Prethodno priopćenje
UDK: 005.334:681.5
Datum primitka članka u uredništvo: 21. 9. 2022.
Datum slanja članka na recenziju: 10. 11. 2022.
Datum prihvaćanja članka za objavu: 13. 12. 2022.

Dr. sc. Ivana Dvorski Lacković*
Prof. dr. sc. Danijela Miloš Sprčić**

UTJECAJ UPRAVLJANJA KIBERNETIČKIM RIZIKOM NA POSLOVNE POKAZATELJE PODUZEĆA

IMPACT OF CYBER-RISK MANAGEMENT ON COMPANIES' BUSINESS INDICATORS

SAŽETAK: U radu je analizirano u kojoj mjeri hrvatska poduzeća upravljaju kibernetičkim rizikom te utjecaj upravljanja kibernetičkim rizikom na poslovne pokazatelje poduzeća. Istraživanje je provedeno na uzorku od 96 hrvatskih poduzeća koja pripadaju skupini poduzeća koja ostvaruju najviše prihode. Rezultati sugeriraju nedostatan udio poduzeća koja upravljaju kibernetičkim rizikom. Formuliran je model ordinalne logističke regresije kojim se ispituje utjecaj upravljanja kibernetičkim rizikom na financijske i nefinancijske pokazatelje poslovanja poduzeća. Potvrđen je značajan negativan utjecaj upravljanja kibernetičkim rizikom na likvidnost poduzeća. Provedeno istraživanje ukazuje na nužnost konstruiranja složenije mjere upravljanja kibernetičkim rizikom u poduzećima i provođenja budućih istraživanja, s obzirom na praktičnu relevantnost, te istovremeni znanstveni manjak istraživanja područja.

KLJUČNE RIJEČI: kibernetički rizik, upravljanje rizicima, poslovni pokazatelji poduzeća

SUMMARY: In this paper it is analysed in what degree Croatian companies manage cyber-risk and its impact on companies' business indicators. The research has been conducted on the sample of 96 Croatian companies pertaining to the category of companies with largest income. The results suggest poor share of companies that manage cyber-risk. In order to test the impact of cyber-risk management on financial and non-financial indicators, an ordinal logistic regression model has been formulated. It is confirmed that cyber-risk management significantly negatively impacts liquidity. The conducted research indicates

* Dr. sc. Ivana Dvorski Lacković, poslijedoktorandica na Katedri za gospodarstvo Fakulteta organizacije i informatike, Pavlinska ulica 2, 42 000 Varaždin, e-mail: idvorski@foi.unizg.hr
** Prof. dr. sc. Danijela Miloš Sprčić, redovita profesorica na Katedri za ekonomiku poduzeća Ekonomskog fakulteta u Zagrebu, Trg J. F. Kennedyja 6, 10 000 Zagreb, e-mail: dmilos@net.efzg.hr

the necessity of constructing a more complex cyber risk management measure and enable more thorough research of cyber risk management area, that is very relevant in practical terms, but at the same time neglected in scientific research.

KEY WORDS: cyber-risk, risk management, business indicators

1. UVOD

Značajna zbivanja tijekom 21. stoljeća – globalna financijska kriza, pandemija koronavirusa, rat u Ukrajini i mogućnost suočavanja europskog prostora s velikom ekonomskom krizom u nadolazećem razdoblju – dovela su do shvaćanja menadžmenta poduzeća da je rizicima potrebno upravljati strateški, s ciljem ostvarivanja poslovnih ciljeva poduzeća. U sklopu tradicionalnog pristupa upravljanju rizicima svaki odjel bavi se rizicima s kojima je suočen, bez jasnog povezivanja rizika s ciljevima poduzeća, analize međuovisnosti različitih vrsta rizika i koordiniranja mjera upravljanja rizicima. Ovakav je pristup utemeljen u shvaćanju da je poduzeće primarno izloženo financijskim rizicima te da su oni u fokusu procesa upravljanja rizicima. Nasuprot tome, suvremeni pristup upravljanju rizicima (tzv. *Enterprise Risk Management*, ERM) jednako važnim smatra strateške i operativne rizike poduzeća, a utemeljen je na shvaćanju da je holističkim i koordiniranim pristupom upravljanju rizicima moguće doprinijeti povećanju stabilnosti poduzeća, ostvarivanju poslovnih ciljeva poduzeća i povećanju vrijednosti poduzeća (Marc i sur., 2018.).

Jedan od rizika kojima su poduzeća, zbog načina odvijanja poslovnih procesa i oslanjanja na informacijsku tehnologiju u poslovanju, znatno izložena jest kibernetički rizik. Neadekvatno upravljanje kibernetičkim rizikom može dovesti do povećanog ukupnog rizičnog profila poduzeća i financijskih posljedica. Upravljanje ovom vrstom rizika zahtijeva suvremeni pristup upravljanju rizicima zbog činjenice da su kibernetički rizici povezani s mnogim drugim vrstama strateških i operativnih rizika poduzeća, a kvalitetno upravljanje njime nemoguće je bez holističkog pogleda i strateškog odgovora poduzeća na svim razinama. Fokus je ovog rada na istraživanju praksi upravljanja kibernetičkim rizikom u hrvatskim poduzećima. Prvi je cilj rada analizirati u kojoj mjeri hrvatska poduzeća upravljaju kibernetičkim rizikom. Drugi je cilj rada analizirati kojim poslovnim pokazateljima doprinosi upravljanje kibernetičkim rizikom. Istraživanje je provedeno anketnim upitnikom, a podatci su obrađeni metodama deskriptivne statistike i ordinalne logističke regresije.

Praktični doprinos ovog rada jest u analizi utjecaja upravljanja kibernetičkim rizikom na financijsku i nefinancijsku izvedbu poduzeća na hrvatskom tržištu. Radovi na ovu temu u postojećoj akademskoj literaturi vrlo su oskudni, što ukazuje na teorijski jaz. Stoga je teorijski doprinos rada upravo u popunjavanju postojećeg jaza, što je predstavljalo glavni poticaj za provođenje ovog istraživanja.

