Pregledni rad
Review paper

JEL Classification: M41, M42

Envera Halilčević*

PRIMJENA DIGITALNE FORENZIKE ZA IDENTIFIKOVANJE PREVARA U FORENZIČKOM RAČUNOVODSTVU

APPLICATION OF DIGITAL FORENSICS TO IDENTIFY FRAUD IN FORENSIC ACCOUNTING

Sažetak

Digitalna forenzika postala je ključni aspekt istrage prevara u savremenom svijetu. Jednom kada stvorimo digitalni otisak, nemoguće ga je izbrisati. Uz širenje digitalnih uređaja, sve veću količinu podataka koje stvaramo, kriminalci su razvili nove načine za počinjenje prevare. Prilikom izvođenja prevare, prevaranti bi mogli pomisliti da su izbrisali datoteke/e-poštu/fotografiju, ali ti podaci nikada ne nestaju. Mijenja se samo ruta do podataka. Intenzitet i sofisticiranost izvođenja prievare učinili su učinkovitu digitalnu forenziku i tehnike istraživanja prevare važnijima nego ikad prije. Digitalna forenzika istražiteljima pruža alate za pronalaženje i kazneni progon osoba koje su sklone finansijskim prevarama. Prevare u vezi informacija i podataka preduzeća predstavljaju područje izloženo stalnom porastu prevara. Finansijski gubici uslijed prevare su veoma značajni. Ukupan trošak prevare se ne može izmjeriti u smislu vremena, produktivnosti i reputacije, uključujući i odnose sa klijentima. U zavisnosti o ozbiljnosti gubitka, preduzeća mogu biti finansijski nepopravljivo oštećena uslijed uticaja prevare. Stoga je za preduzeće od izuzetne važnosti, uspostavljanje čvrstog programa prevencije i detekcije s ciljem identifikacije svih mogućih prevara u okviru preduzeća. Rizici sa kojima se preduzeća susreću su neizbježni i moraju biti procjenjeni, kontrolisani i finansijski neutralisani kako ne bi ugrozili cjelinu poslovanja. Sve dok postoji

* **Doc. dr.sc. Envera Halilčević**, Bingo Doo Tuzla, Category manager; email: enverahalilcevic@gmail.com: envera.halilcevic@bingotuzla.ba

zanemarivanje aktera koji upravljaju preduzećima za zaštitom postojećih informacionih sistema, sigurnost informacionih sistema će biti na niskom nivou. Model globalne organizacije i jake konkurencije zahtjeva novu koncepciju pristupa preduzeća u njihovom poslovanju, implementaciji zaštite informacionih sistema, o čemu svjedoče sve veća ulaganja u specijaliziranu i klijentu orjentiranu tehnologiju. Primjena sigurnosnih standarda u informacijskoj sigurnosti poboljšava smanjenje napada i incidenata, kao i eliminaciju postojećih grešaka u samom informacionom sistemu preduzeća. Kako bi se izbjegli napadi na informacioni sistem, upravljanje informacijskom sigurnošću je obaveza svakog preduzeća i društva, koju je neophodno stalno nadzirati i usavršavati.

Ključne riječi: *prevare, informacioni sistemi, edukacija, Bosna i Hercegovina*

Abstract

Digital forensics has become a key aspect of fraud investigation in the modern world. With the proliferation of digital devices, the ever-increasing amount of data we create, criminals have developed new ways to commit fraud. When running the scam, the scammers might think they've deleted the files/email/photo, but that data never goes away. Only the route to the data changes. The intensity and sophistication of fraud executions have made effective digital forensics and fraud investigation techniques more important than ever before. Digital forensics provides investigators with the tools to track down and prosecute individuals who are prone to financial fraud. Frauds related to company information and data represent an area exposed to a constant increase in fraud. Financial losses due to fraud are very significant. The total cost of fraud cannot be measured in terms of time, productivity and reputation, including customer relationships. Depending on the severity of the loss, companies may be financially irreparably damaged due to the impact of fraud. Therefore, it is extremely important for the company to establish a solid prevention and detection program with the aim of identifying all possible frauds within the company. The risks faced by companies are inevitable and must be assessed, controlled and financially neutralized in order not to endanger the entire business. As long as there is neglect by the actors who manage companies to protect existing information systems, the security of information systems will be at a low level. The model of global organization and strong competition requires a new conception of the approach of companies in their operations, the implementation of protection of information systems, as evidenced by the increasing investments in specialized and client-oriented technology. The application of security standards in information security improves the reduction of attacks and incidents, as well as the elimination of existing errors in the company's information system itself. In order to avoid attacks on the information system, information security management is an obligation of every company and society, which must be constantly monitored and improved.

Key words:: *scams, information systems, education, Bosnia and Herzegovina.*

1. UVOD

Razvoj nauke i tehnologije vremenom je doveo i do pojave digitalnog doba, a time i do promjena u načinu života ljudi, u načinu poslovanja, jer brzina dolaska do informacija neminovno vodi do velikih promjena. Elektronske veze i komunikacije: omogućavaju kontinuirano poslovanje sa velikom efikasnošću, nižim troškovima te manjim greškama i propustima; omogućavaju veliku transparentnost podataka, informacija, znanja i dostupnost svih dijelova tržišta kako velikim tako i malim korisnicima. Stalne promjene i složeniji uslovi poslovanja preduzeća, praćeni kontinuiranim razvojem informacionih tehnologija u poslovanju, formiraju okruženje u kojem postoji veća vjerovatnoća za nastanak grešaka i prevara. Današnju ekonomiju obilježava proces globalizacije, ubrzano kretanje dobara, usluga, kapitala i radne snage, kao i sve veći napredak u razvoju informacionih tehnologija. To se odražava i na sve veću pojavu internetskih prijetnji, razvoja aplikacija čiji je osnovni zadatak nanošenje štete informacijama i informacijskim sistemima. Iako je velika većina informacija danas u digitalnom obliku, preduzeća još uvijek posjeduju pisanu dokumentaciju, u slikama, tablicama i slično. Prevare u vezi informacija i podataka preduzeća predstavljaju područje izloženo stalnom porastu prevara. Finansijski gubici uslijed prevare su veoma značajni. Ukupan trošak prevare se ne može izmjeriti u smislu vremena, produktivnosti i reputacije, uključujući i odnose sa klijentima. Razloga je mnoštvo, od napada, izmjene izvornih podataka poslovanja preduzeća, prisluškivanja, ukidanja servisa preduzeća, identifikacija lozinki i sl. Činjenica je da si informacijski sistemi postali nesigurni, i da se IT tehnologija usmjerava na iznaženje metoda i načina za zaštitu istih. U zavisnosti o ozbiljnosti gubitka, preduzeća mogu biti finansijski nepopravljivo oštećena uslijed uticaja prevare. Stoga je za preduzeće od izuzetne važnosti, uspostavljanje čvrstog programa prevencije i detekcije s ciljem identifikacije svih mogućih prevara u okviru preduzeća.

