KIBERNETIČKA SIGURNOST: KLJUČNI IZAZOV NEOVISNE REVIZIJE

Jurišić, Martina

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

KIBERNETIČKA SIGURNOST:

KLJUČNI IZAZOV NEOVISNE REVIZIJE

Mentor:

doc. dr. sc. Marko Čular

Student:

Martina Jurišić

Split, kolovoz 2022.

SADRŽAJ

1. UVOD

1.1. Predmeti i problem rada

Tehnološki razvoj stavlja naglasak na brz i dinamičan razvoj novih usluga i proizvoda, dok su sigurnosni aspekti, u pravilu, imali vrlo mali utjecaj na široko prihvaćanje novih tehnologija. Korisnici najčešće imaju minimalno znanje o tehnologiji koju koriste, a način primjene je takav da je vrlo teško procijeniti sigurnosna obilježja većine komercijalnih proizvoda obzirom na zaštitu povjerljivosti, privatnosti podataka korisnika. Suvremena su poduzeća duboko prožeta komunikacijskom i informacijskom tehnologijom. Ljudi su povezani putem raznovrsnih tehnologija za prijenos teksta, slike, zvuka. Stvaranjem interneta stvoren je suvereni kibernetički prostor koji sačinjava ne samo već prethodno spomenuta infrastruktura, već i stalno rastuća količina raspoloživih podataka te korisnika koji međusobno komuniciraju u sve većem broju.

Obzirom na zastupljenost informacijskih tehnologija u životima ljudi, kako privatno tako poslovno, odstupanja od ispravnog rada međusobno povezanih sustava više nisu samo tehničke smetnje, već predstavljaju opasnost globalnih sigurnosnih razmjera. Sve je veća izloženost pojedinaca u *cyber* prostoru te je samim time povećana izloženost *cyber* napadima. Stoga, javlja se potreba za zaštitom podataka u elektroničkom obliku koja se naziva kibernetička (*engl. cyber*) sigurnost.[1]

U poslovnim okruženjima većina se podataka, osim u papirnatom obliku, pohranjuje i čuva u e-obliku. Obzirom na delikatnost poslovnih informacija i podataka, upravo je kibernetička sigurnost ta koja može bitno uvećati razinu sigurnosti istih. Kibernetička se sigurnost mora neprestano nadograđivati i razvijati kako bi bila ukorak s tehnološkim razvojem, koji se izmjenjuje gotovo svakodnevno. Problematika ovog rada odražava se u načinu procjene neovisnog revizora kibernetičke sigurnosti kao ključnog prepoznatog rizika poslovanja. Razni su pristupi koji se smatraju kibernetičkim napadima, uvelike krajnji je cilj izazivanje nereda u virtualnom svijetu, saznavanje raznih povjerljivih informacija. Reperkusije takvih postupaka

[1] Središnji državni ured za razvoj digitalnog društva (2022). Kibernetička sigurnost. Preuzeto s https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436

značajne su, u najmanju ruku izazivaju pomutnju, značajnije, izazivaju sigurnosne probleme te „curenje“ povjerljivih informacija u javnost.

Za vrijeme pandemije bolesti Covid-19, ustanovljena je stvarna razina oslanjanja na informacijske tehnologije te je radi istog stavljen naglasak na važnost kibernetičke sigurnosti.[2] Nadalje u radu, bit će obrađene determinante koje su pod pritiskom kibernetičke sigurnosti utjecale na ulogu i važnost neovisne revizije.

1.2. Istraživačka pitanja

Obzirom na definirani predmet i problem rada, bit će odgovorena sljedeća istraživačka pitanja:

- Je li kibernetička sigurnost ključni poslovni rizik?
- U kojem obujmu kibernetički događaji utječu na svjetsku potrošnju na proizvode i usluge na informacijsku sigurnost?
- Koje je izazove donijela pandemija bolesti Covid-a 19 za neovisne revizore?
- Kakva je uloga kibernetičke sigurnosti u provedbi neovisne revizije?
- Na koji način neovisna revizija procjenjuje rizike kibernetičke sigurnosti?

1.3. Cilj rada

Cilj je rada ukazati na sve veću kibernetičku prijetnju poslovnim subjektima obzirom na povećano oslanjanje na tehnologiju kao takvu. Cilj rada jest definirati i odrediti komponente i ulogu kibernetičke sigurnosti u provedbi neovisne revizije, obzirom na važnost iste te izazova koje za njih stvara svakodnevno poslovanje. Također, cilj je rada prikazati korelaciju među povećanim naknadama za reviziju te rizicima od kibernetičkih napada. Uz sve veću izloženost poduzeća kibernetičkim napadima, korelira i povećanje potrošnje na pokušaj obrane od takve vrste napada. Cilj je odrediti koliko se „klasična“ revizija mijenja u uvjetima pojave sigurnosnih događaja ili kibernetičkih napada.

[2] Vlada Republike Hrvatske (2015). Odluka o donošenju nacionalne strategije kibernetičke sigurnosti i akcijskog plana za provedbu nacionalne strategije kibernetičke sigurnosti. Preuzeto s https://www.uvns.hr/UserDocsImages/dokumenti/Odluka_o_dono%C5%A1enju_Nacionalne_strategije_kibernet i%C4%8Dke_sigurnosti_i_Akcijskog_plana_za_provedbu_Nacionalne_strategije_kiberneti%C4%8Dke_sigurno sti.pdf?vel=702079

1.4. Metode istraživanja

Metode koje su korištene u radu su metoda analize, metoda sinteze, metoda deskripcije i metoda eksplantacije, kritička metoda procjene rizika kibernetičke sigurnosti od strane neovisne revizije. Deskriptivna se metoda definira kao metoda jednostavnog objašnjavanja činjenica, korištenje je ograničeno na objašnjavanje temeljnih pojmova. Metodom analize pojedina se cjelina raščlanjuje na dijelove, koji se potom podrobno promatraju i detaljno objašnjavaju. Spajanjem jednostavnih pojmova u složenije u jednu cjelinu, nazivamo metodom sinteze. Obzirom na ograničene resurse, najveći dio podataka prikupljen je na internetu, koristeći sekundarne podatke.

1.5. Doprinos istraživanja

Kibernetička je sigurnost donedavno poduzećima predstavljala isključivo trošak te ista nisu uviđala prednosti ulaganja u istu. Međutim, samim napretkom društva te sve veću integraciju tehnologije u svakodnevno poslovanje, ulaganje u kibernetičku sigurnost predstavlja nužnost poslovne današnjice. Obzirom da su informacije jednom poduzeću najbitnija imovina, ne iznenađuje da se iste žele zaštiti od pokušaja kibernetičkih prijetnji ili napada.

U teorijskom dijelu rada pregledava se dostupna literatura koja se bavi ovom problematikom, dok empirijski dio daje uvid u praktično obavljanje procedura neovisne revizije, napose u uvjetima kibernetičkih događaja. Zaključci na definirana istraživačka pitanja aktualna su tema te su vrijedan izvor informacija za buduća istraživanja koja će se baviti istom problematikom.

1.6. Struktura rada

Završni rad podijeljen je na 6 tematskih cjelina. U prvoj tematskoj cjelini definiran je problem i predmet rada, istraživačka pitanja kojima će se istraživač baviti te su objašnjene metode istraživanja kojima se istraživač koristi. Definirani su ciljevi, doprinosi istraživanja te struktura rada.

Druga tematska cjelina sadrži teorijski okvir kibernetičke sigurnosti, koji je razrađen pregledom dostupne literature te stručnih časopisa.

U trećoj tematskoj cjelini objašnjen je utjecaj pandemije Covid-a 19 na postupke i obavljanje neovisne revizije, te izazov koji to predstavlja neovisnim revizorima.

Empirijski dio rada obrađen je kroz četvrtu i petu tematsku cjelinu kroz koji se razmatra uloga kibernetičke sigurnosti u provedbi neovisne revizije te način na koji se u takvim uvjetima provodi neovisna revizija. Obrađuje se pitanje kako neovisna revizija procjenjuje rizik kibernetičke sigurnosti.

U šestom poglavlju predočen je zaključak te se daju odgovori na definirana istraživačka pitanja.

2. KIBERNETIČKA SIGURNOST

2.1. Kibernetička sigurnost – ključni poslovni rizik

Kibernetička ili *cyber* sigurnost sustavno je i sveobuhvatno planiranje strateški bitnih aktivnosti u svrhu zaštite korisnika suverenih elektroničkih usluga. Implementacijom ovih strateški bitnih aktivnosti želi se postići jedinstveni i organizirani odgovor cijelog niza sektorski nadležnih institucija na sigurnosne prijetnje kibernetičkom sustavu. Razlog tome krije se u kompleksnosti područja kibernetičke sigurnosti i prodiranja iste u sve segmente društva.[3] Određenu razinu pouzdanosti pri korištenju proizvoda/usluga u kibernetičkom prostoru osiguravaju spomenute aktivnosti i mjere koje omogućuju sustavnu zaštitu računala, računalnih mreža, informacijskih i informatičkih infrastruktura, podataka od zlonamjernih napada.[4] Iako moderna tehnologija poduzećima omogućava stvaranje i održavanje konkurentske prednosti, ipak postoje negativne osobine iste, obzirom na ustanovljeni negativni trend u navedenim tehnologijama, a koji je povezan s kibernetičkim napadima i prijetnjama.

Društvena te gospodarska struktura dovedena je u iskušenje krizom uzorkovanom pandemijom bolesti COVID-a 19. Obzirom na zastupljenost informacijske tehnologije u svakodnevnom životu te našu ovisnost o istoj, kriza prouzročena kibernetičkim napadima ima potencijal poprimiti obrise nove pandemije. Potrebno je povećati otpornost informacijskih sustava u cilju zaštite njegovih krucijalnih dijelova.

Pojavljivanjem novih uređaja na mreži, te njihovim povezivanjem s drugim uređajima pospješuje se područje napada u djelokrugu kibersigurnosti. Sve veća zastupljenost „internet stvari“, računarstva u oblaku, sistema velikih podataka te digitalizacije industrije, eksponiraju se slabe točke sustava, čime se u opasnost dovodi veći broj žrtava. Sve je teže biti ukorak s napadima obzirom na njihovu sve veću sofisticiranost. [5]

[3] Ministarstvo unutarnjih poslova (2022). Kibernetička sigurnost. Preuzeto s https://mup.gov.hr/istaknute-teme/nacionalni-programi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335

[4] Središnji državni ured za razvoj digitalnog društva (2022). Kibernetička sigurnost. Preuzeto s https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436

[5] European Union Agency for Network and Information Security ENISA (2019). Threat Landscape Report 2018 – 15 Top Cyberthreats and Trends. Preuzeto s https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Slijedom svega navedenog organizacijske strukture moraju osigurati odgovarajuću zaštitu svoje organizacije implementacijom mjera i aktivnosti kibernetičke sigurnosti, ukoliko ne žele da njihova organizacija bude zahvaćena rizicima od napada ili *cyber* prijetnja.[6]

Kibernetičke prijetnje sigurnosti javljaju se u različitim pojavnim oblicima, ovisno o tome što se s podacima želi učiniti. Moguće je da podaci budu objavljeni ili/i izmijenjeni bez dopuštenja, uništeni te da se uskraćuje pristup istima.[7]

Slika 1: Vrste kibernetičkih prijetnji[8]

[6] Tušek, B. i Halar, P. (2017). Uloga interne revizije u povećanju djelotvornosti procjenjivanja i upravljanja cyber sigurnosti. *Računovodstvo i financije*, *63*(9), 42-53.

