# KIBERNETIČKA SIGURNOST: ULOGA INTERNE I EKSTERNE REVIZIJE I REVIZIJSKIH ODBORA

**Vrdoljak, Kristijan**

**SVEUČILIŠTE U SPLITU**

**EKONOMSKI FAKULTET**

**DIPLOMSKI RAD**

# KIBERNETIČKA SIGURNOST: ULOGA INTERNE I EKSTERNE REVIZIJE I REVIZIJSKIH ODBORA

**Mentor:**

**doc. dr. sc. Marko Čular**

**Student:**

**Kristijan Vrdoljak**

**Split, lipanj, 2024.**

## IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, KRISTIJAN VRDOLJAK,

(ime i prezime)

izjavljujem i svojim potpisom potvrđujem da je navedeni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja na objavljenu literaturu, što pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio navedenog rada nije napisan na nedozvoljeni način te da nijedan dio rada ne krši autorska prava. Izjavljujem, također, da nijedan dio rada nije korišten za bilo koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Split, 28. 06. 2024. godine

Vlastoručni potpis: 

## SADRŽAJ:


1. UVOD ..... 1
   1.1. Problem i predmet istraživanja ..... 1
   1.2. Ciljevi istraživanja ..... 3
   1.3. Istraživačka pitanja ..... 4
   1.4. Metodologija istraživanja ..... 4
   1.5. Doprinos istraživanja ..... 5
   1.6. Struktura i sadržaj diplomskog rada ..... 5
2. KIBERNETIČKA SIGURNOST I RIZICI ..... 7
3. INTERNA REVIZIJA: KIBERNETIČKA SIGURNOST ..... 10
   3.1. Uloga interne revizije u korporativnom upravljanju ..... 10
   3.2. Proces interne revizije kibernetičke sigurnosti ..... 12
4. EKSTERNA REVIZIJA: KIBERNETIČKA SIGURNOST ..... 16
   4.1. Uloga eksterne revizije u korporativnom upravljanju ..... 16
   4.2. Procjena rizika kibernetičke sigurnosti od eksterne revizije ..... 17
5. REVIZIJSKI ODBOR: KIBERNETIČKA SIGURNOST ..... 20
   5.1. Uloga revizijskog odbora u korporativnom upravljanju ..... 20
   5.2. Revizijski odbor i kibernetička sigurnost ..... 20
6. EMPIRIJSKO ISTRAŽIVANJE ..... 22
   6.1. Metodologija ..... 22
   6.2. Interpretacija empirijskog istraživanja ..... 22
   6.3. Rezultat empirijskog istraživanja ..... 33
7. ZAKLJUČAK I RASPRAVA ..... 34

LITERATURA ..... 41

SAŽETAK ..... 50

SUMMARY ..... 50

PRILOZI ..... 51

# 1. UVOD

## 1.1. Problem i predmet istraživanja

Tehnologija donosi promjene na svim poljima svakodnevice, pa tako i u poslovanju. Digitalizacija je omogućila organizacijama efikasnije trošenje materijalnih resursa i vremena potrebnog za obavljanje redovnih zadataka koje čine poslovanje. Čuvanje i pohrana podataka na računalima stvara potrebu za novim načinom zaštite, a takvu zaštitu nazivamo kibernetička sigurnost. Prema Središnjem uredu za razvoj digitalnog društva (2023.); „Kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi."

Predmet rada bit će uloga interne i eksterne revizije, te revizijskih odbora u provođenju internih kontrola, i zaštiti korporativnih tijela od kibernetičkih napada, kao i odgovor na kibernetičke incidente. Istraživanje će se provoditi s pomoću intervjua, u kojem će se postaviti pet pitanja osobama zaposlenih u internoj i eksternoj reviziji, te članovima revizijskih odbora.

Informacijski sustavi u organizacijama igraju važnu ulogu u poslovanju. Količina podataka se povećava, s time rastu i rizici od zlouporabe, krađe ili nepravilnog korištenja imovine poduzeća. Kibernetički incidenti mogu oštetiti poduzeća za milijunske iznose, pa tako postoje primjeri gdje je PlayStation 2011. godine izgubio oko 171 milijun dolara zbog nedostupne web stranice nakon hakerskog napada, Yahoo je 2014. godine izgubio 350 milijuna dolara zbog krađe 3 milijuna korisničkih računa od strane hakera, Uber je bio žrtva krađe 57 milijuna podatak korisnika i 600.000 vozačkih dozvola što je dovelo do reputacijske i financijske štete u 2016. godini (Bao Ngo i Tick, 2021a).

Posljedice pandemije coronavirusa (COVID-19) 2020. godine dodatno su ugrozile sigurnost podataka, zato što se način poslovanja bitno promijenio. Zbog uvođenja lockdowna i karantena diljem Europe i svijeta, poslovi su se odvijali od kuće preko osobnih računala čime se dostupnost podataka povećala prema stranim izvorima. Prema podacima FBI-a u izvješću za travanj 2020. godine, kibernetički napadi u Sjedinjenim Američkim državama su se povećali za 600 % i u svijetu za 300 % (Borkovich i Skovira, 2020).

Allianz Global Corporate & Specialty provodi istraživanje za najveće poslovne rizike na godišnjoj razini, kibernetički kriminal predstavlja najveći rizik za poslovanje u 2020., 2022. i 2023, godini. U 2023. godini 34 % ispitanika odabralo je kibernetičku sigurnost kao najveći poslovni rizik. Istraživanje također prikazuje izloženost kibernetičkim napadima u više kategorija, te podaci navode kako najveću prijetnju

predstavljaju: provaljivanje podataka (53 %), rast ucjenjivačkih softvera (50 %), ometanje poslovanja i lanca nabave (35 %), te rast zloćudnih softvera (28 %), (Allianz Risk Barometer, 2023). Ljudske greške čine veliki dio problema sigurnosti, prema istraživanju IBM-a, takve greške čine 95 % provala sigurnosti, odnosno 19 do 20 kibernetičkih provala izazvano je ljudskim faktorom (Ahola, 2021).

Funkcija interne revizije kao jedan od mehanizama korporativnog upravljanja iznimno je bitna za pravilno funkcioniranje poduzeća, pa tako i za očuvanje sigurnosti podataka. Prema Sabillon et al. (2018) IT revizija mora u poduzeću stvoriti kulturu zaštite od kibernetičkih napada, te sama struktura revizije sadržavati mehanizme s pomoću kojih će se napadi prepoznati, eliminirati i zaštititi u budućnosti. Također, navedena je i potreba za kontinuiranim unaprjeđenjem poduzeća i sudionika u infrastrukturi i znanju na području sigurnosti. Uloga internih revizora u kibernetičkoj sigurnosti sadržava identificiranje slabosti u sustavima koji mogu izazvati provalu, usklađivanje s normama i standardima i zakonima koji uređuju zaštitu podatka (npr. GDPR), te kontinuirano praćenje i kontrola. Učinkovitost interne revizije na kvalitetu i uspješnost provođenja kibernetičke sigurnosti nije jednostavno izračunati, te s obzirom na to da se još radi o tehnologiji koja se brzo razvija, imamo samo nekolicinu radova koji su se dotakli problematike. Istraživanja su pokazala kako je dobra komunikacija između internog revizora, odjela za informacijske tehnologije (IT), kao i vrhovnog menadžmenta temelj za pravilno funkcioniranje zaštite poduzeća i stvaranja veće vrijednosti za cjelinu (Steinbart et al., 2012 i Stafford et al., 2018).

Eksterna revizija temelji svoj rad prvenstveno na ispitivanje vjerodostojnosti i ispravnosti financijskih izvješća, usklađivanje s propisanim standardima, te provjera sustava internih kontrola. Kibernetički napadi, posebno oni usmjereni prema računovodstvenim sustavima, dovode do pogrešnih evidencija koje ugrožavaju vjerodostojnost financijskih izvješća (PWC, Global Economic Crime and Fraud Survey, 2020). Revizorima su ključne politike informacijske sigurnosti koje se provode u poduzeću, jer s pomoću politika revizor određuje razine sigurnosti potrebne za zaštitu podataka i klasificira informacije poduzeća prema relevantnosti i osjetljivosti prema kibernetičkim napadima. Bitno je utvrditi ispunjava li politika kibernetičke sigurnosti poduzeća industrijske i globalne standarde, a to revizor postiže usporedbom s idealnom verzijom (Chimwanda, 2022).

Revizijski odbori su dio upravljačkih tijela kojima je glavna uloga nadzor nad poslovnom i financijskom radu društva, pomaganje u izradi financijskih izvještaja i potpora internoj i eksternoj reviziji u ocjenjivanju zrelosti sustava i kvaliteti izrade financijskih izvještaja (Al-Baidhani, 2014). Prema direktivi Europske unije (EU) 537/2014 dužnosti revizijskog odbora su: izvještavanje nadzornog odbora o ishodu vanjske revizije, objašnjavanje na koji način je zakonska revizija pridonijela integritetu financijskog izvještavanja i koja je

uloga revizijskog odbora u tom procesu, praćenje procesa financijskog izvještavanja i dostava preporuka ili prijedloga za osiguravanje njegovog integriteta, praćenje obavljanja zakonske revizije godišnjih financijskih izvještaja i godišnjih konsolidiranih financijskih izvještaja, ispitivanje i praćenje neovisnosti zakonskih revizora ili revizorskih društava, ispitivanje i praćenje primjerenosti pružanja nerevizijskih usluga subjektu revizije i provođenje i kontrola nad postupkom izbora revizorskog društva te predlaganje imenovanja revizorskog društva.

S obzirom na relativno novi izazov koji kibernetička sigurnost predstavlja upravni odbori nemaju ekspertize u informacijskim tehnologijama, društva sve više zapošljavaju IT stručnjake koje postavljaju u odbore. Najveću prednost koja poduzeća ostvaruju s IT stručnjacima u upravnim odborima jest edukcija ostalih članova u razumijevanju povezanosti digitalnih tehnologija s poslovanjem (Kickenweiz, Sedlock i Daum, 2016). Odgovornost revizijskog odbora u otkrivanju i nadziranju rizika, odnosno praćenje aktivnosti, smjernica i politika koje čine obranu od kibernetičkog napada se povećavaju, zato što revizijski odbori već imaju ulogu nadziranja internih kontrola i učinkovitosti informacijskog sustava (Hartmann i Carmenate, 2021).

### 1.2. Ciljevi istraživanja

Cilj ovog istraživanja je objasniti kako uloga interne i eksterne revizije te revizijskih odbora utječe na obranu i zaštitu poduzeća na postojeće i buduće kibernetičke napade. Istražit će se na koji način funkcioniraju interne kontrole, koje smjernice i standardi pomažu internom revizoru pri otkrivanju i vrednovanju rizika, zatim kako eksterni revizori utvrđuju vjerodostojnost financijskih izvještaja odnosno na koji način otkrivaju informacije i djelovanja koja bitno mogu narušiti ispravno prikazivanje financijskih izvještaja. Istražit će se uloga revizijskih odbora koja je uspostavljena na komunikaciji s eksternim revizorima, potpore internim kontrolama i evaluacije rada interne revizije. Na temelju ovih saznanja dobit će se potpuna slika o ulogama korporativnih tijela i profesije revizije u izazovima koje predstavlja kibernetička sigurnost. Intervjuiranjem internih i eksternih revizora, kao i člana revizijskog odbora želi se utvrditi koje su dužnosti navedenih tijela u zaštiti organizacije od kibernetičkih provala, iskustva sugovornika kroz vlastiti rad, kao i značaj međusobne komunikacije i potpore u procjenjivanju rizika, učinkovitosti internih kontrola, te razumijevanju mrežnih struktura sustava.

### 1.3. Istraživačka pitanja

Istraživačka pitanja daju smjernice s pomoću kojih se stvara bolja slika o problematici koja je predstavljena. Fokus rada temelji se na radu internih kontrola i evaluacijom istih provođenjem revizije, stoga će se istraživačka pitanja odnositi na iskustvo, inovativnost i međusobnu komunikaciju revizora i revizijskih odbora kao glavne odrednice pravilne zaštite i obrane od kibernetičkih napada.

IP1: Koju ulogu kibernetička sigurnost ima u oblikovanju poslovanja i upravljanju s informacijama, te koje su najbolje prakse za kibernetičku zaštitu?

IP2: Koje su najvažnije pouke koje su organizacije naučile iz kibernetičkih incidenata, a koje su posljedice nedostatka revizijskih nadzora ili neadekvatnih praksi u kibernetičkoj sigurnosti?

IP3: Kako revizori mogu pomoći organizacijama u razvijanju proaktivne strategije kibernetičke sigurnosti koje prepoznaju i kako predviđati buduće prijetnje?

IP4: Na koji način revizijski odbori surađuju s internim i eksternim revizorima kako bi poboljšali kibernetičku sigurnost organizacije, te kako revizijski odbori prate i procjenjuju učinkovitost politika i procedura kibernetičke sigurnosti u organizaciji?

### 1.4. Metodologija istraživanja

U istraživanju i izradi rada koristit će se više metoda, dok će naglasak biti na metodi intervjuiranja. Metode koje se koriste su sljedeće (Zelenika, 2000a):

- Metoda intervjuiranja- razgovor koji se vodi između ispitivača i ispitanika s unaprijed pripremljenim pitanjima. Svrha intervjua je dobiti znanstveno korisne i upotrebljive informacije koje se obrađuju za postavljeni problem i ciljeve istraživanja. Intervju se može provoditi kao slobodni, grupni, standardizirani i individualni. Za potrebe ovog istraživanja koristit će se individualni intervju.
- Metoda analize- postupak istraživanja i objašnjenja tematike raščlanjivanjem pojmova na jednostavnije sastavne cjeline s ciljem otkrivanja i proučavanja znanstvene istine.
- Metoda apstrakcije- analiza karakteristika i osobina predmeta u svrhu odabira elemenata potrebnih za istraživanje. Apstrakcija se primjenjuje u istraživanjima u kojima se predmet zbog kompleksne svestranosti mora izdvojiti na bitne i nebitne elemente čime se stvara realnija slika o problemu.

- Metoda generalizacije- postupak u kojem se individualnim opažanjima dolazi do općeg zaključka.
- Metoda dokazivanja i opovrgavanja- dokazivanje istinitosti stavova ili spoznaja postavljanjem teza koje se potvrđuju argumentima. Svrstava se među najsloženije metodološke postupke koji sadržavaju gotovo sve ostale metode. Metoda opovrgavanja suprotna je metodi dokazivanja, u kojoj se teza pobija.
- Komparativna metoda- uspoređivanje činjenica, karakteristika i osobina u svrhu razdvajanja sličnosti i razlika predmeta, pretpostavki ili pojava s ciljem dobivanja novih spoznaja i zaključaka.

### 1.5. Doprinos istraživanja

Istraživanje ima cilj produbiti znanja i prakse u svrhu zaštite društava od financijske i nematerijalne štete uzrokovane kibernetičkim napadima. Intervjuiranjem će se prikupiti informacije na koji način se postiže optimalna zaštita podataka i prevencija od napada. Ovim istraživanjem doprinosi se većoj zaštiti osjetljivih informacija na sljedeći način: identificiraju se rizici, praćenje usklađenosti, praćenje incidenata i performansi, edukacija svih djelatnika i ispitivanje kriznih planova. Time će se povećati otpornost organizacije na kibernetičke napade i podići svijest o kibernetičkoj sigurnosti. Nadalje, cilj je objasniti ulogu internih revizora koji u suradnji s menadžmentom u upravljanju rizicima identificiraju i vrednuju rizike, provode interne kontrole, te pružaju savjetodavne usluge u svrhu učinkovitog upravljanja organizacijom. Uloga eksterne revizije bit će objašnjena kroz elemente kibernetičke sigurnosti koje se odnose na pravilno i vjerodostojno financijsko izvještavanje, te suradnja s internim revizorima, odnosno kako interni revizori mogu pomoći eksternim u razumijevanju organizacije. Doprinos koji se želi postići ovim istraživanjem odnosi se i na ulogu revizijskog odbora; na koji način članovi odbora služe kao podrška internoj reviziji pri odobravanju resursa, nadziranju internih kontrola i stvaranjem dobre komunikacije. Kako članovi revizijskog odbora pomažu u odabiru revizorskog društva, praćenju neovisnosti eksternog revizora i održavanjem redovnih sastanka. I najvažnije, služi li funkcija revizijskog odbora kao snaga u kibernetičkoj sigurnosti i može li djelovanje članova odbora podići organizaciju na višu razinu poslovanja.

### 1.6. Struktura i sadržaj diplomskog rada

Diplomski rad bit će sastavljen od sedam poglavlja. Prvi dio rada odnosi se na uvodno poglavlje. U uvodu je opisan problem i predmet rada, ciljevi istraživanja, istraživačka pitanja, metodologija i doprinos istraživanja.

U drugom dijelu obradit će se teorijska podloga o kibernetičkoj sigurnosti i rizici od kibernetičkog napada. Definiranje pojmova, opisivanje vrsti i evaluacija rizika, kao i utjecaj kibernetičkih incidenata na organizaciju.

