https://doi.org/ 10.7251/EMC2002514T
UDK: 004.056.5:343.533(497.6)
Datum prijema rada: 30. avgust 2020.
Submission Date: August 30, 2020
Datum prihvatanja rada: 04. decembar 2020.
Acceptance Date: December 04, 2020
Časopis za ekonomiju i tržišne komunikacije
Economy and Market Communication Review
Godina/Vol. **X** • Br./No. **II**
str./pp. 514-529

PREGLEDNI NAUČNI RAD / OVERVIEW SCIENTIFIC PAPER

ULOGA INTERNE REVIZIJE U BORBI PROTIV KOMPJUTERSKOG KRIMINALA

Zdravko Todorović | Redovni profesor; Ekonomski fakultet Univerziteta u Banjoj Luci; zdravko.todorovic@ef.unibl.org
Boris Todorović | Docent; Axelyos, d.o.o., Banja Luka; boris.todorovic@gmail.com
Darko Tomaš | Docent; Ekonomski fakultet Univerziteta u Banjoj Luci, darko.tomas@ef.unibl.org

Apstrakt: *Kompjuterski kriminal je u porastu. Kompjuterski kriminal je kriminal koji je usmjeren protiv bezbjednosti informacionih sistema preduzeća, u namjeri da se sebi ili drugima pribavi određena korist ili da se drugome nanese šteta. Oblici kompjuterskog kriminala su krađe, utaje, pronevjere, ili korištenje informacija za protiv pravno prisvajanje koristi. U radu će se predstaviti podaci o kompjuterskom kriminalu kod nas i u svijetu, te pokazati trendovi povećanja kompjuterskog kriminala i najčešći oblici kompjuterskog kriminala. Prema međunarodnim standardima za stručno provođenje interne revizije daje se ovlaštenje internim revizorima za borbu protiv prevara, što podrazumjeva i ovlaštenje za borbu protiv kompjuterskog kriminala. Cilj rada je pronaći model organizovanja interne revizije u borbi protiv kompjuterskog kriminala. Radi toga je potrebno utvrditi: standarde interne revizije kojih se organizacija mora pridržavati u borbi protiv kompjuterskog kriminala, utvrditi sigurnosne zahtjeve za standarde, utvrditi ciljeve, rizike i sigurnosnu politiku u organizaciji, podići svjest zaposlenih o opasnosti od ciber kriminala, uključiti top menadžment u borbi protiv kompjuterskog kriminala, sprovesti obuku zaposlenih o bezjednosti podataka i slično. Interni revizori trebali bi razumjeti utjecaj cyber prijetnji na organizaciju. Model za borbu protiv kompjuterskog kriminala zasnivaće se na COSO (The Committee of Sponsoring Organizations of the Treadway Commission's) integralnom okviru za internu reviziju, a obuhvata pet cjelina i to: 1) kreiranje kontrolnog okruženja za borbu protiv kompjuterskog kriminala, 2) procjena rizika od kompjuterskog kriminala, 3) projektovanje i provođenje aktivnosti u borbi protiv kompjuterskog kriminala, 4) informacije i komunikacije o kompjuterskom kriminalu i 5) praćenje aktivnosti borbe protiv kompjuterskog kriminala. Rezultati istraživanje pokazaće nove naučne činjenice i saznanja o načinima borbe protiv kompjuterskog kriminala u svijetu. Praktičnu korist od rezultata istraživanja imaće menadžeri i interni revizori u kreiranju i provođenju programa za borbu protiv kompjuterskog kriminala.*

Rad je izložen na X međunarodnoj naučnoj konferenciji EDASOL 2020 / *The paper was presented at the X International Scientific Conference EDASOL 2020*

Ključne riječi: *kompjuterski kriminal, interna revizija, COSO okvir, borba protiv kompjuteskog kriminala*

JEL klasifikacija: *M15, M21, M42*

UVOD

Društveni i ekonomski razvoj u posljednjim decenijama je vezan za razvoj informacionih tehnologija. Ta povezanost pored pozitivnih rezultata nosi i značajne prijetnje i rizike od zloupotreba. Kompjuterski kriminal je prisutan od samog početka upotrebe računara i računarske opreme. Kompjuterski kriminal je oblik kriminalnog ponašanja, kod koga se računarske mreže pojavljuju kao sredstvo izvršenja kriminalnog djela (Thomas Stafford, 2018). Na početku, takvo kriminalno ponašanje je bilo beznačajno. Riječ je o kriminalnom djelu koje, uglavnom, obavljaju pojedinci, ali u nekim slučajevima i same organizacije. Takvo kriminalno ponašanje ima za posljedicu neovlašćen pristup povjerljivim informacijama kao i njihovo nedozvoljeno objavljivanje (Mohd Aizuddin Zainal Abidin, 2019). Kompjuterski kriminal danas je postao najveća prijetnja svakoj organizaciji (Cross, 2020) i jedan od navećih izazova sa kojima će se suočiti čovječanstvo u narednom periodu (Md. Shariful Islam, 2018).