Rad je podijeljen u pet dijelova. Nakon uvoda izložen je pregled najsuvremenijih spoznaja o kibernetičkom riziku. Treće poglavlje odnosi se na opis metodologije istraživanja. U četvrtom poglavlju opisani su i diskutirani rezultati istraživanja. Naposljetku su izneseni zaključci i dan je pregled korištene literature.

2. KIBERNETIČKI RIZIK U SUVREMENOJ LITERATURI

Samo su dva istraživanja do sada ispitivala konkretan utjecaj kibernetičke sigurnosti na izvedbu poduzeća. Studija koju su proveli Berlilana i sur. (2021) otkrila je da spremnost organizacije da upravlja kibernetičkom sigurnošću (engl. *cyber security readiness*) ima pozitivan učinak na sigurnosnu izvedbu organizacije, što zauzvrat ima pozitivan utjecaj na nematerijalne i materijalne koristi. U Hasan i sur. (2021) korišten je okvir Tehnologija-Organizacija-Okruženje (TOE) kojim se ispitivao sveobuhvatni skup čimbenika koji utječu na spremnost organizacije da upravlja kibernetičkom sigurnošću te učinke tih čimbenika na organizacijsku izvedbu (financijsku i nefinancijsku) posredovanu poboljšanom organizacijskom sigurnosnom izvedbom. Utvrđeno je da spremnost na kibernetičku sigurnost pozitivno utječe na sigurnosnu izvedbu organizacije, što zauzvrat pozitivno utječe na financijsku i nefinancijsku izvedbu. Premda je upravljanje kibernetičkim rizicima tradicionalno bilo područje kojim su intenzivno upravljale financijske institucije, primarno zbog regulatornih zahtjeva i visoke razine osjetljivosti podataka, pandemija koronavirusa dovela je do transformacije poslovnih procesa i potrebe većeg oslanjanja na informacijsku tehnologiju, ali i razotkrivanja kibernetičkih ranjivosti poduzeća. Stoga su se mnoga poduzeća u vrlo kratkom vremenskom intervalu morala suočiti s potrebom zaštite od povećane izloženosti kibernetičkom riziku i nužnošću povećanja vlastite otpornosti na kibernetičke prijetnje. Visoka učestalost, kao i materijalne i nematerijalne posljedice kibernetičkih napada pokazuju koliko je važno da organizacija ima odgovarajuću razinu kibernetičke sigurnosti za zaštitu organizacijskih resursa koje dokazano mogu poboljšati reputaciju (Smith i sur., 2010) i olakšati postizanje konkurentske prednosti (Ravichandran i Lertwongsatien, 2005).

Kibernetički rizici trenutačno su vodeća vrsta rizika s kojima se poduzeća suočavaju, a očekivano je da će njihova značajnost rasti u nadolazećem razdoblju (Protiviti, 2021; Deloitte, 2021). Rezultati ankete menadžera diljem svijeta o upravljanju rizicima sugeriraju da čak 87 % menadžera smatra da je sposobnost poduzeća da upravlja kibernetičkim rizikom prioritetno područje na koje se poduzeća trebaju fokusirati (Deloitte, 2021). Prema *The Global Risks Report 2022* povećana ovisnost o digitalizaciji i povećanom korištenju informacijske tehnologije u poslovanju dovodi do rasta vjerojatnosti da će poduzeća biti pogođena kibernetičkom prijetnjom (Svjetski Ekonomski Forum, 2022). Povećanje broja kibernetičkih napada posljednjih godina negativno je utjecalo na ukupnu izvedbu organizacija diljem svijeta (Hasan i sur., 2021). Prožimajući i sve češći kibernetički napadi na IT sustave uzrokovali su ljudima i organizacijama brojne probleme povezane s padom reputacije, usklađenosti, financijama i poslovnim operacijama (Lee, 2020). Organizacije koja pripadaju kritičnoj infrastrukturi, odnosno djeluju u području zdravstva, financija, telekomunikacija, transporta, energetike i vodovoda, uvijek su mete napadača te imaju veću izloženost kibernetičkom riziku (Berg, 2010).

Prema Allianz Risk Barometer (2022), kibernetički rizici odnose se na prijetnje ucjenjivačkim softverom (*ransomware*), povrede podataka (*databreach*), povećane ranjivosti zbog rada od kuće, prekide lanaca nabave i probleme s *cloud* tehnologijom. Prethodna istraživanja dokazuju da kibernetička sigurnost značajno utječe na financijski rizik specifičan za tvrtku (Srinidhi i sur., 2015). Zbog ovisnosti suvremenih poduzeća o korištenju informacijske tehnologije i činjenice da su informacijski sustavi okosnica brojnih poslovnih procesa, kibernetički rizici usko su povezani i s mnogim drugim vrstama strateških i operativnih rizika kojima su poduzeća izložena. Primjerice, lanci nabave predstavljaju čestu

metu kibernetičkih napada i vrlo su osjetljivi na kibernetičke rizike. Rat na relaciji Rusije i Ukrajine doprinosi rastu političkih tenzija koje se mogu očitovati i kroz povišenu razinu kibernetičkih prijetnji (University of Cincinnati, 2022). Prema Kure i sur. (2018) kibernetički napadi mogu dovesti do različitih rizika koji utječu na kontinuitet poslovanja kritične infrastrukture, uključujući degradaciju proizvodnje i performansi, nedostupnost kritičnih usluga i kršenje regulatornih odredbi.