Treći dio odnosi se na ulogu interne revizije u korporativnom upravljanju, te procesu interne revizije kibernetičke sigurnosti. U četvrtom dijelu obradit će se uloga eksterne revizije u korporativnom upravljanju i procjena rizika od eksterne revizije. Peti dio obrađuje ulogu revizijskih odbora u korporativnom upravljanju, suradnju s internim i eksternim revizorima, kao i utjecaj revizijskog odbora na kibernetičku sigurnost.

Šesti dio je empirijsko istraživanje, odnosno analiza podataka provedenih intervjua, te interpretacija podataka na saznanja koji su prikupljeni i obrađeni. Završno sedmo poglavlje rada odnosi se na zaključak i raspravu.

## 2. KIBERNETIČKA SIGURNOST I RIZICI

S obzirom na rastuću ulogu zaštite digitalne imovine od hakerskih napada ulaganje u sigurnost je postala ključna komponenta u poslovanju organizacija. Zadaća je na svim zaposlenicima, uključujući sve razine menadžmenta i uprave odgovorno korištenje podataka i softverskih programa na način na koji propisuju standardi i interne kontrole organizacije.

Ulaganja u kibernetičku sigurnost također su u porastu, tržište kibernetičke sigurnosti je u 2020. godini vrijedilo oko 194 milijarde dolara, a očekivanja su da će do 2027. godine narasti do 290 milijardi dolara (Dieli et al., 2020). Otpornost i zaštitu protiv kibernetičkih napada treba promatrati kao dugoročni cilj ojačavanja na razini cijelog sustava, a ne pojedine organizacije zasebno. Razlog tome je što problem na jednom području ugrožava sustav u cijelosti (Galinec, 2023). Podaci se moraju zaštiti na više razina, postavljanjem lozinki i periodično postavljanje novih, ograničen pristup programima i podacima, kao i zaštita antivirusnim programima čine osnovu za sigurno korištenje sustava. Menadžment za zaštitu informacijskog rizika (ISRM) glavni je pokretač stvaranja i održavanja zaštite u poduzećima. To je sustav koji se sastoji od procedura i koraka pristupanju problemu, a to su: identifikacija problema, analiza rizika, prioritiziranje rizika, odgovor na rizike, i praćenje rizika (Bansal i Mamodiya, 2023). Za 2024. godinu predviđa se kako će potrošnja narasti na 215 milijardi dolara na globalnoj razini, što znači da će narasti za 14.3 % u odnosu na 2023. godinu (Knezović, 2023). Potrošnja po segmentima prikazana je u slici 1.

Prema Kamyia et al. (2018) poduzeća koja su poznata, odnosno velika poduzeća koja kotiraju visoko na burzama, poduzeća s velikom nematerijalnom imovinom, te poduzeća u kojima odbori ne daju dovoljno pozornosti menadžmentu u upravljanju rizicima imaju veću mogućnost od kibernetičkog napada od ostalih. Posljedice nakon napada se pokazuju kroz pad investicija, povećanje dugoročnog duga i smanjene apetita za rizik. Velika Poduzeća i poduzeća koja se bave maloprodajom imaju pad u rastu prodaje, dok poduzeća koja se bave trajnim dobrima osjete pad ROA-e i niži novčani tok. Također se pokazalo da predsjednici uprave nakon napada gube svoje bonuse i smanjuje se tolerancija na izlaganje rizicima.

*Slika1. Rast globalne potrošnje u kibernetičkoj sigurnosti*

| segment | potrošnja 2022 | rast 2022 | potrošnja 2023 F | rast 2023 F | potrošnja 2024 F | rast 2024 F |
|---|---|---|---|---|---|---|
| sigurnost aplikacije | 5.047,6 | 10,9% | 5.765,2 | 14,2% | 6.670,3 | 15,7% |
| sigurnost u cloudu | 4.487,4 | 24,0% | 5.616,7 | 25,2% | 7.002,6 | 24,7% |
| privatnost podataka | 1.129,2 | 9,9% | 1.338,7 | 18,5% | 1.667,3 | 24,6% |
| sigurnost podataka | 3.072,9 | 21,4% | 3.692,1 | 20,1% | 4.333,3 | 17,4% |
| upravljanje pristupom identitetu | 13.944,1 | 13,6% | 16.169,1 | 16,0% | 18.556,5 | 14,8% |
| zaštita infrastrukture | 24.089,0 | 19,9% | 28.359,6 | 17,7% | 33.319,6 | 17,5% |
| integrirano upravljanje rizikom | 5.157,3 | 9,6% | 5.687,1 | 10,3% | 6.277,7 | 10,4% |
| oprema za mrežnu sigurnost | 18.932,5 | 11,9% | 21.383,6 | 12,9% | 24.360,1 | 13,9% |
| sigurnosne službe | 73.394,7 | 3,9% | 80.835,7 | 10,1% | 89.996,7 | 11,3% |
| softver za sigurnost potrošača | 7.443,4 | 2,9% | 7.901,7 | 6,2% | 8.406,7 | 6,4% |
| ostalo | 8.029,8 | 50,1% | 11.365,4 | 41,5% | 14.362,8 | 26,4% |
| **ukupno** | **164.728,0** | **10,6%** | **188.114,8** | **14.2%** | **214.953,7** | **14.3%** |

Izvor: Knezović, G. (2023) Kibernetička sigurnost- Globalna potrošnja rast će 14%, Mreža 11/2023, str.18, dostupno na: https://mreza.bug.hr/casopis/studeni-2023/408#tab-magazine-19 (pristupljeno: 22.5.2024.)

Agrawal (2024) navodi pet najvećih kiberntičkih prjetnji:

- Društveni inženjering
- Izlaganje prema trećoj strani
- Slabosti u zaštiti Clouda
- Ucjenjivački softver (eng. *Ransomware*)
- Napadi preko uređaja s „internetom stvari“

Društveni inženjering je vrsta kibernetičkog napada u kojem kriminalci dolaze do imovne ili informacija manipulacijom, lažnim predstavljanjem, pritiscima ili prijetnjama (Breda et. Al, 2017). Primjeri društvenog inženjeringa su: phishing, pred-poruke, mamci i drugi. Ciljana skupina za napade su sve vrste zaposlenika, kupci i prodavači.

Izlaganje trećoj strani (eng. *Third-party induced cyber incident*) je način dobivanja podataka preko trećih strana, obično poduzeća koja obavljaju usluge prema organizaciji. Ovakav način izuzetno je štetan jer ugrožava podatke od obje organizacije (Benaroch 2021).

Slabosti u zaštiti Clouda (eng. *Cloud security vulnerabilities*) obuhvaća niz propusta ili pogreški koji se mogu javiti u serverima što kibernetički kriminalci iskorištavaju. Klijenti koji koriste usluge Clouda nisu sigurni za svoje podatke, stoga postoji niz mjera zaštite koje mogu stvoriti povjerenje. Neke od glavnih

mjera su: ograničena dostupnost, višestruke ovjere i ovlaštenja, te korištenje različitih mehanizama šifriranja (Kumar i Goyal 2019).

Ucjenjivački softveri izvlače informacije i novac s pomoću šifriranja datoteka slanjem štetnih programa. Funkcioniraju na dva načina; šifriranjem datoteka i ograničavanjem pristupa na računala. S pomoću algoritama zaključavaju datoteke i podatke da vlasnici nemaju pristup, potom ucjenjivanjem dolaze do traženih sredstava (Kumhar et al. 2016).

Napadi preko uređaja s internetom stvari (eng. *Internet of Things*.) podrazumijeva provale u sustave kroz uređaje koji su spojeni na mrežu a to mogu biti mobilni telefoni, kamere, senzori, strojevi ili aktuatori u velikim proizvodnim pogonima. Obrana od takve vrste napada vrši se kroz inovativne sustave kao što su Industria 4.0. i cyber-fizički sustavi (Shah i Sengupta 2020).

Motivacija za kibernetičke napade ima više, a s obzirom na opseg i cilj mogu se razvrstati kao; kibernetički kriminal, kibernetička špijunaža, kibernetički terorizam, te kibernetički rat. U kibernetički kriminal spadaju kategorije objašnjenje u prethodnom dijelu, a za cilj imaju ilegalno stjecanje imovinske koristi na štetu organizacije. Kibernetička špijunaža služi za praćenje i krađu podataka u svrhu prikupljanja znanja i vještina od individualaca, organizacija ili vlada. Kibernetički terorizam obuhvaća kibernetički kriminal u širokom obujmu, ostvaruje se kroz prijetnje fizičkog oštećenja ili smrti u cilju stvaranja veće štete za određenu zajednicu. Kibernetički rat provodi se od strane države prema drugim državama ili organizacijama, obično služi za ometanje ili uništavanje vojne opreme, najbolji primjer bio bi Ruski kibernetički napadi za vrijeme rata s Gruzijom i Estonijom (Uma i Padmavathi 2013).

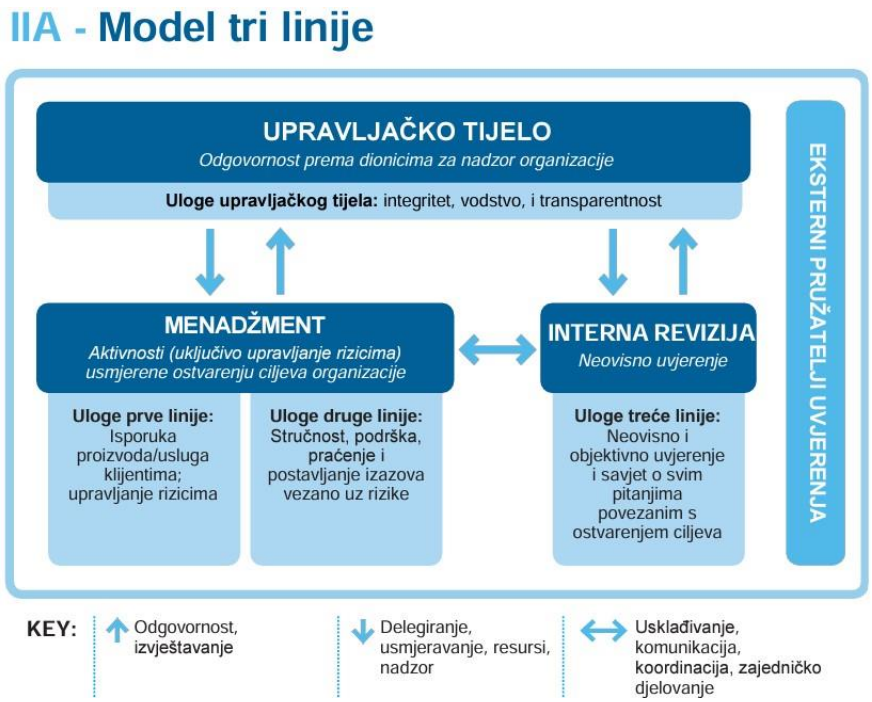
# 3. INTERNA REVIZIJA: KIBERNETIČKA SIGURNOST

## 3.1. Uloga interne revizije u korporativnom upravljanju

Interna revizija je funkcija koja se kontinuirano razvija, u prošlosti interni revizori obavljali su dužnosti procjenama organizacijskih ciljeva i predviđali rizike informalno, dok je u današnje vrijeme ta uloga uključena u organizacijski menadžment. Kroz razvitak profesija interne revizije je od kontrolne uloge postavljena za provjeru računovodstvenih i financijskih podataka postala strateški partner vlasnicima i dioničarima, kao i važan čimbenik u poboljšanju procesa upravljanja. Danas se menadžeri oslanjaju na interne revizore u ocjenjivanju učinkovitosti sustava interne kontrole i upravljanju rizicima pružajući neovisno mišljenje i savjetodavne usluge prema menadžmentu i upravi (Savčuk 2007).

Dolaskom informacijskih tehnologija i njihovim razvitkom kroz 20.st i 21.st., uvođenjem i upravljanjem tehnologijom su vodili odjeli informacijskih tehnologija (IT), pa tako i kibernetička sigurnost ostaje u domeni tog sektora (vodeći se „ostavi IT-u“ logikom). U današnje vrijeme zaštita podataka, informatička pismenost i porast kibernetičkog kriminala, te nastali problemi šire se na sve organizacijske strukture poduzeća pa tako i na tijela korporativnog upravljanja koja se oslanjaju na rad interne revizije kao mjeru osiguranja i kontrole očuvanja informacija unutar organizacije. Rizik se ne može izbjeći, već se njime treba upravljati. Većina organizacija ne daje dovoljno pažnje prema sigurnosti i zaštiti podataka, što dovodi do neadekvatnog upravljanja podacima, gdje se često provodi nepravilna zaštita što čini neke podatke nedovoljno zaštićenima (Galligan i Rau, 2015). Prema Institutu internih revizora zaštita se provodi kroz tri linije, u kojoj prvu liniju čine uprava i ostala upravljačka tijela koja imaju odgovornost prema dioničarima za sigurnost i opstanak poduzeća, kreira strukturu upravljanja i uređuje procese, te određuje razine rizika u kojima će poduzeće poslovati. Druga su menadžeri zaduženi za provođenje odluka uprave, stvaranje i održavanje procedura za upravljanje rizicima, analiziranje i praćenje učinkovitosti sustava u cijelosti kao i internih kontrola. Interni revizori predstavljaju treću liniju kao neovisno tijelo koje komunicira s upravom i menadžmentom o funkcionalnosti sustava interne kontrole, služi kao podrška pri upravljanju s rizicima i provodi zaštitne mjere (The Institute of Internal Auditors, 2020). Grafički prikaz 3 linije obrane prikazan je u slici 2.

*Slika 2. Institut internih revizora: model 3 linije*




Izvor: Institut internih revizora (IIA), (2020), IIA MODEL TRI LINIJE: Ažuriranje modela Tri linije obrane, str. 4, Dostupno na: www.theiia.org

Interni revizori pomažu upravljačkim tijelima u procjenjivanju postignutih ciljeva baziranih na etici, politikama i vrijednostima organizacije. Također, naglašava važnost komunikacije u područjima rizika i kontrola prema svim dionicima procesa, uključujući menadžment internu i eksternu reviziju. U aktivnostima s menadžmentom za upravljanje rizicima sudjeluje u identifikaciji i izloženost riziku, služi kao podrška u uspostavljanju procesa otkrivanja prijevare.

Dužnosti internih revizora u sustavu kontrola odnose se na evaluaciju procesa i operacija, kao i savjetodavnih usluga čime pružaju osiguravajuću ulogu cjelokupnom procesu. Neovisno uvjerenje glavna je značajka interne revizije kao treće linije, u kojoj su odgovornosti usmjerene prema savjetovanju menadžmenta i upravljačkih tijela o pitanjima koja su vezana za postizanje ciljeva. Objektivnost i neovisnost interne revizije prema organizaciji su temelj pravilnog funkcioniranja, stoga revizori služe upravnim tijelima, te izvještavaju prema najvišoj poziciji u organizaciji, neovisni o drugim menadžerskim funkcijama (Pinto et. Al 2013).

Pregledom financijskih i poslovnih informacija koriste sredstva koja služe za identifikaciju, klasifikaciju i mjerenje tih informacija. U pogledu nefinancijskih informacija interni revizori mogu biti zaduženi za

ocjenjivanje ekonomičnosti, funkcionalnosti i učinkovitosti operativnih procesa, uključujući i usklađenost sa zakonima i propisima (Saleem et al. 2019).

### 3.2. Proces interne revizije kibernetičke sigurnosti

Provođenje interne revizije razlikuje se ovisno o kompetencijama revizora, kao i okruženju u kojem se organizacija nalazi. Čimbenici kao što su financije, poslovni model, tehnologija i percepcija o riziku određuju okruženje, dok iskustvo, vještine, motivacija i osobnost čine temeljne kompetencije revizora (Venugopal et al. 2024a). Prema Drogalas et al. (2015) ključni faktori koji utječu na provedbu revizije su: kvaliteta interne revizije, kompetencija revizora, podrška menadžmenta i neovisnost.

Selekcija obuhvaća plan, odabir ciklusa i premet u kojem će se revizija obavljati. Podrazumijeva identifikaciju i evaluaciju rizika na područjima kao što su financijska izvješća, interne kontrole, usklađenost s politikama i standardima, te organizacijske strukture (Obeid i Al-zeaud, 2012). U primjeru kibernetičke sigurnosti interna revizija se može fokusirati na identificiranje ključnih područja rizika, usklađenost sa standardima, politikama i procedurama, autentifikaciju i autorizaciju, sustave za odgovore na rizike, zaštitu mrežne infrastrukture, sigurnost podataka i kontrola pristupa (Kohnke et al. 2016).