Štete zbog kompjuterskog kriminala koštat će svijet 6 biliona američkih dolara godišnje do 2021. godine (Steve Morgan, 2019). Cybersecurity Ventures u svom izvještaju iz 2017. godine predviđa da će do 2022. godine biti 6 milijardi korisnika Interneta, a do 2030. godine 7,5 milijardi korisnika Interneta. Potrošnja za cyber bezbjednost iznosila je 114 milijarde dolara USD u 2018. godini, a za 2019. godinu iznosila je 124 milijarde USD. Cybersecurity Ventures predviđa da će organizacije globalno doživjeti napad na svoj softver svakih 11 sekundi do 2021. godine. Predviđanja su da će do 2021. godine biti nedostatak od 3,5 miliona radnih mjesta na poslovima bezbjednosti komputerskih sistema. Potrošnja na globalnom nivou za kompjutersku bezbjednost kumulativno za razdoblje od 2017. do 2021. godine procjenuje se na 1 bilion USD.

Rukovodstvo organizacije mora biti svjesno rizika i troškova prouzrokovanih kompjuterskim kriminalom (Thomas Stafford, 2018), mora biti upoznato o mogućim počiniocima kompjuterskog kriminala, motivima činjenja i načinima kako se zaštiti od kompjuterskog kriminala.

Cilj istraživanja je opisati kompjuterski kriminal, predstaviti troškove prouzrokovane kompjuterskim kriminalom, istaći značaj uspostavljanja cyber bezbjed-

nosti, te opisati ulogu interne revizije u borbi protiv kompjuterskog kriminala. Predložićemo osnove modela organizovanja interne revizije u cilju uspješnije borbe protiv kompjuterskog kriminala.

U radu smo krenuli od pretpostavke da će se uspostavljanjem modela za borbu protiv kompjuterskog kriminala u internoj reviziji, kao jednoj od linija odbrane od kompjuterskog kriminala, u skladu sa COSO okvirom, moći efikasnije upravljati sa rizicima od kompjuterskog kriminala, što će dovesti do smanjenja troškova prouzrokovanih kompjuterskim kriminalom.

TEORIJSKI ASPEKTI ISTRAŽIVANJA

Kompjuterski kriminal

Pojam „cyber" prvo se pojavio u vojnoj terminologiji, u smislu predviđanja budućih oblika ratovanja. „Cyberwar" predstavlja ratovanje znanjem, odnosno informacijama. Radi se o ratu visoke tehnologije, koji se odnosi na prikupljanje povjerljivih informacija. Pojam cyber crime ili kompjuterski kriminal se može definisati kao oblik kriminalnog ponašanja za čije izvršenje se koristi računarska oprema (Norman Mugarura, 2020). Lica koja obavljaju takve kriminalne radnje su kompjuterski kriminalci (Naci Akdemir, 2020).

Jedan od autora koji je razmatrao problem kompjuterskog kriminala jeste Peter Enderwick. Njegov zaključak je da je: „zloupotreba kompjutera svaki događaj u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac djeluje u namjeri da sebi pribavi ili bi mogao da pribavi korist."

Svjetski rečnik engleskog jezika ovaj pojam određuje na sljedeći način: „Kompjuterski kriminal obuhvata nezakonite aktivnosti koje se vrše na kompjuteru ili kod kojih je kompjuter sredstvo izvršenja. On obuhvata kriminalni upad u drugi kompjuterski sistem, krađu kompjuterskih podataka, ili korišćenja on-line sistema za vršenje ili pomoć u izvršenju prevara."

Opasnost od kompjuterskog kriminala po društvenu zajednicu ogleda se ne samo u ekspanziji njegovih pojavnih oblika, već i u tome što pojedina tradicionalna krivična dela, kao što su prevara, zloupotreba službenog položaja, pronevjera,... itd, korišćenjem kompjuterske tehnologije dobijaju znatno opasnije oblike (Bayraktar, (2017).

Bosna i Hercegovina je 25.05.2006. godine ratifikovala Konvenciju o kompjuterskom kriminalu, koju su 2001. godine donijele članice Vijeća Evrope, a koja naglašava potrebu da se vodi zajednička kaznena politika usmjerena prema zaštiti društva od kompjuterskog kriminala, naročito putem usvajanja odgovarajućeg zakonodavstva i poboljšanja međunarodne saradnje.

Evropska konvencija o kompjuterskom kriminalu predviđa četiri grupe djela i to: djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema (nezakoniti pristup, presretanje, uplitanje u podatke, korištenje uređaja, programa), djela vezana za kompjutere (falsifikovanje i krađe), djela vezana za sadržaje (najčešće se javlja u obliku dječije pornografije, a obuhvata posjedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim ovih materijala), djela vezana za kršenje autorskih prava.

Kompjuterski kriminala se može podjeliti na: **politički** (cyber spijunaža, haking, cyber sabotaža, cyber terorizam, cyber ratovanje), **ekonomski** (cyber prevare, haking, krađa internet usluga i vremena, piratstvo softvera, mikročipovanje i baza podataka, cyber industrijska spijunaža, lažne internet aukcije), **proizvodnja i distribucija nedozvoljenih i štetnih sadržaja** (dječija pornografija, pedofilija, vjerske sekte, širenje rasističkih i nacionalističkih ideja i stavova, zloupotreba žena i djece, trgovina ljudskim organima, oružjem i drogom) i **povrede cyber privatnosti** (nadgledanje elektronske pošte, spam, prisluškivanje i snimanje).

Predmet našeg istraživanja je ekonomski aspekt kompjuterskog kriminala.

Cyber napade izvode profesionalni kriminalci, koji kradu milione i koji žele pristup računarima, brojevima kreditnih kartica i slično. Cyber kriminalci „vrebaju“ iza svojih monitora i teško je dokazati ko je, u stvari, osoba koja pokreće sav taj haos u virtualnom svijetu. Na mrežama je teško odrediti ko vam ne misli dobro. Glavni cilj cyber kriminalca je da ostane anoniman i da izbriše svaki trag, koji bi otkrio njegov identitet i lokaciju.