Pitanje kibernetičke sigurnosti jedno je od vodećih pitanja povezanih s digitalnom transformacijom poduzeća te može značajno povećati rizični profil poduzeća koje prolazi proces digitalne transformacije (RSA, 2019). O važnosti kibernetičke sigurnosti govori i podatak da ju je Europska komisija (2020) svrstala u jedno od prioritetnih područja vezanih uz digitalnu transformaciju, zajedno sa superračunalima, umjetnom inteligencijom, stjecanjem naprednih digitalnih vještina i osiguranjem široke primjene digitalne tehnologije u društvu. Poduzeća koja su na meti kibernetičkih napada i ne upravljaju ovim rizikom na adekvatan način, imaju povećanu izloženost reputacijskom riziku, gubitku povjerenja i smanjenju baze klijenata te posljedično mogu trpjeti i financijske gubitke.

Kibernetička zaštita zahtijeva sudjelovanje ljudi, procesa i tehnologije kako bi se zaštitila organizacija, ljudi te IT infrastruktura od kibernetičkih napada (Ahmed, 2021), stoga je nužna visoka razina osviještenosti i zajednička predanost unutar organizacija za sprječavanje, otkrivanje i suzbijanje kibernetičkih napada da bi organizacije mogle steći kibernetičku sigurnost (Smith i sur., 2010) Organizacijama se preporučuje integrirani pristup upravljanja rizikom kibernetičke sigurnosti koji omogućava procjenu i upravljanje rizicima na proaktivan način (Kure i sur., 2018). Recentna istraživanja upozorila su na nedostatke tradicionalnog upravljanja kibernetičkim rizikom prema metodi funkcionalnih silosa (engl. *Silo-based Traditional Risk Management – TRM*) izolirano od ostalih vrsta poslovnih rizika te je prepoznata potreba da se ovaj proces unaprijedi kroz integrirano upravljanje svim poslovnim rizicima (engl. *Enterprise Risk Management – ERM*) (Stine i sur., 2020; Suroso i sur., 2017). U Jarjoui i Murimi (2021) predstavljen je upravo jedan takav okvir za integrirano upravljanje kibernetičkim rizikom kroz ugradnju višestrukih međusobno povezanih dimenzija kao podloge za identifikaciju i ublažavanje rizika kibernetičke sigurnosti.

Premda zaposlenici poduzeća mogu uzrokovati značajne probleme na informacijskom sustavu i time povećati ranjivost poduzeća, prouzročiti poteškoće u odvijanju poslovnih aktivnosti i uzrokovati financijske gubitke, pod pojmom kibernetičkog rizika dominantno se podrazumijevaju vanjski napadi na poduzeće. Kako bi se poduzeća zaštitila od kibernetičkih rizika, nužno je identificirati kibernetičke ranjivosti, implementirati kibernetičke protokole i aktivno podizati „kibernetičku higijenu“ kroz edukaciju zaposlenika o potencijalnim prijetnjama (University of Cincinnati, 2022). Kibernetički napadi obično su usmjereni na pristup, promjenu i uništavanje osjetljivih podataka, iznudu novca od druge strane ili ometanje uobičajenog tijeka poslovnih procesa. Upravljanje kibernetičkim rizikom i podizanje kibernetičke sigurnosti primarno se odnosi na zaštitu sustava, mreža i programa poduzeća od napada (CISCO). Kibernetički napadi mogu dovesti do privremene nemogućnosti korištenja informacijskih sustava i obavljanja poslovnih aktivnosti, stoga je nužno da poduzeća raspolažu unaprijed definiranim planom kontinuiteta poslovanja, kojim su obuhvaćene mjere postupanja s kibernetičkim rizikom. Uspostava adekvatne organizacijske kulture u području kibernetičkog rizika podrazumijeva da svaki zaposlenik bude svjestan rizika s kojima se može suočiti na radnom mjestom i metoda kako odgovoriti na takve rizike.

U većim poduzećima nužno je uspostaviti efikasan sustav informacijske sigurnosti, a na čelu sustava najčešće je osoba zadužena za informacijsku sigurnost – *Chief Information Security Officer* (CISO), koja surađuje sa zaposlenicima poduzeća koji su upoznati s kibernetičkim prijetnjama u različitim segmentima poslovanja. Ovakva suradnja utemeljena je u jasno definiranim strategijama, politikama i procedurama poduzeća koje jasno delegiraju odgovornosti, načine komunikacije i cjelovit pristup upravljanju rizicima (Miloš Sprčić i sur., 2020). Kod manjih poduzeća nužno je razmotriti optimalnu organizaciju upravljanja kibernetičkim rizikom kroz zaduživanje postojećih zaposlenika ili eksternalizaciju.

3. METODOLOGIJA ISTRAŽIVANJA

3.1. Podaci

Istraživanje je provedeno na hrvatskom tržištu. Populacija istraživanja obuhvaća najuspješnija hrvatska poduzeća prema kriteriju ukupnog prihoda. Temelj definiranja populacije je lista objavljena od strane Financijske agencije i časopisa Lider, naziva „1.000 najvećih hrvatskih tvrtki prema ukupnom prihodu". S obzirom na to da su poduzeća koja pripadaju financijskoj ili osiguravateljskoj djelatnosti visokoregulirana te su u obvezi upravljati svim vrstama rizika kojima su izložena, fokus je ovog istraživanja na poduzećima kod kojih upravljanje rizicima nije zakonska obveza. Također, mikro i mala poduzeća, zbog resursnih ograničenja, ne uvode sustave upravljanja rizicima, usporedive s velikim i srednjim poduzećima te nisu u fokusu ovog istraživanja. Stoga su s navedene liste uklonjena poduzeća koja se bave financijskom ili osiguravateljskom djelatnošću te mikro i mala poduzeća. Populaciju istraživanja čini ukupno 918 velikih ili srednjih poduzeća koja pripadaju različitim djelatnostima, osim financijske ili osiguravateljske. Temeljem definiranih ciljeva i procjene financijskih troškova istraživanja, definiran je uzorak istraživanja, kojim je obuhvaćeno ukupno 430 poduzeća (46,84 % populacije).