Svrha ovog rada je bila ta, i da se ukaže na potrebu davanja značaja digitalnom forenzičkom računovodstvu i forenzičkoj reviziji u savremenom poslovanju, u smislu sprečavanja i otkrivanja manipulacija, te finansijskih prevara i kriminalnih radnji. Zadaci i ciljevi forenzičke revizije su razlog drugačijem pristupu finansijskim izvještajima preduzeća, po pitanju materijalnosti, obuhvatanja prevare, te načina prikupljanja dokaza o prevari. Razvoj sigurnosnih standarda u informacijskoj sigurnosti i implementaciji informacionog sistema koji će pomoći preduzeću da se u svakom momentu može suočiti sa prijetnjama, te na vrijeme reagovati na sigurnosne incidente, i imati sistem koji upravlja sigurnošću informacija. Činjenica je da si informacijski sistemi postali nesigurni, i da se IT tehnologija usmjerava na iznaženje metoda i načina za zaštitu istih. U zavisnosti o ozbiljnosti gubitka, preduzeća mogu biti finansijski nepopravljivo oštećena uslijed uticaja prevare. Stoga je za preduzeće od izuzetne važnosti, uspostavljanje čvrstog

programa prevencije i detekcije s ciljem identifikacije svih mogućih prevara u okviru preduzeća. Razvoj sigurnosnih standarda u informacijskoj sigurnosti i implementaciji informacionog sistema koji će pomoći preduzeću da se u svakom momentu može suočiti sa prijetnjama, te na vrijeme reagovati na sigurnosne incidente, i imati sistem koji upravlja sigurnošću informacija.

2. SIGURNOSNI STANDARDI U INFORMACIJSKOJ SIGURNOSTI

Prema navodima autora rada referenca [1] Serija ISO standarda ISO27000 rezervirana je od strane ove organizacije i propisuje infomacijsku sigurnost. Historijski gledano, prvi dokumenat koji se bavio ovom problematikom je bio „Code of Practice" od British Standard Institute-a, iz 1993.godine koji je 1995 godine postao Britanski standard 7799. Nakon 5 godina ISO ga je prihvatio kao ISO17799:2000 – međunarodni standard za informacijsku sigurnost. 2005 godine, zbog naglog razvoja informacijskih znanosti i nedostatnosti verzije 2000 standarda, objavljena je inačica ISO17799:2005. ISO27001 iz oktobra 2005.godine , kao zamjena za BS7799-2 predstavlja specifikaciju za sustav za upravljanje informacijskom sigurnošću-on specificira što bi trebalo uraditi kako bi sustav bio siguran. ISO27002, odnosno alias ISO17799 standarda, predstavlja zbirku pravila iz prakse, odnosno specificira na koji način bi trebalo uraditi da informacijska sigurnost bude na visokoj razini. Pored ova dva standarda postoje i ISO27003, ISO27004, ISO27005 i ISO27006. Ovi standardi predstavljaju preporuke za implementaciju ISMS-a, zatim upravljanje mjerenjima i metrikom u informacijskoj sigurnosti, upravljanje rizicima, kao i sam proces akreditacije i ISMS certificiranja organizacije. Prema autoru rada Miljić B referenca [2] Najnovija inačica ovog standarda je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. Najvažnije izmjene u verziji 2013. se odnose na strukturu glavnog dijela standarda, zainteresirane strane, ciljeve, praćenje i mjerenje. Međutim, sve te izmjene nisu zapravo mnogo promijenile standard u cjelini – njegova temeljna filozofija se i dalje bazira na procjeni i obradi rizika, a zadržane su iste faze uspostave, primjene, pregledavanja i poboljšavanja. Ova nova verzija standarda je lakša za čitanje i razumijevanje, te je mnogo jednostavnija za integriranje s drugim standardima upravljanja kao što su ISO 9001, ISO 22301, itd. (ISO/IEC, ISO/IEC 27000 family - Information security management systems, 2018).

Prema navodima autora rada Miljić B. Zakonske regulative po pitanju informacijske sigurnosti u Bosni i Hercegovini doneseni su samo par okvirnih zakona koji pokrivaju ovu oblast, sam zakon, kao „Zakon o informacijskoj sigurnosti" ne postoji, mada je za njega urađen nacrt, a bilo je i nekoliko prijedloga ali do dan danas nije usvojen. Dok se čeka usvajanje ovog zakona, po pitanju

informacijske sigurnosti u Bosni i Hercegovini, postoje zakoni koji su izuzetno značajni po ovom pitanju, a to su: - Zakon o zaštiti tajnih podataka (Službeni glasnik BiH br. 54/05. i prečišćeni 12/09.; - Zakon o zaštiti osobnih/ličnih podataka (Službeni glasnik BiH br.32/01, 49/06, 76/11. i prečišćeni 89/11.; - Zakon o centralnoj evidenciji i razmjeni podataka (Službeni glasnik br.32/01, 16/02, 32/07. i 44/07 (prečišćeni)); - Zakon o komunikacijama (Službeni glasnik BiH br. 31/03, 75/06, 32/10 i 98/12. ; - Odluka - Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine (Službeni glasnik BiH br.38/17.), U Parlamentu BiH je u proceduri Zakon o Agenciji za razvoj informacijskog društva (ZARID) od listopada 2008.godine, ali do danas nije donesen. Za razliko od ovoga, formirana je Agencija za zaštitu osobnih podataka, prema preporukama Europske unije (EU) koja jednim dijelom radi i na zaštiti informacijskih sustava institucija BiH, ali samo u segmentu administracije i upravljanja /radio-relejnom mrežom putem koje su povezane sve institucije BiH). U Entitetu Republike Srpske formirana je Agencija za informacijsko društvo koji se bavi stanjem informacijskog sustava (AIDRS- koje je počelo sa radom 01.07.2015.godine, Službeni glasnik RS br.70/11.) što nažalost, ista nije usvojena i na državnoj razini. Za razliku od Bosne i Hercegovine kao države koja nema CERT (Computer Energency Response Team) koja bi se bavila koordinacijom i suradnjom u rješavanju sigurnosnih incidenata između zemalja, radili na edukaciji korisnika Interneta i državne mreže na prevenciji sigurnosnih incidenata, Entitet Republike Srpske ima oformljeno „Odjeljenje za informacijsku bezbjednost“ (OIB) koji vrši funkciju CERT-a Republike Srpske. OIB – CERT Republike Srpske je za sada jedini organ ove vrste u Entitetu Republike Srpske i Bosne i Hercegovine. (CERT RS, 2019).

Prema referenci [1] Najbitniji segment informacijskog sustava jednog preduzeća je sigurnosna politika. Ukoliko informacijsku sigurnost promatramo kao osobu, sigurnosna politika bi bila njen centralni nervi sustav. Ona predstavlja jezgro informacijske sigurnosti, i pokriva sve aspekte od organizacijske sigurnosti, sigurnosti osoblja-fizičke sigurnosti, klasifikacije prijetnji IS-u, prava pristupa itd. Detaljno poznavanje legislative kroz proces razvoja i implementacije sigurosnih standarda je nedovoljno kako bi se mogao implementirati jedan tako kompleksan plan. Potrebno je uložiti mnogo više napora – biti spreman na efektivnu komunikaciju, imati potporu menadžmenta, identificirati kvalitetnog voditelja projekta, te imati suradnju IT osoblja. Prema ISO17799:2000 standardu prijetnje s obzirom na uzorke nastanka mogu biti: prirodne katastrofe, tehnički problemi, nenamjerne ljudske pogreške, namjerne ljudske pogreške.