Krivična djela iz oblasti kompjuterskog kriminala u ekonomiji regulisana su Krivičnim zakonom Bosne i Hercegovine i Krivičnim zakonom Republike Srpske. Krivičnim zakonom BiH navedena su krivična djela protiv sistema elektronske obrade podatka, a koja se odnose na: oštećenje računarskih podataka i programa, računarsko krivotvorenje, računarska prevara, ometanja rada sistema i mreže elektronske obrade podataka, neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka i računarska sabotaža.

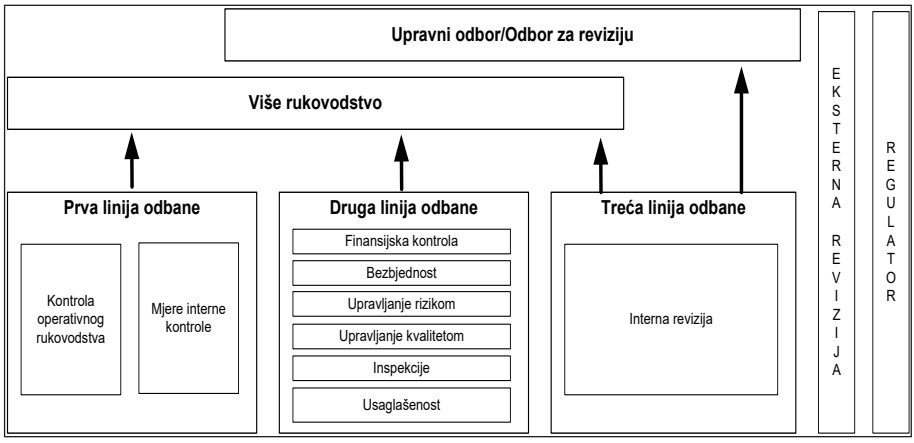
Kompjuterski kriminal svakim danom sve više raste i stvara ogroman problem pojedincima i državi (Manning, 2018). Zemlje u razvoju su posebna meta hakera ili cyber kriminalaca. Kompjuterski kriminal danas pravi veću štetu nego trgovina drogama.

Uloga interne revizije u borbi protiv kompjuterskog kriminala

Model "tri linije odbrane" (The Institute of Internal, 2013) obezbjeđuje jednostavan i efikasan način za upravljanje rizicima, među kojima su i rizici od kompjuterskog kriminala. Različite nadležnosti po pitanju upravljanja i kontrole rizika dodjeljeni su različitim odjeljenjima i sektorima u organizaciji i potrebno je da se koordinisano provode u cilju efektivnog i efikasnog upravljanja rizicima.

Prema modelu "tri linije odbrane" u prvoj liniji odbrane su *operativno rukvodstvo* koje je odgovorno za provođenje konkretnih korektivnih mjera za otklanjanje učenih nedostataka u funkcionisanju procesa i kontrola. U drugu liniju odbrane uključene su *funkcije u organizaciji* koje služe za nadgledanje rizika kao što su: finansijska kontrola, bezbjednost, upravljanje rizikom, upravljanje kvalitetom i slično.

Slika 1. Tri linije odbrane za efektivni proces upravljanja rizikom i sistem interne kontrole



Izvor: (The Institute of Internal, 2013)

Interna revizija kao treća linija obrane u cilju poboljšanja cyber bezbjednosti treba preduzeti slijedeće aktivnosti (Sezer Bozkus Kahyaoglu, 2018):

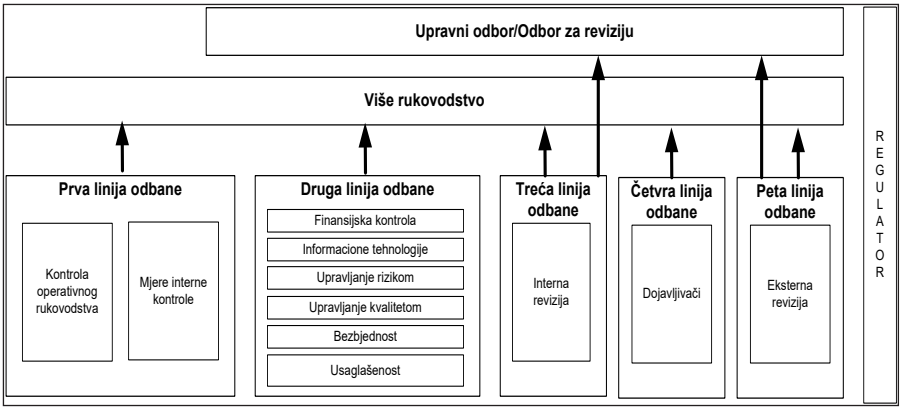
1. Raditi sa menadžmentom i upravnim odborom na razvoju strategije i politike cyber bezbjednosti.
2. Nastojati da organizaja postane efikasnija u poboljšanju sposobnosti da iden-