Istraživanje je provedeno anketnim upitnikom koji je upućen poštom na Upravu poduzeća, Glavne izvršne direktore ili Glavne menadžere rizika poduzeća iz uzorka. Ispitanicima je ponuđena mogućnost da upitnik ispune i vrate poštom, ali i da pristupe online verziji upitnika. Istraživanje je provedeno u ukupnom trajanju od pet tjedana, pri čemu su nakon prva tri tjedna istraživanja poduzeća koja u tom razdoblju nisu odgovorila dodatno kontaktirana telefonskim putem, s ciljem povećanja odaziva na istraživanje. Nakon pet tjedana prikupljen je ukupno 101 anketni upitnik. Od toga je pet upitnika nepotpuno ispunjeno te su zbog toga eliminirani iz daljnje obrade. Ukupni uzorak istraživanja iznosi 96 poduzeća, što je 22,33 % uzorka istraživanja i zadovoljavajuće za ovaj tip istraživanja i generalizaciju rezultata.

3.2. Statističke metode

Kako bi se ispitao utjecaj upravljanja kibernetičkim rizikom na poslovne pokazatelje, formuliran je model ordinalne logističke regresije:

$$\text{Pokazatelj poslovanja poduzeća}_i = \beta_0 + \beta_1 * \text{kibernetički rizik}_i + \beta_2 * \text{starost}_i + \beta_3 * \text{veličina}_i + \beta_4 * \text{Zagrebačka burza}_i + \beta_5 * \text{orijentacija}_i + \varepsilon_i$$

Pri tome su oznake i značenja varijabli modela sljedeći:

- ***Pokazatelj poslovanja poduzeća$_i$:*** jedna od definiranih zavisnih varijabli modela (povećanje profitabilnosti, poboljšanje likvidnosti, poboljšanje solventnosti te uštede u troškovima, svijest zaposlenika o rizicima kojima je poduzeće izloženo, efikasnije donošenje odluka, povećanje sposobnosti poduzeća da ostvari zadane poslovne ciljeve, poboljšanje korporativne reputacije i jačanje slike odgovornog poduzeća koja se odašilje vanjskim dionicima poduzeća te inicijativa za promjenama ili inovacijama poduzeća) u poduzeću *i*, pripadnost poduzeća *i* određenoj homogenoj skupini poduzeća formiranoj temeljem sličnosti integriranog upravljanja rizicima
- ***kibernetički rizik$_i$:*** dummy varijabla kojom se određuje upravlja li poduzeće *i* kibernetičkim rizikom ili ne
- ***starost$_i$:*** logaritmirana vrijednost godina od osnutka poduzeća *i*
- ***veličina$_i$:*** logaritmirana vrijednost broja zaposlenih u poduzeću *i*
- ***Zagrebačka burza$_i$:*** dummy varijabla kojom se određuje kotira li poduzeće *i* na Zagrebačkoj burzi ili ne
- ***orijentacija$_i$:*** dummy varijabla kojom se određuje geografska orijentacija poduzeća *i*, tj. tržište na koje je poduzeće i primarno usmjereno.

Zavisna varijabla istraživanja su pokazatelji poslovanja poduzeća. U radu je analiziran utjecaj na više zavisnih varijabli koje su financijske i nefinancijske prirode. Zavisne varijable financijske prirode su povećanje profitabilnosti, poboljšanje likvidnosti, poboljšanje solventnosti te uštede u troškovima, a nefinancijske povećana svijest zaposlenika o rizicima kojima je poduzeće izloženo, efikasnije donošenje odluka, povećanje sposobnosti poduzeća da ostvari zadane poslovne ciljeve, poboljšanje korporativne reputacije i jačanje slike odgovornog poduzeća koja se odašilje vanjskim dionicima poduzeća, te inicijativa za promjenama ili inovacijama poduzeća. Podatci o zavisnim varijablama prikupljeni su anketnim upitnikom. Poduzeća su na Likertovoj skali od 1 do 5 procjenjivala svoje slaganje s tvrdnjama o doprinosu sustava upravljanja rizicima poduzeća različitim pokazateljima poslovanja na prethodno opisanoj listi od devet pokazatelja uspješnosti poslovanja. Pri tome ocjena 1 znači „izrazito se ne slažem“, 2 „ne slažem se“, 3 „niti se slažem niti se ne slažem“, 4 „slažem se“, a ocjena 5 „izrazito se slažem“. Pristup samoprocjene utjecaja integriranog upravljanja rizicima na financijske i nefinancijske pokazatelje uspješnosti poslovanja korišten je kod Peljhan i sur. (2018).

Nezavisna varijabla modela jest upravljanje kibernetičkim rizikom, pri čemu ova varijabla poprima binarnu vrijednost: 1 u slučaju da poduzeće upravlja ovom vrstom rizika te 0 u suprotnom slučaju.

Kontrolne varijable modela su starost poduzeća, veličina poduzeća, geografska orijentacija poduzeća na različita tržišta i pripadnost poduzeća Zagrebačkoj burzi. Ove su varijable izlučene temeljem postojeće znanstvene literature u kojoj je dokazana njihova relevantnost za integrirano upravljanje rizicima. Kontrolne varijable mjerene su kao:

1. starost poduzeća (*log godine*): logaritmirana vrijednost godina od osnutka poduzeća (Peljhan i sur., 2018)
2. veličina poduzeća (*log zaposleni*): logaritmirana vrijednost broja zaposlenih u poduzeću (Liebenberg i Hoyt, 2003; Beasley i sur., 2005; Pagach i Warr, 2011)

3. pripadnost Zagrebačkoj burzi (*ZSE*): *dummy* varijabla koja poprima sljedeće vrijednosti: 0 – poduzeće ne kotira na Zagrebačkoj burzi, 1 – poduzeće kotira na Zagrebačkoj burzi (Dvorski Lacković, 2021)
4. geografska orijentacija (*orijentacija*): *dummy* varijabla koja poprima sljedeće vrijednosti: 0 – nacionalno, 1 – regionalno, 2 – europsko i 3 – međunarodno tržište (Lechner i Gatzert, 2017; Peljhan i sur., 2018).