Opravdanje, racionalizacija ili nedostatak integriteta su faktor rizika prevare i opravdanja tog djela. „Primjeri racionalizacije:

- meni je potrebno više nego ostalim ljudima (teorija Robina Huda),

- ja samo pozajmljujem novac i vratiću ga,
- nitko neće biti povrijeđen,
- kompanija je dovoljno velika da to priušti,
- uspješan ugled je naziv prihvatljive društvene igre,
- svi to rade.

Počinioci prevare da bi napravili sam čin prevare moraju imati motiv za prevaru. Neki od motiva mogu biti osveta, pohlepa, ali i finansijske poteškoće. Ukoliko netko vrši pritisak na osobu (menadžment, nadređena osoba, neka treća osoba), također, mogu biti uzročnici prevare. Poslodavci teško mogu predvidjeti koji je motiv prevare bio, s obzirom, da zaposleni nerjetko porodične probleme kriju od poslodavaca, nadređenih osoba ili kolega na poslu. Finansijske teškoće mogu poticati iz raznih razloga kao npr.: ovisnost o drogama ili kockanju, održavanju luksuznog načina života, ili vanredne okolnosti poput bolesti i sl. I globalna finansijska kriza može biti jedan od razloga finansijskih poteškoća, nesigurnost radnog mjesta, nemogućnost dobivanja kredita, sve to mogu biti razlozi koji i poštene zaposlenike mogu navesti na prevaru. Presjednik Udruženja Ovlaštenih Ispitivača prevara ACFE navodi: "Očajni ljudi su spremni na sve. Odani zaposlenici imaju račune koje moraju plaćati i obitelji koje moraju prehraniti. U stabilnoj ekonomiji te osobe nikada ne bi pomislile na čin prevare kako bi nanijeli štetu svojim poslodavcima. Zbog toga organizacije moraju biti spremne u ovim turbulentnim vremenima osigurati prikladne mjere sprečavanja prevara".

Priliku za prevaru će omogućiti nekvalitetan sistem internih kontrola, neadekvatna kontrola zaposlenih od strane menadžmenta, kao i neadekvatna organizacijska struktura. Pri narušenom povjerenju kolektiva preduzeća otvaraju se mogućnosti za prevaru. Referenca [3] Ako je kompanijsko pravilo vođenja i etike u skladu sa kontrolnim sistemom, sistem će biti dizajniran da spriječi i detektuje pokušaje zaobilaženja tih kontrola. Dok neetičko ponašanje Uprave preduzeća ili manjak pravila i vođenja može direktno djelovati na finansijsko izvještavanje, operacionu efikasnost i efektivnost ili zakonsku saglasnost. Kao takvi kulturni elementi mogu indirektno djelovati na oportunističku tačku trokuta prevare: kada slaba ili „oštećena" etička kultura preduzeća postoji, veća je mogućnost da će sistem interne kontrole biti manjkav, i veći je potencijal za postojanje većeg broja iluzionih kontrola. Nekada se dešava da počinilac prevare nema nekih finansijskih poteškoća, ali počini prevaru iz osvete prema poslodavcu ili pohlepe. Kada osoba koja ima motivaciju počini prevaru, spozna način na koji to može učiniti i prođe nekažnjeno, i u slučaju da prevara bude otkrivena. Kako narodna poslovica kaže „prilika čini lopova", prilika je jedini elemenat trokuta prevare na koju preduzeće može direktno djelovati. Zbog toga je zadatak preduzeća da uspostavi efikasne mjere sprečavanja prevara kako bi se mogućnosti nastanka istih svele na minimum.

Referenca [4] navodi da stvarni trošak prevare je teško, ako ne i nemoguće, kvantitativno mjeriti iz četiri glavna razloga:

- Empirijske studije pokazuju da samo mali dio svih prevara, bude otkriven.
- Čak ako je prevara i otkrivena, nisu svi slučajevi objavljeni jer kompanije pokušavaju sačuvati svoj ugled otpuštanjem počinitelja prevare, te se prave da se incident nije nikada ni dogodio.
- Ankete o prevarama u izvještavanju stepena i veličine prevare nisu uvjek tačne, te su podložne ograničenjima tipične ankete u smislu da sudionici često iskazuju svoju percepciju, a ne stvarnost.
- Kompanije obično ne provode građanske ili kaznene akcije; otpuštanjem počinitelja prevare mnoge kompanije vjeruju da su spriječile daljne pojave prevare.

Razmatranjem značajnosti svakog potencijalnog rizika, menadžment može i u slučaju da je došlo do prevare ublažiti neželjene događaje. Međutim, da bi se identifikovao rizik prevare potrebne su informacije iz internog i eksternog okruženja. Prema navodima autora rada Gill referenca [5] Procjena rizika prevare odnosi se na tri ključna elementa:

- identifikacija inherentnog rizika prevare, razmatranje svih šema i scenarija prevare, poticaja, pritisaka, mogućnosti da se počini prevara i IT rizik prevare specifičan za to preduzeće,
- procjena vjerovatnoće i značajnosti inherentnog rizika prevare, procjeniti relativnu vjerovatnoću i potencijalnu značajnost identificiranja rizika prevare zasnovanog na istorijskim podacima, poznatim šemama prevare, razgovora sa zaposlenicima, i
- odgovor na moguće i značajne inherentne i ostale rizike. Odlučiti kako odgovoriti na identificirane rizike i provoditi cost-benefit analizu rizika prevare nad kojim preduzeće želi uspostaviti kontrole ili specifične procedure detekcije prevara.

Procjenu je potrebno provoditi konstantno i postepeno, dok uspostava odgovarajućih kontrola prevencije i efikasnih sistema internih kontrola predstavljaju najuspješnije načine sprečavanja prevara. Menadžment se može zaštititi od grešaka i prevara i dobrom praksom zapošljavanja, te poticanjem adekvatnih internih kontrola preduzeća, pa i na taj način svesti poslovne gubitke preduzeća na minimum. Ukoliko se uspiju razdvojiti dužnosti, obezbjediti fizičke zaštite, isprave autorizacije odgovarajućih dokumenata tada se rizik smanjuje. Interni revizori se fokusiraju na dijelove poslovanja preduzeća gdje se utvrdi najveći stepen rizika. Uz pomoć menadžmenta, revizori mogu spriječiti rizik u sljedećim aktivnostima:

- planiranje gdje se utvrđuju slabosti, preko procjene rizika, koji se odnosi na ispitivanje etičke klime u preduzeću,
- revizija gdje se ispituje i provjerava djelotvornost sprečavanja prevara,
- izvještavanje gdje se stiče podrška od menadžmenta za kreiranje snažne kontrole sprečavanja rizika i dovođenje do toga da menadžment bude svjestan rizika u slabljenju kontrola.