tifikuje, procjeni i ublaži rizik koji mogu uticati na cyber bezbjednost.
3. Prepoznati prijetnje prema cyber bezbjednost koje dolaze iz vana i od zaposlenih ili poslovnog partnera.
4. Dostavljati informacije upravnom odboru i odboru za reviziju u cilju povećanja svijesti i znanje o cyber prijetnjama i važnosti podizanja nivo cyber bezbjednosti na što viši nivo.
5. Insistirati da se rizici cyber bezbjednosti ugrade u plan interne revizije i da postanu dio plana upravljanja rizicima organizacije.
6. Predstaviti kako nove tehnologije i trendovi utiču na organizaciju, njegov profit, ali i na rizike od cyber kriminala.
7. Uspostaviti okvir za cyber bezbjednost prema NIST (Nacionalnom institutu za standarde i tehnologiju). Procijeniti program cyber bezbjednosti organizacije prema Okviru za cyber bezbjednost koje obuhvataju zahtjeva ISO 27000 koje se odnose na Sistem upravljanja bezbjednošću informacija.
8. U saradnji sa upravom organizacije raditi na podizanju cyber bezbjednosti na viši nivo, kombinujući ljudske i tehnološke potencijale (vještine, znanje, svijest, budnost i tehnološke alate).
9. Naglasiti da praćenje cyber bezbjednosti i pridržavanje jasnih protokola prilikom cyber incidenata predstavljaju prioritetni zadatak rukovodstva.
10. Obavjestiti rukovodstvo organizacije o nedostatku kadrovskih i ostalih resursa za provođenje interne revizije i upravljanja rizicima cyber bezbjednosti.

METODOLOGIJA

Ideju ”tri linije obrane” iskoristićemo da uspostavima efikasan model za upravljanje rizicima od kompjuterskog kriminala, tako da ćemo ga proširiti u model ”osam linija odbrane”.

Slika 2. Model pet linija odbrane od kompjuterskog kriminala



Izvor: (The Institute of Internal, 2013) i dopuna autora

Odbrana od kompjuterskog kriminala zavisi od efikasnosti uspostavljenog sistema odbrana u organizaciji, a može se napisati kao:
OKK= f (UO, VR, OR, SK, IR, D, ER, R)
OKK= Odbrana od kompjuterskog kriminala
UO = Odgovornost upravnog odbora
VŠ = Odgovornost višeg rukovodstva
OR = Odgovornost operativnog rukovodstva i interne kontrole
SK = Odgovornost ostalih kontrolnih službi u organizaciji, posebno službe za bezbjednost informacionih sistema (CISO)
IR = Interna revizija
D = Dojavljivači
E = Eksterne revizije
R = Regulator

Pošto je cilj našeg istraživanja analiziranje uloge interne revizije u sistemu odbrane od kompjuterskog kriminala posmatraćemo samo internu revizuju kao nezavisnu varijablu, a ostale varijable ćemo držati konstantnim. Prema tome možemo reći da efikasnost odbrana od kompjuterskog kriminala zavisi i od dobro uspostavljenog programa interne revizije za borbu protiv kompjuterskog kriminala.

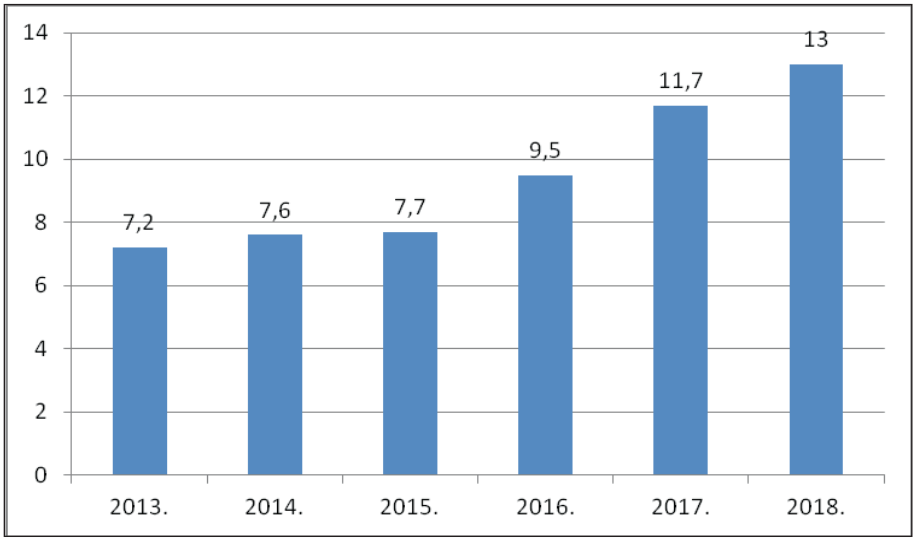
REZULTATI ISTRAŽIVANJA

Troškovi prouzrokovani kompjuterskim kriminalom su različiti po pojedinim zemljama, a zavise od brojnih faktora među kojima možemo nabrojati: strukturu i veličinu organizacija, vrstu industrije, vrstu cyber napada, efikasnosti odbram-

benih sistema od kompjuterskog kriminala i slično.

Finansijske posljedice cyber napada iz godine u godinu se povećavaju. Na Slici 3. predstavljeni su prosječni globalni troškovi kompjuterskog kriminala za period od pet godina izraženi u milionima američkih dolara.

