 21-41.
13. Melina, Sukono, Napitupulu, H., & Mohamed, N. (2023). A Conceptual Model of Investment-Risk Prediction in the Stock Market Using Extreme Value Theory with Machine Learning: A Semisystematic Literature Review. *Risks*, *11*(3), 60. https://doi.org/10.3390/risks11030060
14. Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybersecurity Ventures*.
15. Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options, International Journal of Critical Infrastructure Protection, Volume 3, Issues 3–4, December 2010, 103-117, https://doi.org/10.1016/j.ijcip.2010.10.002
16. PwC. (2024). Global Digital Trust Insights Survey 2024. *PricewaterhouseCoopers*.
17. Ravlić, S., Unukić, I. (2025). Uloga kibernetičke sigurnosti u jačanju regionalne gospodarske otpornosti: institucionalne i geopolitičke perspektive. *Festung*, 1(2), 143-149.
18. Raković, L., Sakal, M., Matković, P., & Marić, M. (2020). Shadow IT–systematic literature review. Information Technology and Control, 49(1), 144-160, https://doi.org/10.5755/j01.itc.49.1.23801

19. Yu, H., Lee, M. i Chung, S. (2024). A Stochastic Simulation Based Approach for Transportation Demand Forecast and Safety. *Tehnički vjesnik, 31* (4), 1199-1205. https://doi.org/10.17559/TV-20231010001011

THE ECONOMIC DIMENSION OF CYBER RESILIENCE: AN OVERVIEW OF THE NIS2 DIRECTIVE IMPACT ON INVESTMENT STRATEGIES AND MARKET DYNAMICS

Abstract

The escalation of malicious cyber activities and the market's failure to self-regulate have prompted the adoption of the NIS2 Directive, the economic impact of which extends beyond mere legal compliance. This paper analyzes the Directive's economic mechanisms, focusing on investment strategies and supply chain dynamics. The methodological approach relies on a synthesis of theoretical literature on the economics of security and an analysis of secondary quantitative data from global industry reports. Research results confirm that NIS2 transforms cybersecurity from a variable technical cost into a fixed regulatory cost, driving ex-ante investments regardless of the threat level. Furthermore, the analysis reveals an asymmetric increase in transaction costs due to the shift from relational to verified trust, resulting in a "flight to quality" phenomenon and market consolidation. In conclusion, the paper demonstrates that the new regulatory framework establishes high entry barriers for small and medium-sized enterprises, making security compliance not just a legal obligation but a fundamental prerequisite for economic survival and participation in modern value chains, particularly within smaller markets like Croatia.

Keywords: NIS2 Directive, economics of cybersecurity, transaction costs, supply chain, investment strategies