Slapničar et al. (2022) opisuje faze revizije kroz tri koraka; planiranje, provođenje i izvještavanje u omjeru 40:40:20. Planiranje se zasniva na proaktivnošću u razumijevanju kibernetičkog okruženja; izlaganju organizacije u okolini, gledanju prema naprijed u trenutnim i nadolazećim prijetnjama, promjenama u regulacijama i trendovima u industriji. Provođenje procjene rizika dio je planiranja, a da bi se dobio utjecaj rizika i učinak na organizaciju bitno je identificirati najvrjednije informacije zbog kojih bi organizacija pretrpjela visoke gubitke u slučaju provale. Visinu gubitka nije jednostavno procijeniti, osobito u situacijama gdje informacije nemaju nominalu vrijednost, već bi se njihovom zlouporabom narušio reputacijski ugled, prekid u operativnim zadacima ili novi sudski sporovi. Provođenje podrazumijeva opseg prikupljanja dokaza i razinu detalja pronalazaka. U ciklusu provođenja revizije podaci se prikupljaju sistematski u četiri domene: ranjivost, prijetnje, upravljanje incidentima i krizama. U provođenju revizori se koriste alatima koji utječu na učinkovitost procesa, a to mogu biti: alati za šifriranje, alati mrežne ranjivosti, antivirusni programi i mnogi drugi. Treći korak je izvještavanje nalaza prema revizijskom odboru i upravi. Isključivo sveobuhvatnim izvještavanjem može se otkriti materijalne slabosti kontrola i izbjeći pružanje lažnog osjećaja sigurnosti.

Planiranje interne revizije u kibernetičkoj sigurnosti zahtjeva razumijevanje kibernetičke okoline, a to znači iskustva i znanja o industriji u kojoj se organizacija nalazi, ispitivanje slabih točki sustava gdje je izražena izloženost rizicima, sposobnost predviđanja budućih prijetnji, upućenost u regulacije i nadolazeće trendove u industriji. Od revizora se očekuje proaktivno razmišljanje da bi se incidenti mogli spriječiti prije nego se pojave (Kahyaoglu i Çaliyurt, 2018a). Procjena okruženja u kibernetičkom prostoru izvodi se dubljom analizom administrativnih i tehničkih kontrola, odnosno vrednovanjem protokola šifriranja podataka u prenošenju i spremanju, posebno najosjetljivijih informacija. U planiranje spada i provjera implementacije sustava provjere autentičnosti s više značajki (eng. *multi-factor authentication*, MFA) u svrhu smanjenja rizika od neovlaštenih upada, kao i ispitivanje osjetljivosti kritičnih točki sustava preko neadekvatnih zaporki (Blasquino, 2024). Ključna komponenta planiranja je procjena rizika. Procjena sadrži tri koraka; utjecaj rizika i razina štete koju može prouzročiti, vjerojatnost događaja za svaki rizik i ranjivost sustava kroz provjeru postojećih mjera za zaštitu sigurnosti informacija (Russo et al. 2019). Pravilo funkcioniranje sustava za upravljanje rizicima zahtjeva kontinuirano praćenje kontrolnih područja, što omogućava prepoznavanje osjetljivih područja na vrijeme. Samoprocjena kontrola (eng. *Control self-assessment*, CSA) je alat kojim se služe revizori u svrhu uključivanja ostalih dionika u organizaciji. CSA pomaže zaposlenicima prepoznati i nadzirati kritična područja koja su esencijalna za optimalno funkcioniranje sustava, motivira ih za kontinuirano unaprjeđenje, te pomaže pri shvaćanju problematike i važnosti kontrola u cjelokupnom sustavu (Terry i Gilbert 2001). U izradi plana samoprocjene kontrola (CSA) funkcija interne kontrole oslanja na se okvire i standarde za interne kontrole (Kahyaoglu i Çaliyurt, 2018b). Okviri koji se najčešće koriste u praksi su Kontrolni ciljevi za informacijske i srode tehnologije (eng. *Control Objectives for Information and Related Technologies,* COBIT 2019) koji je razvijen od ISACA-e, standardi za kibernetičku sigurnost od Međunarodne organizacije za standardizaciju (ISO:27001, 2022) i NIST (2018) standardi od Nacionalnog instituta za standarde i tehnologiju u Sjedinjenim Američkim državama.

Prema međunarodnom standardu ISO 27005 (2022a) informacijska sigurnost, kibernetička zaštita i zaštita privatnosti procjenjivanje rizika dijeli se na 3 faze:

- Identifikacija rizika
- Procjena rizika
- Evaluacija rizika

Identifikacija rizika sastoji se od predviđanja događaja, uzroke nastanka rizika, te iznos za koji bi oštetio organizaciju. Elementi identifikacije su: imovina, prijetnje i ranjivosti, utjecaj i postojeće kontrole. Aktivnosti koje obuhvaćaju proces identifikacije su: identifikacija imovine koja obuhvaća informacije, zaposlenika i procese, identifikacija postojećih kontrola, identifikacija slabosti i nedostatka, identifikacija prijetnji iz vanjske i unutarnje okoline i identifikacija posljedica (ISO 27005:2022b).

Procjena rizika predstavlja metodologiju s kojom se pristupa, obuhvaća kvalitativne i kvantitativne metode, tehnike, alate koje su najpovoljnije za svaki rizik. Elementi analize su: vjerojatnost, utjecaj i procjena posljedica. Aktivnosti vezane za analizu započinju procjenom posljedica, odnosno utjecajem mogućih ili sadašnjih incidenata u području informacijskih sustava, te traženjem izvora problema koji se očituje u kršenju protokola sigurnosti, ljudskim greškama i propustima u zaštiti imovine. Sljedeća je aktivnost procjena vjerojatnosti nastanka incidenta koja se provodi na postojećim kontrolama i zaštiti. Zadnja aktivnost postavlja razinu rizika za svaku situaciju do koje se došlo prethodnim analizama.

Evaluacija rizika uključuje uspoređivanje postavljenih tolerancija rizika s rizicima koji su dobiveni analizom. Nakon što revizor napravi usporedbu postavlja prioritete rizika koji najviše odstupaju od zadane tolerancije (ISO 27005:2022c).

Nakon što se odredi ciljano područje, prikupe informacije i ustanovi način funkcioniranja internih kontrola, interni revizori započinju s fazom provođenja interne revizije, odnosno prikupljanjem dokaza. Prema istraživanju Shamki i Alhajri (2017) postoji značajna korelacija između učinkovitosti i opsega interne revizije u uzorku sa zaposlenicima, dok je povezanost interne revizije neznačajna s uzorkom s menadžerima, stoga je u provođenju revizije ključno motivirati zaposlenike da se u svom radu oslanjaju na kompetencije i iskustva revizora. U pogledu na kibernetičku sigurnost revizija vrši nadzor na jedan ili više područja sigurnosti, a to mogu biti; programska sigurnost i zaštita, sigurnost Clouda, zaštita podataka, dopuštenja prema trećim stranama, kibernetička forenzika i upravljanje ranjivim područjima (Sabilon 2021). Dokazi se prikupljaju ispitivanjem, prikupljanjem, analitičkim postupcima, promatranjem i inspekcijom (ISA 500). Prikupljanjem dokaza želi se naznačiti pravilno funkcioniranje operativnih procesa ili automatiziranih sustava. Također, cilj je prikazati izloženost i mogućnosti ostvarivanja kibernetičkih napada, kao i razumijevanje organizacije na potencijalne napade, planirane korake u vraćanju sustava u optimalno stanje i prihvatljivu razinu rizika. Forenzičkim postupcima revizija dobiva sliku o načinu izrade izvješća o napadima, trenutnoj situaciji i razumijevanje prijetnji iz unutarnje i vanjske okoline (Almatari et al. 2018). Učinkovitost interne revizije u kibernetičkoj sigurnosti također ovisi i o alatima koje organizacija

koristi za zaštitu i prevenciju kao što su; antivirusni programi, upravljanje vatrozidnom zaštitom, skenerski alati za zaštitu mrežnih stranica i alati za šifriranje podataka (Pfleeger et al. 2014).

Izvještavanje dobivenih rezultata interni revizori čine prema upravnom odboru i revizijskom odboru. Da bi izvještavanje bilo učinkovito, komunikacija treba bit; sažeta, jasna, točna, potpuna, te pravovremena. Izvještaj mora sadržavati ciljeve revizije, djelokrug, zaključke i preporuke, i također, revizor mora izraditi plan provedbe (Venugopal et al. 2024b). Komunikacija prema upravi i revizijskom odboru o nalazima interne revizije kibernetičke sigurnosti predstavlja dodatan izazov zbog terminologije koje je povezana s informacijskim tehnologijama. Direktori za sigurnost informacijskih sustava služe kao podrška ostaku odbora za utvrđivanje kompleksnih pojmova, a odgovornost revizijskih odbora je pratiti nadolazeće trendove u kibernetici, poznavati regulacije i zakone za zaštitu podataka i ključne prijetnje i rizike koje okružuju organizaciju i industriju u cjelini (Goedeker 2014).

Nadzor nad uspostavljenim kontrolama provodi se nakon procesa interne revizije, te se on mora obavljati kontinuirano i periodično. Tehnologija omogućava automatizaciju sustava, što čini nadzor sigurnijim u pogledu pravovremenog reagiranja i ispravnosti potrebnih informacija za zaštitu sustava. Prednosti koje se postižu tehnologijom povećaju učinkovitost i snižavaju operativne troškove, također zaposlenici neće biti skloni prevarama u sustavu koji pravilno funkcionira. Svaki nadzor sastoji se od četiri koraka; prioritiziranje rizika, identifikacija kontrola, identifikacija informacija i uspostavljanje nadzora (ISACA 2010).

# 4. EKSTERNA REVIZIJA: KIBERNETIČKA SIGURNOST

## 4.1. Uloga eksterne revizije u korporativnom upravljanju

U korporativnom upravljanju menadžment je zadužen za sastavljanje godišnjih financijskih izvještaja u skladu su poslovnim rezultatima i financijskog stanja organizacije. Izvješća koja se izrađuju za potrebe dioničarima i ostalim dionicima (regulatori, kreditori, investitori) nemaju potpunu vjerodostojnost s obzirom na mogućnost manipulacije podacima koja se nalaze u godišnjim financijskim izvještajima. Stoga je uloga eksternog revizora kao tijelo neovisno o menadžmentu ustvrditi vjerodostojnost s pomoću nalaza i dokaza te ih prezentirati dioničarima na glavnoj skupštini (Alabede 2012). Razlika između informacija kojim raspolažu vlasnici i onima koje ima uprava stvara asimetriju informacija koja potiče oportunitetno ponašanje upravljačkih tijela (Jensen i Meckling 1976). Kvaliteta revizije ne ovisi samo o radu revizora, već se oslanja na uspostavljeni sustav internih kontrola i odgovornosti upravnih tijela prema kibernetičkoj sigurnosti. Učinkovita uprava donosi višu razinu zaštite podataka, osigurava bolje korištenje resursa od menadžera i zapošljava kvalitetnije revizore što dovodi do efikasnijeg upravljanja usmjerenog prema interesima vlasnika (Almasria 2021). Dužnosti revizora usmjerene su prema vjerodostojnosti financijskih izvještaja, stoga je fokus na informacije u informacijskom sustavu prema stavkama koje potencijalno narušavaju fer prikaz financijskih izvještaja. Revizori ne formuliraju mišljenje prema ukupnom kibernetičkom riziku organizacije već isključivo onim djelom koji je utječe na pripremu izvještaja. Procjena rizika zahtijeva zapažanje vanjske i unutarnje okoline, što podrazumijeva strukturu informacijskog sektora kao i podsustave koji se mogu povezati s procesom izrade financijskih izvješća (Hann 2019).

DeAngelo (1981) definira kvalitetu revizije kao tržišno razvijena pretpostavka da će revizor prepoznati i otkriti, te istaknuti pogrešno prikazivanje ili materijalnu štetu i prijaviti nadležnim tijelima potpune informacije. Od revizora se očekuje sposobnost i stručnost, i naglašava nužnost moralnih i etičkih načela. Na kvalitetu revizije utječu politike i procedure s pomoću kojih revizor osigurava svoju poziciju u skladu s očekivanjima povezanih stranka da se revizija izvodi prema propisanim standardima. Čimbenici koji utječu na kvalitetu revizije su: Objektivnost i neovisnost, upravljanje zaposlenicima, odnos prema klijentima, revizija nad revizijskim odjelima, nadzor i savjetovanje (Salih i Flayyih 2020).

Neovisnost i integritet revizora važna je za poslovanje organizacije kao mjera osiguranja vjerodostojnog prikazivanja financijskih izvještaja i ispunjenja obveza prema dioničarima, a s time i informiranjem investitora i ostalih interesnih skupina organizacije. Revizori moraju provoditi procese nepristrano i neovisno ni od jednoj strani prikazujući objektivno informacije i nalaze u svom opsegu (Delaney 2006).

Upravljanje zaposlenicima obuhvaća strukturirani proces s politikama i procedurama usmjereni prema uspostavljanju odgovarajućih kvalifikacija prema svakom revizoru s ciljem alokacije zaposlenih na mjesta prema njihovim tehničkim vještinama i iskustvu. Također pomaže u trenažnom procesu za svakog revizora individualno osiguravajući pravilnu edukaciju i iskustva za izvršenje revizorskog rada (Aguolu et al, 2018).

Odnos prema klijentima gradi se unutar revizorske kuće i služi kao temelj opstanka organizacije u budućnosti. Revizori moraju raditi u skladu s politikama i procedurama koje vode prema dobrim odnosima prema dionicima koji ih koriste za usluge. Klijentima se pruža jamstvo za kvalitetu revizije, te nastavak dobrih odnosa integritetom i profesionalnom etikom (Svanberg i Ohman 2019).

### 4.2. Procjena rizika kibernetičke sigurnosti od eksterne revizije

Identifikacija i upravljanje rizicima u kibernetičkoj sigurnosti zahtjevan je proces zbog kontinuiranih promjena koje se događaju u informacijskim tehnologijama. Kibernetički sustavi mijenjaju se ovisno o uvođenju novih tehnologija, promjena u upravljanju s informacijama i kompleksnosti mrežnih struktura (Ganin et al. 2017). Procjena rizika razlikuje se ovisno o opsegu, pa se tako prema modelu revizije kibernetičke sigurnosti (eng. *Cybersecurity Audit Model,* CASM) može bazirati na isključivo na jednu domenu, na odabrane domene ili na cjelokupni sustav (Sabilon 2022). Iako se modeli mogu razlikovati, može se reći kako su četiri zajedničke aktivnosti: identifikacija imovine, identifikacija i vrednovanje prijetnji, identifikacija i vrednovanje osjetljivih područja i menadžment rizika (Sanchez-Garcia et al. 2023).

Poznavanje okruženja organizacije prvi je korak u upravljanju rizicima. Međunarodni odbor za standarde revidiranja MRevS 315 (2019) dijeli okruženje na vanjsku okolinu, interne kontrole i usklađenost s okvirima financijskog izvještavanja. U procedurama procjene rizika revizor treba steći razumijevanje organizacijske strukture, strukture vlasništva, te poslovni model i u kolikom opsegu organizacija koristi informacijske tehnologije u redovnom radu. U pregledu okruženja također spada industrija, regulatorna tijela i drugi vanjski čimbenici. U vidu financijskog izvještavanja, potrebno je razumjeti računovodstvene politike koje se koriste, kao i razloge promjene računovodstvenih politika u slučaju da su se mijenjale. U nadzoru internih kontrola revizor stječe razumijevanje kontrola, procedura i strukture tako da provjerava kako menadžment ispunjava svoje obveze nadzora, neovisnost onih koji upravljaju ako su odvojeni, alokaciju odgovornosti organizacije, te kako postupa s odgovornostima pojedinaca za zadane obveze u internim kontrolama. Revizor također radi procjene u sustavu uvidom u kulturu, etičnost i odnose prema organizaciji i kontrolama, služi li kontrolno okruženje kao podrška ostalim sustavima interne kontrole

uzimajući u obzir kompleksnost i tip organizacije, te kako identificirani nedostaci utječu na ostatak strukture internih kontrola (MRevS 315, 2019a).

Revizori moraju identificirati i procijeniti rizike koji će stvoriti značajne materijalne pogreške u financijskim izvještajima uzrokovane pogreškama ili prijevarama. Organizacije u kojima kibernetički incidenti stvaraju velike gubitke i utječu na financijsko izvještavanje trebaju imati adekvatno vodstvo i nadzor koji će biti sposobno razumjeti rizike povezane s kibernetičkom sigurnošću i predvidjeti potencijalne događaje koje će stvoriti značajne štete. Posljedice kibernetičkog napada mogu biti otvaranje rezerviranja i potencijalnih obveza što stvara troškove u vidu plaćanja kazni, nadoknade šteta ili obveze u sudskim procesima. Zatim promjena fer vrijednosti imovine kao rezultat kibernetičkog napada u određenoj industriji ugrožava transakcije s poduzećima u toj industriji, pad vrijednosti imovine zbog smanjenja operativnih novčanih tokova zbog prekida poslovanja uzrokovanog kibernetičkim napadom i smanjenje sposobnosti organizacije s neograničenim poslovanjem (Jurišić i Čular 2022).