3. PROCJENA RIZIKA FINANSIJSKIH PREVARA

Računovodstveni odjel pruža iformacije o nabavljenom materijalu, prodajnim cijenama proizvoda, platama zaposlenika, a i o strukturi prihoda i rashoda preduzeća. Ukoliko se zloupotrijebe važne informacije o poslovanju preduzeća, rizik se može ispoljiti ne samo u finansijskim i poslovnim gubicima nego i zloupotrebe informacija koje ugrožavaju kontinuitet i rast poslovanja preduzeća. Procjena rizika finansijskih prevara koje mogu imati uticaj na značajno pogrešno prikazivanje finansijskih izvještaja razlikuje dvije vrste grešaka i nepravilnosti: prevare menadžmenta koje djeluju na pogrešno finansijsko izvještavanje i nepravilnosti vezane za otuđivanje sredstava. Faktori koji mogu biti osnova za materijalne greške su: motivacija menadžmenta za nekorektno finansijsko izvještavanje vezano za velike kompenzacije, pogrešne prognoze i ciljeve poslovanja preduzeća koji su nerealni, iskrivljivanje finansijskog rezultata u cilju smanjivanja poreskih obaveza. Signali mogu biti i loš odnos menadžera preduzeća prema finansijskom izvještavanju, loš odnos menadžera preduzeća prema revizorima u vidu formalnih ili neformalnih ograničenja revizije. Navodi autora Gill pokazuju da faktori finansijske stabilnosti preduzeća koji mogu biti uzrok prevara su: nemogućnost ostvarivanja zdravog novčanog toka, finansijski izvještaji su urađeni na nerealnim računovodstvenim procjenama, pretjerano velika profitabilnost preduzeća, prevelika prezaduženost preduzeća i sl. Otuđenje sredstava izazvano je faktorima rizika a koji mogu biti: velike sume finansijskih sredstava kojima rukuju pojedinci, karakteristike zaliha, dostupnost dijelova koji su skupi, zbrka u računovodstvenom sistemu, nedostatak procedura kontrole, neadekvatna podjela dužnosti i ovlaštenja, kao i nedostatak zaliha, novca i opreme. Razmatranjem značajnosti svakog potencijalnog rizika, menadžment može i u slučaju da je došlo do prevare ublažiti neželjene događaje. Međutim, da bi se identifikovao rizik prevare potrebne su informacije iz internog i eksternog okruženja. Prema referenci [5] autor rada Gill „Procjena rizika prevare odnosi se na tri ključna elementa:

- identifikacija inherentnog rizika prevare, razmatranje svih šema i scenarija prevare, poticaja, pritisaka, mogućnosti da se počini prevara i IT rizik prevare specifičan za to preduzeće,

- procjena vjerovatnoće i značajnosti inherentnog rizika prevare, procjeniti relativnu vjerovatnoću i potencijalnu značajnost identificiranja rizika prevare zasnovanog na istorijskim podacima, poznatim šemama prevare, razgovora sa zaposlenicima, i
- odgovor na moguće i značajne inherentne i ostale rizike. Odlučiti kako odgovoriti na identificirane rizike i provoditi cost-benefit analizu rizika prevare nad kojim preduzeće želi uspostaviti kontrole ili specifične procedure detekcije prevara.

Procjenu je potrebno provoditi konstantno i postepeno, dok uspostava odgovarajućih kontrola prevencije i efikasnih sistema internih kontrola predstavljaju najuspješnije načine sprečavanja prevara. Menadžment se može zaštititi od grešaka i prevara i dobrom praksom zapošljavanja, te poticanjem adekvatnih internih kontrola preduzeća, pa i na taj način svesti poslovne gubitke preduzeća na minimum. Ukoliko se uspiju razdvojiti dužnosti, obezbjediti fizičke zaštite, isprave autorizacije odgovarajućih dokumenata tada se rizik smanjuje. Interni revizori se fokusiraju na dijelove poslovanja preduzeća gdje se utvrdi najveći stepen rizika. Uz pomoć menadžmenta, revizori mogu spriječiti rizik u sljedećim aktivnostima:

- planiranje gdje se utvrđuju slabosti, preko procjene rizika, koji se odnosi na ispitivanje etičke klime u preduzeću,
- revizija gdje se ispituje i provjerava djelotvornost sprečavanja prevara,
- izvještavanje gdje se stiče podrška od menadžmenta za kreiranje snažne kontrole sprečavanja rizika i dovođenje do toga da menadžment bude svjestan rizika u slabljenju kontrola, te preko revizorskih izvještaja.

Međutim, treba biti svjestan da će uvijek netko naći priliku kako zaobići kontrolu ili u saradnji s nekim počiniti prevaru. Rizik finansijskih prevara se povećava zbog nepostojanje preventivnih mjera kontrole i korporativne kulture koje dosljedno sankcionišu nezakonita djelovanja. Uvođenjem vlastitog kodeksa etike preduzeća mogu djelovati na smanjenje motiva za manipulacije i kriminalne radnje. Često prevare u finansijskim izvještajima počnu nekim manje značajnim pogrešnim prikazivanjima zarada, koje na kraju prerastu u značajno zavaravajuće godišnje finansijske izvještaje. U malim preduzećima često interni revizori otkriju prevare, a najčešće su slučajno otkrivene.

Prema referenci [6] autor rada Stanišić pokazuje da planiranje aktivnosti interne revizije treba da se zasniva na ocjeni rizika i da se radi najmanje jednom godišnje. U ovom procesu treba razmotriti učešće višeg rukovodstva i Upravnog odbora. Internom revizijom se procjenjuje sistem internih kontrola, daje stručno mišljenje kao i preporuke za poboljšanje internog sistema i poslovanja posmatranog preduzeća. Interna revizija pomaže u postizanju ciljeva uz primjenu disciplinarnog

pristupa vrednovanju i poboljšanju efikasnosti upravljanja rizicima, kontroli i privređivanju. Provodi se zbog pregleda računovodstvenog, finansijskog i drugog poslovanja (kvalitet i efikasnost poslovnih izještaja). Prilikom procjene prevare uloga internog revizora se sastoji u: procjenama efikasnosti internih kontrola postavljenih od strane mandžmenta preduzeća u skladu sa strategijom preduzeća, identifikaciji rizika na svim organizacijskim nivoima preduzeća, definiranju rasporeda odgovornosti za procjenu rizika i osiguranje procedura za izvještavanje menadžmenta, raspolaganju informacijama, posebno gdje se procjenjuje da su svi rizici kritični. Interna revizija je glani akter u procesu upravljanja rizicima. Prema literaturi veći procenat otkrivenih prevara pripada forenzičkim računovođama na temelju dobrovoljnih priznanja, anonimnih dojava i sl. Forenzički računovođa ili forenzički revizor: kreira set misli o osjetljivost na neobično, gdje ništa nije standardno, fokus svog interesa stavlja na neuobičajenosti ili na izuzetke i šablon ponašanja, nastoji otkriti mogućnosti narušavanja kontrole u preduzeću u svrhu prevare koristi mnogo nižu granicu materijalnosti (akumulativnu materijalnost) kao razlog istraživanja prevare. Prvobitna uloga forenzičkog računovodstva je bila prikupljanje dokaza za sudske parnice. Prema mišljenju autora Crumbley forenzičko računovodstvo se temelji na primjeni računovodstvenih, revizijskih, poreznih, finansijskih i istraživačkih vještina, te poznavanje zakonskih regulativa i pravnih procesa za potrebe prikupljanja, analize i prezentovanja podataka u sudskim procesima. Posao revizora se sastoji u prikupljanju dokaza za izdavanje mišljenja o pozicijama iz finansijskih izvještaja, dok forenzički revizori se više fokusiraju na neobične pojave i nešto što nije uobičajeno. Revizori procjenjuju snagu sistema interne kontrole, dok se forenzički revizor fokusira na slabosti interne kontrole koje se mogu iskoristiti za prevare. Revizori se koriste teorijama finansijskog računovodstva, stečenim iskustvom, dok forenzički revizori imaju pristup analize velikog broja informacija uz traženje izvršioca prevare i manipulacija finansijskim izvještajima.