[7] Contact Committee of the Supreme Audit Institutions of the European Union (2020). Cybersecurity in the EU and its Member States. Preuzeto s https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf

[8] Ibid

Uobičajene vrste kibernapada jesu:

- zlonamjerni programi (engl. malware)
- ucjenjivački program (npr. engl. WannaCry)[9]
- distribuirani napadi uskraćivanjem usluga (tzv. DDos)[10]
- mrežni napadi (npr. engl. Drive-by)
- ubacivanje zlonamjernog koda (engl. formjacking)[11]
- socijalni inženjering (npr. engl. psihing)[12]
- napadi trajne prijetnje[13]

Kibernetički napadi posljednjih godina postaju gorući problem. 2016. godine 80% poduzeća u EU prijavljuje barem jedan incident vezan uz kibernetičku sigurnost.[14] Istraživanje provedeno 2018. godine ukazuje na to da je 40% ispitanika, koji se dnevno služe robotikom i automatizacijom u okviru svoga radnog mjesta, prijavilo smetnje u radu koje opisuju kao najtežu posljedicu kibernetičkih napada na sustave poslovanja. Iako svjesne rizika kibernetičkih napada, poduzeća nerijetko imaju ili neadekvatne sustave za obranu od napada ili ih nemaju uopće.[15] Serioznost, broj napada, financijski troškovi uzrokovani istima od tada nastavljaju rasti. Procijenjeno je da su 2021. godine financijski troškovi uzrokovani kibernetičkim napadima narasli na 6 bilijuna USD. Isti taj trošak u 2015. godini iznosi 3 bilijuna USD. U usporedbi s 2015. godinom taj iznos 3 je bilijuna USD veći u odnosu na 2021. godinu.[16] Procjenjuje se da se prosječan trošak kibernetičkih incidenta povećao za 72% u odnosu na 2015. godinu.[17] Istraživanjem iz 2020. godine utvrđeno je da kibernetički kriminal zahvaća različito

[9] Greenberg, A. (2017). Hold North Korea Accountable For Wannacry – and the NSA, too. Preuzeto s https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/

[10] De Bolle, C. (2018). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

[11] European Union Agency for Network and Information Security ENISA (2020). Threat Landscape – Web-based attacks. Preuzeto s https://www.enisa.europa.eu/publications/web-based-attacks

[12] De Bolle, C. (2018). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf

[13] Lee-Makiyama, H. (2018). *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* European Centre for International Political Economy (ECIPE), 2(18), 1-20.

[14] Wainwright, R. (2017). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/iocta/2017/FOREWORD.html

[15] The Global State of Information Security (2017). Survey 2017 – Moving forward with cybersecurity and privacy. Preuzeto s https://www.pwc.com/gsiss2015

[16] Morgan, S. (2019). Official Annual Cybercrime Report – Herjavec Group. Preuzeto s https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[17] European Systemic Risk Bord (2020). ESRB recommends establishing a systemic cyber incident coordination framework. Preuzeto s https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr.220127~f1548f677e.en.html

pojedinačne gospodarske resore.[18] Najveću ugrozu prijevarne bi radnje uzrokovale u tijelima vlasti, javnoj upravi, sektoru zdravstva, tehnologije, telekomunikacije i medija. Nešto manje, ali svejedno značajnu ugrozu prijevarne radnje uzrokovale bi u financijskom, proizvodnom i industrijskom sektoru.

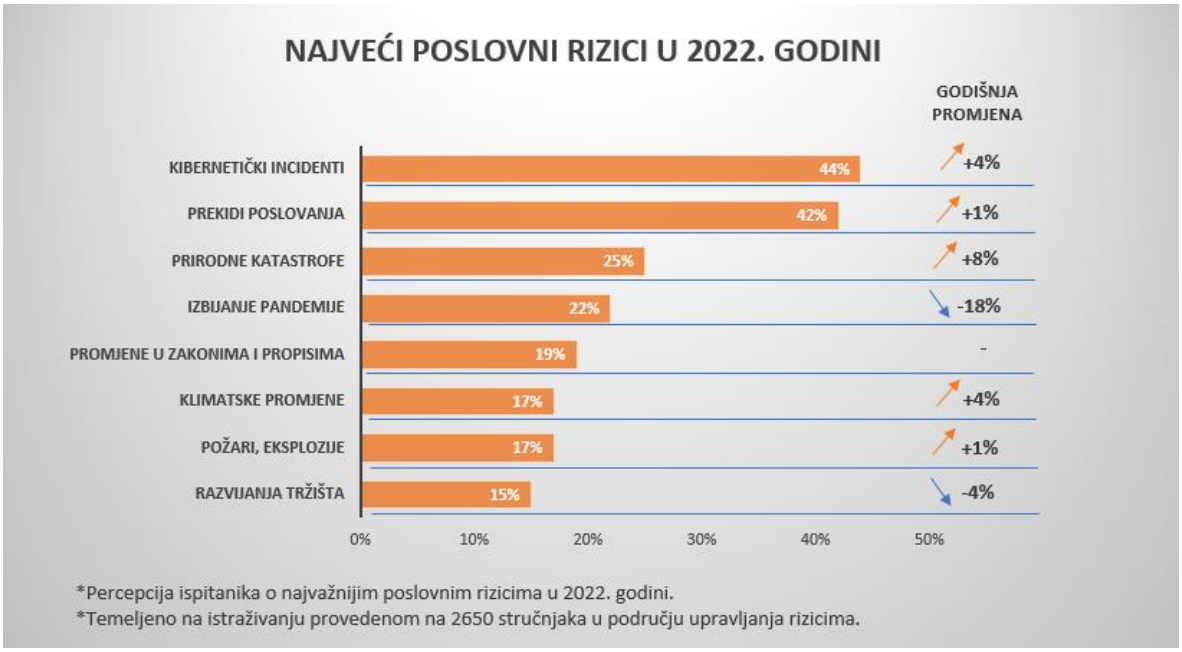
Po broju kibernetičkih napada, 2021. godina bila je rekordna, te se iz tog razloga predvidjelo da će u 2022. godini kibernetička sigurnost biti „top" rizik svakog poslovanja. Situaciju nastalu radi pandemije korona virusa te premještaj zaposlenih na hibridni i *remote* način rada. *Cyber* kriminalci i dalje vješto koriste ranjivosti sustava za izvršenje raznih *cyber* prijetnji i napada. Neovisno o veličini i vrsti djelatnosti, mnoga su poduzeća iskusile neku vrstu *cyber* incidenta ili pokušaj *cyber* proboja. Obzirom na činjenicu da „cyberkriminalne" aktivnosti nisu posustajale ni prethodnih godina, očekuje da će se isti trend nastaviti i u 2022. godini. Preduvjet za adekvatno planiranje zaštite poslovnih informatičkih i informacijskih sustava podrazumijeva poznavanje trendova koje se mogu očekivati u tekućoj godini. Očekivani problemi s kojima će se industrije susretati u tekućoj godini bit će nedostatak *cyber* sigurnosnih vještina. Svaki od tih digitalnih odnosa predstavlja novi skup kibernetičkih ranjivosti. Potreba za sigurnošću i način na koji se ona provodi moraju biti pažljivo uravnoteženi s potrebama organizacije za učinkovitim radom i aktivnim postizanjem svojih budućih ciljeva. Iako nije moguće u potpunosti eliminirati rizik od kibernetičkog napada, dobro osmišljen, aktivan program kibernetičke sigurnosti umanjit će negativan utjecaj na kratkoročne i dugoročne poslovne ciljeve.[19]

Novo istraživanje koje je proveo Allianz Global Corporate & Specialty postavilo je 2.650 stručnjaka za upravljanje rizicima najveće poslovne rizike za 2022. godinu. Ovi stručnjaci potječu iz 89 zemalja svijeta te su *cyber* incidente ocijenili kao najveći rizik za poslovanje. Prirodne katastrofe i učinci klimatskih promjena također su dobili na važnosti kao čimbenici koji utječu na globalno poslovanje. Više od 40 posto stručnjaka anketiranih od strane Allianz Global Corporate & Specialty smatra da će kibernetički kriminal i prekidi poslovanja biti najveći poslovni rizici u 2022. Grafikonom je prikazan udio ispitanika koji sljedeće rizike smatra najrelevantnijim za 2022. godinu.[20]

[18] PwC (2020). Global Economic Crime and Fraud Survey. Preuzeto s https://www.pwc.com/gx/en/services/forensics/economic-crime-survey-2020.html

[19] Zandt, F. (2022). The Biggest Business Risks in 2022. Preuzeto s https://www.statista.com/chart/26631/most-relevant-business-risks-in-2022/

[20] Ibid



Slika 2: Top poslovni rizici 2022. godine

Izvor: Izrada autora prema AGC&S (2022.)

EUROPOL 2019. godine naglašava dugoročnost i upornost mnoštva krucijalnih prijetnji kibernetičkog kriminala: [21]

- napadima ucjenjivačkih programa, u odnosu na druge zlonamjerne programe, uzrokuje se značajna gospodarska šteta te zbog toga i jer su relativno jednostavan izvor prihoda ostaju i dalje prijetnja broj jedan
- psihing napadi primarni su vektori prenošenja zlonamjernih programa
- podatci su i dalje razlog, meta te pokretač kibernetičkog kriminala

Europol navodi da su se kibernapadi koji su namjenjeni trajnom i dugotrajnom oštećenju podataka udvostručili u prvoj polovici 2019. godine, ponajviše u proizvodnom sektoru. Ovakvom vrstom napada trajno se i nepovratno oštećuju i brišu podaci poduzeća.[22]

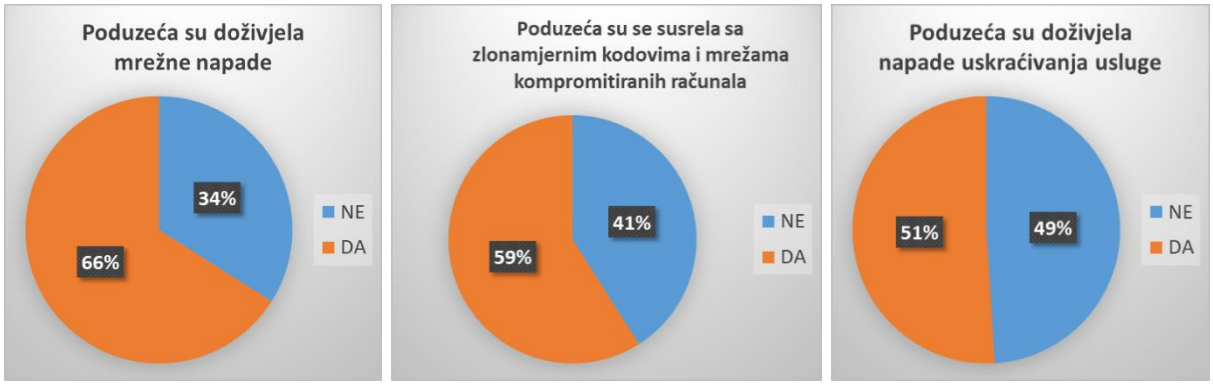
Neki od najpoznatijih primjera takvih *cyber* napada jesu:

- hakiranje 77 milijuna računa Playstationa, koje je poduzeće za posljedicu mjesec dana neaktivnosti stranice, koštalo 171 milijuna dolara

[21] De Bolle, C. (2019). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

[22] De Bolle, C. (2019). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

- izloženost 3 milijarde Yahoo korisničkih računa srušila je 350 milijuna dolara s Yahooove prodajne cijene u 2014
- krađa osobnih podataka 57 milijuna korisnika Ubera i 600 000 brojeva vozačkih dozvola uništila je Uberov ugled i novac u 2016.
- pojava 419-540 milijuna zapisa Facebook ID-a i telefonskih brojeva u travnju i rujnu 2019. najveći je skandal u povijesti Facebooka[23]



Slika 3: Kibernetički napadi u poduzećima

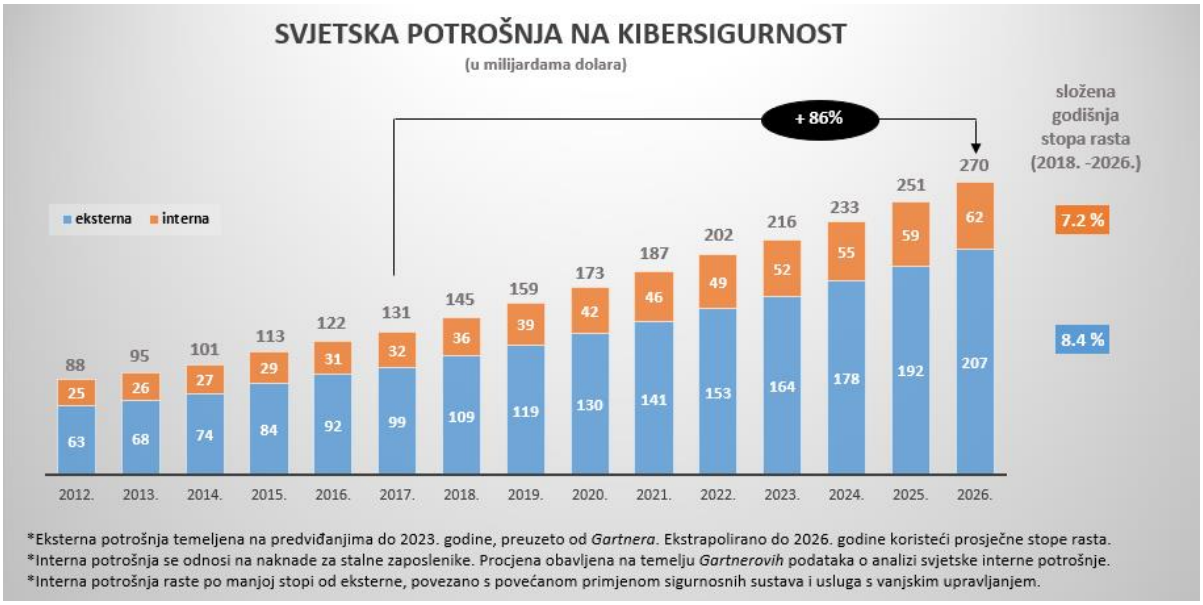
Izvor: Izrada autora prema Varonis (2019.)