Dodatak 5 MRevS-a 315 (2019b) donosi smjernice u razumijevanju subjektovog korištenja informacijskih tehnologija u komponentama sustava interne kontrole. Korištenje informacijskih tehnologija ima utjecaj na koji način se komuniciraju, koriste i pohranjuju podaci koji su potrebni za sastavljanje financijskih izvještaja. Interne kontrole sadržavanju ručne i automatizirane komponente, te kombinacija između njih razlikuje se ovisno o prirodi i kompleksnosti informacijskih tehnologija koje organizacija koristi. Automatizirane kontrole obično su pouzdanije od ručnih jer ih je teže preskočiti ili zaobići, te su manje podložne propustima i pogreškama. Eksterni revizori u svrhu stjecanja razumijevanja IT okruženja prikupljaju informacije o karakteristikama aplikacija i prirodi korištenja IT strukture u obradi podataka i transakcija. U kontekstu identifikacije rizika povezanim s uporabom informacijskih tehnologija unutar internih kontrola i općih IT kontrola dodatak 5 navodi područja u kojima postoji povećani rizik. Neovlašteni pristup može dovesti do pogrešnih informacija, evidentiranja nepostojećih transakcija, krađe ili uništavanja podataka, posebno gdje više osoba ima pristup istoj bazi podataka. Nedovoljno zaštićen pristup podacima omogućuje IT zaposlenicima neovlašteno korištenje privilegiranih informacija. Nadalje, korištenje zastarjele tehnologije koje se ne više održavaju na potrebnoj razini laka su meta hakerima koji bez poteškoća ulaze u sustav. Industrija u kojoj se organizacija nalazi također može imati povećan rizik, posebno ako se radi o specifičnoj industriji gdje postoji veći inherentni rizik zbog vrste posla i povijesnih događaja kao što je bio slučaj sa zdravstvenom sektorom za vrijeme pandemije koronavirusa (Jurišić i Čular 2022).

Kada se utvrdi rizik koji značajno dovodi do pogrešnog prikazivanja stavki u financijskim izvještajima, revizorima se savjetuje korištenje smjernica MRevS 315 (2019) standarda, odnosno korištenje usluga od zaposlenika koji imaju više iskustva i znanja u predstavljenom problemu. U tom slučaju uključuju se stručnjaci iz područja informacijskih tehnologija koji će svojim vještinama uključiti dodatne elemente u analizu, smanjiti nepredvidivost u revizijskim postupcima i modificirati postupke u svrhu vjerodostojnih podataka s više potkrepljujućih revizijskih dokaza (ISCA 2020).

# 5. REVIZIJSKI ODBOR: KIBERNETIČKA SIGURNOST

## 5.1. Uloga revizijskog odbora u korporativnom upravljanju

Revizijski odbori su ključna komponenta u korporativnom upravljanju za nadzor, praćenje revizijskih procesa i podrška internoj i eksternoj reviziji u odabiru revizora, te podizanju kvalitete financijskog izvještavanja. Jun Lin et al. (2008) navodi percepciju revizijskih odbora kao simboličnu ulogu korporativnih tijela zaduženu za stvaranje bolje slike o organizaciji, unaprjeđivanje komunikacije između revizora i uprave, te rješavanje konflikata između menadžmenta i revizije. Suprotno percepciji uloga revizijskih odbora je puno dublja, dužnosti koje se odnose na odbore uključuju poboljšanje interne revizije, usklađenosti sa standardima i politikama, praćenje izrade financijskih izvještaja i praćenje procesa revizije. Razuman omjer neovisnih članova koji nisu dio izvršnih direktora bitno je zbog vjerodostojnosti i neovisnosti članova, što umanjuje vremenski rok revizijskog izvještavanja. Neovisnost također utječe oportunističko ponašanje i mogućnost prijevare čime se štiti interes dioničara i osigurava pravilno i pravovremeno objavljivanje financijskih izvješća (Soyemi et al. 2019).

Prema istraživanju Almasria (2022a) revizijski odbori igraju vitalnu ulogu nadziranja sveukupnog sustava upravljanja. Također, komunikacija s eksternom revizijom čini glavni element revizijskog odbora u mehanizmima upravljanja što uključuje izdavanje pojašnjenja i potvrda, vrednovanje učinkovitosti eksterne revizije, pripremu zahtjeva provođenja revizije, održavanje redovnih sastanaka i poduzimanja potrebnih radnji. Kontinuirano praćenje procesa revizije osigurava neovisnost revizora, rješava postojeće i sprječava događanje potencijalnih konflikata između dionika revizije i korporativnog upravljanja u cjelini. Eksterni revizori u istraživanju navode kako uključenost revizijskog odbora u određivanju zahtjeva revizije značajno utječu u kvalitetu svih procesa revizije.

## 5.2. Revizijski odbor i kibernetička sigurnost

Uspješno nadziranje programa kibernetičke zaštite zahtjeva kontinuiran i sveobuhvatan angažman revizijskog odbora i uprave s proaktivnim razmišljanjem. Revizijski odbor ima stratešku ulogu u koordiniranju planova, procesa i inicijativa u kibernetičkoj obrani, te vrednovanje učinkovitosti istih. Efektivnost se postiže upravljanjem resursa, postavljanjem očekivanja, fokusiranje na ranjive sustave i raspodjela odgovornosti prema menadžmentu (Deloitte 2017a). Dužnosti i raspon obveza koji revizijski odbor ima razlikuje se ovisno o organizacijskoj strukturi i industriji u kojem se nalazi, određene

organizacije upravljaju rizicima kroz zasebne odbore, dok drugi odgovornost zadržavaju u upravama. Bez obzira na koji način organizacije funkcioniranju rastući trend kibernetičkih provala i incidenata zahtijevaju od članova revizijskih odbora kontinuirano praćenje zakona, standarda, regulacija i edukaciju na području informacijskih tehnologija koji su postali obveza svih zaposlenih u organizaciji (Čular 2023).

Da bi članovi revizijskih odbora stekli uvide u funkcioniranju sustava za upravljanje kibernetičkim rizicima, u komunikaciji s menadžmentom i revizorima moraju postaviti pitanja koja se fokusiranju u dva glavna smjera: vrsta podataka koja izlaze iz organizacije i sustava nadzora, te postoji li plan u slučaju kibernetičkog napada i je li taj plan pravovremeno ažuriran (Ilollari i Islami 2017). Deloitte (2017b) donosi set pitanja koji članovi moraju postaviti za razumijevanje internih kontrola organizacije:

- Koja je opća strategija i plan za zaštitu imovine?
- Koliko su snažni komunikacijski planovi i odgovori na incidente u organizaciji?
- Koji su kritični podaci i s njima povezani rizici koje treba zaštititi?
- Na koji način se identificiraju slabosti organizacije?
- Kako se otkrivaju rizici?
- Kako se usklađuje kritična infrastruktura s regulatornim zahtjevima?
- Koje kontrole se koriste za zaštitu Clouda, opskrbnih mreža i softvera na uređajima organizacije?
- Koje digitalne informacije izlaze iz organizacije, gdje odlaze i na koji način se prate?
- Ima li organizacija adekvatno educirane zaposlenike koji mogu predvidjeti kibernetičke rizike?
- Je li se u organizaciji poznaje tko ima pristup mreži i jesu li informacije primjerene za svaku poziciju?

# 6. EMPIRIJSKO ISTRAŽIVANJE

## 6.1. Metodologija

Za potrebe rada korišten je standardizirani intervju (Zelenika 2000b). Sudionici su odabrani na temelju znanja, iskustva i radnog mjesta (Teddlie i Tashakkori 2003). Cilj intervjuiranja je produbljivanje znanja o problematici, međusobnim odnosima u ostvarivanju ciljeva i razvijanja područja za buduće izazove. Izabrane su tri anonimne osobe od kojih je svaka zaposlena na jednom području iz tematike, odnosno prva osoba radi kao interni revizor, druga osoba kao eksterni revizor i treća kao član revizijskog odbora. Sastavljen je set od pet pitanja za svakog ispitanika zasebno. Pitanja daju odgovore na uloge njihovih profesija u kibernetičkoj sigurnosti, opis rada, međusobna suradnja, te savjeti i osobna predodžba o tematici u kojoj su ispitani.

Kvalitativnim istraživanjem želi se doći do saznanja o funkcioniranju interne revizije i sustavu internih kontrola u segmentu kibernetičke sigurnosti, odnosima internog revizora s ostalim dionicima u organizaciji i poboljšanjima u radu interne revizije s ciljem jačanja kibernetičke obrane i predviđanja budućih rizika povezanim s informacijskim tehnologijama. Nadalje, za cilj je razumjeti poziciju eksternog revizora u vrednovanju rizika, na koji način funkcionira komunikacija s internim revizorima i određivanju područja kibernetičke sigurnosti koja značajno utječe na vjerodostojnost financijskih izvješća. Istraživanje se također odnosi i na funkcioniranje revizijskog odbora u segmentu kibernetičke sigurnosti, točnije kako kibernetička sigurnost utječe na odabir eksternog revizora, koje ekspertize članovi odbora imaju u informacijskim tehnologijama, kako postupaju članovi pri kibernetičkim incidentima i izvještavanje o kibernetičkoj sigurnosti prema upravi.

Prvi intervju je proveden s internim revizorom (IR) 7. lipnja 2024. godine. Drugi intervju je napravljen s eksternim revizorom (ER) 10. lipnja 2024. godine, te treći intervju s članom revizijskog odbora (RO) 11. lipnja 2024. godine. Svi razgovori su snimljeni i transkribirani uz dopuštenje sudionika koji će ostati anonimni.

## 6.2. Interpretacija empirijskog istraživanja

Analizom podataka intervju su podijeljeni u četiri teme. Prva tema odnosi se na ulogu interne revizije općenito i u smislu kibernetičke sigurnosti. Druga tema je uloga eksterne revizije i njen značaj u

kibernetičkoj sigurnosti. Treća tema bavi se ulogom revizijskih odbora, dok četvrta tema obrađuje suradnju između prethodnih tijela kao i njihovu percepciju o ulogama u kibernetičkoj sigurnosti.

Prva tema- uloga interne revizije: općenito gledajući profesiju revizije može se reći kako je orijentirana na rizike, to uključuje sveobuhvatno upravljanje od procjene, identifikacije, simuliranja nastanka događaja do smanjenja vjerojatnosti incidenta. Rizici se ne smiju eliminirati, vjerojatnost može biti niska ali nikada ne može biti nula. Sustavi internih kontrola su glavno područje u kojima se upravlja s rizicima, a revizor sve poteze usmjerne u kontrolama izvodi zajedno s menadžmentom. O ulogama interne revizije, rizicima i komponentama internih kontrola interni revizor je rekao sljedeće:

IR: *„U kibernetičkoj sigurnosti temeljne odgovornosti su slične kao i s drugim procesima, sve kreće od procjene rizika (eng. risk assessment), zatim ovisno o angažmanu koji je dogovoren s menadžmentom provodi se revizija. Kibernetička sigurnosti ima više komponenti, odnosno kontrola vezane za kibernetičku sigurnost. Interna revizija se uvijek fokusira na interne kontrole koje smanjuju te rizike koji su vezani za određeno područje. Po pitanju kibernetičke sigurnosti postoje razne vrste kontrola, neke su kontrole pristupa (eng. access control), može se gledati hardver, može se gledati je li su licence na mjestu, je li su ažurirani softveri koji se koriste „most up to date“ kao naprimjer antivirusni antimalware softveri, da su zaštićene mreže, zatim firewall koji ograničava promet podataka, odnosno da eksterni korisnici ne upadaju u internu mrežu firme ili organizacije tako da se sve te stvari mogu gledat.“*

Odgovornosti internog revizora u planiranju i nadzoru internih kontrola, izdavanju neovisnog mišljenja, provjere kvalitete jednako se odnose i u dijelu kibernetičke sigurnosti. Razina odgovornosti ovisi o razvijenosti informacijskog sektora u organizaciji, aktivnosti u IT odjelima određuju intenzitet provjera, upravljanja i nadzora nad subjektom, pa tako i utječu na angažman interne revizije. Interni revizor navodi sljedeće:

IR: *„Ovisno o razvijenosti same kibernetičke sigurnosti u određenoj organizaciji tako se sukladno tome mijenjaju odgovornosti revizora. Odgovornost internog revizora je da odradi angažman u dogovoru naravno s menadžmentom, a angažmani su uvijek usmjereni na gledanje internih kontrola za davanje neovisnog mišljenja je li su one dizajnirane adekvatno, te je li one dizajnirane funkcioniraju kako treba, odnosno postoje li manjkavosti.“*

Nastavno na prethodni citat odnosi unutar organizacije i suradnja s informacijskim sektorom ključna je za provedbu kvalitetne i učinkovite interne revizije. Percepcija o funkciji interne revizije često zna biti

negativna jer sama bit revizora u organizaciji je poboljšati rad drugih zaposlenih što obično zahtijeva kritiku, savjetovanje i promjenu rada, a to će mnogo osoba teško prihvatiti i sagledati situaciju u negativnom kontekstu. Od revizora se očekuju razvijene socijalne vještine i sposobnost rješavanja konflikata, kao i izgradnja povjerenja, odnosno odnosa gdje će se na revizora gledati kao osobu koja pomaže, a ne osobu koja stvara dodatan posao. Održavanje redovnih sastanaka i razumijevanje materije kibernetičke sigurnosti služe kao čvrst temelj u povjerenju, što sugovornik i sam navodi:

IR: *„Najbitnije je imati čestu komunikaciju, i generalno u svakoj organizaciji ljudi su zaposleni, te je teško uspostaviti otvorenu komunikaciju pogotovo kad se radi o internoj reviziji. Ne gledaju sve službe internu reviziju kao partnera, neko tko im može pomoći, već su percipirani kao policajci, netko tko im smeta, odnosno potencijalno može nametnuti dodatno posla za koji oni smatraju da nije bitan. Zbog toga je bitno uspostaviti dobru komunikaciju. Kada se komunikacija i partnerski odnos uspostavi, tad se održavaju regularni sastanci, obično na kvartalnoj bazi gdje se napravi procjena rizika, listiraju se određeni rizici, zatim se prodiskutira ima li novih rizika, te se kroz komunikaciju vidi može li interna revizija pomoći u angažmanu bilo to u okviru revizije ili neki savjetodavni, ne mora nužno biti kroz reviziju. Kroz regularnu interakciju koja se odvija na kvartalnoj bazi, s menadžmentom se komentiraju rizici kada se procjena napravi, je li su rizici relevantni, je li su oni veći ili manji.“*

U procesu procjene rizika koriste se razni programi i softveri koji omogućuju planiranje, nadzor, identifikaciju i analiziranje podataka u svrhu ispunjavanja zadatka. Sofisticiranost i kvaliteta programa uvjetovana je troškom, stoga organizacije koje posluju u djelatnostima i industrijama koje ne koriste osjetljive i privatne informacije programi nisu od koristi, odnosno stvaraju veći trošak od koristi. Obično u takvim organizacijama okvire za upravljanje rizicima izrađuju sami revizori i nadopunjavaju sadržaj ovisno o vlastitim potrebama i zahtjevima na tržištu i regulacijama. Programi koji se koriste u kibernetičkoj sigurnosti odnose se na penetracijske testove, zaštitu i praćenje podataka s Clouda, aplikacije za otkrivanje slabosti sustava, alati za nadzor mreže i drugi. Na primjeru iskustva sugovornika-internog revizora navodi programe s kojim se on susreće:

IR*: „Što se tiče alata ništa sofisticirano, obično se u Excelu napravi neka forma „risk-assessmenta“ ili registar rizika, za sve to se koristi uglavnom excel. Postoje softveri kao naprimjer „audit board“, nekakvi IT softveri i aplikacije u kojima se može radit procjena rizika međutim to s jedne košta s druge strane nema neki veliki benefit u odnosu na excel konkretno za procjenu rizika.“*

Osim upravljanja rizicima interni revizori mogu biti zaduženi za procjene učinkovitosti sustava kibernetičke obrane, te usklađenosti s politikama i procedurama organizacije, kao i regulatornim

okvirima. Poduzeća ne moraju koristiti usluge iz unutarnjeg izvora, već se taj segment može i obavljati preko stručnjaka izvan organizacije kao izdvajanje posla (eng. *outsourcing*). U primjeru organizacije sugovornika zaposlenici unutar organizacije nemaju potrebna znanja i vještine za obavljanje zadatka, te se procijenilo kako se radi o niskorizičnom procesu, stoga se navodi sljedeće:

IR: *„U mojoj organizaciji je taj segment eksternaliziran, to ne radi nitko unutar organizacije već postoji specijalizirana tvrtka koja se bavi s time jer su to znanja vještine i ekspertiza koju mi ne posjedujemo u našoj organizaciji, Shodno tome mi ne provjeravamo jer smo procijenili kao niskorizični proces. Provjerili smo jeli ta firma dovoljno stručna, ima li reference i znanja te smo bili zadovoljni s referencama i stručnosti koje ta organizacija ima.“*

Uspješnost rada interne revizije provodi se unutar organizacije i proveden je od strane internih revizora zajedno s menadžmentom. Pitanje o uspješnosti odnosi se na opće procedure i segment vezan uz kibernetičku sigurnost zbog toga što se segment ne može izolirati od cjelokupnog procesa. Uspješnost se provodi preko ključnih indeksa performansi- KPI (eng. Key performance index) koji uključuje postotak obavljenog revizijskog rada, postotak implementiranih preporuka, količina sati utrošena u reviziji, broj certifikata izdanih revizorima i mnogi drugi. Indikatori koji se odnose na kibernetičku sigurnost uključuju razine pripremljenosti, identifikacija pristupa mreže, broj incidenata i proboja, prosječno vrijeme otkrivanja i prosječno vrijeme rješavanja incidenta i drugi. U primjeru organizacije internog revizora navodi se sljedeće:

IR: *„Postoje indikatori performansi točnije KPI (eng. key performance indicator) koje smo razvili za funkciju interne revizije i neki od tih indikatora su naprimjer broj nalaza, odnosno ne toliko o broju koliko da li menadžment uspije implementirati i postotak implementacije nalaza interne revizije. Kada se bavimo segmentom kibernetičke sigurnosti najvažniji je period za otkriće proboja ili incidenta i period u kojem se ti incidenti riješe, a i treba obratiti pažnju na sve neautorizirane pristupe mreži koji najčešće i budu izvor problema. Također, najvažniji indikator je indikator revizije, svaka revizija napravi plan za period od godine ili dulji period, zatim se evaluira se jesu li su svi angažmani ispunjeni prema planu koji je zacrtan te u vremenskim rokovima koji su određeni.“*

Završni dio prve teme odnosi se na budućnost i izazove. Kao što je već naglašeno u radu, kibernetička sigurnost je u fazi razvoja i kontinuiranog unaprjeđenja, izloženost sustava i podataka i dalje je previsoka bez obzira na veličinu i tip organizacije. Broj kibernetičkih incidenata je gotovo u eksponencijalnom rastu, a organizacije nalaze razne načine da se bolje zaštite. Iako sustav može biti osiguran na svakom području dovoljan je trenutak nepažnje da se podaci kompromitiraju ili ukradu, nepažnja trećih strana također

ozbiljno ugrožava sustav na što je teško imati utjecaj. Interni revizori su pod velikim pritiskom jer je jako teško pratiti zbivanja i educirati se dovoljno kvalitetno i brzo, stoga je konstantan zaostatak za inovacijama kibernetičkih kriminalaca, kao što navodi sugovornik:

IR: *„Pa mislim da je to područje koje se rapidno razvija. Stvari se, mijenjaju tolikom brzinom da nekad ni poduzeća ni interne revizija ne mogu pratiti sve te nove razvoje i načine na koje se može provoditi kibernetički napad i samim time može se nanijeti šteta organizaciji, a da interna revizija nije bila spremna ili upozoriti na to menadžment ili je izvršila nekakvu reviziju gdje je rekla da je sve bilo u redu. Međutim, ipak su osobe koje vrše kibernetičke napade našli nekakve rupe i izvršili kibernetički napad, ukrali podatke ili bilo kakve posljedice koje se mogu reputacije tvrtke dogoditi, tako da je to da sumiramo znači sofisticiranosti i brz razvoj i kreativnost kibernetičkih napada. Rizik je da interna revizija i sama organizacija ili poduzeće neće moći pratiti i pratiti razvoje u sofisticiranosti kibernetičkih napada.“*

Druga tema- uloga eksterne revizije: zadatak eksternog revizora temeljen je na financijska izvješća, vjerodostojnost podataka, pravilnog prikazivanja i sprečavanja oportunističkog ponašanja upravljačkih tijela i menadžmenta. U pogledu kibernetičke sigurnosti revizori se osvrću na stavke koje potencijalno izazivaju značajnu materijalnu štetu koja narušava fer prikaz informacija u financijskim izvještajima. Eksterni revizori procjenu sustave internih kontrola, pružaju savjetodavne usluge prema internim revizorima, menadžmentu i upravljačkim tijelima, dok istovremeno i surađuju s istim. O odgovornostima eksterne revizije sugovornik navodi sljedeće:

ER*: „Glavna odgovornost je za sustav upravljanja internih kontrola, računovodstveno informacijski podaci ne smiju biti izmijenjeni, odnosno napadnuti od treće strane izvan povezanosti sa organizacijom. Stoga u procesu revizije bitno je identificirati ranjiva područja, prepoznati prijetnje i savjetovati na koji način unaprijediti sustav, kao i ublažiti posljedice od nastalih provala.“*

Za bolje razumijevanje funkcije eksterne revizije napravljena je usporedba s internom revizijom. Temeljne razlike u ovim funkcijama odnose se na vremenski opseg i razinu podataka koje obrađuju. Interna revizija kao dio organizacije, iako i ta funkcija može biti korištena od treće strane, ima pristup svim podacima i značajkama sustava što znači da puno detaljnije razrađuje sustav internih kontrola i bolje poznaje od eksterne revizije koja daje ocjenu na uspostavljene sustave podržane od interne revizije. Eksterni revizor na istom tragu navodi:

ER*: „Razlika je opseg rada, naime interna revizija bavi se problematikom sukladno planu i programu tijekom cijele godine, dok eksterni revizori vrše provjeru na godišnjoj razini. Interna revizija također ima druga zaduženja u organizaciji povezana s revizijskim radnjama. Tako da možemo reći da interna revizija puno detaljnije ulazi u problematiku, dok eksterna kao neovisno tijelo procjenjuje rad koji je interna revizija napravila i simulira rad sustava prema realnosti.“*

Pri procjeni rizika eksterna revizija koristi međunarodni revizijski standard MRevS 315. Kao što je već spomenuto u radu, MRevS 315 se odnosi na procjenu i identifikaciju rizika povezanih značajnim pogrešnih prikazivanjima u financijskim izvještajima. Procedure u upravljanju rizicima razlikuju se ovisno o industriji u kojoj se organizacija nalazi. Eksterni revizor navodi sljedeće:

ER: *„S pomoću MRevS-a 315 stječe se razumijevanje subjekta i okruženja u kontekstu informacijskog sustava. Nakon što se upozna sustav i njegova izloženost, te se utvrdi rizik, tada se provodi evaluacija i reakcija na rizik. Ne postoji jednoznačan odgovor zbog različitosti u organizacijama i industrijama u kojem se nalaze.“*

Dužnosti eksternog revizora koje se odnose na usklađenost s politikama i procedurama koje proizlaze iz zakona, pravilnika i statuta organizacije ili međunarodnih instituta profesije procjenjuju učinkovitost sustava u identifikaciji slabosti sustava i savjetuje u poboljšanju na temelju vlastitih znanja i iskustava. U kontekstu kibernetičke sigurnosti revizori moraju pratiti usklađenja koja se odnose na softverske programe, mrežne pristupe i autorizaciju, zaštitu servera i sigurnosnih kopija. O procesima usklađenja eksterni revizori navodi:

ER*: „Prvo se vrši pregled postoje li uopće politike i programi za kibernetičku sigurnost, i ako postoje tada se testira implementacija i funkcioniranje toga što su propisali sa stvarnom situacijom. Kada postoje provode se testovi kontrola na kritičnim točkama. U praksi je teže odrediti upravo zbog razloga što se sustavi razlikuju, odnosno nisu jednoznačni i razlikuju se od organizacije do organizacije. Čimbenici koji određuju mogu biti više lokacija na koje se mora obratiti pažnja, postoji li vanjski pristup programima i računalima, postoje li duplikati servera itd.“*

Kada se provodi testiranje sustava internih kontrola prema kibernetičkoj obrani revizori ocjenjuju spremnost organizacije s pomoću preventivnih, detektivnih i korektivnih metoda. Da bi se organizacija okarakterizirala spremnom mora imati uspostavljenu profesionalnu i sveobuhvatnu kulturu koja se odnosni na svakog pojedinca i koja stvara svijest o opasnostima i rizicima koje kibernetički napadi predstavljaju. Također, mora imati razumijevanje prema svim mogućim rizicima i analizirati izloženost prema istim, pratiti razinu komunikacije u internim kontrolama i kontinuirano vrednovati sustave nadzora. Čak i kada organizacija ima posložen sustav nikada se ne može karakterizirati kako apsolutno spremna ili zaštićena, zato što sofisticiranost štetnih programa i rapidan razvitak kibernetičkog prostora omogućavaju provale i zbog najmanje greške. Prema vlastitom iskustvu sugovornik navodi:

ER: *„Što se tiče općenito spremnosti teško je reći da je neki sustav u potpunosti spreman, zato što znanja o kibernetici su još u fazi uvođenja, potrebna je sekunda nepažnje da se podaci kompromitiraju ili ukradu i svaka organizacija je doživjela neke napade bez obzira na njenu veličinu i spremnost kontrola i informacijskog sektora. Revizor može procijeniti kontrole preventivnim, detektivnim i korektivnim metodama. Okruženje se toliko ubrzano mijenja da nijedna organizacija ne može biti 100 % spremna na kibernetički napad, što je i dokazano na tržištu jer gotovo je svakome u određenom trenutku upalo u sustav. Organizacije često zaboravljaju da je sustav jak koliko i najslabija karika, dovoljno je da jedna osoba otvori jedan kompromitirani mail.“*

Savjetodavne usluge eksternog revizora u kibernetičkoj sigurnosti odnose se na svakodnevne i proceduralne radnje, kao naprimjer zaštita sustava kontinuiranim mijenjanjem lozinki, ažuriranjem

antivirusnih i vatrozidnih programa, ograničenja pristupa mreži od trećih strana, kao i ograničenja pristupa podacima ovisno o poziciji svakog zaposlenika. Jedna od metoda zaštite podataka je izrada kopija u više primjeraka i fizičko odvajanje od servera i ostalih sustava i programa. Problem s kojim se eksterni revizori susreću pri savjetovanju ali i cjelokupnom radu je što ne dobivaju relevantne informacije, zbog čega ograničavaju reviziju i izražavanje mišljenja. Probleme u savjetodavnim uslugama i prikupljanjem dokaza eksterni revizor navodi sljedeće:

ER: *„Najčešće preporučujem da dodatno pojačaju sustav, u smislu antivirusnih programa, učestalije izmjene lozinki, ograničenje pristupa mreži, te da imaju više nezavisnih kopija sustava na dnevnoj bazi jer najčešće se napravi jedna kopija koja bude na istom računalu odnosno serveru kao i originalni podaci. Obično se rade greške s tvrdim diskom kojeg se ostavi u serveru, a kada padne sustav u cjelini to obuhvati i tvrdi disk, stoga je bitno da su kopije neovisne jedna o drugoj jer inače nema smisla ih uopće raditi. Danas su podaci uglavnom u oblaku (Cloud) što otežava davanje primjedbi jer se ne može saznati kako funkcioniraju, organizacije obično skrivaju potpune informacije zbog zahtjeva internih kontrola. Nitko ne daje radne odgovore, gdje se sve kopiraju podaci čak i kada se predstavite kao revizor. Kada pitate gdje su sigurnosne kopije daje se opći generički odgovor bez puno informacija što ipak nije dostatno dokazima revizije.“*

Treća tema- uloga revizijskog odbora: kao tijelo korporativnog upravljanja, revizijski odbori odgovorni su za nadzor internih kontrola i osiguravanje resursa internoj reviziji, provođenje procesa eksterne revizije i praćenje neovisnosti revizora, te održavanje sastanaka i poboljšanje komunikacije između internih i eksternih revizora. U pogledu kibernetičke sigurnosti uloga revizijskih odbora razlikuje se ovisno o veličini i industriji u kojoj se organizacija nalazi. Temeljna odgovornost uz nadziranje, osiguravanje resursa i praćenje rada eksterne revizije, od članova revizijskih odbora se traži podizanje svijesti o opasnostima u kibernetičkom prostoru, što zahtjeva poznavanje problematike informacijskih tehnologija od barem jednog člana odbora. O ulozi revizijskog odbora iz vlastitog iskustva sugovornik navodi:

RO: *„Nažalost u mom radu nisam se puno bavio kibernetičkom sigurnošću. Poduzeće u kojem sam član revizijskog odbora iako ima velik broj zaposlenih zaštita podataka nije prioritetna, jer podaci koje imamo i koje koristimo nisu relevantni niti vrijedni trećoj strani. Isto mogu reći i za interne kontrole koje se provode u poduzeću, stoga gotovo nikad ne komuniciramo o tome.“*

Kao što je već naglašeno prethodno u tekstu odgovornosti revizijskih odbora razlikuju se od organizacije do organizacije, stoga znanja i iskustva članova uvelike ovise o organizacijama u kojim se nalaze. Članovi koji su dio organizacije s razvijenim sustavom kibernetičke sigurnosti imaju razumijevanje poslovnih okolnosti i rizika koje ugrožavanju sigurnost podataka, zaduženi su za postavljanje ciljeva i određivanje zadataka prema prioritetu, te prate funkcioniranje sustava internih kontrola, provođenja politika i standarda. Na temelju odgovora i iskustva sugovornika može se zaključiti kako revizijski odbori nemaju snagu u stvaranju veće vrijednosti organizacije u kibernetičkoj zaštiti ako sustavi unutar organizacije nisu postavljeni ili dovoljno razvijeni u segmentu kibernetičke sigurnosti, čime prikazuje revizijski odbor kao funkciju koja nadograđuje postojeće i već postavljene sustave i ovisi o njima da bi uopće bila produktivna, što član revizijskog odbora i navodi:

RO: *„Ne mogu dati prave odgovore na vaša pitanja, praksa poduzeća po tom pitanju je u cijelosti sadržana u informatičkom sektoru koji se zadovoljava minimalnim zahtjevima kao što su postavljanje lozinki na računala, te instaliranje i ažuriranje antivirusnih programa. Iako postoje standardi i smjernice u pristupanju kibernetičkoj sigurnosti, ne bavim se s time jer poduzeće nema interne kontrole koje provode kibernetičku zaštitu, stoga ni ja neman odgovornosti u naziranju i planiranju sustava koji ne postoji. Moj rad uvelike ovisi o prethodnim radnjama u poduzeću, te ako neki segmenti ne postoje, onda se ni ja ne osvrćem.“*

Četvrta tema- suradnja interne i eksterne revizije, te revizijskih odbora: segment kibernetičke sigurnosti u organizacijama funkcionira na principu „lanac je jak koliko i njegova najslabija karika“, stoga je međusobna komunikacija i suradnja između navedenih tijela od ključne važnosti. Prvi dio obuhvaća percepciju internog revizora o suradnji s eksternom revizijom i revizijskim odborom, drugi dio odnosi se na percepciju eksternog revizora prema internoj reviziji i revizijskom odboru, i treći na percepciju člana revizijskog odbora prema internoj i eksternoj reviziji.

Suradnja interne revizije s eksternom stvara veću vrijednost u financijskom izvještavanju, eksterni revizori bi trebali podijeliti svoja izvješća s internim revizorima u svrhu izbjegavanja dupliciranja posla, olakšanja rada svih dionika i bolje upravljanje rizicima. Iako standardi i regulatorna tijela u svojim preporukama naglašavaju suradnju kao bitan čimbenik u ostvarivanju vjerodostojnih financijskih izvješća što obuhvaća i pravilno funkcioniranje kibernetičke sigurnosti, u primjeru internog revizora može se vidjeti kako u praksi svijest o kibernetičkoj sigurnosti nije na optimalnoj razni, te on navodi sljedeće:

IR: *„Eksterni revizori se ne fokusiraju na tu tematiku, oni su više usmjereni na financijske izvještaje. Čak i vezi financijskih Izvještaja jako rijetko komuniciraju, čisto zbog pro forme odrade, pošalju mail gdje pitaju za naše interne izvještaje, ali ta suradnja nije na visokoj razini. U više situacija tražili smo mi sastanke s njima koji se ne bi organizirali. Pogotovo za temu kibernetičke sigurnosti eksterna revizija dosad nije imala neke upite po tom pitanju.“*

Percepcija interne revizije prema revizijskim odborima je da odbor surađuje s revizorima kao „ton s vrha“ (eng. tone at the top), što bi značilo da je revizijski odbor tijelo koje nadzire rad, potvrđuje planove i ocjenjuje uspješnost internih kontrola, odnosno služi kao podrška. Komunikacija među ove dvije funkcije iznimno je važa jer revizijski odbori odobravaju budžet internih kontrola i revizije, stoga je bitno da se resursi troše optimalno. Interni revizor o suradnji s revizijskim odborom navodi sljedeće:

IR: *„Revizijski odbori, što se tiče internih kontrola služe da propitkuju menadžment. I na takav način šalje se „ton s vrha“. On se nameće menadžmentu, višem menadžmentu, a samim time viši menadžment se nameće ostatku organizacije kako su interne kontrole bitne. Također očituje se kroz izvještaj interne revizije koja se šalje revizijskom odboru, oni te izvještaje prihvate i komentiraju skupa s internom revizijom i menadžmentom te na takav način oni daju podršku internim kontrolama. Nadalje, oni podržavaju internu reviziju tako da osiguravaju resurse interne revizije. To znači kada se rade budžeti osiguravaju da budžet ima dovoljno sredstava za sve aktivnosti koje interna revizija mora provoditi, uključujući i zaposlenike, te da interna revizija ima dovoljan broj ljudi da može obavljati svoje zadatke koje smo zacrtali.“*

Iako se u literaturi često naglašava komunikacija između internih i eksternih revizora kao krucijalnom stavkom u učinkovitom funkcioniranju sustava organizacije i korporativnom upravljanju, iz perspektive eksternog revizora se također može vidjeti kako u praksi nije isto. Kao problem se navodi uloga interne revizije, koja s obzirom na tip industrije ne mora biti obvezana u protokolima kibernetičke sigurnosti, već se ta funkcija zadržava u sektoru informacijskih tehnologija. Zadaća eksternog revizora je prvo procijeniti interne kontrole da bi se smatrale relevantnima kao što sugovornik navodi:

ER*: „U praksi interna i eksterna revizija ne moraju surađivati zajedno, interna revizija često nema zacrtano u svom planu i programu da se bavi kontrolama u kibernetičkoj sigurnosti. U slučaju kada imaju u planu i programu tada surađuješ, ali tek nakon što se potvrdi da su neovisni i dosljedni u svom radu, a kada to nisu, tada ih se potpuno izostavlja iz rada.“*

Suradnja eksterne revizije i revizijskog odbora započinje već s odabirom revizora u kojem revizijski odbori igraju ključnu ulogu preporukama i u nekim slučajevima i biranjem revizora. Zadaća članova odbora je kontinuirano praćenje procesa revizije i osiguravanje neovisnosti i integriteta revizora. Nadalje članovi su zaduženi pomagati revizorima u identificiranju i rješavanju problema s financijskim izvještavanjem, usklađenosti s politikama i standardima, kao i rješavanju konflikata u slučaju kad se pojave. Praksa je ipak pokazala kako suradnja nije na razini na kojoj se očekuje, te eksterni revizor iz svoje perspektive navodi sljedeće:

ER: *„Prema mom iskustvu revizijski odbori su iako definirani slabo uključeni u rad na način na koji je zakonodavac zamislio, obično održe par sjednica u toku godine, ali njihov angažman, ne računajući velike listane korporacije nije na poželjnoj razini. Iskomuniciraju se stvari koje standardi nalažu, ali za podršku i detaljne pojašnjenje stvari nema veće koristi.“*

Održavanje regularnih sastanaka i kontinuirano komuniciranje između internog revizora i članova revizijskog odbora omogućava funkcioniranje sustava internih kontrola i kontinuirano unaprjeđuje organizaciju i zaposlenike prema višim ciljevima. Kvalitetno komuniciranje pomaže revizijskom odboru u boljem razumijevanju unutarnjeg okruženja organizacije i potrebama interne kontrole što u konačnici dovodi do veće sigurnosti podataka, pravilnog funkcioniranja sustava, usklađenje s politikama i racionalnije trošenje resursa. Interni revizori koji imaju podršku revizijskog odbora motiviraniji su u svom radu, lakše rješavaju predstavljene probleme, dolaze do potrebnih resursa, te imaju potvrdu o dobro obavljenom poslu s pomoću osiguranja koje pruža revizijski odbor. U praksi komuniciranje nije uvijek na razini u kojoj se postižu željeni rezultati, i to se može vidjeti na primjeru sugovornika iz revizijskog odbora:

RO: *„Komunikacija koju imam s internim revizorima nije česta, uglavnom se sastajemo na redovnim sastancima koji se održavanju jednom ili dvaput na godišnjoj razini. Obično se iskomuniciraju postavljeni planovi, te kako su oni provedeni. U poduzeću u kojem sam član odbora nema značajnih promjena u rizicima koje se nalaze u okolini, stoga ni sama komunikacija nije toliko česta, posebice ako pričamo o kibernetičkoj sigurnosti.“*

### 6.3. Rezultat empirijskog istraživanja

Na temelju provedenih intervjua i prikupljanjem podataka došlo se do zaključka kako svijest o kibernetičkoj sigurnosti nije na razini koja bi pružila organizacijama zaštitu podataka i cjelokupnog poslovanja. Zaduženja interne revizije odnose se na upravljanje rizicima koji ugrožavaju informacijske sustave od provala, krađe podataka, industrijske špijunaže ili narušavanje informacija koje utječu na vjerodostojnost financijskih izvještaja. Interni revizori oslanjaju se na revizijski odbor kao mjeru osiguranja koja se ostvaruje nadzorom internih kontrola, odobravanje resursa potrebnih za provođenje procesa i usklađivanje s politikama organizacije. U provođenju eksterne revizije interni revizori pomažu eksternim u razumijevanju funkcioniranja i strukture internih kontrola, te ako eksterni revizor procjeni sustav kao funkcionalan, koristi ga kao potporu u procesu. Glavna skupština, odnosno dioničari organizacije oslanjaju se u ekspertize revizijskog odbora pri odabiru društva za obavljanje eksterne revizije i praćenje neovisnosti revizora.

Sugovornici u intervjuima su pokazali kako razumijevanje problematike vezane uz kibernetičku sigurnost i međusobna komunikacija nisu na razini koju dioničari, zakonodavci i donositelji standarda očekuju. Održavanje sastanaka, korištenje sustava internih kontrola i podrška u radu ne predstavljaju snagu u kibernetičkoj obrani, te se komunikacija odvija formalno. Upravljanje rizicima kibernetičke sigurnosti se pristupa površno i zadržava u sektoru informacijskih tehnologija ili se za takve usluge koriste druge organizacije. Revizijski odbori nisu uključeni u rad, ne služe kao potpora internim revizorima, te ne sudjeluju u procesima obavljanja eksterne revizije. Eksternim revizorima nisu omogućene potrebne informacije, odnosno dobivene informacije nedostatne su za izražavanje razumnog mišljenja o stanju internih kontrola i usklađenosti sa standardima. Ubrzan razvitak digitalnog prostora, porast kibernetičkog kriminala, te ugrožavanje privatnih podataka i imovne glavni su motivi koji pokreću svijest o kibernetičkoj sigurnosti, jer u protivnom šteta izazvana kibernetičkim provalama izaziva dalekosežne posljedice u budućnosti

# 7. ZAKLJUČAK I RASPRAVA

Kibernetička sigurnost bitan je čimbenik digitalnog doba i tehnološkog razvoja. Razvojem informacijskih tehnologija organizacije koriste računala za komunikaciju, upravljanje, spremanje podataka i poslovanje u sve većem obujmu. U današnje vrijeme virtualni svijet je dio okruženja, internet stvari je prisutan i svim segmentima života uključujući privatni i poslovni život, što čini pristup informacijama preko mnogobrojnih kanala ugrožavajući podatke i osobne informacije prema trećim osobama što uključuje i zlonamjerne pristupe kibernetičkim kriminalcima. Zaštita privatnosti i osobnih informacija jedan je od ključnih izazova s kojim se organizacije i fizičke osobe moraju suočiti.

Postoje mnogobrojni razlozi za napade, motivi ne moraju biti povezani sa stjecanjem tuđe imovne, već se napadi izvode u svrhu ostvarivanje štete, špijunaže, narušavanja ugleda ili zastrašivanja, a uključene mogu biti i države kao na primjeru Ruske federacije protiv Estonije, Gruzije i trenutnog rata protiv Ukrajine. Napadi se ostvaruju na više načina, te postaju sofisticiraniji s vremenom, stoga je važno kontinuirano unaprjeđivati sustav i stjecati nova znanja na području informacijskih tehnologija. S pomoću društvenog inženjeringa napadi se provode manipulacijama i zamkama u vidu phisnig poruka i raznim vrstama mamaca u kojim napadači koriste lažno predstavljanje i prijetnje u svrhu stjecanja imovine. Razvijanjem ucjenjivačkih softvera (eng. *ransomware*) napadači preuzmu sustave i blokiraju pristup, te traženjem otkupnine ucjenjuju vlasnike podataka. Izlaganje trećoj strani također je ranjiva točka, jer bez obzira na učinkovitost vlastite obrane protiv napada sustav se probija s pomoću nezaštićenih sustava organizacije s kojima se obavlja poslovanje čineći štetu na obje strane i istovremeno naglašava kako je za kibernetičku sigurnost od krucijalne važnosti da svi sudionici moraju biti zaštićeni koliko je god moguće.

Globalni poslovni rizici uključuju rizike od kibernetičkih napada i okarakteriziraju ih kao rastući problem, posebice nakon globalne pandemije koronavirusa, te je u 2024. godini kibernetički rizik na prvom mjestu globalnih rizika. Posljednice od uspješnih kibernetičkih napada su velike i dugotrajne, mogu uništiti reputacijski ugled organizacija, prekinuti poslovanje, ugroziti investicije, pa čak i ugroziti industrije u cjelini, te se procjenjuje kako će kibernetički napadi napraviti štetu u 2024. godini u iznosu od 9.5 bilijuna dolara na globalnoj razini. Stoga je ulaganje u kibernetičku sigurnost jedno od prioritetnih ulaganja za organizacije u bilo kojoj industriji ili zemlji, što dokazuje potrošnja za kibernetičku zaštitu u iznosu od 188 milijardi dolara u 2023, godini i očekivana potrošnja za 2024. godinu u iznosu od 214 milijardi dolara na globalnoj razini, odnosno porast od 14.3 % u odnosu na prethodnu godinu. Do 2027. godine očekuje se da će potrošnja narasti na 290 milijardi dolara. Podizanje svijesti o zaštiti kibernetičkog prostora zadatak

je za sve sudionike organizacija i nekoć problem sektora informacijskih tehnologija sada je problem kojeg svi moraju poznavati.

Kibernetička zaštita provodi se na više načina, potrebno je zaštiti svaki segment i nedopušteni pristup podacima jer sustav je jak koliko i njegova najslabija pozicija. Sve započinje samim pristupom u sustav. Organizacije moraju zaštiti svoju imovinu od pristupa trećih strana, razina i vrsta podataka mora se raspodijeliti ovisno o pozicijama zaposlenika kojima su potrebne informacije. U slučaju napada ili urušavanja sustava organizacije moraju izrađivati kopije, te postupati s njima odvojeno od servera i neovlaštenog pristupa. Postavljanjem lozinki na računala i podatke, te kontinuiranim ažuriranjem antivirusnih programa, kao i postavljanjem vatrozidne zaštite na mreže moraju biti prioritetni menadžmentu informacijske sigurnosti.

Može se zaključiti da je kibernetička sigurnost jedan od ključnih rizika u današnjem poslovanju. Primjeri iz prakse pokazuju da šteta izazvana kibernetičkim incidentima ima dalekosežne posljedice za organizacije, ugrožavajući imovinu, zaposlenike, ugled, investicije i poslovanje u cjelini. Stoga je ulaganje u kibernetičku sigurnost prioritet za svaku organizaciju bez obzira na veličinu i industriju. Ulaganje u licence, softverske programe i zapošljavanje stručnog osoblja u informacijskom sektoru, kao i edukacija zaposlenika temeljni su izdaci koje organizacija mora izdvojiti u svrhu zaštite podataka i poslovanja.

Funkcija interne revizije bitan je faktor u određivanju i vrednovanju rizika u organizaciji, kao i uspostavljanju i upravljanju internim kontrolama u suradnji s menadžmentom. Kibernetička sigurnost i povezani rizici postali su integrirani dio rada internih revizora, stoga je stjecanje znanja u informacijskim tehnologijama izazov s kojim se svaki interni revizor susreće. Institut internih revizora (IIA) educira i priprema interne revizore u radu, uključujući i upravljanje kibernetičkom sigurnosti. Povezivanjem, pribavljanjem resursa i uvođenjem standarda pomažu internim revizorima u razvoju organizacija u kojim se nalaze. Izdavanjem certifikata povezanim s informacijskim tehnologijama interni revizori stječu znanja u razumijevanju izvora podataka, prepoznavanju elemenata pravilnog upravljanja podacima, uvođenju u procese upravljanja, konceptima podatkovne pismenosti, analizi podatka, prepoznavanju kibernetičkih prevara i mnoge druge.

Doprinos internih revizora u organizaciji je osiguranje nadzornim tijelima i menadžmentu da funkcioniranje sustava i dizajn postavljenih kontrola održavaju organizaciju prema postavljenim ciljevima. Da bi to uspjeli, interni revizori moraju imati iskustva i znanja, te što je jednako bitno integritet i razvijene komunikacijske vještine. Također, nepristranost prema nijednoj funkciji u organizaciji omogućuje revizorima da objektivno i realno mogu procijeniti situacije i tako doprinijeti u proaktivnom razmišljanju i

pripremanju ciljeva za budućnost. Neovisnost interne revizije ključan je čimbenik, te omogućava slobodu u radu oslobođen od smetnji i pristranosti izgrađujući povjerenje i vjerodostojnost. Upravljačka tijela preko funkcije interne revizije stječu potvrdu o usklađenju s politikama, pravilnom funkcioniraju internih kontrola i procesa, te primjerenom dizajnu upravljačkih struktura. Da bi sustav pravilno funkcionirao mora postojati visoka razina komunikacije između upravljačkih tijela i menadžmenta kao i s internom revizijom. Komunikacija pomaže internim revizorima u razumijevanju unutarnjeg i vanjskog okruženja organizacije, te pomaže menadžmentu u procjeni rizika i usklađenosti s politikama i standardima. Također, dobra komunikacija sprječava dupliranje posla, odnosno nepotreban trošak vremena i resursa što podiže produktivnost.

U procesu interne revizije revizori započinju određivanjem jednog ili više područja kojem pristupaju. Ovisno o opsegu rada područja koja se odnose na kibernetičku sigurnost mogu biti struktura informacijskog sektora, spremanje podataka, prijenosi i zaštita, politike i procedure koje su određene u organizaciji. Predrevizijske radnje zahtijevaju od internog revizora razumijevanje unutarnjeg sustava uključujući i mrežnu infrastrukturu, kao i poznavanje zaposlenika koje raspoređuju ovisno o potrebama. Zatim se identificiraju prijetnje i rizici koje stvaraju, te raspoređuju ovisno o potencijalnoj šteti i vjerojatnosti nastanka. To uključuje štetne programe, korištenje zabranjenih aplikacija, nedozvoljeni pristupi, ukradene lozinke i slično. Nakon identifikacije započinje se upravljanjem rizicima izradom plana reakcije na incidente u kojem revizori pojašnjavaju prioritetne rizike, načine sprječavanja nastanka, dokumentaciju i alate za zaštitu, kao i komunikacijski plan koji uključuje edukaciju i kontinuirani razvitak. Učinkovita interna revizija koja ima potrebna znanja u informacijskim tehnologijama i sposobnost identificiranja i vrednovanja rizika, služi organizaciji kao najpouzdaniji savjetnik i snaga u kibernetičkoj sigurnosti. Pouzdani interni revizori stvaraju veću razinu povjerenja prema zaposlenicima, što omogućava provođenje savjetodavnih usluga u poboljšanju svih funkcija unutar organizacije. Praksa je pokazala da interni revizori nemaju znanja i prakse u informacijskim tehnologijama zato što organizacije ne smatraju kibernetičku sigurnost kao ključan rizik. Za savjetodavne usluge koriste se eksternalizirani izvori, te stručnjaci iz IT sektora. Podupirući interne revizore u boljem razumijevanju kibernetičke sigurnosti organizacije postižu sigurniju zaštitu podataka, zadržavaju osjetljive informacije unutar organizacije, razvijaju vlastiti kadar, što u konačnici dovodi i do uštede resursa i vremena.

Rad internog revizora uključuje i proaktivno razmišljanje, kao i kontinuiran nadzor internih kontrola i informacijskih sustava vodeći se taktikom „bolje spriječiti nego liječiti.“ Kvalitetan rad interne revizije može uvelike pridonijeti organizaciji, smanjiti troškove, obučiti zaposlenike i pomoći eksternoj reviziji što

dovodi do vjerodostojnih prikazivanja imovine i financijskih izvještaja, te povjerenju između dioničara i vlasnika prema upravljačkim tijelima organizacije. Razvoj koji nameće ubrzan razvoj tehnologije zahtijeva kontinuirano educiranje i praćenje trendova u informacijskim tehnologijama i kibernetičkom prostoru, sofisticiranost zlućudnih aplikacija i softvera predstavlja veliki izazov u budućnosti i s obzirom na opasnosti i potencijalnu štetu koju izaziva organizacije moraju koristiti sve moguće resurse za zaštitu podataka, imovine i vlastitih zaposlenika.

Uloga eksterne revizije u korporativnom upravljanju je ispitivanje vjerodostojnosti financijskih izvještaja. Zbog asimetrije informacija između dioničara, odnosno vlasnika organizacije i upravljačkih tijela motiviraju članove uprave u manipulaciji informacijama i pogrešnim prikazivanjima stavki imovine ili prihoda u svrhu stjecanja koristi. Stoga glavna skupština kao tijelo koje predstavlja vlasnike pred organizacijom imenuje revizorsko društvo da provede reviziju i preda ocjenu o vjerodostojnosti prikazane imovine u financijskim izvještajima. Tako i u slučaju kibernetičke sigurnosti, eksterni revizori su odgovorni pregledati sustav kibernetičke sigurnosti i segmente informacijskog sektora koji u slučajevima kibernetičkih incidenata, dovode do pogrešnih prikazivanja stavki u financijskim izvještajima. Revizori uz potrebna iskustva i znanja koja su potrebna za obavljanje revizije moraju ostati potpuno neovisni prema organizaciji u kojoj obavljaju usluge revizije, te očuvati svoj integritet kao pojedinca i integritet društva kojeg predstavljaju, jer je to najvažnija vrlina koju revizori mogu posjedovati.