Podatci o nezavisnoj i kontrolnim varijablama prikupljeni su kroz anketni upitnik.

3.3. Validnost istraživanja

Logistička je regresija često korištena metoda za predviđanje diskretne zavisne varijable temeljem više nezavisnih varijabli koje mogu biti kontinuirane, diskretne, dihotomne ili sve od navedenog (Tabachnick i Fidell, 2014). S obzirom na to da je zavisna varijabla modela pokazatelj uspješnosti poslovanja poduzeća, mjerena Likertovom skalom, korištena je metoda ordinalne logističke regresije. Premda je multinomijalna logistička regresija relativno nerestriktivna metoda u smislu pretpostavki i zahtjeva (Tabachnick i Fidell, 2014), potrebno je voditi računa da među nezavisnim varijablama ne postoji visoka razina korelacije. Za ispitivanje utjecaja upravljanja kibernetičkim rizikom na pokazatelje uspješnosti poslovanja korišten je logit model uz Newton-Raphsonov algoritam. Kao mjera značajnosti modela korištena je -2Log (vjerojatnost).

4. REZULTATI ISTRAŽIVANJA I DISKUSIJA

Tablica 1. prikazuje strukturu anketiranih poduzeća prema vrsti djelatnosti koju obavljaju. Premda nešto više od trećine poduzeća pripada prerađivačkoj djelatnosti (36,46 %), struktura ispitanika sugerira da su istraživanjem obuhvaćene sve relevantne nefinancijske djelatnosti.

Tablica 1. Struktura ispitanika prema sektoru djelatnosti

Djelatnost	**Broj**	**Udio**
Poljoprivreda, šumarstvo i ribarstvo	3	3,13 %
Prerađivačka	35	36,46 %
Opskrba električnom energijom i plinom	6	6,25 %
Opskrba vodom i gospodarenje otpadom	2	2,08 %
Građevinarstvo	7	7,29 %
Trgovina	18	18,75 %
Prijevoz	11	11,46 %
Pružanje smještaja	5	5,21 %
Informacije i komunikacije	6	6,25 %
Ostalo	3	3,13 %
Ukupno	**96**	**100,00 %**

Kao što je vidljivo u Tablici 2., uzorak istraživanja možemo stratificirati i prema pripadnosti poduzeća Zagrebačkoj burzi. Gotovo trećina poduzeća (30,21 %) kotira na Zagrebačkoj burzi, dok 69,79 % pripada velikim i srednjim poduzećima koja nisu članice Burze.

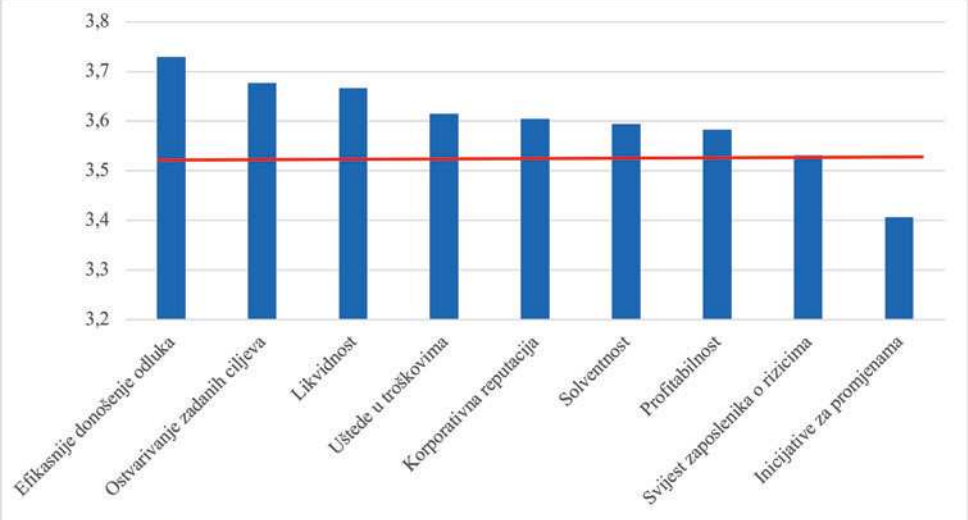
Tablica 2. Struktura ispitanika prema pripadnosti Zagrebačkoj burzi

Stratum	**Broj**	**Udio u uzorku**
Poduzeća koja kotiraju na Zagrebačkoj burzi	29	30,21 %
Ostala velika i srednja poduzeća	67	69,79 %
Ukupno	**96**	**100,00 %**

Čak se 59,37 % poduzeća izjasnilo da ne upravlja kibernetičkim rizikom. S obzirom na argumente o važnosti proaktivnog upravljanja kibernetičkim rizikom, koji su izneseni u teorijskom dijelu ovog rada, navedeni je podatak zabrinjavajući. Ako je među najuspješnijim hrvatskim poduzećima, mjereno ukupnim prihodima, samo 40,63 % poduzeća prepoznalo važnost upravljanja kibernetičkim rizikom, opravdano je zapitati se kolika je razina ranjivosti poduzeća, koliko je njihovo poslovanje stabilno te koliko su poslovni podatci ugroženi.