Slika 3. Prosječni globalni troškovi kompjuterskog kriminala

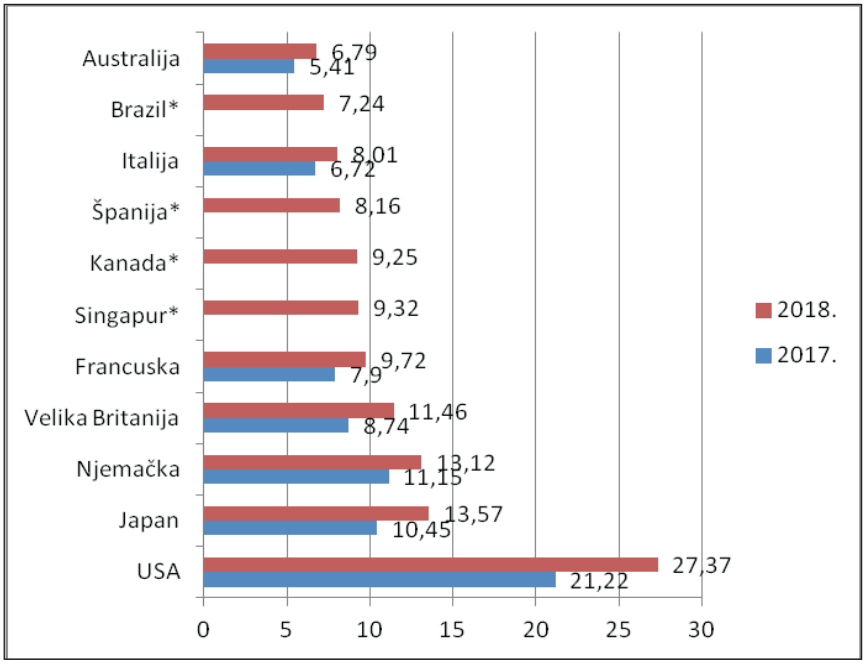


Izvor: (Kelly Bissell, Ryan M. Lasalle, Paolo Dal Cin, 2019)

Prosječni globalni troškovi kompjuterskog kriminala iznosili su 7,2 milijarde američkih dolara u 2013. godini, a 2018. godine iznosili su 13 milijardi američkih dolara, što predstavlja povećanje za 80 %.

Slika 4. prikazuje procijenjene prosječne troškove kompjuterskog kriminala za jedanaest zemalja, uključujući u periodu od dvije godine. Države sa oznakom zvjezdica imaju podatke samo za 2018. godinu. Firme iz SAD prikazuju najveći ukupni prosječni trošak za 2018. godinu u iznosu od 27,37 milion USD, a firme iz Australija najniža ukupna prosječni trošak od 6,79 milijuna USD.

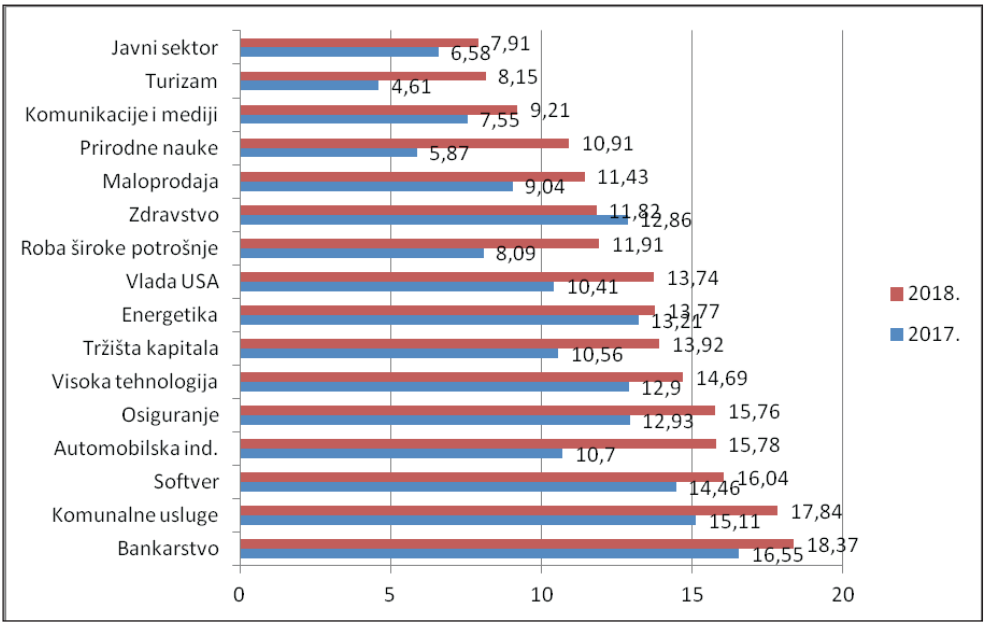
Slika 4. Procijenjeni prosječni troškovi kompjuterskog kriminala



Izvor: (Kelly Bissell, Ryan M. Lasalle, Paolo Dal Cin, 2019)

Prosječni godišnji troškovi kompjuterskog kriminala variraju po segmentima industrije. U radu su poređeni procijenjeni troškovi prouzrokovani kompjuterskim kriminalom za 16 različitih industrijskih sektora. Kao što je prikazano na slici 5., troškovi kompjuterskog kriminala za kompanije u bankarstvu imaju najveći godišnji trošak od 16,55 miliona USD. Nasuprot tome, kompanije iz oblasti javnog sektora u prosjeku su imale najniže troškove.

Slika 5. Prosječni godišnji troškovi kompjuterskog kriminala po segmentima industrije



Izvor: (Kelly Bissell, Ryan M. Lasalle, Paolo Dal Cin, 2019)

Interna revizija ima ključnu ulogu u pružanju pomoći organizacijama u borbi protiv cyber pretnji, kako kroz nezavisnu procjenu postojećih i potrebnih kontrola, tako i pomažući odboru za reviziju i upravnom odboru u uspostavljanju sistema za borbu protiv kompjuterskog kriminala.