Prema nedavnom istraživanju iz 2019. godine 66% poduzeća doživjelo je napade realizirane na webu; 66% iskusilo je napade krađe identiteta i društvenog inženjeringa; 59% poduzeća iskusilo je zlonamjerni kod; 51% iskusilo je napade uskraćivanja usluge.[24] 68 % poslovnih lidera reklo je da im se povećavaju i rizici kibernetičke sigurnosti.[25] Tek je 5 % mapa je zaštićeno.[26]

[23] Bao Ngo, T. N. i Tick, A. (2021). Cyber-security Risks Assessments by External Auditors. *Interdisciplinary Description of Complex Systems: INDECS*, *19*(3), 375-390.
[24] Milkovich, D. (2019). 15 Alarming Cyber Security Facts and Stats. Preuzeto s https://www.cybintsolutions.com/cyber-security-facts-stats/
[25] Accenture Security (2019). The cost of Cybercrime. Preuzeto s https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study- Final.pdf#zoom=50
[26] Varonis (2019). Globas Dana Risk Report From The Varonis Data Lab. Preuzeto s https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf

Do 30. lipnja prijavljeno je 3.813 kršenja, što je otkrilo više od 4,1 milijardu zapisa. U usporedbi sa sredinom 2018., broj prijavljenih kršenja porastao je za 54%, a broj otkrivenih zapisa za 52%.[27]

"Svjetska potrošnja na proizvode i usluge informacijske sigurnosti dosegnut će više od 114 milijardi dolara u 2018., što je povećanje od 12,4 posto u odnosu na prošlu godinu, prema posljednjoj prognozi Gartnera, Inc. U 2019. godini predviđa se rast tržišta 8,7% na 124 milijarde dolara."[28] Ove impresivne brojke podigle su svijest o ozbiljnosti problema povezanih s rizicima kibernetičke sigurnosti svjetskog poslovanja.



Slika 4: Stope rasta svjetske potrošnje na kibernetičku sigurnost 2016.-2026.

Izvor: Izrada autora prema GI (2019.)

Prema najnovijoj prognozi poduzeća Gartner, Inc., globalna IT potrošnja iznosit će 4,4 bilijuna dolara u 2022., što je povećanje od 4% u odnosu na 2021. godinu. Geopolitički poremećaji, inflacija, fluktuacije valuta i izazovi u lancu opskrbe među brojnim su čimbenicima koji utječu na odluke direktora odgovornih za implementaciju i upotrebljivost informacijskih i računalnih tehnologija. Situacija ove godine, suprotna je onome što smo vidjeli početkom 2020., direktori

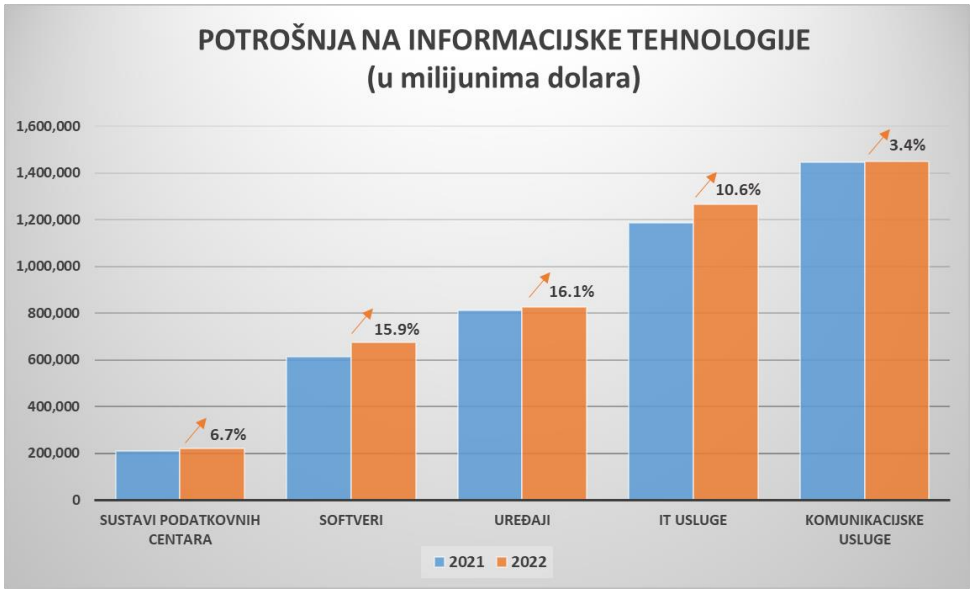
[27] RiskBased Security (*2019).* 2019 on track to being the „worst year on record" for breach activity. Preuzeto s https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[28] Moore, S. (2019). Gartner Forecasts Worldwide Information Security Spending to Exceed $ 124 Billion in 2019. Preuzeto s https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

ubrzavaju ulaganja u IT jer prepoznaju važnost fleksibilnosti i agilnosti u reagiranju na poremećaje.

Povećana se potrošnja u IT sektoru očituje u inflatornim utjecajima na IT hardver, softver i usluge. Davatelji tehnoloških usluga povećavaju svoje cijene, plaćaju skuplje svoje zaposlene, Očekuje se da će potrošnja softvera porasti 9,8%, na 674,9 milijardi USD u 2022., a IT predviđa rast usluga od 6,8% do 1,3 bilijuna dolara.

Uzlet poslovnog aplikacijskog softvera, infrastrukturnog softvera i upravljanih usluga u kratkoročnom i dugoročnom razdoblju pokazuje da je trend digitalne transformacije sustavan i dugoročan. Infrastruktura kao usluga, na primjer, podupire svaku veću online ponudu i mobilnu aplikaciju usmjerenu na potrošače, čineći značajan dio povećanja potrošnje na softverska rješenja, gotovo 10% u 2022. godini.
Gartner predviđa da će optimizacija lanaca opskrbe i iskustvo krajnjih korisnika potaknuti dvoznamenkasti rast potrošnje na poslovne aplikacije i softvere za infrastrukturu u 2023. godini. [29]



Slika 5: Potrošnja - informacijske tehnologije

Izvor: Izrada autora prema GI (2022.)

[29] Rimol, M. (2022). Gartner Forecasts Worldwide Information Security Spending to Reach $4.4 Trillion in 2022. Preuzeto s https://www.gartner.com/en/newsroom/press-releases/2022-04-06-gartner-forecasts-worldwide-it-spending-to-reach-4-point-four-trillion-in-2022

2.2. Svjetska potrošnja na proizvode i usluge za informacijsku sigurnost

Svjesne ozbiljnosti kibernetičkih napada, mnoga su poduzeća usvojile različite metode za upravljanje prijetnjama kibernetičke sigurnosti. Neka poduzeća pokušala su izgraditi vlastite metrike i mjere kibernetičke sigurnosti u nadi da će istima moći napraviti provjeru svojih sigurnosnih kontrola, istražujući vlastite sigurnosne snage i slabosti.[30]

Neka od poduzeća pokušale su drugačijim pristupom, označavajući svoje informacije na temelju dodijeljenog stupnja osjetljivosti, koji omogućuje ljudima na različitim razinama s posebnim ovlaštenjima za pristup osjetljivim informacijama radi boljeg upravljanja i zaštite informacija.[31]

Prema Smettersovom istraživanju,[32] autor pokazuje da se neuspjeh postojećeg sigurnosnog sustava pripisuje poteškoćama korisnika u upravljanju sigurnošću i njihovoj nesposobnosti da shvate izvršavanje svojih sigurnosno kritičnih zadataka. Zbog navedenih razloga samo 51% korisnika stvarno ažurira njihov antivirusni softver, iako 92% njih misli da su već učinili, a njih 73% misli da su uključili firewall dok samo 64% to zapravo čini. Stoga, Smetters zaključuje da organizaciji trebaju dobro osmišljeni alati za vizualizaciju informacija za jače upravljanje administracijom sigurnosno kritičnih sustava.[33]

Istraživanjem koje je provedeno 2018. godine, od strane vrhovnih revizijskih institucija (VRI), utvrđeno je da gotovo polovica istih nikada nije provodila reviziju u području kibernetičke sigurnosti. Obzirom na rastuće prijetnje, utvrđene rezultatima istraživanja, vrhovne revizijske institucije primorane su posvećivati veći stupanj pažnje i aktivnosti u području kibernetičke sigurnosti. Poseban naglasak stavlja se na zaštitu podataka te spremnost sustava da reagira na kibernetičke napade i prijetnje.

Stavlja se naglasak na *zero trust* model uslijed povećanog korištenja *ransomwarea*[34] koji korisniku onemogućavaju pristup računalnim resursima. Nulta vjerodostojnost (*engl. zero trust*) model jest sigurnosni sustav koji zahtijeva da svi korisnici, kako na mreži organizacije,

[30] Black, P. E., Scarfone, K. i Souppaya, M. (2008). Cyber security metrics and measures. *Wiley Handbook of Science and Technology for Homeland Security*, 1-15.
[31] Irvine, C. E. (2014). *Multilevel Security*. U J. G. Voeller (Ur.), *Cyber Security* (9-28). John Wiley & Sons Inc.
[32] Smetters, D.K. (2014). Cyber Security Technology Usability and Management. U J. G. Voeller (Ur.), *Cyber Security* (41-55). John Wiley & Sons, Inc.
[33] Ibid
[34] Stop Ransomware (2020). Ransomware 101. Preuzeto s https://www.cisa.gov/stopransomware/ransomware-101

tako i izvan nje, prođu provjeru autentičnosti, autorizaciju i stalnu provjeru konfiguracije i sigurnosnog stanja prije nego što im se odobri ili pohrani pristup aplikacijama i podacima.[35] U današnjim uvjetima, organizacije će trebati posvetiti više vremena i pažnje osiguranju IT sigurnosnih operativnih alata.[36]

Prema podacima Europske komisije iz 2017. godine, 69% EU- a poduzeća ne razumiju izloženost vlastitog poslovanja kibernetičkim napadima, 60% njih nikada nije napravila procjenu eventualnih financijskih gubitaka.[37] Zanimljiv ishod istraživanja iz 2018. godine ukazuje na to da bi jedna trećina poduzeća radije riskirala plaćanje otkupnine hakerima nego li investirala u informacijsku sigurnost.[38]