S obzirom na to da je cilj suvremenog pristupa upravljanju rizicima doprinos stvaranju vrijednosti poduzeća, u sklopu istraživanja analizirano je kako upravljanje rizicima utječe na poslovne pokazatelje: (1) povećanje profitabilnosti, (2) poboljšanje likvidnosti, (3) poboljšanje solventnosti, (4) uštede u troškovima, (5) povećanu svijest zaposlenika o rizicima kojima je poduzeće izloženo, (6) efikasnije donošenje odluka, (7) povećanje sposobnosti poduzeća da ostvari zadane poslovne ciljeve, (8) poboljšanje korporativne reputacije i jačanje slike odgovornog poduzeća, koja se odašilje vanjskim dionicima poduzeća te (9) inicijativa za promjenama ili inovacijama poduzeća. Prva četiri navedena pokazatelja odnose se primarno na financijsku perspektivu poslovanja, dok se preostali pokazatelji odnose na nefinancijsku perspektivu.

Slika 1. Analiza doprinosa sustava upravljanja rizicima poslovnim pokazateljima



Na Slici 1. prikazan je doprinos sustava upravljanja rizicima poslovnim pokazateljima, pri čemu su pokazatelji prikazani sukladno procjeni koju su ispitanici iznijeli. Ispitanici su se izjasnili da je glavni doprinos sustava upravljanja rizicima u poduzeću vidljiv kroz efikasnije donošenje odluka. Slijede, uz ujednačen procijenjen doprinos, povećana sposobnost poduzeća da ostvari zadane poslovne ciljeve te poboljšanja u likvidnosti. Ispitanici su procijenili doprinos sustava upravljanja rizicima kao ispodprosječan u segmentu poboljšanja profitabilnosti, povećanju svijesti zaposlenika o različitim rizicima kojima je poduzeće izloženo, a najniže je procijenjen doprinos inicijativama poduzeća za promjenama ili uvođenjem inovacija. Vrlo je neobično primijetiti da ispitanici percipiraju ispodprosječnim doprinos sustava upravljanja rizicima povećanju svijesti zaposlenika o rizicima kojima je poduzeće izloženo. Jedan od stupova suvremenog pristupa upravljanju rizicima jest adekvatna organizacijska kultura rizika, koja, između ostalog, podrazumijeva da je svaki zaposlenik svjestan rizika povezanih s poduzećem i posebno vlastitim radnim mjestom, kao i mjerama postupanja s rizicima. Kada ovaj podatak povežemo s činjenicom da se samo 40,63 % poduzeća izjasnilo da upravlja kibernetičkim rizikom, možemo zaključiti da je sustav upravljanja rizicima u hrvatskim poduzećima tradicionalno orijentiran te da je nužno osvještavati poduzeća kako da osuvremene vlastiti stav o upravljanju rizicima i uvedu sustave koji će im pomoći da proaktivno upravljaju rizicima kojima su izloženi.

U Tablici 3. prikazana je korelacijska matrica između nezavisne i kontrolnih varijabli modela. Između navedenih varijabli ne postoji visoka korelacija. Upravljanje kibernetičkim rizikom u pozitivnoj je korelaciji s veličinom i starošću poduzeća, orijentacijom poduzeća na nacionalno i europsko tržište te činjenicom da poduzeće ne kotira na Zagrebačkoj burzi. Upravljanje kibernetičkim rizikom negativno je korelirano s kotacijom poduzeća na Zagrebačkoj burzi te orijentacijom poduzeća na regionalno i globalno tržište.

Rezultati provedene ordinalne logističke regresije prikazani su u Tablici 4. Od ukupno devet analiziranih modela ordinalne logističke regresije, dva su modela značajna: model kojim se ispituje utjecaj upravljanja kibernetičkim rizikom na likvidnost i reputaciju poduzeća. Pri tome je jedino u modelu kojim se ispituje utjecaj na likvidnost poduzeća potvrđena statistička značajnost varijable upravljanje kibernetičkim rizikom, a smjer njezina utjecaja je, suprotno očekivanjima, negativan. Rezultati su u suprotnosti s dosadašnjim istraživanjima, koja su potvrdila iznimnu važnost upravljanja kibernetičkim rizikom za poduzeća, analizirano putem različitih financijskih i nefinancijskih pokazatelja, primjerice Hasan i sur. (2021) te Berlilana i sur. (2021.), koji su potvrdili pozitivan utjecaj spremnosti organizacije za kibernetičku sigurnost kroz aktivno upravljanje kibernetičkim rizikom na financijsku i nefinancijsku izvedbu poduzeća.

Potencijalni razlog zašto su samo dva modela ordinalne logističke regresije značajna može biti uzrokovan činjenicom da su ispitanici koristili metodu samoprocjene o pokazateljima uspješnosti poslovanja. Stoga je preporuka za buduća istraživanja koristiti objektivnije pokazatelje uspješnosti poslovanja, barem u domeni financijskih pokazatelja koje je moguće izlučiti iz financijskih izvještaja poduzeća. Vezano uz dokazan negativan utjecaj upravljanja kibernetičkim rizikom na likvidnost poduzeća, autori sugeriraju u budućim istraživanjima koristiti kompleksniju mjeru upravljanja kibernetičkim rizikom, kojom bi se ispitalo više faktora koji utječu na kibernetičku sigurnost poduzeća i provođenje istraživanja na većem uzorku poduzeća.