Referenca [7] navodi da prema definiciji Udruženja ovlaštenih istraživača prevara (ACFE) prevara se definira kao korištenje profesije i iskustva za osobnu korist kroz promišljeno zloupotrebljavanje ili krađu resursa odnosno krađu imovine preduzeća. Iako prevaru nije lako istrijebiti i nerealno je očekivati da će potpuno nestati, države nastoje uvoditi zakone kako bi se što više zaštitilo pojedince od teških posljedica obmane, a počinioce kaznilo na što učinkovitiji način. U savremenoj literaturi često se postavlja pitanje kolika je revizorova odgovornost u otkrivanju prevare. Prema Međunarodnim revizijskim standardima uloga revizora je utvrđivanje usklađenosti finansijskih izvještaja preduzeća s međunarodnim računovodstvenim standardima i međunarodnim standardima finansijskog izvještavanja. Zadatak revizora je da uz razumno uvjerenje utvrdi posluje li preduzeće u skladu sa zakonskim i računovodstvenim okvirima. Forenzički revizori nastupaju kada revizor posumnja

na prevaru pa odluči angažirati stručnjaka – forenzičkog revizora ili kada je sam forenzički revizor pozvan od strane dioničara, zaposlenika ili regulatora.

Nedavno objavljeno Izvješće Udruge certificiranih ispitivača prijevara (ACFE) za 2022. nacijama pruža važnu perspektivu s visoke razine o porastu prijevara na radu. Izvješće je sveobuhvatna studija o troškovima, metodama, žrtvama i počiniteljima profesionalne prijevare, sastavljena od 2110 stvarnih slučajeva prijevare istraženih u 133 države, koji su ukupno iznosili 3,6 milijardi američkih dolara gubitaka, s prosječnim gubitkom po slučaju od 1,78 milijuna američkih dolara. Ove prevare, koje su počinili pojedinci protiv svojih poslodavaca, utjecale su na organizacije u svakoj regiji i industriji. Izvješće je pokazalo da organizacije gube otprilike 5 posto prihoda svake godine zbog prevara, uglavnom zbog zloupotrebe imovine, korupcije i prijevare u finansijskim izvješćima. Tri primarne kategorije prevarnih šema najčešće su prevladavale u pregledanim slučajevima:

- Zloupotreba imovine, koja uključuje krađu ili zloupotrebo imovine preduzeća. Ova vrsta prevare je najčešća, događa se u 86 posto prijavljenih slučajeva, ali je i najmanje skupa, s procijenjenim srednjim gubitkom od 100.000 USD.
- Prevara u financijskim izvješćima, koja uključuje namjerno pretjerano ili podcjenjivanje iznosa finansijskih izvješća kako bi se prevarili korisnici finansijskih izvješća – dioničari, vjerovnici, bankari, klijenti, porezna tijela i šire tržište u cjelini. Ova vrsta prevare rjeđa je od pronevjere imovine, javlja se u samo 9 posto pregledanih slučajeva, ali je najskuplja, s procijenjenim srednjim gubitkom po slučaju od 593.000 USD.
- Korupcijske šeme, koje uključuju nepošteno ponašanje ljudi na položaju, što uključuje, između ostalog, podmićivanje, mito, sukob interesa i iznudu. Te su se šeme dogodile u 50 posto pregledanih slučajeva i uzrokovale su procijenjeni srednji gubitak od 150.000 USD.

Danas je forenzičko računovodstvo potpuno formirana profesija koja se razvijala kako se poslovni svijet mijenjao i napredovao, kako na domaćem tako i na međunarodnom planu. Priroda posla ostaje općenito ista kao i uvijek - odgovorite na "tko/što/kada/koliko" u situacijama u kojima percepcija i stvarnost nisu usklađeni, bilo da se radi o izračunu štete, procjeni vrijednosti, prijevari ili drugoj klasi pitanja koja se iznose pred odlučujući forum radi razmatranja i donošenja presude. Već nekoliko godina postoji sve veće oslanjanje na forenzičke računovođe da koriste svoju stručnost za pomoć u parničnim stvarima.

4. ULOGA DIGITALNE FORENZIKE U IDENTIFIKOVANJU I SPREČAVANJU FINANSIJSKIH PREVARA

Udruga ovlaštenih ispitivača prijevara (ACFE) opisuje finansijsku prevaru kao namjerni čin prevare koji uključuje finansijske transakcije u svrhu osobne dobiti. Uticaj finansijskih prevara je značajan i ne utiče samo na žrtve koje su izravno pogođene, već i na cjelokupno društvo. Narušava povjerenje u finansijske sustave, potkopava povjerenje investitora i može dovesti do ozbiljnih finansijskih gubitaka za preduzeća. U digitalnom dobu, u kojem je svijet prihvatio tehnologiju, prevaranti su na sličan način usvojili digitalne metode za održavanje finansijske prijevare, što služi kao imperativ forenzičkim istražiteljima da usklade svoje metode s ovom digitalnom promjenom. Digitalna forenzika, također poznata kao računalna forenzika, grana je forenzičke znanosti koja uključuje identifikaciju, prikupljanje, analizu i očuvanje digitalnih dokaza iz elektroničkih uređaja i računalnih sustava u svrhu istraživanja i sprječavanja kibernetičkog kriminala, povrede podataka i drugih digitalno -povezanih incidenata. Obuhvaća širok raspon tehnika i metodologija s ciljem otkrivanja, tumačenja i prezentiranja digitalnih dokaza na pravno dopušten način.

Postoje bitne razlike između tradicionalne eksterne revizije finansijskih izvještaja i forenzičke revizije. Forenzička revizija treba da otkrije ko je počinio prevaru, kolika je materijalna šteta, u kojim transakcijama je učinjena prevara, način na koji je prevara izvršena i treba da pruži dokaz o učinjenoj prevari. Potrebno je da forenzički revizor zna da li zakon tu prevaru tretira kao krivično djelo. U mnogim postupcima lažnih nabavki počinioci koriste tzv. „fantom firme“ kako bi činili i prikrili kriminalnu radnju. Pregledom dokumenata i finansijskih izvještaja forenzički revizor može naići na sljedeće indikatore o postojanju tzv. „fantomskih“ firmi:

- dokumenta poslovnog partnera (npr. faktura, otpremnica i dr.) su sačinjena na najprostijim obrascima. Na tim dokumentima ne postoje adrese, telefoni, matični i poreski identifikacioni brojevi,
- iznosi na dugovnom i potražnom saldu iznose često nula, što je neuobičajno za poslovanje preduzeća, prilikom plaćanja i naplate po transakcijama,
- često se dešava da postoje zaokružene sume novca,
- postoji kratak vremenski period poslovanja sa određenim poslovnim partenrom i više se nikada ne pojavljuje u poslovanju,
- „životni vijek“ fantom firme traje veoma kratko. Sumnju izaziva da neka firma radi samo nekoliko mjeseci ili u nekim slučajevima samo nekoliko dana.