Istraživanje Eurobarometra iz 2020. godine ukazuje na to da se situacija postepeno mijenja, osjetan je rast informiranosti i zabrinutosti građana, a u pogledu narednog: građanstvo je najviše zabrinuto zbog moguće zlouporabe osobnih podataka (46%), sigurnosti *online* transakcija (41%), *online* kupovine roba/ usluga (22%). 76 % ili tri četvrtine ispitanika smatra se podložnima za kibernetičke napade, što ukazuje na činjenicu da osjetno porasta svijest korisnika interneta. 52% ispitanih smatraju da su kompetentni zaštiti se od ovakve vrste napada, a tek njih 11% smatra da su o ovoj temi dostatno informirani.[39]

[35] Raina, K. (2021). Zero trust security explained: Principles of the zero trust model. Preuzeto s https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

[36] Petric, I. (2022). Kibernetička sigurnost u 2022. godini – opasnosti i izazovi za tvrtke. Preuzeto s https://duplico.io/kiberneticka-sigurnost-u-2022-godini-opasnosti-i-izazovi-za-tvrtke/

[37] Europska komisija (2019). Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a. Preuzeto s https://eur-lex.europa.eu/legal-content/HR/TXT/DOC/?uri=CELEX:52017JC0450&from=EN

[38] NTT Security (2018). 2018 Risk: Value Report. Preuzeto s https://assets.sig.org/s3fs-public/srcDocs/2018_Risk_Value_Report_NTT_Security.pdf?file=1&type=node&id=14846&

[39] Directorate General for Communication (2020). Europska komisija, Special Eurobarometer 499: Europeans' attitudes towards cyber security (cybercrime). Preuzeto s https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en

3. KIBERNETIČKA SIGURNOST U NEOVISNOJ REVIZIJI ZA VRIJEME PANDEMIJE COVID-A 19

U uvjetima pandemije COVID-a 19 poduzeća su većinu svojih zaposlenika premjestile na rad na daljinu kako bi zaštitile svoje radnike dok su nastavile služiti svojim klijentima. Rad na daljinu uključivao je aktivnost na virtualnu postavku. Poduzeća širom svijeta jako su brzo prepoznale *cyber* ranjivost ovog načina poslovanja, no nisu si mogle dopustiti prestanak rada zbog osiguranja kontinuiteta i sigurnosti poslovanja. Promjene u daljinskom pristupu uključivale su dodavanje više poslužitelja, implementaciju novih ili inkrementalnih kontrola virtualne privatne mreže i implementaciju višefaktorske provjere autentičnosti. Nadalje, poduzeća su bila u mogućnosti zahtijevati nove kontrole u vezi s novim tehnološkim alatima, aplikacijama ili uređajima koje zaposlenici mogu koristiti dok rade od kuće.[40]

Iznimka nisu ni revizori, koji su morali obavljati takozvanu „reviziju na daljinu". Revizori su morali ažurirati svoje razumijevanje IT okruženja kako su se poduzeća razvijala, kako bi odgovorile na ove nove ili rastuće kibernetičke rizike, kao i revidirati procjene rizika i revizijske postupke kako bi odgovorili na sve nove ili različite rizike materijalno značajnih pogrešaka koje bi mogle utjecati financijska izvješća.[41]

Pandemija COVIDA-19 rezultirala je nastajanjem nesigurnosti i izazova koji za posljedicu imaju veću vjerojatnost nastanka nepredviđenih događaja te neizvjesnost trajanja tih istih događaja. Kao rezultat tih okolnosti prepoznajemo moguće pomicanje rokova financijskog izvještavanja, a što može utjecati na reviziju financijskog izvještavanja pri utvrđivanju naknadnih događaja. Ako je došlo do odgode rokova financijskog izvještavanja, revizor će u kontekstu naknadnih događanja trebati provesti dodatne postupke, u svrhu potkrepljenja cijelog razdoblja revizijskih dokazima.[42]

[40] Borkovich, D. J. i Skovira, R. J. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Information Systems*, *21*(4), 234-246.
[41] CAQ (2020). Understanding Cybersecurity and the External Audit in the Covid-19 Environment. Preuzeto s https://www.thecaq.org/wp-content/uploads/2020/07/caq_understanding-cybersecurity-covid-19_2020-07.pdf
[42] Tušek, B., Ježovita, A. i Halar, P. (2020). Izazovi djelovanja interne i eksterne revizije u eri pandemije Covid-19. *Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru*, (26), 111-130.

Prosudbe menadžmenta u ovim uvjetima bile su od velike važnosti te je revizorov zadatak bio zadržati visoku razinu profesionalne prosudbe pri kojem se mora voditi profesionalnim skepticizmom u ocjeni poslovanja.[43]

Izvještavanje neovisnog revizora također je bilo podložno modifikacijama zbog novonastalih okolnosti u poslovanju, novih uvjeta u kojima se obavlja angažman, znatnoj neizvjesnosti u kontekstu vremenske ograničenosti poslovanja. U takvim nepredvidljivim uvjetima, korisnici financijskih izvještaja imali su velika očekivanja od revizije financijskih izvješća. U svrhu premošćivanja jaza doprinijele su razne objave u kojima se pojašnjavaju učinci pandemije.[44]

Zaključno, eksterni revizori u uvjetima pandemije bili su izloženi višestrukim izazovima koji su se s jedne strane ogledali u neophodnosti modifikacija revizijskih procedura, povećanja obima ispitivanja, prisilne i ubrzane digitalizacije te s druge strane, znatnoj primjeni profesionalnog skepticizma, profesionalne prosudbe u svrhu stjecanja razumnog i fer uvjerenja u financijska izvješća.[45]

[43] Ibid
[44] Tušek, B., Ježovita, A. i Halar, P. (2020). Izazovi djelovanja interne i eksterne revizije u eri pandemije Covid-19. *Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru*, (26), 111-130.
[45] Ibid

4. ULOGA KIBERNETIČKE SIGURNOSTI U PROVEDBI NEOVISNE REVIZIJE

Iako kibernetička sigurnost ima implikacije u svim poslovnim sektorima, na financijski sektor stavlja se najveći fokus jer, prema Kamiya et al.,[46] napadi na financijske informacije uzrokuju negativnu reakciju tržišta dionica, pad rasta prodaje za velika poduzeća i maloprodajna poduzeća, porast financijske poluge, pogoršanje financijskog zdravlja i kratkoročno smanjenje ulaganja. Kao rezultat toga, nema sumnje da skandal s hakiranjem financijskih informacija može brzo srušiti čak i veliku korporaciju u kratkom vremenu. Posljedično vlasti i donositelji normi posljednjih su godina sve zabrinutiji zbog opasnosti od kibernetičkih napada, zbog čega su neovisni revizori obvezni posvećivati više pažnje kod svojih angažmana.[47]

Više je razloga zbog kojih neovisni revizori moraju posvećivati više pažnje poduzećima koja su bila žrtvom događaja kibernetičke sigurnosti. Potrebna je temeljita procjena klijentovog računovodstva za gubitke, potraživanja i obveze povezane s incidentom kibernetičke sigurnosti.[48]

Također, u slučaju izravnih *cyber* napada na računovodstveni sustav poduzeća, neovisni revizori moraju uzeti u obzir internu kontrolu nad financijskim izvješćivanjem, jer bi incident mogao uključivati rizik manipulacije računovodstvenom evidencijom poduzeća, što rezultira u manje vjerodostojnim financijskim izvještajima.[49] Čak i ako *cyber* napadi ne utječu na sustav računovodstvenog evidentiranja, revizori su i dalje dužni uložiti dodatne napore u svom revizijskom radu budući da postoje naznake o slabostima unutarnjih kontrola poduzeća, koje bi mogle biti rizici.[50] Budući da su vanjski revizori pod ogromnim pritiskom kada revidiraju poduzeća kod kojih se dogodio kibernetički incident, potrebno je otkriti kako takvi događaji utječu na njihov angažman.

---

[46] Kamiya, S., Kang, J. K., Kim, J., Milidonis, A. i Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? (No. w24409). *National Bureau of Economic Research*.

[47] International organization of securities commissions (2016). Cyber Security in Securities Markets – An International Perspective. Preuzeto s https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

[48] Center for Audit Quality (2014). Cybersecurity and the External Audit. Preuzeto s http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit

[49] Public Company Accounting Oversight Bord (2014). Standing Advisory Group Meeting: Cybersecurity. Preuzeto s http://pcaobus.org/News/Events/Documents/0624252014_SAG_Meeting/06252014_Cybersecurity.pdf

[50] Li, H., No, W.G. i Boritz, J.E. (2020). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.

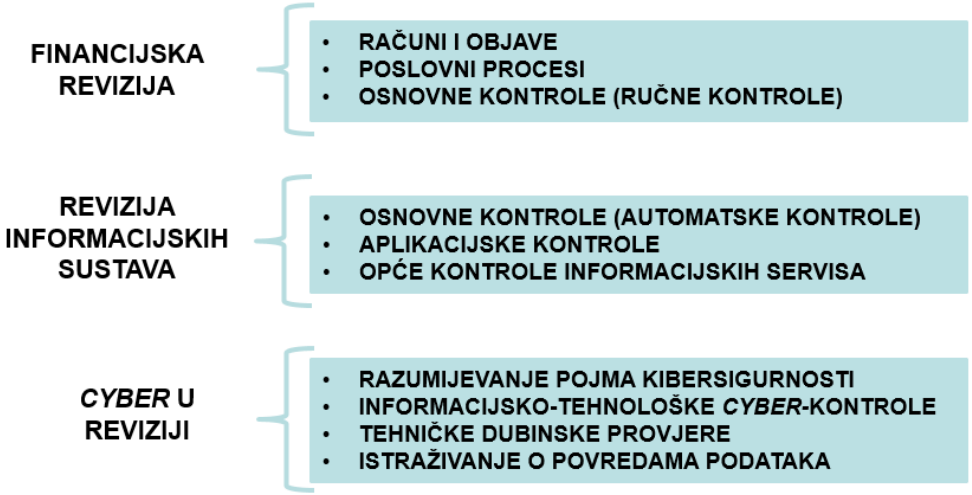
Dakle, rizici kibernetičke sigurnosti ne utječu samo na poslovanje poduzeća, već i na neovisnog revizora koje isto mora revidirati. Kao i samo poduzeće, neovisni se revizor snažno oslanja na kontinuitet i pouzdanost automatizirane obrade podataka te na testiranje takozvanih općih IT kontrola.[51]

Prilikom provođenja revizije, revizor prvo mora razumjeti način na koji poduzeće koristi IT i koliki je utjecaj IT-a na financijska izvješća. Potrebno je razumjeti raspon automatiziranih kontrola poduzeća u odnosu na financijsko izvješćivanje. To bi trebalo uključivati razumijevanje općih IT kontrola koje utječu na automatizirane kontrole, te pouzdanost podataka i izvješća korištenih u reviziji koje je proizvelo poduzeće. Revizor te iste kontrole testira u ovom procesu kako bi utvrdio njihovu učinkovitost u dizajnu i radu. Ako te kontrole djeluju učinkovito, neovisni revizor stječe dodatno razumno uvjerenje (povrh vlastitog kontrolnog testiranja u financijskim procesima) da je osiguran integritet financijskih podataka.[52]

Razlog za razumijevanje informatičkog sustava i kontrola jest procjena rizika materijalno značajnih pogrešnih prikaza u financijskim izvještajima, uključujući IT rizike koji proizlaze iz neovlaštenog pristupa.
Stoga je fokus revizije na pristupu i promjenama sustava i podataka koji bi utjecali na financijska izvješća i učinkovitost interne kontrole nad financijskim izvješćivanjem, a ne na cjelokupnu IT platformu poduzeća. Sukladno tome, izvršenje revizije financijskih izvještaja i internih kontrola vjerojatno neće uključiti područja koja bi se bavila kršenjem kibernetičke sigurnosti izvan tog uskog područja. No, ako se otkrije značajna povreda, revizor bi trebao razmotriti utjecaj na financijsko izvješćivanje, uključujući objave, i utjecaj na interne kontrole. Prema gore navedenom, primarna pozornost revizora u smislu IT-a trebala bi biti usmjerena na kontrole i sustave relevantne za reviziju. To može uključivati sustave za planiranje resursa poduzeća, jednonamjenske aplikacije kao što je sustav dugotrajne imovine i sve druge sustave koji sadrže podatke o financijskim izvještajima.[53]

[51] Dutch Civil Code (1988). Book 2: Legal Persons. Preuzeto s http://www.dutchcivillaw.com/legislation/dcctitle2299aa.htm#sec299
[52] Center for Audit Quality (2014). Cybersecurity and the External Audit. Preuzeto s http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit
[53] Tysiac, K. (2014). Auditors have important role in cybersecurity. Preuzeto s https://www.journalofaccountancy.com/news/2014/mar/20149835.html

Praktični pristup kibernetičkoj sigurnosti u reviziji uključuje suradnju IT i neovisne revizije gdje CitA testiranje podržava IT reviziju testiranjem automatskih kontrola. CitA- om (kibernetičko testiranje) testiraju se mjere kibernetičke sigurnosti koje sprječavaju / otkrivaju zaobilaženje IT aplikacija i kontrola poduzeća. Kibernetičko testiranje dio je općih IT kontrola.[54]



Slika 6: Položaj *cyber* testiranja u reviziji

Izvor: Izrada autora prema ECC (2021.)