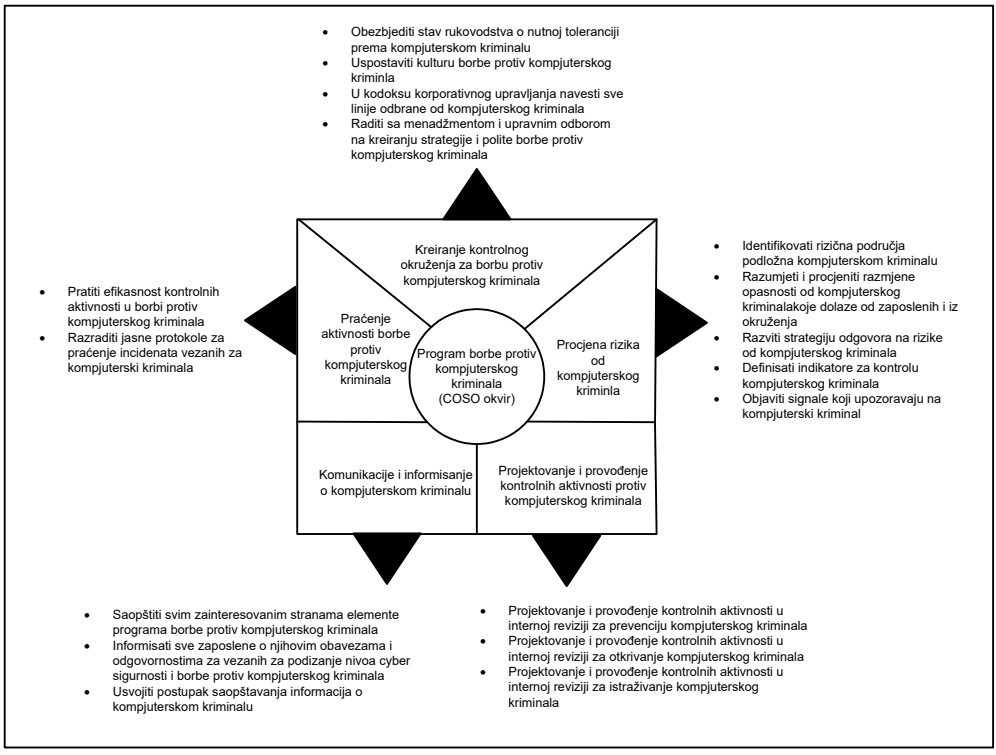
Interna revizija u borbi protiv kompjuterskog kriminala mora razmotriti slijedeća pitanja (Britz 2004):

- Da li organizacija ima strategiju cyber bezbjednosti?
- Da li organizacija obavlja godišnju provjeru strategije cyber bezbednosti?
- Da li interna revizija ima odgovarajuće resurse i osoblje za povođenje revizije kontrole kompjuterskog kriminala?
- Da li organizacija ima protokole u slučaju cyber incidenta?
- Da li je organizacija provodi kontinuiranu obuku na svim nivoima u cilju borbe protiv komputerkog kriminala?
- Da li organizacija ima planove i strategije za poboljšanje upravljanja rizicima u oblasti cyber bezbednosti?
- Da li je organizacija identifikovala povjeriljive podatke koje je potrebno staviti pod zaštitu?

- Da li je organizacija procjenila potencijalne izvore cyber napada i razvila strategiju borbe u slučaju napada?
- Da li organizaja poštuje propisane standarde i propise iz oblasti cyber bezbjednosti i da li postoji kontrola usaglašenosti?

U želji da istaknemo ulogu interne reviziju u borbi protiv kompjuterskog kriminala iskoristili smo COSO okvir i predložili program borbe interne revizije protiv kompjuterskog kriminala. Program ima pet elemenata i to: kreiranje kontrolnog okruženja za borbu protiv kompjuterskog kriminala, procjena rizika od kompjuterskog kriminala, projektovanje i provođenje kontrolnih aktivnosti protiv kompjuterskog kriminala, komunikacije i informisanje o kompjuterskom kriminalu i praćenje aktivnosti borbe protiv kompjuterskog kriminala.

Slika 6. COSO okvir i za organizovanje interne revizije za provođenja programa borbe protiv kompjuterskog kriminala

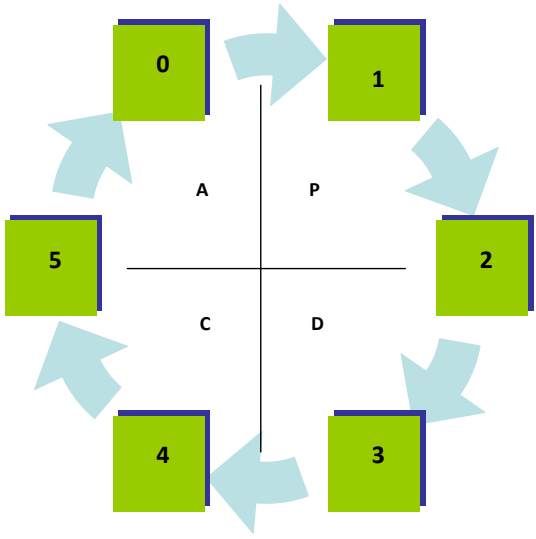


Izvor: (Laxman, 2014) i dopuna autora

Za svaki element programa u internoj reviziji za borbu protiv kompjuterskog kriminala definisani su pojedinačni kriteriji. Kod svakog pojedinačnog kriterija procjenjuje se nivo ispunjenosti zahtjeva.