U pogledu na kibernetičku sigurnost naglašava se razumijevanje općih kontrola i informacijskih tehnologija, što znači da kontrole moraju kontinuirano pratiti rad Informacijskih službi, obradu i integritet informacija, kao i pravilno funkcioniranje sustava u cjelini. Sustav koji služi za pristup podacima najbitniji je segment za eksternog revizora, te na koji način funkcionira proces autentifikacije i autorizacije koji zadržava osjetljive informacije u ovlaštenim okvirima. Okruženje informacijskih tehnologija sastoji se od aplikacija, infrastrukture i procesa upravljanja za koje revizori moraju stjeći razumijevanje za identifikaciju rizika i prijetnji.

Identifikacijom se predviđaju događaji, identificiraju prijetnje i utvrđuju slabosti organizacije u informacijskim strukturama. Procjenom se s pomoću alata identificirane slabosti vrednuju preko vjerojatnosti, utjecaj i posljedice nastanka događaja. Nakon što eksterni revizor utvrdi rizike, postavlja prioritetne rizike ovisno o vjerojatnosti i veličini štete. Kvaliteta eksterne revizije može stvoriti dodatnu vrijednost preko interne revizije, odnosno ako eksterni revizor procjeni da sustav interne kontrole pravilno funkcionira, te uspostavi dobru komunikaciju s internim revizorima, stječe bolje razumijevanje organizacije, podiže produktivnost i jača zaštitu podataka, što u konačnici dovodi do većeg povjerenja

između menadžmenta i vlasnika, kao i vrijednosti organizacije. Na temelju prikupljenih informacija preko intervjua može se reći kako funkcija eksterne revizije obavlja proces samostalno bez podrške interne revizije i komunikacije s revizijskim odborom. Eksterni revizori imaju znanja u razumijevanju mrežnih sustava i informacijskog sektora, te mogu pomoći organizaciji u boljoj zaštiti. Savjeti vezani za upravljanje rizicima očituju se kroz; očuvanje neovisnih kopija sustava, jačanje sigurnosti boljim lozinkama i antivirusnim programima, te ograničenja pristupa mreži. Problem s kojim se revizori susreću je nedostupnost ili nepotpunost informacija koje dobivaju od organizacija. Da bi eksterna revizija bila snaga organizaciji u kibernetičkoj zaštiti moraju se revizorima pružiti sve potrebne informacije kako bi se dobila potpuna slika o funkcioniranju sustava što dovodi o razumnog uvjerenja i sposobnosti pružanja savjetodavnih usluga.

Revizijski odbori su dio upravljačkih tijela, kao odbori nadzornog odbora. Barem jedan član odbora mora imati znanja i iskustva u području računovodstva, financija i revizije. Članovi revizijskih odbora moraju razumjeti okruženje i regulatorne okvire organizacije, planove, ciljeve i smjer u kojem se organizacija razvija, status revizije financijskih izvještaja i drugih procesa u tijeku, kao i vlastite odgovornosti i uloge u organizaciji. Uloge i zaduženja razlikuju se ovisno o industriji i veličini organizacije, a zajedničko svim odborima je sudjelovanje u odabiru revizorskog društva za obavljanje eksterne revizije, nadzor nad internim kontrolama i održavanje redovnih sastanaka po pitanju plana revizije.

Izrada plana interne revizije i praćenje sustava internih kontrola provodi se uz podršku revizijskog odbora. Revizijski odbori moraju stvoriti dobru komunikaciju s internim revizorima zbog boljeg razumijevanja potreba internih kontrola u odobravanju budžeta, zapošljavanja ili raspodjele radne snage i upravljanja rizicima. S obzirom na razvoj kibernetičke sigurnosti, od članova revizijskog odbora se očekuje poznavanje informacijskih tehnologija u mjeri koje utječu na financijsko izvještavanje. Također, dio odgovornosti je u podizanju svijesti o opasnostima u okruženju i kibernetičkom prostoru za zaštitu podataka kojim organizacija raspolaže. Revizijski odbor treba biti funkcija koja organizaciju i interne kontrole podiže na višu razinu i potvrđuje pravilno funkcioniranje sustava kibernetičke obrane kroz nadzor i podršku.

U postupcima odabira revizorskog društva, uloga članova revizijskog odbora sudjeluje i savjetuje dioničare i glavnu skupštinu koja potvrđuje odabir, a u često u praksi članovi odbora sami odabiru društvo. Eksterni revizori uz suradnju s internim revizorima, održavaju sastanke s revizijskim odborom koji pomaže u razumijevanju politika, regulatornih tijela i standarda koje organizaciju obvezuje zakonodavac i industrija u kojoj se nalaze. S obzirom na to da je dužnost revizijskog odbora praćenje procesa revizije i osiguranje neovisnosti eksternog revizora, dužni su inicirati sastanke i provoditi kvalitetnu komunikaciju, što

uključuje sprečavanje konflikata i stvaranje međusobnog povjerenja. Pravilno funkcioniranje revizijskog odbora organizacijama stvara dodatnu vrijednost i ostvaruje konkurentsku prednost. Kao nadzorni mehanizam organizacije, članovi revizijskog odbora stječu razumijevanje funkcioniranja sustava što omogućava učinkovitiju provedbu internih kontrola, budžetiranje i kvalitetnije kadroviranje interne revizije, te bolju komunikaciju i podršku eksternoj reviziji. Praksa je pokazala da članovi revizijskih odbora ne daju dovoljno pažnje i interesa prema kibernetičkoj sigurnosti. Suradnja s funkcijama interne i eksterne revizije je na minimalnoj razini unutar zakonskog okvira, što je nedovoljno za postizanje pune podrške i snage u kibernetičkoj sigurnosti. Podizanjem svijesti i educiranjem članova revizijskog odbora organizacije bi dobile učinkovitije interne kontrole koje bi imale mogućnost komuniciranja potreba i problema s kojima se susreću, te bi se eksterna revizija kvalitetnije provela uz potrebne informacije i komunikaciju koju funkcionalni revizijski odbori donose.

Utvrđivanjem zakonskih i regulatornih zahtjeva koji se stavljaju pred interne i eksterne revizore, kao i revizijske odbore, te istraživanjem provedenim preko intervjua s osobama uključene u problematiku može se zaključiti kako postoji mnogo prostora za napredak. Razumijevanje opasnosti i visine rizika koje kibernetička sigurnost predstavlja nisu na razini koja bi trebala zaštiti organizacije i okruženje u kojem se nalaze. Funkcija interne revizije ne upravlja s kibernetičkim rizicima kao prioritetnim, te ne posvećuje dovoljno pažnje u testiranju kontrola od mogućih kibernetičkih incidenata, što potvrđuje korištenje usluga drugih organizacija u upravljanju s kibernetičkim rizicima i tretirajući ga kao niskorizičan proces. Komunikacija koju interna revizija uspostavlja s eksternom i revizijskim odborom nije dovoljno razrađena ili je gotovo nepostojeća u pogledu na kibernetičku sigurnost, što ugrožava funkcioniranje informacijskih struktura i zaštitu podataka. Eksterni revizori sudjeluju u procesu revizije samostalno, bez suradnje s internom revizijom, naglašava se problem neovisnosti i predanosti interne revizije prema kibernetičkoj sigurnosti, kao i nepotpunost informacija koje eksterni revizori dobivaju za razumijevanje funkcioniranje sustava mrežnih struktura i procedura informacijske zaštite, što ugrožava razumno uvjerenje eksternog revizora o kibernetičkoj sigurnosti. Dodatan problem stvara i loša komunikacija s revizijskim odborom, gdje je involviranost članova odbora jako slaba, odnosno na razini obveznih sastanaka bez dodatne potpore i suradnje. Revizijski odbori nemaju znanja i educiranost u kibernetici sigurnosti, te se oslanjaju na sektore informacijskih tehnologija u zaštiti sustava i očuvanja podataka, iako je dokazano da se kibernetički napadi događaju svim organizacijama bez obzira na industriju i veličinu. U svrhu poboljšanja sustava i jačanja kibernetičke sigurnosti postoji snažna potreba za napretkom i edukacijom u informacijskim tehnologijama kod svih tijela koja su predmet ovog rada. Funkcija interne revizija mora surađivati s IT sektorom te ih uključiti u rad internih kontrola, steći znanja na području upravljanja

mrežnim strukturama i sustavima za pristup podacima. Interni revizori moraju biti proaktivni u planiranju, te savjeti koji upućuju upravnim tijelima moraju podupirati svijest o boljoj zaštiti podataka i ulaganje u sigurnost. U procesima eksterne revizije moraju se osigurati sve potpune informacije koje će revizorima pomoći u stjecanju razumijevanja sustava i donošenja razumnog mišljenja, uz suradnju tijela unutar organizacije koji moraju komunicirati s eksternim revizorima kada je njihova pomoć potrebna. Revizijski odbori u nadzoru moraju pokazati spremnost organizacije na promjene i ulaganje u interne kontrole u svrhu unapređenja i jačanja kibernetičke sigurnosti. Članovi odbora se moraju više angažirati po pitanju kibernetičke sigurnosti i uključiti IT stručnjake u rad, te poticati komunikaciju i suradnju između interne i eksterne revizije za bolje razumijevanje potreba koje organizacija ima u zaštiti podataka.

Za očekivati je kako će u budućnosti rizik kibernetičke sigurnosti ostati u vrhu globalnih poslovnih rizika, zbog kontinuiranog razvoja tehnologije i sofisticiranosti zloćudnih programa. Motiviranost kibernetičkih kriminalaca ne proizlazi samo iz stjecanja tuđe imovine, već se očituje kroz stvaranje štete, strateških planova u ratovanju, uništavanju konkurencije i terorizma, stoga meta može biti svaka organizacija ili grupa ljudi. Od krucijalne važnosti je ulagati i pratiti trendove u kibernetičkoj sigurnosti, kontinuirano educiranje i podizanje svijesti, te uključivanje svakog zaposlenika koji djeluje u organizaciji.

## LITERATURA


1. Agarwal, A. (2024). The Top 5 Cybersecurity Threats and How to Defend Against Them, ISACA, Izvor: https://www.isaca.org/resources/news-and-trends/industry-news/2024/the-top-5-cybersecurity-threats-and-how-to-defend-against-them?gad_source=1&gclid=CjwKCAjwr7ayBhAPEiwA6EIGxCo5RfGbEIpn4085bCM5TSmo1_twzCzdkwFZO-pHl_ACbkj9rGGyjBoCOc8QAvD_BwE (pristupljeno: 22.5.2024.)
2. Aguolu, O., Igwe, A., Okoyeuzu, C., Ukpere, W. I. (2018). Strategies and constraints for effective communication in internal auditing quality assurance delivery in the university system. International Journal Development, Vol. 9(3), str. 248-267.
3. Ahola, M., (2021). The Role of Human Error in Successful Cyber Security Breaches. Usecure., izvor: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches (pristupljeno: 5. 11. 2023.)
4. Alabede, J., O. (2012). The role, compromise and problems of the external auditor in corporate governance, Research Journal of Finance and Accounting, Vol. 3, No 9. ISSN 2222-1697.
5. Al-Baidhani, (2014). The Role of Audit Committee in Corporate Governance: Descriptive Study, izvor: https://dx.doi.org/10.2139/ssrn.2487167
6. Allianz Risk Barometer, (2023)., izvor: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html (pristupljeno: 3. 11. 2023.)
7. Almasria, N. (2021). Determinant Governance Mechanisms Affecting the Quality of Auditing: the External Auditors' Perceptions. 18. 38-65., izvor: https://dx.doi.org/10.2139/ssrn.4223799
8. Almasria, N. (2022). Corporate Governance and the Quality of Audit Process: An Exploratory Analysis Considering Internal Audit, Audit Committee and Board of Directors, European Journal of Business and Management Research, Vol. 7 (1). Str. 78-99. DOI: http://dx.doi.org/10.24018/ejbmr.2022.7.1.1210
9. Almatari, O., Helal, I., Mazen, S., Elhennawy, S. (2018). Cybersecurity Tools for IS Auditing. 2018 Sixth International Conference on Enterprise Systems (ES), Limassol, Cyprus. Str. 217-223, doi: 10.1109/ES.2018.00040.

10. Bansal, Y., Mamodiya, U. (2023). Technical Security Known as Cyber Security: A Review. Journal of Computer Technology & Applications. Vol 13, No 3., Izvor: https://www.researchgate.net/publication/367177262_Technical_Security_Known_as_Cyber_Security_A_Review

11. Beasley, M. S. i Petroni, K. R. (2001). Board Independence and Audit-Firm Type, Auditing, 20, str. 97-114.

12. Benaroch, M. (2021) Third-party induced cyber incidents—much ado about nothing?, Journal of Cybersecurity, Volume 7, Issue 1, tyab020, https://doi.org/10.1093/cybsec/tyab020

13. Blasquino, E. (2024, 29. veljače), The Crucial Role of Internal Audit in Cybersecurity Strategy, internal audit 360, izvor: https://internalaudit360.com/the-crucial-role-of-internal-audit-in-cybersecurity-strategy/ (pristupljeno 25.5.2024.)

14. Borkovich, D. J., Skovira, R. J., (2020). WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. Issues in Information Systems Volume 21, Issue 4, str. 234-246, izvor: https://iacis.org/iis/2020/4_iis_2020_234-246.pdf

15. Braun, V. Clarke, V., (2006). Using thematic analysis in psychology. Qualitative Research in Psychology. 3. 77-101. DOI:10.1191/1478088706qp063oa

16. Breda, F., Barbosa, H., Morais, T. (2017) SOCIAL ENGINEERING AND CYBER SECURITY, INTED2017 Proceedings, pp. 4204-4211.

17. Chen, Y., Hsu, J., Huang, M., Yang, P. (2013). Quality, Size, and Performance of Audit Firms. International Journal of Business and Finance Research. 7.

18. Chimwanda, E., CISA, CIA, CISSP, (2022). Essentials for an Effective Cybersecurity Audit, izvor: https://www.isaca.org/resources/news-and-trends/industry-news/2022/essentials-for-an-effective-cybersecurity-audit (pristupljeno: 13. 12. 2023.)

19. Committee of Sponsoring Organizations of the Treadway Commission, (2017) Enterprise Risk Management: Integrating with Strategy and Performance, Executive Summary, str. 3, izvor: https://aaahq.org/portals/0/documents/coso/coso_erm_2017_-_exec_summary.pdf

20. Čular, M. (2023). Kibernetička sigurnost i uloga revizijskih odbora, Računovodstvo i financije, 2/2023. str. 95-98. Stručni članak UDK 657.6

21. DeAngelo, E. L. (1981). Auditor independence, 'low balling', and disclosure regulation, Journal of Accounting and Economics, Vol. 3, (2). str. 113-127. Izvor: https://doi.org/10.1016/0165-4101(81)90009-4

22. Delaney, M. O., (2006). Auditor Independence - Its Importance to the External Auditor's Role in Banking Regulation and Supervision, Conference Proceedings of the IBFR Conference, Costa Rica and Elsevier Journals, Izvor: https://dx.doi.org/10.2139/ssrn.1407177

23. Deloitte, (2017). Cybersecurity: The changing role of audit committee and internal audit, Izvor: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cybersecurity-the-changing-role.pdf

24. Dieli, O.J., Opara, E. U., Osho, G. S., Erhuanga G. A., (2020). THE MARGINAL IMPACT AND SPILLOVER EFFECTS OF INCREASED EXPENDITURE ON CYBER SECURITY IN US IT INDUSTRY AND GDP GROWTH RATES. JOURNAL OF SMART ECONOMIC GROWTH Vol 5 No 2, izvor: https://jseg.ro/index.php/jseg/article/view/107

25. Drogalas, G., Karagiorgos T. & Arampatzis K. (2015). Factors associated with Internal Audit Effectiveness: Evidence from Greece. Journal of Accounting and Taxation, 7(7), 113 – 122

26. Flick, U., (2018). An Introduction to Qualitative Research. Šesto izdanje, Str. 57. Sage

27. Galinec, D. (2023). Cyber Security and Cyber Defense: Challenges and Building of Cyber Resilience Conceptual Model. International Journal of Applied Sciences & Development. 1. str. 83-88. 10.37394/232029.2022.1.10., izvor: https://www.researchgate.net/publication/368943316_Cyber_Security_and_Cyber_Defense_Challenges_and_Building_of_Cyber_Resilience_Conceptual_Model

28. Galligan, M., E., Rau, K., (2015). Coso in the cyber age, Deloitte, izvor: https://www.coso.org/Shared%20Documents/COSO-in-the-Cyber-Age.pdf

29. Ganin, A. A., Quach, P., Panwar, P., Collier, Z. A., Keisler J. M., Marchese, D., Linkov, I., (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management, Special Issue:Engineering Systems and Risk Analytics, Vol. 40. str. 183-199. Izvor: https://doi.org/10.1111/risa.12891

30. Goedeker, M., A. (2014). "Cyber Security: Future IT-Security Challenges for Tomorrow's Leaders and Businesses." In Impact of Emerging Digital Technologies on Leadership in Global Business, str. 235-254.