Postavlja se pitanje u kojoj mjeri je relevantno kibernetičko testiranje za reviziju financijskih izvještaja? Potrebno je steći razumijevanje o tome kako se rizici kibernetičkoj sigurnosti određuju i kontroliraju u okruženju u sklopu ne samo poznatih aktivnosti razumijevanja IT-a, već i proširivanjem ove aktivnosti s razumijevanjem kibernetike. To bi trebalo uključivati ne samo tehnički fokus, već i fokus na procese - poput odgovora na incidente kibernetičke sigurnosti te upravljanje – potrebno je utvrditi tko je odgovoran za utvrđivanje rizika i mjera kibernetičke sigurnosti. Ovisno o danom odgovoru na prethodna pitanja, utvrđuje se je li potrebno vršiti daljnja i dublja testiranja kibernetičkih kontrola. Pomoću ove aktivnosti identificiraju se nedostatci u cjelokupnoj kibernetičkoj sigurnosti poduzeća.[55]

Profil kibernetičkog rizika može se odrediti analizom procesa jednog poduzeća. Takav profil rizika kombinacija je kibernetičkih prijetnji s kojima se poduzeće suočava i ovisnost o

[54] EC-Council (2021). Certified Threat Intelligence Analyst. Preuzeto s https://www.eccouncil.org/programs/threat-intelligence-training/

[55] NBA Van hype naar aanpak (2016). Publieke managementletter over cybersecurity. Preuzeto s https://www.nba.nl/globalassets/projecten/kennis-delen-pmls/cybersecurity/pml-cyber-security.pdf

adekvatnoj kibernetičkoj obrani, koja se može utvrditi na temelju razumijevanja procesa poduzeća.

Kada su u pitanju kibernetičke prijetnje, potrebno je razmišljati o *cyber* prijetnjama specifičnim za industriju, visokom (višem) riziku od insajderskih prijetnji, glavnim prihodima generiranim na internetu, *cyber* kaznama te je li organizacija prethodno bila hakirana ili ne.[56]

Oslanjanje neovisne revizije na IT sustave, kao najvažnije imovine jednog poduzeća, visoka razina automatizacije, integrirani lanac opskrbe i usklađenost s propisima, sve su to teme koje treba uzeti u obzir pri razmatranju *cyber* ovisnosti.

Kod testiranja mjera kibernetičke sigurnosti, moguće je odabrati jednu ili više *cyber* IT kontrola, koje se odabiru na temelju identificiranog profila kibernetičkog rizika. Upravljanje kibernetičkom sigurnošću, tehničko jačanje i operacije kibernetičke sigurnosti su sve teme koje pokrivaju *cyber* IT kontrole. Sigurnosni nadzor, odgovor na kibernetičke incidente, svijest o sigurnosti i sigurnost u oblaku primjeri su postupaka zaštite, otkrivanja i reagiranja koji bi trebali postojati. Ove kontrole se testiraju na isti način kao što se testiraju opće IT kontrole, i mogu se smatrati dodatkom standardnim općim IT kontrolama.[57]

Kao rezultat neučinkovitih kibernetičkih kontrola, mogu postojati sigurnosni rizici u IT okruženju. Kao rezultat toga, moramo odabrati teme *deep dive-a*/pronalaženja činjenica koje su relevantne za scenarij. Red Teaming, SAP Security, Phishing aktivnosti, SIEM pregledi i procjena sigurnosti u oblaku primjeri su *deep dive-a* koji se mogu povezati s procijenjenim kibernetičkim kontrolama.[58] *Deep dive* pruža dodatan uvid u nedostatke kibernetičkih kontrola u smislu stvarnog tehničkog učinka. Iako se kibernetičke kontrole mogu pokazati neučinkovite, moguće je da tehnološka implementacija ne sadrži sigurnosne nedostatke.[59]

Ukoliko se utvrdi da se tijekom financijske godine dogodila povreda kibernetičke sigurnosti, ili je poduzeće toga svjesno, prvenstveno je potrebno odrediti aktera prijetnje te je li ovo trajna i

[56] KPMG (2022). Cybersecurity considerations 2022 – Trust through security. Preuzeto s https://assets.kpmg/content/dam/kpmg/au/pdf/2022/cyber-security-considerations-2022.pdf
[57] Ibid
[58] Lingscheid, A. (2021). SAP Solutions for Cyber Security and Data Protection. Preuzeto s https://blogs.sap.com/2021/07/16/sap-solutions-for-cyber-security-and-data-protection/
[59] van Veen, M. (2016). Cyber Security: A Paradigm Shift in IT Auditing: How to Deal with Cyber Security Risks in the Financial Statement Audit. *Compact*, *3*, 53-59.

napredna prijetnja. Potom je potrebno odrediti motivaciju aktera – je li cilj hakiranja krađa intelektualnog vlasništva, osjetljivih podataka, novca ili sabotaža poslovanja? Prethodno spomenuto ukazuje nam na moguća oštećenja i njihov raspon.

Sve prethodno spomenute poduzete akcije trebale bi neovisnom revizoru pomoći odrediti koja su to potencijalna područja na koje je kibernetički napad utjecao. Neke od kategorija na koje kibernetički napad može utjecati jesu: [60]

a) Intelektualna imovina, postavlja se pitanje hoće li vrijednost intelektualne imovine zadržati jednaku vrijednost ukoliko je ista ukradena te je postala općepoznata. U ovakvim situacijama neminovno je značajno opadanje vrijednosti pozicije.

b) Narušavanje bankarskog sustava, u slučaju prijevarnih aktivnosti potrebno je napraviti službenu prijavu te utvrditi količinu novca koja je nestala kako bismo mogli ocijeniti koliki utjecaj prijevara ima na financijske izvještaje.

c) Zaobilaženje ili *bypass* automatskih kontrola, ukoliko se ustanovi da su se automatske kontrole „zaobišle" neovisni se revizor na iste neće moći osloniti.

d) Privatnost podataka, ponekad će kibernetički napadi biti usmjereni na osobne i druge podatke, o takvim kršenjima potrebno je obavijestiti nadležne. U suprotnom slučaju poduzeće se kažnjava sa 10% ukupnog prometa.

e) Koncept stalnog poslovanja, u slučaju velikih poremećaja u IT sektoru poduzeća moguć je prekid poslovanja, obzirom da se većina poslovanja uvelike oslanja na isti.

[60] van Veen, M. (2016). Cyber Security: A Paradigm Shift in IT Auditing: How to Deal with Cyber Security Risks in the Financial Statement Audit. *Compact*, *3*, 53-59.

5. KAKO NEOVISNA REVIZIJA PROCJENJUJE RIZIK KIBERNETIČKE SIGURNOSTI?

Tijekom posljednjih nekoliko godina došlo je do značajne integracije tehnologije u poslovanje poduzeća, uključujući povećano oslanjanje na vezu s internetom, što je također ubrzano kao odgovor na pandemiju COVID-a 19. Kako je u radu već prethodno spomenuto, iako postoje enormne mogućnosti za poduzeća u usvajanju tehnologije, i integraciju u poslovanje, povećana povezanost i oslanjanje na internet povećava rizik od *cyber* napada.[61]

Donaldson i suradnici razlikuju tri vrste revizija kibernetičke sigurnosti: [62]

- revizija prijetnji: ova vrsta pristupa revizije usredotočuje se na kibernetičke prijetnje i traže dokaze u IT okruženjima
- revizija procjene: ovaj pristup revizije ocjenjuju kontrole kibernetičke sigurnosti koje su usklađene s okvirima, regulatornim zahtjevima, standardima ili, u nekim slučajevima, specifičnom kibernetičkom prijetnjom
- procjene valjanosti: procjene se provode na kontrolama kibernetičke sigurnosti kako bi se utvrdila njihova učinkovitost u odnosu na dizajnirane i dokumentirane zahtjeve.

Od revizora se zahtijeva da identificiraju i procijene rizike materijalno značajnih pogrešaka u financijskim izvještajima, bilo zbog prijevare ili pogreške. Potrebno je osmisliti i provesti revizijske postupke koji će odgovarati na rizike koji se pojavljuju kao djelom svakodnevnog poslovanja. Ovisno o činjenicama i okolnostima poduzeća, izostanak sigurnog kibernetičkog okruženja može doprinijeti podložnosti pogrešnog prikazivanja određenih iznosa i objava u financijskim izvještajima subjekta.[63]

Odgovorno je rukovodstvo, uz nadzor onih koji su zaduženi za upravljanje, odgovorno za pripremu financijskih izvještaja u skladu s primjenjivim okvirom financijskog izvještavanja te za osmišljavanje i provedbu internih kontrola. Prepoznavanje i upravljanje rizicima ključni je segment uloge menadžmenta i onih koji su zaduženi za upravljanje. Istaknutost kibernetičkog

[61] CAQ (2020). Understanding Cybersecurity and the External Audit in the Covid-19 Environment. Preuzeto s https://www.thecaq.org/wp-content/uploads/2020/07/caq_understanding-cybersecurity-covid-19_2020-07.pdf
[62] Donaldson, S., Siegel, S., Williams, C. K. i Aslam, A. (2015). *Enterprise cybersecurity: how to build a successful cyberdefense program against advanced threats*. Apress.
[63] van Veen, M. (2016). Cyber Security: A Paradigm Shift in IT Auditing: How to Deal with Cyber Security Risks in the Financial Statement Audit. *Compact*, *3*, 53-59.

kriminala znači da je kibernetička sigurnost poslovni rizik za mnoge subjekte koje treba uzeti u obzir i istima upravljati.[64]

Za subjekte na čije bi poslovanje događaj kibernetičke sigurnosti mogao imati značajan utjecaj, odgovorno rukovodstvo uz nadzor onih koji su zaduženi za nadzor, treba razmotriti rizike povezane s kibernetičkom sigurnošću te pokušati predvidjeti kada se takav događaj može dogoditi te kakve bi implikacije na financijska izvješća jednog takvog događaja bile.[65]

Kao posljedica kibernetičkog incidenta prepoznajemo moguće sljedeće situacije:

- otvaranje rezerviranja ili/i nastanka potencijalnih obveza kao posljedica povrede podataka, a koji se mogu javiti kao rezultat novčanih kazni ili kazni od strane regulatora, kao i mogućnost pravnih radnji i postupaka od pogođenih strana u kojima su izgubljeni osjetljivi podaci
- promjena fer vrijednosti imovine kao rezultat *cyber* događaja - na primjer kada je pogođena određena industrija, može postojati oklijevanje u transakciji sa subjektima pogođene industrije
- umanjenje vrijednosti imovine zbog smanjenih operativnih novčanih tokova kao posljedica *cyber* napada - na primjer, kada je napad prekinuo poslovanje subjekta na značajno vremensko razdoblje ili gdje je napad utjecao na reputaciju poduzeća ili brenda
- općenite implikacije na sposobnost subjekta da nastavi s neograničenim poslovanjem.[66]

Revizorov opći cilj je dobiti razumno uvjerenje da financijsko izvješće ne sadrži materijalno pogrešno prikazivanje. Naredni postupci objašnjavaju tijek svake revizije:

- utvrđivanje i procjena rizika značajnih pogrešnih prikazivanja, bilo zbog nepoštenih radnji ili pogrešaka, na temelju razumijevanja organizacije i njezine okoline (prema MRevs-u 315)

[64] ASIC (2021). Cyber resilience good practices. Preuzeto s https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/
[65] Cossin, D. i Lu, A. H. (2021). Bord Oversight of Cyber Risks and Cybersecurity. Preuzeto s https://www.imd.org/research-knowledge/articles/Board-Oversight-Cyber-Risks-Cybersecurity/
[66] Bems, M. R., Caselli, F. G., Grigoli, F., Gruss, B. i Lian, W. (2018). *Is inflation domestic or global? Evidence from emerging markets*. International Monetary Fund.