Skala za procjenjivanje nivoa ispunjenosti zahtjeva se zasniva na Demingovom PDCA[1] krugu kvaliteta i predstavljena je na sljedeći način (Slika 8):
0 - nema dokaza ili postoje djelimični, nepouzdani dokazi ispunjenja zahtjeva (potpuno novo ili strano u organizaciji);
1 - Zahtjev je planiran – postoji samo na papiru – P (plan);
2 - Zahtjev je planiran i djelimično proveden – i na papiru i primjenjen – D (djelo);
3 - Zahtjev je planiran, proveden i prate se efekti – C (provjera);
4 - Zahtjev je planiran, proveden, prate se efekti i porede sa drugima – A (poređenje);
5 - Zahtjev je planiran, proveden, prate se efekti i uvode stalna prilagođavanja i poboljšanja na osnovu poređenja sa najboljima.

Slika 7. Demingov PDCA krug kvaliteta za procjenjivanje kriterija prevenciji i otkrivanja prevara



Izvor: autor

[1] PDCA (plan–do–check–act or plan–do–check–adjust) je interativni način upravljanja kroz četiri koraka koji se koristi za kontrolu i kontiuirano poboljšanje procesa i proizvoda. Poznat je pod nazivom Demingov krug kvaliteta.

DISKUSIJA

Kako su se mijenjala ovlaštenja i odgovornosti upravnog odbora i odbora za reviziju u organizaciji tako su se mijenjala ovlaštenja i odgovornosti interne revizije. U početku interna revizija je imala primarni zadatak reviziju finansijskog poslovanja, gdje je predmet posmatranja bila samo računovodstvena evidencija i informacije. Kasnije obuhvat interna revizije je proširen na poslovanje organizacije koje je usmjereno na ispitivanje svih poslovanih procesa. Savremena interna revizija obuhvata reviziju koja se odnosi na upravljanje ciljevima organizacije, upravljanje rizicima poslovanja, kontrolu korporativnog upravljanja, borbu protiv prevara, a u posljednje vrijeme i reviziju cyber bezbjednosti i borbu protiv kompjuterskog kriminala.

Rezultati provedih empirijskog istraživanja (Petros Lois, 2020)u svijetu pokazuje da se obuhvat interne revizije stalno proširuje i da danas možemo govoriti o savremenom pristupu internoj reviziji. Stepen razvoja interne revizije u našim preduzećima ne korespondira sa dostignutim stepenom razvoja te profesije u zemljama razvijene tržišne privrede. U prilog tome ide činjenica da je upravljačka revizija tek manjim dijelom zastupljena u pojedinačnim revizijama (Claudia Colicchia, 2018).

Istraživanja provedena u razvijenim zemljama Europske unije (EU) i svijeta, pokazuju da finansijske investicije i tehnološka dostignuća nisu dovoljni za stvaranje informacijskog društva te se sve razvijene zemlje posljednjih godina ubrzano i intenzivno okreću programima informacione bezbjednosti u svim segmentima državnog i privrednog sektora, ali i programima razvoja bezbjednosne kulture u najširima slojevima stanovništva.

Aktualne promjene u zakonodavstvu EU u posljednjih nekoliko godina, usmjerene su na razvoj bezbjednosne politike EU koja se odnosi na borbu protiv kompjuterskog kriminala.

Proces harmonizacije zakonodavstva Bosne i Hercegovine sa zakonodavstvom EU, vremenom će dovesti do usaglašenosti svih nacionalnih i entitetskih propisa sa zahtjevima EU, pa tako i u području informacione bezbjednosti u borbi protiv kompjuterskog kriminala.

U cilju stvaranja konkurentnosti privrede i privlačnosti zemlje za inostrane investitore, uspjeh u uspostavljanju informacione bezbjednosti i borbe protiv kompjuterskog kriminala može biti ključni faktor.

ZAKLJUČAK

Sasvim je jasno da se određenoj pojavi društvo adekvatno može suprotstaviti ukoliko sagleda sve njene karakteristike i uđe u sve pore njenih specifičnosti. S obzirom da su načini zloupotrebe kompjuterske tehnologije svakim danom sve savršeniji i komplikovaniji za otkrivanje i da je vrlo teško ići u korak sa tim kriminalnim aktivnostima, potrebno je sistemski pristupiti borbi protiv kompjuterskog kriminala. Programi borbe protiv kompjuterskog kriminala moraju uvažavati zakonsku regulativu, standarde cyber bezbjednosti i uspostaviti sve neophodne linije odbrane. Ohrabruje činjenica da su mnoge države postale svjesne ove pojave i da su u svom pozitivnom krivičnom zakonodavstvu predvidjele pojavne oblike kompjuterskog kriminala kao posebna krivična dijela. Sa druge strane, ohrabrujuće je i to što se u sve većem broju naučnih i stručnih radova pažnja posvećuje upravo ovom obliku kriminalnog ponašanja. Na taj način dolazi do razotkrivanja mnogih specifičnosti kompjuterskog kriminala, a istovremeno se otvara mogućnost suprotstavljanju njegovim oblicima od strane društvene zajednice. U radu smo razrađivali samo jedan aspekt odbrane, a koji se odnosi na internu reviziju. Iskoristili smo COSO okvir za organizovanje interne revizije za provođenja programa borbe protiv kompjuterskog kriminala. Uspješna borba protiv kompjuterskog kriminala podrazumjeva uspostavljenje jednog cjelovitog sistema borbe protiv kompjuterskog kriminala kojeg smo predstavili u dijelu koji se odnosi na metodologiju istraživanja.