Tablica 3. Korelacijska matrica

	Log dani	**Log zaposleni**	**Orijenta-cija-0**	**Orijenta-cija-1**	**Orijenta-cija-2**	**Orijenta-cija-3**	**ZSE-0**	**ZSE-1**	**KIBER-NETIČKI RIZIK-0**	**KIBER-NETIČKI RIZIK-1**
Log dani	**1**	0,160	0,021	-0,051	0,041	-0,010	-0,232	0,232	-0,073	0,073
Log zaposleni	0,160	**1**	-0,022	0,037	0,021	-0,031	-0,198	0,198	-0,259	0,259
Orijentacija-0	0,021	-0,022	**1**	-0,315	-0,306	-0,380	0,118	-0,118	-0,061	0,061
Orijentacija-1	-0,051	0,037	-0,315	**1**	-0,289	-0,359	-0,019	0,019	0,047	-0,047
Orijentacija-2	0,041	0,021	-0,306	-0,289	**1**	-0,348	0,019	-0,019	-0,024	0,024
Orijentacija-3	-0,010	-0,031	-0,380	-0,359	-0,348	**1**	-0,111	0,111	0,036	-0,036
ZSE-0	-0,232	-0,198	0,118	-0,019	0,019	-0,111	**1**	-1,000	-0,036	0,036
ZSE-1	0,232	0,198	-0,118	0,019	-0,019	0,111	-1,000	**1**	0,036	-0,036
KIBERNETIČKI RIZIK-0	-0,073	-0,259	-0,061	0,047	-0,024	0,036	-0,036	0,036	**1**	-1,000
KIBERNETIČKI RIZIK-1	0,073	0,259	0,061	-0,047	0,024	-0,036	0,036	-0,036	-1,000	**1**

Tablica 4. Rezultati modela ordinalne logističke regresije

Zavisna varijabla	**(1) Profita-bilnost**	**(2) Likvid-nost**	**(3) Solvent-nost**	**(4) Upravljanje troškovima**	**(5) Svijest zaposlenika**	**(6) Donošenje odluka**	**(7) Ostvarivanje poslovnih ciljeva**	**(8) Reputa-cija**	**(9) Promjene/ inovacije**
Starost poduzeća	0,543 (0,618)	0,677 (0,633)	0,104 (0,619)	0,462 (0,627)	0,781 (0,628)	0,702 (0,678)	0,353 (0,628)	-0,357 (0,665)	0,211 (0,602)
Veličina poduzeća	-0,310 (0,329)	-0,359 (0,330)	-0,268 (0,331)	-0,612 (0,330)	-0,849 (0,331)	-0,696 (0,362)	-0,584 (0,325)	-0,588 (0,334)	-0,675 (0,335)
Geografska orijentacija – regionalno	0,010 (0,556)	-0,337 (0,560)	-0,518 (0,561)	-0,427 (0,555)	-0,577 (0,546)	-1,041 (0,620)	-0,420 (0,561)	-0,582 (0,560)	-0,371 (0,557)
Geografska orijentacija – europsko	-0,592 (0,558)	-0,695 (0,549)	-0,615 (0,545)	0,155 (0,548)	-0,372 (0,554)	-0,752 (0,603)	0,034 (0,548)	-1,031 (0,561)	-0,065 (0,547)
Geografska orijentacija – međunarodno	0,211 (0,524)	-0,204 (0,526)	-0,358 (0,529)	0,258 (0,529)	-0,255 (0,523)	-0,452 (0,568)	0,167 (0,528)	-0,162 (0,525)	-0,035 (0,524)
Zagrebačka burza –kotira (1)	-0,350 (0,451)	-0,140 (0,445)	0,249 (0,443)	0,297 (0,451)	0,361 (0,437)	0,601 (0,484)	0,404 (0,441)	1,020 (0,451)	0,857 (0,445)
Kibernetički rizik –upravlja (1)	-1,128 (0,424)	**-1,658 (0,442)**	-1,647 (0,439)	-1,128 (0,423)	-0,765 (0,404)	-0,766 (0,453)	-0,893 (0,416)	-1,112 (0,429)	-0,972 (0,417)
N	96	96	96	96	96	96	96	96	96
-2Log (Vjerojatnost)	0,071	**0,003**	0,006	0,025	0,038	0,063	0,088	**0,002**	0,021

5. ZAKLJUČAK

Ciljevi provedenog istraživanja bili su utvrditi u kojoj mjeri hrvatska poduzeća upravljaju kibernetičkim rizikom i kakav je utjecaj upravljanja njime na pokazatelje poslovanja poduzeća. Rezultati istraživanja sugeriraju da relativno malen udio poduzeća upravlja kibernetičkim rizikom. Ovakvi su rezultati obeshrabrujući kada se uzme u obzir da su istraživanjem obuhvaćena najuspješnija hrvatska poduzeća, mjereno ukupno ostvarenim prihodima, kao i značajan broj poduzeća koja kotiraju na Zagrebačkoj burzi. Ispitani menadžeri trebali bi prakticirati korporativnu odgovornost, između ostalog, i kroz upravljanje ovim rizikom kao jednim od vodećih s kojima se poduzeća u posljednje vrijeme suočavaju, a očekuje se porast njegove značajnosti u nadolazećem razdoblju. Opravdano je zapitati se kakvi bi rezultati bili da su istraživanjem obuhvaćena poduzeća koja su manje uspješna temeljem ostvarenih prihoda.

U radu je dokazano da upravljanje kibernetičkim rizikom ima značajan negativan utjecaj na likvidnost poduzeća. S obzirom na to da je za mjerenje kibernetičkog rizika korištena jednostavna mjera, tj. *dummy* varijabla, to ujedno predstavlja i ograničenje istraživanja. Stoga je preporuka da se u budućim istraživanjima upravljanje kibernetičkim rizikom mjeri kroz složeniju mjeru kojom bi bile obuhvaćene višestruke dimenzije upravljanja kibernetičkim rizikom. Također, jedno od potencijalnih ograničenja istraživanja jest korištenje metode samoprocjene ispitanika, vezano uz pokazatelje uspješnosti poslovanja. Premda je navedeni pristup u postojećoj znanstvenoj literaturi korišten i za financijske i nefinancijske pokazatelje poslovanja, preporuka je da se u budućim istraživanjima kao zavisna varijabla uključe i objektivni pokazatelji financijske uspješnosti poduzeća temeljem podataka iz financijskih izvještaja poduzeća.