- prepoznavanje i procjenjivanje rizika značajnih pogrešnih prikazivanja kroz stjecanje razumijevanja subjekta i njegovog okruženja [67]
- razvoj i provedba mjera odgovora na procijenjene rizike (prema MRevs-u 330 - Odgovori revizora na procijenjene rizike).[68]

Bez obzira na to je li došlo do kibernetičkog napada ili kibernetičkog događaja ili ne, revizor u okviru svojih postupaka procjene rizika moraju uzeti u obzir implikacije kibernetičke sigurnosti na financijsko izvješće. MRevs 315[69] od revizora traži da stekne uvid, kako u subjekta i njegovu okolinu, također i u sustav unutarnjih kontrola koji je relevantan za prepoznavanje i određivanje rizika. To uključuje razumijevanje načina na koji organizacija koristi informacijsku tehnologiju i utvrđivanje rizika povezanih s tim.
Iako posljednje izdanje MRevs-a 315 još nije na snazi, ključno poboljšanje u novoj verziji jest pojačano razmatranje rizika uzrokovanih informacijskom tehnologijom u sklopu Dodatka 5 - Razmatranja za razumijevanje informacijske tehnologije i Dodatka 6 - Razmatranja za razumijevanje općih IT kontrola. MRevs 315 kroz novu inačicu nudi značajne nove smjernice o razumijevanju IT-a i identificiranju primjenjivih rizika koje će revizori smatrati korisnima.[70] MRevs 240 - Revizorove odgovornosti u svezi s prijevarom u reviziji financijskog izvješća usredotočuje se na to kako se MRevs 315 primjenjuje u odnosu na prijevaru i koristan je revizorima u ocjenjivanju kibernetičke sigurnosti.[71]

Odgovornost revizora u pogledu kibernetičke sigurnosti, kao i kod ostalih rizika, jest prvo razmotriti rizik materijalnih pogrešnih prikaza u financijskim izvještajima u okviru postupaka procjene rizika te odgovaranje na odgovarajući način u slučaju da se utvrdi rizik od značajnih pogrešnih prikazivanja. Zadatak uprave jest provođenje postupka procjene rizika kako bi se identificirali rizici poput kibernetičke sigurnosti, kao i također za provedbu i praćenje

[67] Međunarodni odbor za standarde revidiranja i izražavanja uvjerenja IAASB (2013). Prepoznavanje i procjenjivanje rizika značajnih pogrešnih prikazivanja kroz stjecanje razumijevanja subjekta i njegovog okruženja. Preuzeto s https://www.srr-fbih.org/sites/default/files/standards/2021-12/Medunarodni%20revizijski%20standard%20315%20%28izmijenjen%29.pdf
[68] Hrvatska revizorska komora (2022). Posebna razmatranja u reviziji financijskih instrumenata. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/full/2022_02_17_179.html
[69] Međunarodni odbor za standarde revidiranja i izražavanja uvjerenja IAASB (2013). Prepoznavanje i procjenjivanje rizika značajnih pogrešnih prikazivanja kroz stjecanje razumijevanja subjekta i njegovog okruženja. Preuzeto s https://www.srr-fbih.org/sites/default/files/standards/2021-12/Medunarodni%20revizijski%20standard%20315%20%28izmijenjen%29.pdf
[70] Hrvatska revizorska komora (2004). Razumijevanje poslovnog subjekta i njegovog okruženja te procjenjivanje rizika značajnog pogrešnog prikazivanja. Preuzeto s http://www.propisi.hr/print.php?id=5695
[71] Ibid

mehanizama unutarnje kontrole kako bi se odgovorilo na te rizike.[72] Ocjenjuje se kako kibernetička sigurnost može utjecati na reviziju i odgovornost revizora povezana s procjenom rizika.

Sljedeći postupci odgovornost su revizora kod procjene kibernetičkog rizika:[73]

1. Za kvalitetnu procjenu rizika potrebno je razmotriti *cyber* sigurnost kao dio stjecanja razumijevanja o subjektu i njegovu okruženju te sustavu interne kontrole.
2. Identificirati i procijeniti rizike značajnog pogrešnog prikazivanja povezane s kibernetičkom sigurnošću na razini financijskog izvješća i tvrdnji.
3. Definirati postoji li potreba za odgovorom na identificirani *cyber* rizik te odrediti odgovor na temelju relevantnih standarda.
4. Periodično provoditi procjene rizika u svrhu identifikacije kibernetičkih prijetnji, ranjivosti imovine, potencijalne učinke na poslovanje, uključujući one vezane uz vanjske funkcije, treće strane i poslovne partnere. Ustanoviti ima li subjekt plan odgovora na IT sigurnosni incident te je li isti ažuriran i testiran periodično.[74]
5. Utvrditi postoje li nalazi procjene rizika kibernetičke sigurnosti koji bi potencijalno utjecali na financijska izvješća.
6. Utvrditi je li subjekt implementirao programe i kontrole kibernetičke sigurnosti temeljene na riziku kako bi smanjio mogućnost kibernetičkih događaja te prati li menadžment te uspostavljene programe i kontrole.
7. Uvjeriti se da je kibernetički plan utemeljen na priznatom standardu.
8. Ispitati je li poduzeće ulagalo/ili planira ulagati u sigurnosne proizvode.
9. Utvrditi uloge i odgovornosti za kibernetičku sigurnost, te je li ista spomenuta Upravnom ili Revizijskom odboru.

Koraci koji se poduzimaju u cilju zaštite imovine:

1. Utvrditi postoji li značajna digitalna/elektronička imovina koja bi mogla biti ciljem kibernetičkog napada (intelektualno vlasništvo, patenti, materijal zaštićen autorskim

[72] CAQ (2019). Understanding Cybersecurity and the External Audit. Preuzeto s https://www.thecaq.org/wp-content/uploads/2019/03/cybersecurity_and_external_audit_final.pdf
[73] Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf
[74] Security Compliance Associates – SCA (2020). Cyber security risk report. Preuzeto s https://scasecurity.com/

pravima) te postoji li uspostavljeni prioritet važnosti zaštite na temelju poslovne vrijednosti.

2. Utvrditi je li potrebno prikupljanje osobnih podataka obzirom na prirodu poslovanja subjekta, obzirom na Zakon o zaštiti osobnih podataka.[75]
3. Ispitati je li organizacija izradila popis svoje informacijske imovine koju je potrebno zaštititi (baze podataka kupaca, poslovne tajne, bitne informacije o projektu i financijski podaci).
4. Utvrditi čuva li organizacija važne sigurnosne kopije podataka.
5. Ispitati kako Uprava prati i procjenjuje pristup digitalnoj/elektronskoj imovini te kako prati neovlašteni pristup.

Kada i ako se dogodi kibernetički događaj:

1. Otkriti anomalnu kibernetičku aktivnost ili incident.
2. Ako je do kibernetičkog incidenta zaista došlo, napraviti presjek incidenta, ustanoviti razloge te analizirati temeljni uzrok, utjecaj te definirati mjere odgovora. Ustanoviti mjeru u kojoj je događaj utjecao na financijske izvještaje.

Prosječno vrijeme za otkrivanje i obuzdavanje kršenja kibernetičke sigurnosti je otprilike 280 dana, što je važno razmatranje za revizore. Revizori bi trebali biti svjesni mogućnosti kršenja kibernetičke sigurnosti koja obuhvaća više razdoblja financijskog izvješćivanja i razumjeti svoje odgovornosti prema MRevs 560.[76]

Kibernetički incidenti obično počinju na internoj mreži, koji su odvojeni od aplikacija, baze podataka i operacijskih sustava koji su uključeni u testiranje kontrole pristupa sustava koji utječu na financijska izvješća. Postupci revizije mogu uključivati testiranje kontrola pristupa aplikaciji, bazi podataka i operacijskom sustavu, onim redoslijedom važnosti i fokusa. Ostali širi sigurnosni elementi oko perimetra i mrežnih slojeva obično su izvan opsega revizije financijskih izvještaja. Najčešći izvori potencijalnih pogrešaka u financijskim izvještajima

[75] European Union law (2016). Uredba Europskog parlamenta i vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive. Preuzeto s https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679

[76] IBM (2020). How much does a dana breach cost? Preuzeto s https://www.ibm.com/sg-en/security/data-breach

povezani su s pristupom na razini transakcije putem aplikacije. Ostali elementi sigurnosti unutar interne mreže mogu varirati ovisno o poslovanju i okruženju poduzeća.[77]

U akademskoj literaturi postoje mnoge hipoteze o utjecaju incidenata kibernetičke sigurnosti na odgovor vanjskih revizora putem naknada za reviziju.[78] Da budemo precizniji, Li i sur.[79] otkrivaju da *cyber* incidenti imaju pozitivan utjecaj na naknade za reviziju korištenjem 229 kibernetičkih incidenata iz baze podataka o kibernetičkoj sigurnosti Audit Analytics i Centra za zaštitu prava privatnosti između 2010. i 2014. To znači da će poduzećima koje dožive povrede kibernetičke sigurnosti biti naplaćene veće naknade za reviziju. Rezultati istraživanja Smitha i Pinskera[80] podržavaju zaključak Lija i suradnika[81] da postoji pozitivan odnos između prošlih i budućih otkrivanja kršenja i naknada za reviziju.
Prema nekoliko istraživača, veće revizijske naknade povezane su s: većim ulaganjima u IT jer IT složenost otežava revizorima otkrivanje računovodstvenih nepravilnosti,[82] većom asimetrijom informacija,[83] ozbiljnijim *cyber* incidentima[84] i manje aktivnom revizijom povjerenstva.[85]

Revizor je odgovoran za planiranje i provedbu odgovora na te procijenjene rizike, ako je rizik značajnog pogrešnog predstavljanja financijskog izvješća otkriven putem kibernetičke sigurnosti u sklopu postupaka procjene rizika.[86]

[77] Center for Audit Quality (2014). Cybersecurity and the External Audit. Preuzeto s http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit
[78] Rosati, P., Gogolin, F. i Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. *The International Journal of Accounting 53*(3), 1-75.
[79] Li, H., No, W. G. i Boritz, J.E. (2020). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.
[80] Smith, T. i Pinsker, R. (2019). Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*, *33*(2), 177-204.
[81] Li, H., No, W. G. i Boritz, J.E. (2020). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.
[82] Han, S., Rezaee, Z., Xue, L. i Zhang, J. H. (2016). The association between information technology investments and audit risk. *Journal of Information Systems*, *30*(1), 93-116.
[83] Frino, A., Palumbo, R. i Rosati, P. (2013). Does Information Asymmetry Predict Audit Fees? Evidence from Italian Listed Companies. Priopćenje na American Accounting Association Annual Meeting, Anaheim, CA.
[84] Li, H., No, W. G. i Boritz, J.E. (2020). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.
[85] Smith, T. i Pinsker, R. (2019). Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*, *33*(2), 177-204.
[86] Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf

Financijski utjecaj na poduzeća može biti značajan te uzrokovati temeljnu štetu u cijelom poduzeću za subjekte. *Cyber* napadi također mogu ostati neotkriveni, što rezultira financijskim implikacijama na subjekt koje se možda nisu odrazile u financijskim izvještajima.[87]

Ovisno o prirodi organizacije, rizici kibernetičke sigurnosti mogu imati sveprisutan utjecaj na financijske izvještaje te utjecati na nekoliko različitih elemenata kao što su rezerve, fer vrijednost imovine ili vremensku neograničenost poslovanja. Kada dođe do *cyber* događaja, posao revizora je procijeniti utjecaj na financijsko izvješće i utvrditi odražava li financijsko izvješće realno utjecaj *cyber* događaja i je li prikazano u svim materijalnim aspektima u skladu s primjenjivim okvirom financijskog izvješćivanja.[88]

MRevs 315 zahtijeva od revizora da temeljito razumije poduzeće i njegovo okruženje, što uključuje poslovni model subjekta i mjeru u kojoj uključuje korištenje tehnologije. Pored toga, potrebno je razumjeti strukturu i složenost informatičkog okruženja subjekta, uključujući opseg korištenja sustava trećih strana ili vanjskih IT pružatelja usluga. Na primjer, mogu postojati poznate ranjivosti u softveru koji subjekt koristi ili da vanjski IT pružatelj posluje s malo ili nimalo nadzora menadžmenta i onih koji su zaduženi za upravljanje. [89]

Industriju u kojoj poduzeće radi također je važno procijeniti, budući da određene industrije, kao što su financijske usluge,[90] mogu biti ranjivije zbog povijesti kršenja podataka i osjetljive vrste podataka koje posjeduje subjekt. Iako kibernetička sigurnost predstavlja rizik za većinu poduzeća, ovaj rizik ne rezultira uvijek rizikom značajnog krivotvorenja financijskog izvješća, što zahtijeva revizorsko oblikovanje i provedbu odgovora.