LITERATURA

Bayraktar, D. K. (2017). The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime, 24*(2), 329-3446. doi: https://doi.org/10.1108/JFC-05-2016-0035

Claudia Colicchia, A. C. (2018). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal, 24*(2), 215-240. doi:https://doi.org/10.1108/SCM-09-2017-0289

Cross, C. (2020). Reflections on the reporting of fraud in Australia. *Policing: An Internationa lJournal, 43*(1), 49-61. doi:10.1108/PIJPSM-08-2019-0134

Enderwick, P. (2019). Understanding cross-border crime: the value of international business research. *Critical perspectives on critical perspectives on, 15*(2/3), 119-138. doi:10.1108/cpoib-01-2019-0006

Kelly Bissell, Ryan M. Lasalle, Paolo Dal Cin. (2019). *Cost of Cyber Crime Study.* Traverse City: Ponemon Institute LLC.

Laxman, S. (2014). The Fight Against Fraud. *Internal Auditor*, 1-8.

Manning, P. (2018). Behavioural economics and social economics: opportunities for an expanded curriculum. *International Journal of Social Economics*, 1-13. doi:10.1108/IJSE-05-2018-0250

Md. Shariful Islam, N. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, 1-34. doi:https://doi.org/10.1108/MAJ-07-2017-1595

Mohd Aizuddin Zainal Abidin, A. N. (2019). Customer data security and theft: a Malaysian organization's experience. *Information & Computer Security*, 1-21. doi:10.1108/ICS-04-2018-0043

Naci Akdemir, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Emerald Publishing*, 3. doi:10.1108/INTR-10-2019-0400

Norman Mugarura, E. S. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, 1-19. doi:10.1108/JMLC-11-2019-0092

Petros Lois, G. D. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business, 15*(2), 1-13. doi:10.1108/EMJB-07-2019-0097

Sezer Bozkus Kahyaoglu, K. C. (2018). Cyber security assurance process from the. *Managerial Auditing Journal, 33*(4), 360-376. doi:https://doi.org/10.1108/MAJ-02-2018-1804

Steve Morgan. (2019). *2019 Official Annual Cybercrime Report.* Toronto: Herjavec group.

The Institute of Internal. (2013). *IIA Position Paper: The three lines of defense in effective risck Management and control.* Florida: The Institute of Internal.

Thomas Stafford, G. D. (2018). "The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, 2-16. doi: https://doi.org/10.1108/MAJ-07-2017-1596

THE ROLE OF INTERNAL AUDIT IN THE FIGHT AGAINST CYBER CRIME

Zdravko Todorović

Full professor; Faculty of Economics, University of Banja Luka; zdravko.todorovic@ef.unibl.org

Boris Todorović

Assistant Professor, Axelyos, Banja Luka, boris.todorovic@gmail.com

Darko Tomaš

Assistant Professor, Faculty of Economics, University of Banja Luka, darko.tomas@ef.unibl.org

Summary: The internet is constantly changing the way we live and conduct business. Global business surroundings impose all organizations across to have a secure digital infrastructure for fighting against cybercrime. Cyber crime is on the raise in this decade. Cyber crime is a criminal activity that is focused against compromising security of information systems in

enterprises, in order to acquire certain profits, or to incur damage, theft or loss. Types of cyber crime include theft, evasion, or using information in order to unlawfully obtain profits from them. This paper will present certain information about cyber crime and most common types of it. According to international standards for internal audits, internal auditors are authorized for fight against fraud, which means authorization for fight against cyber crime. Main purpose of this paper is to find model for organizing internal audit for purpose of fighting cyber crime. Therefore, it is necessary to determine: internal audit standards that your organization must adhere to in fight against cybercrime, identify security requirements for standards, determine the goals, risks and security policy of the organization, raise employee awareness of the dangers of cybercrime, involve top management in the orbit against cybercrime, conduct employee training on data security and the like. Cyber security is basically about managing future risk, and requires insight into current and future vulnerabilities and how to prevent or reduce them, the likelihood of threats and costs associated with potential outcomes, and how to mitigate them. Internal auditors must be aware of impending regulatory changes based on IIA standards (The International Standards for the Professional Practice of Internal Auditing) related to computer security. Internal auditors should understand the impact of cyber threats on the organization. In particular, they should include this in their internal audit plan based on the risk of cybercrime. Internal auditors should have a strong partnership with the CIO (Chief Information Officer) and CISO (Chief Information Security Officer), for the sake of a trusted advisor in the fight against cybercrime. Internal auditors should provide an independent overview of the cyber security strategy. Modal will be based on COSO (The Committee of Sponsoring Organizations of the Treadway Commission's) **Internal Control — Integrated Framework** *and will feature five core principles: 1) creating control environment for fighting against cyber crime, 2) risk assessment for cyber crime, 3) projecting and implementing activities for fighting against cyber crime, and 5) monitoring activities. Research results will show new scientific facts and knowledge about methods for fighting cyber crime worldwide. Managers and internal auditors will have practical benefit from research results for implementing cyber crime prevention programs.*

Keywords: Cyber Crime, Internal Audit, COSO Framework, Combating Cyber Crime

The JEL Classification: M15, M21, M42