U kontekstu podrške u parnici, forenzički računovođe mogu se uključiti u ranoj fazi kako bi dodali vrijednost pripremom popisa dokumenata, koji bi mogli pomoći u slučaju u parnici u svrhu otkrivanja. Posljedično, oni mogu osigurati cjelovitost dokumenata za objavljivanje, sastaviti pojedine financijske dokumente i informacije

te protumačiti i prenijeti priču iza složenih transakcijskih podataka. Forenzički računovođe također mogu poduzeti procjene prije parnice kako bi obavijestili klijente je li vjerojatnost izvršenja presude potencijalno mala, kako bi se izbjeglo 'bacanje dobrog novca za lošim'. Forenzički računovođe posjeduju kombinaciju stručnosti u financijskoj oštroumnosti i tradicionalnih tehnika prikupljanja informacija. To je dopunjeno vrhunskom tehnologijom za prikupljanje i razumijevanje uzoraka u velikim skupovima podataka. I upravo ćemo ovu posljednju točku detaljnije istražiti u kontekstu parničenja: preko potrebnih kompetencija za forenzičke računovođe prekriva se zahtjev da se njihove analitičke vještine poboljšaju računalno potpomognutim metodama. Kada zaposlenik, menadžer, službenik ili vlasnik organizacije počini prijevaru na štetu poslovanja, to je poznato kao profesionalna prijevara. Kada se tehnologija koristi za počinjenje takve prijevare, to se naziva računalnom profesionalnom prijevarom.

Trendovi profesionalnih prijevara koji obuhvaćaju razdoblje covida-19 povezani su s naglim prelaskom u udaljene urede: mnogi su zaposlenici brzo prešli raditi u manje sigurna okruženja. Istodobno je odmah došlo do povećanja elektroničke komunikacije. Redovne procedure su poremećene, a rad na daljinu pruža pogodno okruženje za sheme profesionalne prijevare: lakše je stvarati lažne potpise, zahtijevati lažna plaćanja i krivotvoriti fakture ili druge računovodstvene evidencije bez nadzora. Osim unutarnjih prijetnji, povećane su i vanjske prijetnje: udaljeni radnici su ranjiviji na kibernetičke napade kao što su pokušaji krađe identiteta, koji prijevarom navode primatelje da preuzmu zlonamjerni softver ili nevino i nesvjesno daju pristup osjetljivim informacijama tvrtke. Koronavirus je internim revizorima otežao sprječavanje, otkrivanje, odvraćanje i istraživanje prijevara zbog ograničenja putovanja, stalnih kašnjenja u komunikaciji i angažmanima te nedostatka pristupa dokazima. Stručnjaci za borbu protiv prijevara obično navode tri izazova povezana s radnom snagom na daljinu: izazove intervjua, promjenu kontrole i nedostatak nadzora. Druga perspektiva ovoga je ogromna prilika za pojavu prevare.

Osim sigurnosnih problema povezanih s pandemijom, najistaknutiji finansijski trend koji je pridonio porastu slučajeva prevare bio je porast tehnologije blockchain i povezana upotreba kriptovaluta. U digitalnom krajoliku koji se razvija, potonji je stvorio nove metode za pranje novca, posebno kada je riječ o počiniteljima koji sudjeluju u šemama podmićivanja i provizije kako bi pomogli konverziju nezakonito prisvojene imovine. ACFE primjećuje da približno 8 posto svih slučajeva prevare sada uključuje korištenje kriptovaluta. Implikacija za forenzičke računovođe je jasna: prevare na poslu su u porastu, kako se moglo očekivati. Osobito su ranjive one organizacije koje su bile previše uvjerene u zaštitu svojih podataka. Zajednička nit u gotovo svakoj publikaciji koja pokriva krajolik prevara od početka pandemije jest da je onima koji žele poništiti finansijske pogreške potreban specijalizirani alat kako bi razumjeli bezbroj načina na koje se provodi

savremeni finansijski kriminal. Kako su onda forenzički računovođe najprikladniji za pomoć u borbi protiv tako neobuzdanog zlostavljanja?

Kada razmišljamo o velikim podacima u istragama prevara, zamišljamo neprobojni labirint brojki: brojevi transakcija, unosi u dnevnik, vremenske oznake, imena, mjesta, tekstualne poruke, telefonski zapisi, pritisci tipki, klikovi mišem, IP adrese, odnosi i drugi identifikatori. Ovo nije daleko od stvarnosti. Ne postoji službeni prag za veličinu podataka koji se mogu nazvati 'veliki podaci'. Njegova je klasifikacija, kao i njegov sadržaj, mnogo složenija od broja, iako se čini da je jedan terabajt trenutačno prihvaćen kao skup podataka koji se kvalificira kao 'veliki podaci'. Takve goleme zbirke informacija nastaju kao mehanički rezultat prikupljanja i stvaranja velikih količina transakcijskih informacija iz nekoliko međusobno povezanih industrija: između ostalog, transporta, telekomunikacija, marketinga, zabave, bankarstva, financijskih usluga, zdravstvene zaštite, vlade i kibernetičke sigurnosti. Posebno vezano uz te industrije i njihovo prelijevanje informacija, analitika velikih podataka postala je popularna tema istraživanja posljednjih desetljeća. S druge strane, slučaj korištenja velikih podataka u forenzičkom računovodstvu odnosi se na implikacije i za skrivanje dokaza o prevari i za otkrivanje dokaza o prevari. Nakon procesa prikupljanja podataka slijedi integracija tih informacija. Budući da je informacije dohvaćene iz različitih izvora često teško usporediti, krajnji cilj faze integracije je da će relevantne podatke, prikupljene iz različitih izvora i u različitim formatima, na kraju trebati objediniti i vizualno prikazati u nečemu što se može zamisliti kao svojevrsna kronologija odnosa. Pritom se forenzički računovođe bave stalnim i sve većim izazovima svojstvenim integriranju podataka kako bi se oni mogli vizualizirati i pretočiti u znanje koje se može primijeniti u okruženju parnice. Određene vrste istraga sklonije su problemima s velikim podacima nego druge. Prevare s kreditnim karticama, tržišne manipulacije, korporativne prijevare i pitanja pranja novca najčešće opterećuju pravne timove golemim količinama transakcijskih informacija u kojima se značaj i značenje lako previde ili pogrešno shvate. Isto tako, posljedica širenja digitalizacije je da će mnoge druge vrste predmeta, koje ranije nisu bile sklone takvom opterećenju podacima, predstavljati slične izazove u budućnosti.

Upotreba velikih podataka za forenzičke računovođe prilično je različita:

- U kontekstu istrage praćenja imovine, istražitelji često koriste softver posebno dizajniran za ilustraciju, između ostalog, osobnih i profesionalnih veza između pojedinaca i tvrtki uključenih u kretanje imovine koja se prati. Osnova za utvrđivanje veza je njihova blizina kretanju imovine koja se ispituje – od kojih neka uopće nisu očita. Mnoge informacije, kao što su imena pojedinaca i preduzeća, adrese, telefonski brojevi, datumi rođenja, internetske domene, podaci o knjigovodstvenim knjigama, podaci o

bankovnom računu itd., integrirani su s ciljem identifikacije mjesta imovine i osoba koje su odgovorne za njihovu pokreta.