Revizori koji postavljaju pitanje je li došlo do *cyber* napada također su uključeni u razmatranje kibernetičke sigurnosti kao dio procjene rizika. Ako jest, revizor bi obično ispitao u kojoj je

[87] Hamm, K. M. (2019). Cybersecurity: Where We Are: What More Can Be Done? A Call for Auditors to Lean In. Priopćenje na Baruch College 18th Annual Financial Reporting Conference, New York, NY.
[88] ISCA (2018). Cybersecurity Risk Considerations in a Financial Statements Audit. Preuzeto s https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf
[89] Hrvatska revizorska komora (2004). Razumijevanje poslovnog subjekta i njegovog okruženja te procjenjivanje rizika značajnog pogrešnog prikazivanja. Preuzeto s http://www.propisi.hr/print.php?id=5695
[90] Frost, J. i Shapiro, J. (2021). Cyber attacks 'the biggest risk in banking'. Preuzeto s https://www.afr.com/companies/financial-services/cyber-is-the-biggest-risk-in-banking-today-20210330-p57f5n

mjeri kršenje moglo utjecati na financijsko izvješćivanje. Kada je financijsko izvješćivanje ugroženo, revizor može odlučiti intervenirati.[91]

Ako se utvrdi rizik kibernetičke sigurnosti koji bi mogao rezultirati značajnim rizicima pogrešnog prikazivanja na razini financijskih izvještaja, revizor bi trebao koristiti MRevs 315 kao vodič za kreiranje i provedbu općih odgovora. To bi moglo uključivati dodjeljivanje iskusnijeg osoblja ili onih sa specijaliziranim vještinama, kao što su IT stručnjaci, uključivanje dodatnih elemenata nepredvidivosti u odabir dodatnih revizijskih postupaka koji će se izvršiti i promjenu prirode revizijskih postupaka kako bi se dobili uvjerljiviji i potkrepljiviji revizijski dokazi.[92]

Na pouzdanost revizijskih dokaza utječu njihov izvor, priroda i okolnosti pod kojima su dobiveni, uključujući, gdje je primjenjivo, kontrole nad njihovom pripremom i održavanjem.[93] Ukoliko revizorsko poduzeće nema IT stručnjake, revizor može preporučiti da uprava angažira vanjske IT konzultante za provođenje dijagnostike spremnosti za kibernetičku sigurnost, što je puno opsežnija opcija koja uključuje osoblje s većim stupnjem stručnosti te koja je usredotočena na cjelokupni rizik, procese i kontrole subjekta u vezi s kibernetičkom sigurnošću, te uključuje, između ostalog, testiranje operativne učinkovitosti kontrola koje ublažavaju rizik kibernetičke sigurnosti.[94]

Dodatak 5 MRevs 315 sadržava smjernice o tome gdje može postojati povećani rizik:

- postojanje transakcija na webu koristeći vanjska sučelja
- neovlašteni pristupi IT okruženju i podacima: uključuje uzimanje u obzir trećih strana koje mogu imati ranjivosti u svom IT okruženju koje pružaju ulaznu točku u IT okruženje subjekta
- IT osoblje koje stječe prava pristupa iznad potrebnih

[91] Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf
[92] ISCA (2018). Cybersecurity Risk Considerations in a Financial Statements Audit. Preuzeto s https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf
[93] Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf
[94] ISCA (2018). Cybersecurity Risk Considerations in a Financial Statements Audit. Preuzeto s https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf

- korištenje naslijeđene tehnologije koju dobavljači više ne podržavaju može izložiti sustave subjekta riziku
- ciljani čimbenici industrije kao što su specifične industrije: iako će svi sektori vjerojatno biti ranjivi na prijetnje kibernetičke sigurnosti, neki imaju veći inherentni rizik zbog prirode svojih operacija i povijesti napada (napadači su, na primjer, 2020. ciljali zdravstvene i transportne organizacije[95]

Neka poduzeća sa slabim IT programima i kontrole možda niti ne shvaćaju da su bile predmet *cyber* napada. Revizori bi stoga trebali provoditi reviziju s načinom razmišljanja koji prepoznaje mogućnost stvarnog *cyber* napada, bez obzira na dosadašnja iskustva sa subjektom i bez obzira na revizorovo uvjerenje o obrambenim sposobnostima subjekta za kibernetičku sigurnost.[96]

Cyber napad može imati značajan utjecaj na poslovanje poduzeća i, u ekstremnim slučajevima, njegovu sposobnost da nastavi kao neograničeno poslovanje, na primjer:[97]

- ransomware napadi šifriraju ključne sustave ili zapise, ograničavajući sposobnost subjekta da radi određeni dulji period. Kao rezultat ransomwarea, izgubljeni su važni zapisi kao što su analitike potraživanja
- DDoS napadi na internetsku infrastrukturu subjekta, kao što je internetska trgovina, sustav dostave, automatizirano skladište ili sustav faktura i plaćanja
- reputacijska šteta robne marke od *cyber* napada koji utječu na buduće operacije/novčani tijek
- nastala šteta kupcima kojima su njihovi podaci ukradeni kao dio kršenja podataka.

[95] Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf
[96] Hamm, K. M. (2019). Cybersecurity: Where We Are: What More Can Be Done? A Call for Auditors to Lean In. Priopćenje na Baruch College 18th Annual Financial Reporting Conference, New York, NY.
[97] Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf

6. ZAKLJUČAK

Održavanje sigurnog okruženja kibernetičke sigurnosti u poduzećima ključno je u eri rastućih prijetnji i promjenjivih okolnosti. Krucijalno je da bitne informacije te resursi poduzeća budu zaštićeni. Danas su kibernetički napadi pitanje sigurnosti s kojima se suočava većina poduzeća. Poduzeća su primorana koristiti razne alate, operacije te korisničku podršku na različitim razinama kako bi se nosile sa sve većom prijetnjom kibernetičkih napada. U uvjetima konstantnih *cyber* prijetnji provođenje neovisne revizije znatno je otežano.

Kibernetička sigurnost krucijalno je poslovno pitanje, a obzirom na porast samih kibernetičkih napada visokog profila, dobiva sve veću pozornost poslovne zajednice. Kada je sigurnost poduzeća kompromitirana i povjerljivi podaci o klijentima ili vlasnički poslovni podaci budu ukradeni ili izgubljeni, isto može pretrpjeti reputacijsku štetu, smanjeno povjerenje investitora, izgubljeno poslovanje i potencijalne regulatorne kazne. Kibernetička sigurnost se više ne smatra samo "IT" pitanjem. Umjesto toga, rješava se kao dio većeg poslovnog pitanja.

Svjesne ozbiljnosti i frekventnosti kibernetičkih napada, mnoga poduzeća počinju mjeriti svoju izloženost prema takvoj vrsti napada te u sve većem broju počinju ulagati u kibernetičku sigurnost shvaćajući važnost iste. Trend „cyberkriminalnih“ aktivnosti nije posustajao ni prethodnih godina te se očekuje da će se isti nastaviti 2022. te narednih godina koje dolaze, što ukazuje na važnost ulaganja u kibernetičku sigurnost. Financijski troškovi koji su u korelaciji s napadima te svjetska potrošnja, također rastu eksponencijalno. Iz svega navedenog uistinu zaključujemo da je kibernetički rizik u vrhu poslovnih rizika današnjice kakvu poznajemo.

U poslovnom svijetu gdje su posljedice kibernetičkog kriminala ovih dana sve teže, poduzeća koja su napadnuta, mogu biti u kušnji skrivati pravu sliku stanja svojih poduzeća kako bi umirile svoje investitore i dioničare. Rezultat toga jest veći pritisak na neovisne revizore koji su odgovorni za pružanje razumnog uvjerenja da su financijski izvještaji poduzeća prikazani fer i realno.

Neovisni revizori posljedicom toga, obvezni su sve više pažnje posvećivati IT okruženju i kibernetičkoj sigurnosti kod svojih angažmana. Rizici kibernetičke sigurnosti imaju sveprisutan utjecaj na financijska izvješća. Obzirom da potencijalni gubitci, potraživanja i obveze povezane

s kibernetičkim incidentom utječu na financijsko izvještavanje klijenta, potrebna je temeljita procjena revizora da utvrdi jesu li financijski izvještaji klijenta iskazani fer, realno i istinito. To dakle znači da rizici kibernetičke sigurnosti utječu ne samo na poslovanje klijenta, već i na neovisnog revizora koje isto mora revidirati.

Za provođenje ovakvog angažmana revizor utvrđuje koliki je utjecaj IT- a na financijska izvješća. Procjenjuje opće te automatizirane kontrole, pouzdanost podataka i izvješća korištenih u reviziji koje je proizvelo poduzeće. Razlog i svrha ove procjene jest procjena materijalno značajnih pogrešnih prikazivanja u financijskim izvještajima.

Istraživanja pokazuju da su veće revizijske naknade povezane s većim ulaganjima u IT jer IT složenost otežava revizorima otkrivanje nepravilnosti, asimetrijom informacija, kibernetičkim incidentima i manje aktivnom revizijom povjerenstva.