Teorijski je doprinos rada u analizi postojeće znanstvene literature iz područja upravljanja kibernetičkim rizikom, pri čemu je uočen jaz između praktične važnosti područja kibernetičke sigurnosti poduzeća i znanstvenih istraživanja koja se bave ovim područjem. U znanstvenom smislu, ovo je inicijalno istraživanje kojim se područje upravljanja kibernetičkim rizikom ispituje u hrvatskim uvjetima, kao dio šireg okvira integriranog upravljanja rizicima. U praktičnom smislu, radom je znanstvenoj zajednici, ali i stručnjacima iz prakse, skrenuta pozornost na nužnost konstruiranja sveobuhvatne mjere upravljanja kibernetičkim rizikom i provođenja daljnjih analiza vezanih uz utjecaj na različite dimenzije poslovanja poduzeća.

POPIS LITERATURE

1. Ahmed, E. M. (2021). Modelling information and communications technology cyber security externalities Spillover EFFECTS on sustainable economic growth. *Journal of the Knowledge Economy*. 12, 412–430.
2. Allianz (2022). *Allianz Risk Barometer 2022*. Allianz Global Corporate and Specialty.
3. Beasley, M., Clune, R., Hermanson, D. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, Vol. 24 (6), str. 521-531.

4. Berg, H. P. (2010). Risk management: Procedures, methods and experiences. *Risk Management,* 1, str. 79–95.
5. Berlilana, Noparumpa T., Ruangkanjanases A., Hariguna T., Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. *Sustainability*. 13 (24): 13761. https://doi.org/10.3390/su132413761.
6. CISCO. *What is Cybersecurity*? Dostupno na: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
7. Deloitte (2021). *Global Risk Management Survey, 12th Edition*. Deloitte Insights LLC.
8. Dvorski Lacković, I. (2021). *Analiza integriranoga upravljanja rizicima i povezanost s poduzetničkom orijentacijom i uspješnošću hrvatskih poduzeća*. Doktorska disertacija. Ekonomski fakultet Sveučilišta u Zagrebu.
9. Europska komisija (2020). *What is digital transformation*, Dostupno na: https://ec.europa.eu/croatia/what_is_digital_transformation_changing_hr Pristupano: 01. 09. 2022.
10. Hasan, S., Ali, M., Kurnia, S., Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications,* Volume 58, DOI: 10.1016/j.jisa.2020.102726. Available on-line https://www.sciencedirect.com/science/article/abs/pii/S2214212620308656?via%3Dihub
11. Jarjoui. S., Murimi R., (2021). *A Framework for Enterprise Cybersecurity Risk Management*. Book Chapter – Advances in Cybersecurity Management, str.139-161, DOI:10.1007/978-3-030-71381-2_8
12. Kure H. I., Islam, S., Razzaque, M. A. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*. 8 (6) :898. https://doi.org/10.3390/app8060898
13. Lechner, P., Gatzert, N. (2017). Determinants and Value of Enterprise Risk Management: Empirical Evidence from Germany. *The European Journal of Finance*. Vol. 24 (10), str. 867-887.
14. Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*. 12 (9) : 157. https://doi.org/10.3390/fi12090157
15. Liebenberg, A. P., Hoyt, R. E. (2003). The determinants of enterprise risk management: evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, Vol. 6 (1), str. 37-52.
16. Marc, M., Miloš Sprčić, D., Mešin *Žagar*, M. (2018). Is enterprise risk management a value added activity? *Ekonomika a management*, XXI (1), str. 68-84.
17. Miloš Sprčić, D., Dvorski Lacković, I., Bedeković, K. (2020). *Strategic, financial and operational risk management through Enterprise Risk Management model* // Enterprise Risk Management: Theory and Practice with Selected Case Studies of Multinational Companies / Miloš Sprčić, Danijela (gl. ured.); Zoričić, Davor, Sabol, Andrija, Pecina, Ena, Dvorski Lacković, Ivana (ur.). Ekonomski fakultet Sveučilišta u Zagrebu, 2020. str. 63-127. Pristupano: 02. 09. 2022.
18. Pagach, D., Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of Risk and Insurance*, Vol. 78 (1), str. 185–211.

19. Peljhan, D., Miloš Sprčić, D., Marc, M. (2018). Strategy and organizational performance: The role of risk management system development. *Performance Measurement and Management Control: The Relevance of Performance Measurement and Management Control Research*. Emerald Group Publishing Limited.
20. Protiviti (2021). *2021&2030 Executive Perspectives on Top Risks*. NC State University, ERM Initiative and Protiviti.
21. Ravichandran, T., Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: A resource based perspective. *Journal of Management Information System*. 21, str. 237–276.
22. RSA (2019). *Managing Digital Risk. 8 Types of Digital Risk and How to Manage Them*. Dostupno na: https://www.ciosummits.com/Online_Assets_RSA_How_to_Manage_Eight_Types_of_Digital_Risk.pdf Pristupano: 22. 03. 2022.
23. Smith, S., Winchester, D., Bunker, D., Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. MIS Q. 34, str. 463–486.
24. Srinidhi, B., Yan, J. and Tayi, G. (2015). Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. *Decision Support Systems,* 75, str. 49-62.
25. Stine, K, Quinn, S., Witte, G., Gardner, R. K. (2020). Integrating cybersecurity and enterprise risk management (ERM). *NISTIR 8286, National Institute of Standards and Technology,* Gaithersburg, Maryland, USA.
26. Suroso, J. S., Harisno, Noerdianto J. (2017. Implementation of COSO ERM as security control framework in cloud service provider. *Journal of Advanced Management Science 5*.
27. Svjetski Ekonomski Forum (2022). *The Global Risks Report 2022*, World Economic Forum, Cologne/Geneva, World Economic Forum, 2022.
28. Tabachnick, B., Fidell, L. (2014). *Using Multivariate Statistics*. Pearson Education.
29. University of Cincinnati (2022). *War in Ukraine – Business and Risk Management Implications*. Dostupno na: https://www.uc.edu/news/articles/2022/04/gc-war-in-ukraine--business-and-risk-management-implications.html Pristupano: 10. 05. 2022.