- U kontekstu pranja novca, vlasti se obično pokreću jednom ili više crvenih zastavica koje pokreće finansijski sustav: neuobičajene transakcije, naizgled nelogična plaćanja velikih količina, trenutačno povlačenje sredstava s računa, nedosljednosti u potvrdi identiteta ili due diligence postupak i česte pretvorbe da spomenemo samo neke. Nakon što je istraga u tijeku, kretanje sredstava kroz brojne bankovne račune i račune vrijednosnih papira često je neophodno kako bi se otkrila određena obilježja pranja novca: plasman, slojevitost i integracija. Informacije koje se primjenjuju na takve slučajeve uglavnom su podaci o transakcijama na bankovnom računu, iako ne postoji vanjska veza s sferom informacija koja bi se također mogla pozvati da potkrijepi ili potkopa objašnjenje naizgled nedopuštenih obrazaca transakcija, nakon što se otkriju.
- Pitanja vrednovanja predstavljaju potpuno druge probleme velikih podataka. U kontekstu zakonskih sudskih sporova za procjenu, poput onih koji se zahtijevaju prema Odjeljku 238 Zakona o trgovačkim društvima Kajmanskih otoka (revizija iz 2022.), nalozi za objavu često se sastavljaju na način koji od predmetne tvrtke zahtijeva da proizvede velike količine finansijskih podataka koji uključuju (najmanje) količine internih i eksternih komunikacija, zapisnika sa sastanaka i financijskih projekcija, uključujući zastarjele verzije, nacrte, popratne dokumente i interne izračune. Dok otkrivanje u takvim stvarima obično nameće značajne obaveze preduzeću i često zahtijeva da preduzeće proizvede količine podataka koji su neizbježno beskorisni za procjenu vrijednosti, to je neophodno jer, iz perspektive procjene, stručnjaci za procjenu moraju steći potpuno i točno razumijevanje stanja preduzeća, njegove prošlosti i budućih izgleda na relevantni datum vrednovanja. Razvrstavanje kroz proizvodnju otkrića i identificiranje dokumenata od interesa često je veliki podatkovni izazov uz pomoć umjetne inteligencije. Najveća vrijednost velikih podataka je njihova sposobnost da rasvijetle dosad neviđene uvide. Ali ti su podaci zapravo beskorisni ako ih namijenjena publika ne može lako razumjeti. Zato je toliko važno kako se to komunicira. Nekoliko analitičkih softverskih programa može ponuditi mogućnost pretvaranja podataka u grafikone odnosa ili druge vizualne formate, kako bi se dobila jasnija slika namjeravanih uvida.

Softver za vizualnu bazu podataka primjenjuje se za izradu analize veza koja sažima i ilustrira prikupljene informacije. Ova naizgled različita mreža podatkovnih tačaka, nakon što se integrira, može se koristiti za provođenje analize veza kako bi se odredio naslov imovine ili identificirali odnosi između različitih entiteta i pojedinaca. Na primjer, International Consortium of Investigative Journalists (ICIJ) sa sjedištem u Washingtonu održava ICIJ Offshore Leaks Database, što je vrlo

dobar, javno dostupan primjer vizualizacije pomoću Neo4j i Linkurious softvera primijenjenog na velike skupove podataka. Kao javni izvor, iako sadrži rezultate nekoliko neugodnih povreda javnih podataka, ICIJ Offshore Leaks Database također je vrlo vrijedan alat za podučavanje koji ilustrira kako softver omogućuje razumijevanje velikih podataka. Štoviše, ICIJ Offshore Leaks Database namjerava povećati svijest o prekograničnom kriminalu, korupciji i odgovornosti moći. Kako bi učinkovito testirali, otkrili, potvrdili, ispravili i nadzirali sustave kontrole protiv lažnih aktivnosti, poslovni subjekti i organizacije oslanjaju se na specijalizirane tehnike analitike podataka kao što su rudarenje podataka, podudaranje podataka, zvučna funkcija, regresijska analiza, analiza grupiranja i analiza praznina. Tehnike koje se koriste za otkrivanje prijevara spadaju u dvije osnovne klase: statističke tehnike i umjetna inteligencija. Neki forenzički računovođe specijalizirali su se za računalnu forenzičku analitiku, što je nabava i analiza elektroničkih podataka za rekonstrukciju, otkrivanje ili na drugi način potkrijepljenu tvrdnju o finansijskoj prevari. Glavni koraci u forenzičkoj analitici su prikupljanje podataka, priprema i integracija podataka, analiza podataka, tumačenje i izvještavanje. Na primjer, forenzička analitika može se koristiti za pregled kupovne aktivnosti kartice zaposlenika kako bi se procijenilo je li neka od kupnji preusmjerena ili preusmjerena za osobnu upotrebu.

Umjetna inteligencija, grana računalne znanosti koja se bavi automatizacijom ponašanja inteligencije, uključuje nekoliko tehnika poput strojnog učenja i dubokog učenja koje također mogu pomoći. Rješenja umjetne inteligencije mogu se klasificirati u dvije kategorije: 'nadzirano' i 'nenadzirano' učenje. Ove metode pretražuju račune, kupce, dobavljače i tako dalje koji se ponašaju 'neuobičajeno' kako bi ispisali rezultate sumnje, pravila ili vizualne anomalije, ovisno o metodi. Nadzirano učenje temelji se na podacima o obuci poznatih prijevara i legitimnih slučajeva, dok se nenadzirano učenje koristi podacima koji nisu označeni kao takvi. Bedfordov zakon,8 koji se obično koristi kao osnova za određivanje je li skup podataka autentičan ili izmišljen, primjer je učenja bez nadzora. U nadziranom učenju uzima se nasumični poduzorak svih zapisa i ručno klasificira kao 'lažni' ili 'neprijevarni'. Relativno rijetki događaji kao što je prijevara možda će morati biti više uzorkovani da bi se dobila dovoljno velika veličina uzorka. Zapisi koji su ručno klasificirani kao 'lažni' zatim se koriste za treniranje nadziranog algoritma strojnog učenja. Nakon izgradnje modela korištenjem podataka o obuci, pravilno uvježban algoritam trebao bi moći klasificirati nove transakcije kao "potencijalno lažne" ili "malo vjerojatno lažne". Bilo da se koriste nadzirane ili nenadzirane metode, rezultat nam daje samo naznaku prevare. Niti jedna samostalna statistička analiza ne može osigurati da je određena transakcija lažna, ali ih može identificirati s vrlo visokim stupnjem tačnosti. Kao rezultat toga, učinkovita suradnja između modela strojnog učenja i forenzičkog računovođe ključna je i za uspjeh aplikacija za otkrivanje prevara i, u okruženju parnice, za sposobnost smislenog objašnjenja