31. Hann, K. (2019). Cybersecurity: Where Are We, and What More Can Be Done? The CPA Journal, Izvor: https://www.cpajournal.com/2019/09/16/cybersecurity-where-are-we-and-what-more-can-be-done/ (pristupljeno 30.5.2024.)

32. Hartmann, C. C., Carmenate, J. (2021). Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. Current Issues in Auditing; 15 (2): A9–A23., izvor: https://doi.org/10.2308/CIIA-2020-034

33. IAASB, (2013). International Assurance and Auditing Standards Board, ISA 610 (REVISED 2013), USING THE WORK OF INTERNAL AUDITORS, Standards and Pronouncements 978-1-60815-149-3.

34. Ilollari, O., Islami, M. (2017). Auditing as a way to increase cyber security, ECONOMICUS 15/2017, Izvor: https://uet.edu.al/economicus/wp-content/uploads/2022/01/economicus-15_5.pdf

35. Institute of Internal Auditors (IIA) (2024) Corporate Governance. The Institute of Internal Auditors Homepage. https://Na.theiia.org (pristupljeno 23.5.2024.)

36. Institute of Singapore Chartered Accountants-ISCA, (2018). Cybersecurity Risk Considerations in a Financial Statements Audit, izvor: https://isca.org.sg/docs/default-source/default-document-library/tech/isca-cyber-security-risk-report.pdf?sfvrsn=95ecfe5f_0

37. International Organization for Standardization, (2015). Quality management systems — Requirements, (ISO Standard No. 9001:2015), izor: https://www.iso.org/standard/62085.html

38. International Organization for Standardization, (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks, (ISO/IEC 27005:2022). Izvor: https://www.iso.org/standard/80585.html

39. International Organization for Standardization, (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements, (ISO/IEC 27001:2022), izvor: https://www.iso.org/standard/27001

40. ISA 500. (2009). International Standard on Auditing (ISA) 500, Audit Evidence, izvor: https://www.ifac.org/_flysystem/azureprivate/publications/files/A023%202012%20IAASB%20Handbook%20ISA%20500.pdf

41. ISACA, (2010). Monitoring Internal Control Systems and IT: A Primer for Business Executives, Managers and Auditors on How to Embrace and Advance Best Practices, ISBN 978-1-60420-110-9.

42. ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives, Information Systems Audit and Control Association, ISBN: 1604207280, 9781604207286

43. ISOCO, (2016). Cyber Security in Securities Markets: An International Perspective, The Board of the International Organization of Securities Commissions izvor: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

44. Jensen, M. C. i Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs, and ownership structure. Journal of financial economics, 3(4), 305-360

45. Jun Lin, Z., Xiao, J.Z., Tang, Q. (2008), "The roles, responsibilities and characteristics of audit committee in China", Accounting, Auditing & Accountability Journal, Vol. 21 No. 5, str. 721-751. Izvor: https://doi.org/10.1108/09513570810872987

46. Jurišić, M., Čular, M., (2022). Kibernetička sigurnost i revizija, Računovodstvo i financije, 11/2022., str. 66-67. Stručni članak UDK 657.6.

47. Kahyaoglu, B. S., i Caliyurt, K. (2018), "Cyber security assurance process from the internal audit perspective", Managerial Auditing Journal, Vol. 33 No. 4, str. 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

48. Kamiya, S., et al. (2018). What is the Impact of Successful Cyberattacks on Target Firms? Working Paper series: no. w24409, National Bureau of Economic Research, NBER, Cambridge, izvor: https://www.nber.org/papers/w24409

49. Kickenweiz, B., Sedlock, G., Daum, J. H. (2016). Technology in the boardroom: Five things directors should be thinking about. SpencerStuart., Izvor: https://www.spencerstuart.com/research-and-insight/technology-in-the-boardroom-five-things-directors-should-be-thinking-about (pristupljeno: 9 .5. 2024.)

50. Kohnke, A., Shoemaker, D., Sigler, K. E., (2016). The Complete Guide to Cybersecurity Risks and Controls, Auerbach Publications, ISBN: 9781498740579

51. Kumar, R., Goyal, R. (2019) On cloud security requirements, threats, vulnerabilities and countermeasures: A survey, Computer Science Review, Volume 33, str. 1-48, https://doi.org/10.1016/j.cosrev.2019.05.002

52. Kumhar, M., Kansagra, D., Jha, D. (2016). Ransomware: A Threat to Cyber security. International Journal of Computer Science & Communication. 7. str. 224-227.

53. Međunarodni odbor za standarde revidiranja (IAASB), (2019). Međunarodni revizijski standard 315 (izmijenjen 2019), Identificiranje i procjenjivanje rizika značajnih pogrešnih prikazivanja, Izvor: https://www.iaasb.org/publications/mrevs-315-izmijenjen-2019-identificiranje-i-procjenjivanje-rizika-znacajnih-pogresnih-prikazivanja

54. Mitra, S., Hossain, M. and Deis, D. R. (2007). The Empirical Relationship between Ownership Characteristics and Audit Fees, Rev Quant Finance Acc., Vol. 28, str. 257-285.

55. Obeid, S. i Al-zeaud, H. (2012). MANAGEMENT SUPPORT AND ITS IMPACT ON PERFORMANCE OF INTERNAL AUDITORS AT JORDANIAN PUBLIC INDUSTRIAL SHAREHOLDING COMPANIES. Global Journal of International Business Research. 5.

56. PCAOB, (2016). Staff Inspection Brief. Public Company Accounting Oversight Board, Division of Registration and Inspections, Washington D.C., izvor: https://pcaobus.org/Inspections/Documents/Inspection-Brief-2016-3-Issuers.pdf

57. Pfleeger, S., Sasse, M. & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. Journal of Homeland Security and Emergency Management, 11(4), str. 489-510. https://doi.org/10.1515/jhsem-2014-0035

58. Pinto, J., Pereira, A. C., Imoniana, J. O., Peters, M. R. (2013). Role of internal audit in managerial practice in organisations. African Journal of Business Management. DOI:10.5748/9788599693094-10CONTECSI/PS-209.

59. PwC (2020), Global Economic Crime and Fraud Survey, Izvor: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey-2020.html (pristupljeno: 1. 12. 2023.)

60. Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC Text with EEA relevance. (2014). Official Journal, L 158, str. 77-112., izvor: http://data.europa.eu/eli/reg/2014/537/oj

61. Russo, P., Caponi A., Leuti, M., Bianchi G. (2019). A Web Platform for Integrated Vulnerability Assessment and Cyber Risk Management. Information. 10(7):242. https://doi.org/10.3390/info10070242

62. Sabillon, R. (2021). Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM. 10.4018/978-1-7998-4162-3.

63. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2018). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017 (Vol. 2017-November, pp. 253-259). Institute of Electrical and Electronics Engineers Inc., Izvor: https://doi.org/10.1109/INCISCOS.2017.20

64. Sabilon, R. (2022). The CyberSecurity Audit Model (CSAM), Research Anthology on Business Aspects of Cybersecurity, str. 77-139. DOI: 10.4018/978-1-6684-3698-1.ch005

65. Saleem, A., Okur, S., Zraqat, O. (2019). The Effect of Internal Audit Quality (IAQ) on Enterprise Risk Management (ERM) in Accordance to COSO Framework. 10.13140/RG.2.2.22520.08962.

66. Salih, I. J., Flayyih, H. H. (2020). Impact of Audit Quality in Reducing External Audit Profession Risks, International Journal of Innovation, Creativity and Change, Vol. 13, (7), str. 176-199.

67. Salleh, Z., Stewart, J., Manson, S. (2006). The Impact of Board Composition and Ethnicity on Audit Quality: Evidence from Malaysian Companies, Malaysian Accounting Review, 5, str. 61-83.

68. Sánchez-García, I. D., Mejía, J., San Feliu Gilabert, T. (2023). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. Applied Sciences. 13(1):395. izvor: https://doi.org/10.3390/app13010395

69. Savčuk, O. (2007). Internal Audit Efficiency Evaluation Principles, Journal of Business Economics and Management, 8(4), str. 275-284 DOI: 10.3846/16111699.2007.9636180

70. Sawan, N., Alsaqqa, I. (2012). Audit firm size and quality: Does audit firm size influence audit quality in the Libyan oil industry? African Journal of Business Management Vol. 7(3), str. 213-226.

71. SEC, (2014). Cybersecurity Roundtable. Securities and Exchange Commission, Washington D.C., Izvor: https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml

72. SEVOI GRUPACIJA, (2019, 2. veljače). COSO okvir u Republici Hrvatskoj, SEVOI Hrvatska, Izvor: https://sevoi.eu/sevoi-hrvatska/coso-okvir-u-republici-hrvatskoj/ (pristupljeno: 23.5.2024.)

73. Shah, Y., Sengupta, S. (2020). A survey on Classification of Cyber-attacks on IoT and IIoT devices. 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 0406-0413.

74. Shamki, D., i Alhajri, T.A. (2017). Factors Influence Internal Audit Effectiveness. International Journal of Biometrics, 12, 143.

75. Slapničar, S., Vuko, T., Čular, M., Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems. 44.10.1016/j.accinf.2021.100548.

76. Soyemi, K. A., Sanyaolu, W. A., Salawu, R. O. (2019). Corporate governance practices and external auditors' reporting lag in Nigeria. In: Accounting and taxation review 3 (4), Str. 15 - 31. Izvor: http://hdl.handle.net/11159/4444

77. Središnji državni ured za razvoj digitalnog društva, Kibernetička sigurnost, izvor: https://rdd.gov.hr/kiberneticka-si-gurnost-1436/1436 (pristupljeno: 3. 11. 2023.)

78. Srivastava, A. Thomson, S. B., (2008). Framework analysis: A qualitative methodology for applied policy research.

79. Stafford, T., Deitz, G. and Li, Y. (2018). "The role of internal audit and user training in information security policy compliance", Managerial Auditing Journal, Vol. 33 No. 4, str. 410-424., izvor: https://doi.org/10.1108/MAJ-07-2017-1596

80. Steinbart, P., J., Raschke, R., L., Gal, G., Dilla, W., N.,(2012). The relationship between internal audit and information security: An exploratory investigation, International Journal of Accounting Information Systems, Volume 13, Issue 3, pp. 228-243, izvor: https://doi.org/10.1016/j.accinf.2012.06.007

81. Svanberg, J., Öhman, P. (2019). Auditors issue contingency of reduced audit quality acts: perceptions of managers and partners, International Journal of Accounting, Auditing and Performance Evaluation, Vol. 15, No. 1, str. 57–88

82. Teddlie, C. Tashakkori, A., (2003). Major issues and controveries inthe use of mixed methods in the social and behvioral sciences. Handbook of mixed methods in social & behavioral research, str. 3-50.

83. Terry, J. E., Gilbert, W. J., (2001). Use of control self-assessment in audits, The CPA Journal; New York Vol. 71, Iss. 8, str. 46-49.

84. Tick, A., Ngo, T. N. B., (2021), Interdisciplinary Description of Complex Systems 19(3), str. 375-390, izvor: https://hrcak.srce.hr/file/382392

85. Uma, M. i Padmavathi, G. (2013). A survey on various cyber attacks and their classification. International Journal of Network Security. 15. str. 391 - 397.

86. US National Institute of Standards and Technology (NIST), (2018). standards: Framework for Improving Critical Infrastructure Cybersecurity V1.1. izvor: https://www.nist.gov/

87. Venugopal, P. A., Saat, M. M., & Mohamed, N. N. N. (2024). Internal Audit's Impact on Malaysian Banking: Conceptual Framework with Management Support as a Moderator. International Journal of Academic Research in Business and Social Sciences, 14(1), 1206–1216.

88. Yatim, P., Kent, P., i Clarkson, P. (2006). Governance Structures, Ethnicity, and Audit Fees of Malaysian Listed Firms, Managerial Auditing Journal 21(7), DOI:10.1108/02686900610680530.

89. Yen, J. C., Lim, J. H., Wang, T., Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches, Journal of Accounting and Public Policy, Vol. 37, Issue 6, str. 489-507. https://doi.org/10.1016/j.jaccpubpol.2018.10.002

90. Zanani, W., Abdullah, W., Shahnaz, I. & Nurasyikin, J. (2008). The impact of board composition, ownership and ceo duality on audit quality: The malaysian evidence. Malasyan Accounting Review, Vol. 7, No. 2.

91. Zelenika, R. (2000), Metodologija i tehnologija izrade znanstvenog i stručnog djela. Ekonomski fakultet Sveučilišta u Rijeci.

## SAŽETAK

Cilj rada je utvrditi što je kibernetička sigurnosti i koje su uloge interne i eksterne revizije, te revizijskih odbora. Istraživanjem se želi podići svijest o kibernetičkim rizicima, opasnostima koje predstavljaju i posljedicama na organizacije, pojedince i društvo u cjelini. Kibernetička zaštita provodi se nad svim procesima i segmentima organizacije zaštitom podataka i mrežnih infrastruktura s pomoću zaključavanja i šifriranja računala i podacima na njima, korištenjem i redovitim ažuriranjem antivirusnih programa, kao i izradama kopija sustava odvojeno od pristupa serverima. Uloga interne revizije je upravljanje rizicima i uspostavljanje funkcionalnog sustava internih kontrola i usklađenost s politikama i standardima u suradnji s menadžmentom i potporom revizijskog odbora. Eksterni revizori imaju odgovornosti u procjeni sustava internih kontrola i identifikaciji kibernetičkih rizika koje mogu narušiti vjerodostojnost financijskih izvještaja. Revizijski odbori služe kao potpora internim revizorima osiguravajući potrebne resurse i nadziranjem procesa internih kontrola. U pogledu na eksternu reviziju, sudjeluju u odabiru revizorskog društva, te prate neovisnost revizora u procesima eksterne revizije.

Ključne riječi: Kibernetička sigurnost, revizija, revizijski odbor

## SUMMARY

The work aims is to determine what cyber security is and what are the roles of internal and external audits and audit committees. The research aims to raise awareness of cyber risks, the dangers they represent and the consequences for organizations, individuals and society as a whole. Cyber protection is carried out over all processes and segments of the data protection organization and network infrastructure by locking and encrypting computers and data on them, using and regularly updating antivirus programs, as well as creating copies of the system separately from access to servers. The role of internal audit is to manage risks and establish a functional system of internal control and compliance with policies and standards in cooperation with management and the support of the audit committee. External auditors are responsible for assessing the system of internal controls and identifying cyber risks that may undermine the credibility of financial statements. Audit committees serve to support internal auditors by providing the necessary resources and overseeing the internal control process. Regarding the external audit, they participate selecting the audit company, and monitor the auditor's independence in the external audit processes.

Key words: cyber security, audit, audit committee

## PRILOZI

Slika1. Rast globalne potrošnje u kibernetičkoj sigurnosti ..... 8
Slika 2. Institut internih revizora: model 3 linije ..... 11

PITANJA ZA INTERVJU:

INTERNA REVIZIJA:

1. Opišite ukratko temeljne odgovornosti internog revizora u kibernetičkoj sigurnosti, te na koji način surađujete s IT službom u procjeni rizika od kibernetičkih napada?

2. S pomoću kojih alata procjenjujete rizike, te na koji način provjeravate učinkovitost sustava obrane, odnosno usklađenje s politikama i kontrolama povezanih s kibernetičkom sigurnosti?

3. Na koji način interni revizori surađuju s eksternim revizorima, te kako eksterni revizori mogu pomoći u kibernetičkoj obrani?

4. Kako se u vašoj organizaciji ocjenjuje uspješnost rada interne revizije, te na koji način revizijski odbori služe kao podrška internim kontrolama u obrani od kibernetičkih napada?

5. Koji su najveći izazovi i prijetnje u budućnosti za internu reviziju u pogledu kibernetičke sigurnosti?

EKSTERNA REVIZIJA

1. Koje su glavne odgovornosti funkcije eksterne revizije u kontekstu kibernetičke sigurnosti, te na koji način se razlikuje od interne revizije?

2. Kako procjenjujete rizike vezane za kibernetičku sigurnost, te kako procjenjujete usklađenost s politikama i procedurama, kao i učinkovitost sustava internih kontrola?

3. Na koji način surađujete s internim revizorima, te koje su glavne karakteristike internih kontrola pri procjeni spremnosti organizacije na kibernetičke napade?

4. Koliko komunicirate s revizijskim odborom, te kako oni mogu doprinijeti kvaliteti procesa revizije?

5. Koje su preporuke koje najčešće dajete organizacijama za poboljšanje sustava obrane od kibernetičkih napada?

REVIZIJSKI ODBOR

1. Koja je uloga revizijskog odbora u zaštiti i razvoju organizacije u kibernetičkoj sigurnosti?

2. Kako revizijski odbor sudjeluje u izradi strategije i procedura kibernetičke sigurnosti, te na koji način prati provođenje tih strategija?

3. Kako revizijski odbor postupa prilikom kibernetičke provale ili incidenta?

4. Na koji način revizijski odbor služi kao podrška internoj reviziji, te koliko često komunicira s eksternom revizijom u vezi s kibernetičkoj sigurnosti?

5. Kada revizijski odbor izvještava upravu o stanju internih kontrola, te koje informacije su ključne za informiranje o kibernetičkoj sigurnosti?