LITERATURA

1. Accenture Security (2019). The Cost of Cybercrime. Preuzeto s https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study- Final.pdf#zoom=50
2. ASIC (2021). Cyber resilience good practices. Preuzeto s https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/
3. Auditing and Assurance Standards Board – AUASB (2021). The Consideration of Cybersecurity Risks in an Audit of a Financial Report. Preuzeto s https://www.auasb.gov.au/media/ll2ofjj0/aasbcs20170_cyberbulletinv3.pdf
4. Bao Ngo, T. N. i Tick, A. (2021). Cyber-security Risks Assessments by External Auditors. *Interdisciplinary Description of Complex Systems: INDECS*, *19*(3), 375-390.
5. Bems, M. R., Caselli, F. G., Grigoli, F., Gruss, B. i Lian, W. (2018). *Is inflation domestic or global? Evidence from emerging markets*. International Monetary Fund.
6. Black, P. E., Scarfone, K. i Souppaya, M. (2008). Cyber security metrics and measures. *Wiley Handbook of Science and Technology for Homeland Security*, 1-15.
7. Borkovich, D. J. i Skovira, R. J. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Information Systems*, *21*(4), 234-246.
8. CAQ (2019). Understanding Cybersecurity and the External Audit. Preuzeto s https://www.thecaq.org/wp-content/uploads/2019/03/cybersecurity_and_external_audit_final.pdf
9. CAQ (2020). Understanding Cybersecurity and the External Audit in the Covid-19 Environment. Preuzeto s https://www.thecaq.org/wp-content/uploads/2020/07/caq_understanding-cybersecurity-covid-19_2020-07.pdf
10. Center for Audit Quality (2014). Cybersecurity and the External Audit. Preuzeto s http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit
11. Contact Committee of the Supreme Audit Institutions of the European Union (2020). Cybersecurity in the EU and its Member States. Preuzeto s https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf
12. Cossin, D. i Lu, A. H. (2021). Bord Oversight of Cyber Risks and Cybersecurity. Preuzeto s https://www.imd.org/research-knowledge/articles/Board-Oversight-Cyber-Risks-Cybersecurity/

13. De Bolle, C. (2018). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf
14. De Bolle, C. (2019). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf
15. Directorate General for Communication (2020). Europska komisija, Special Eurobarometer 499: Europeans' attitudes towards cyber security (cybercrime). Preuzeto s https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en
16. Dutch Civil Code (1988). Book 2: Legal Persons. Preuzeto s http://www.dutchcivillaw.com/legislation/dcctitle2299aa.htm#sec299
17. EC-Council (2021). Certified Threat Intelligence Analyst. Preuzeto s https://www.eccouncil.org/programs/threat-intelligence-training/
18. European Systemic Risk Bord (2020). ESRB recommends establishing a systemic cyber incident coordination framework. Preuzeto s https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr.220127~f1548f677e.en.html
19. European Union Agency for Network and Information Security ENISA (2019). Threat Landscape Report 2018 – 15 Top Cyberthreats and Trends. Preuzeto s https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
20. European Union Agency for Network and Information Security ENISA (2020). Threat Landscape – Web-based attacks. Preuzeto s https://www.enisa.europa.eu/publications/web-based-attacks
21. European Union law (2016). Uredba Europskog parlamenta i vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive. Preuzeto s https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32016R0679
22. Europska komisija (2019). Otpornost, odvraćanje i obrana: jačanje kibersigurnosti EU-a. Preuzeto s https://eur-lex.europa.eu/legal-content/HR/TXT/DOC/?uri=CELEX:52017JC0450&from=EN
23. Frino, A., Palumbo, R. i Rosati, P. (2013). Does Information Asymmetry Predict Audit Fees? Evidence from Italian Listed Companies. Priopćenje na American Accounting Association Annual Meeting, Anaheim, CA.
24. Frost, J. i Shapiro, J. (2021). Cyber attacks 'the biggest risk in banking'. Preuzeto s https://www.afr.com/companies/financial-services/cyber-is-the-biggest-risk-in-banking-today-20210330-p57f5n

25. Greenberg, A. (2017). Hold North Korea Accountable For Wannacry – and the NSA, too. Preuzeto s https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/
26. Hamm, K. M. (2019). Cybersecurity: Where We Are: What More Can Be Done? A Call for Auditors to Lean In. Priopćenje na Baruch College 18th Annual Financial Reporting Conference, New York, NY.
27. Han, S., Rezaee, Z., Xue, L. i Zhang, J. H. (2016). The association between information technology investments and audit risk. *Journal of Information Systems*, *30*(1), 93-116.
28. Hrvatska revizorska komora (2004). Razumijevanje poslovnog subjekta i njegovog okruženja te procjenjivanje rizika značajnog pogrešnog prikazivanja. Preuzeto s http://www.propisi.hr/print.php?id=5695
29. Hrvatska revizorska komora (2022). Posebna razmatranja u reviziji financijskih instrumenata. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/full/2022_02_17_179.html
30. IBM (2020). How much does a dana breach cost? Preuzeto s https://www.ibm.com/sg-en/security/data-breach
31. International organization of securities commissions (2016). Cyber Security in Securities Markets – An International Perspective. Preuzeto s https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
32. Irvine, C. E. (2014). *Multilevel Security*. U J. G. Voeller (Ur.), *Cyber Security* (9-28). John Wiley & Sons Inc.
33. ISCA (2018). Cybersecurity Risk Considerations in a Financial Statements Audit. Preuzeto s https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf
34. ista.com/chart/26631/most-relevant-business-risks-in-2022/
35. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A. i Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? (No. w24409). *National Bureau of Economic Research*.
36. KPMG (2022). Cybersecurity considerations 2022 – Trust through security. Preuzeto s https://assets.kpmg/content/dam/kpmg/au/pdf/2022/cyber-security-considerations-2022.pdf
37. Lee-Makiyama, H. (2018). *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* European Centre for International Political Economy (ECIPE), 2(18), 1-20.

38. Li, H., No, W. G. i Boritz, J.E. (2020). Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151-171.
39. Lingscheid, A. (2021). SAP Solutions for Cyber Security and Data Protection. Preuzeto s https://blogs.sap.com/2021/07/16/sap-solutions-for-cyber-security-and-data-protection/
40. Međunarodni odbor za standarde revidiranja i izražavanja uvjerenja IAASB (2013). Prepoznavanje i procjenjivanje rizika značajnih pogrešnih prikazivanja kroz stjecanje razumijevanja subjekta i njegovog okruženja. Preuzeto s https://www.srr-fbih.org/sites/default/files/standards/2021-12/Medunarodni%20revizijski%20standard%20315%20%28izmijenjen%29.pdf
41. Milkovich, D. (2019). 15 Alarming Cyber Security Facts and Stats. Preuzeto s https://www.cybintsolutions.com/cyber-security-facts-stats/
42. Ministarstvo unutarnjih poslova (2022). Kibernetička sigurnost. Preuzeto s https://mup.gov.hr/istaknute-teme/nacionalni-programi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335
43. Moore, S. (2019). Gartner Forecasts Worldwide Information Security Spending to Exceed $ 124 Billion in 2019. Preuzeto s https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
44. Morgan, S. (2019). Official Annual Cybercrime Report – Herjavec Group. Preuzeto s https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
45. NBA Van hype naar aanpak (2016). Publieke managementletter over cybersecurity. Preuzeto s https://www.nba.nl/globalassets/projecten/kennis-delen-pmls/cybersecurity/pml-cyber-security.pdf
46. NTT Security (2018). 2018 Risk: Value Report. Preuzeto s https://assets.sig.org/s3fs-public/srcDocs/2018_Risk_Value_Report_NTT_Security.pdf?file=1&type=node&id=14846&
47. Petric, I. (2022). Kibernetička sigurnost u 2022. godini – opasnosti i izazovi za tvrtke. Preuzeto s https://duplico.io/kiberneticka-sigurnost-u-2022-godini-opasnosti-i-izazovi-za-tvrtke/
48. Public Company Accounting Oversight Bord (2014). Standing Advisory Group Meeting: Cybersecurity. Preuzeto s

http://pcaobus.org/News/Events/Documents/0624252014_SAG_Meeting/06252014_Cybersecuri ty.pdf

49. PwC (2020). Global Economic Crime and Fraud Survey. Preuzeto s https://www.pwc.com/gx/en/services/forensics/economic-crime-survey-2020.html
50. Raina, K. (2021). Zero trust security explained: Principles of the zero trust model. Preuzeto s https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/
51. Rimol, M. (2022). Gartner Forecasts Worldwide Information Security Spending to Reach $4.4 Trillion in 2022. Preuzeto s https://www.gartner.com/en/newsroom/press-releases/2022-04-06-gartner-forecasts-worldwide-it-spending-to-reach-4-point-four-trillion-in-2022
52. RiskBased Security (*2019).* 2019 on track to being the „worst year on record" for breach activity. Preuzeto s https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report
53. Rosati, P., Gogolin, F. i Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. *The International Journal of Accounting 53*(3), 1-75.
54. Security Compliance Associates – SCA (2020). Cyber security risk report. Preuzeto s https://scasecurity.com/
55. Smetters, D.K. (2014). Cyber Security Technology Usability and Management. U J. G. Voeller (Ur.), *Cyber Security* (41-55). John Wiley & Sons, Inc.
56. Smith, T. i Pinsker, R. (2019). Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems*, *33*(2), 177-204.
57. Središnji državni ured za razvoj digitalnog društva (2022). Kibernetička sigurnost. Preuzeto s https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436
58. Stop Ransomware (2020). Ransomware 101. Preuzeto s https://www.cisa.gov/stopransomware/ransomware-101
59. The Global State of Information Security (2017). Survey 2017 – Moving forward with cybersecurity and privacy. Preuzeto s https://www.pwc.com/gsiss2015
60. Tušek, B. i Halar, P. (2017). Uloga interne revizije u povećanju djelotvornosti procjenjivanja i upravljanja cyber sigurnosti. *Računovodstvo i financije*, *63*(9), 42-53.
61. Tušek, B., Ježovita, A. i Halar, P. (2020). Izazovi djelovanja interne i eksterne revizije u eri pandemije Covid-19. *Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru*, (26), 111-130.

62. Tysiac, K. (2014). Auditors have important role in cybersecurity. Preuzeto s https://www.journalofaccountancy.com/news/2014/mar/20149835.html
63. van Veen, M. (2016). Cyber Security: A Paradigm Shift in IT Auditing: How to Deal with Cyber Security Risks in the Financial Statement Audit. *Compact, 3*, 53-59.
64. Varonis (2019). Globas Dana Risk Report From The Varonis Data Lab. Preuzeto s https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf
65. Vlada Republike Hrvatske (2015). Odluka o donošenju nacionalne strategije kibernetičke sigurnosti i akcijskog plana za provedbu nacionalne strategije kibernetičke sigurnosti. Preuzeto s https://www.uvns.hr/UserDocsImages/dokumenti/Odluka_o_dono%C5%A1enju_Nacionalne_strategije_kiberneti%C4%8Dke_sigurnosti_i_Akcijskog_plana_za_provedbu_Nacionalne_strategije_kiberneti%C4%8Dke_sigurnosti.pdf?vel=702079
66. Wainwright, R. (2017). IOCTA Internet Organised Crime Threat Assessment. Preuzeto s https://www.europol.europa.eu/iocta/2017/FOREWORD.html
67. Zandt, F. (2022). The Biggest Business Risks in 2022. Preuzeto s https://www.stat

POPIS SLIKA

SAŽETAK

Kibernetička sigurnost jedno je od najsloženijih i najrazvijenijih pitanja s kojima se suočavaju poduzeća danas. Informacije su vrijedna imovina svakog poduzeća te je neminovno je ulaganje u područje kibernetičke sigurnosti kako bi se zaštitilo poslovanje i interesi poduzeća. Cilj ovog rada je ukazati na važnost kibernetičke sigurnosti, približiti važnost djelovanja neovisnih revizora u procjeni rizika kibernetičke sigurnosti. Potrebno je konstantno unapređenje znanja neovisnih revizora u području informacijskih tehnologija, obzirom na sve veću potrebu za revidiranjem klijenata koji imaju ili složene IT sustave ili su meta kibernetičkih napada. Sumarno rečeno, područje kibernetičke sigurnosti kompleksno je te je krucijalno područje u kojem su potrebna unapređenja kako bi se poslovni rizici, a vezano s tim i potrošnja smanjili. Uloga i zadatak neovisnog revizora jest dati razumno uvjerenje da su financijski izvještaji prikazani fer i realno, te da nema značajnih materijalnih pogrešnih prikazivanja koje bi mogle utjecati na neograničeno poslovanje poduzeća te na takav način ugroziti dioničare iste.

Ključne riječi: kibernetička sigurnost, neovisni revizori, materijalno značajna pogrešna prikazivanja.

SUMMARY

Cybersecurity is one of the most complex and developed issues facing companies today. Information is a valuable asset of any company and is an inevitable investment in the field of cyber security to protect the business and interests of the company. The aim of this paper is to point out the importance of cyber security, to bring closer the importance of the work of independent auditors in assessing the risks of cyber security. There is a need to constantly improve the knowledge of independent auditors in the field of information technology, given the growing need to audit clients who have either complex IT systems or are the target of cyberattacks. In summary, the field of cybersecurity is complex and is a crucial area where improvements are needed to reduce business risks and related spending. The role and task of the independent auditor is a reasonable belief that the financial statements are presented fairly and realistically, and significant material misstatements that could affect the company's unrestricted operations and thus endanger its shareholders.

Key words: cybersecurity, independent auditors, material misstatements.