njihovih rezultata. U okruženju parnice, većina potrebnih transakcijskih podataka zahtijeva objašnjenje i kontekst prije nego što ih namjeravana publika može razumjeti. Imajući malo razumijevanja za pravosuđe koje također sada treba razumjeti kako demonstriraju prijevare o kojima je riječ, najučinkovitija upotreba forenzičkog računovođe je filtriranje spornih materijalnih transakcija i komuniciranje njihove temeljne suštine. U konačnici, rizik prepuštanja istrage finansijskih zapisa i velikih podataka u neuvježbane ruke jest taj da priča u tim podacima neće biti niti vjerno rekonstruirana niti jezgrovito priopćena. Rudarenje podataka identificira obrasce i odnose skrivene u podacima i dio je šireg procesa koji se zove 'otkrivanje znanja', koji opisuje korake koje je potrebno poduzeti kako bi se osigurali značajni rezultati. To čini rudarenje podataka vrlo vrijednim u sprječavanju i otkrivanju prevara budući da klasificira i segmentira grupe podataka i traži uzorke. Sumnjivi obrasci se zatim uče i koriste za otkrivanje daljnjih ponavljajućih obrazaca. Tehnike analize velikih podataka i rudarenja podataka pomažu forenzičkim računovođama da identificiraju obrasce i generiraju hipoteze, ali same po sebi ne potvrđuju hipoteze. Dokazi prikupljeni korištenjem velikih podatkovnih rješenja mogu imati veliku težinu, ali u kombinaciji s analizom forenzičkih računovodstvenih istražitelja i vještaka sposobnih prenijeti svoje implikacije, njihova je moć dodatno poboljšana i mogu dovesti do uvjerljivih zaključaka. Besprijekorno miješanje ova dva vrlo različita istražna pristupa može, u mnogim slučajevima, dovesti do jasnog uspjeha u istrazi prevare. Dok prevare nastavljaju rasti, rastu i posljedice povezanih aktivnosti. Otkrivanje prijevara s velikim podacima u rukama forenzičkih računovođa inovativan je način korištenja trendova za sprječavanje i otkrivanje sumnjivih transakcija i aktivnosti budući da se čak i male razlike mogu pokupiti, analizirati i crveno označiti kao potencijalne prijevarne aktivnosti.

Tehnike koje se koriste u digitalnoj forenzici i istragama pevara brzo su se razvile posljednjih godina. U nastavku je prikaz procesa digitalne forenzike.

- Planiranje: prvi i najvažniji korak u istrazi digitalne forenzike je planiranje. To uključuje utvrđivanje opsega istrage, definiranje njenih ciljeva i postavljanje nacrta plana akcije. Ovaj korak uključuje identificiranje alata i tehnika potrebnih za istragu i izradu vremenskog okvira za isto. Oduzimanje i očuvanje digitalnih dokaza: Ova faza uključuje identifikaciju i prikupljanje digitalnih dokaza relevantnih za istragu. To također uključuje očuvanje i izolaciju relevantnih uređaja i medija za pohranu, stvaranje kopije podataka bit-po-bit kako bi se spriječilo neovlašteno mijenjanje izvornih podataka.
- Snimanje: Ovaj korak zahtijeva stvaranje forenzičke slike uređaja za pohranu podataka kako bi se osiguralo da su dokazi sačuvani u izvornom obliku. Stvara se bit-po-bit kopija izvornog uređaja, koja se može analizirati bez mijenjanja izvornih podataka.

- Obrada: Ova faza zahtijeva od forenzičkog analitičara da pregleda podatke kako bi došao do svih relevantnih informacija koje će se koristiti kao dokaz. Podaci se analiziraju za skrivene datoteke koje možda neće biti odmah vidljive. Također se može obraditi kako bi se identificirali obrasci ili anomalije.
- Analiza: U ovoj fazi analitičari tumače podatke pomoću specijaliziranog softvera ili alate za prepoznavanje obrazaca, veza i potencijalnih potencijalnih klijenata, ako postoje, koji mogu pomoći u istragama.
- Izvještavanje i svjedočenje: Posljednja faza uključuje predstavljanje nalaza na jasan i koncizan način. Izrađuje se izvještaj koji sažima prikupljene dokaze, provedenu analizu i izvedene zaključke. Od analitičara se također može tražiti da svjedoči na sudu kako bi objasnio nalaze sucu ili poroti.

U današnjem tehno-pametnom svijetu, prijevara je postala sveopći problem. A u borbi protiv ove prijetnje potrebna je učinkovita digitalna forenzika. U nastavku su navedene neke od najboljih praksi u digitalnoj forenzici i istragama prijevara kako bi se osiguralo da su prikupljeni dokazi prihvatljivi na sudu i da se istraga provodi transparentno i etički.

- Planirati unaprijed: Uvijek je bolje zadržati se na dobro planiranom pristupu koji ocrtava ciljeve, opseg i postupak istrage.
- Slijediti lanac nadzora (COC): Za svaku istragu digitalne forenzike vrlo je važno održavati lanac nadzora (COC). Ako se COC ne održava, digitalni dokaz možda neće biti prihvatljiv na sudu.
- Koristiti odgovarajuće alate i tehnike: Uvijek treba koristiti samo licencirani softver i obučenu radnu snagu, jer je digitalni dokaz vrlo nepostojan i može se mijenjati ako se njime ne upravlja ispravno.
- Poštivanje standarda: Digitalna forenzika i istrage prijevara moraju se pridržavati pravnih i etičkih standarda. Analitičari se moraju pridržavati lokalnih, državnih i saveznih zakona i etičkih standarda koje propisuje njihova profesija. Također moraju poštivati prava na privatnost pojedinaca i osigurati da istraga ne krši zakone i propise o privatnosti.

Prevaranti se vješto razvijaju usporedo s promjenama i napretkom, usklađujući svoje metode. Te nezakonite aktivnosti često iskorištavaju ranjivosti u digitalnim sustavima i koriste tehnologiju za provođenje svojih šema. Rješavanje tih rizika postaje sve važnije kako se finansijske transakcije sve više sele na digitalne platforme.

Organizacije mogu iskoristiti digitalnu forenziku za sprečavanje finansijskih prevara na sljedeće načine:

- Procjena i planiranje: za kompanije bi bilo neophodno da započnu s procjenom svoje digitalne infrastrukture, identificiranjem potencijalnih rizika i stvaranjem sveobuhvatne strategije zaštite od finansijskih prevara koja uključuje digitalnu forenziku.
- Ulaganje u vrhunske digitalne forenzičke alate i tehnologiju koji mogu kontinuirano pratiti i ispitivati podatke u potrazi za indikacijama finansijske prevare.
- Obrazovanje i iskustvo: neophodna je edukacija na polju digitalne forenzike za svoj tim ili raditi s vanjskim konzultantima koji mogu voditi kroz osiguravanje digitalnih dokaza.
- Imati strategiju odgovora na incidente koja je dobro definirana. Ova bi strategija trebala uključivati digitalnu forenziku kako bi se zajamčio brz i učinkovit odgovor na svaku sumnju na finansijsku prevaru.
- Redovne revizije i ažuriranja: kako bi ostali na vrhu, neophodno je redovno poboljšavati svoju digitalnu forenziku i mjere za sprječavanje finansijskih prevara.

Digitalna forenzika igra ključnu ulogu u istraživanju finansijskih prevara putem:

- Analize finansijskih transakcija: Digitalna forenzika pomaže u otkrivanju elektroničkih pohranjenih informacija (ESI) kao što su skriveni računi ili imovina, identificira obrasce lažnih aktivnosti i prati finansijske transakcije. Ovo je posebno kritično u situacijama koje uključuju pranje novca i pronevjeru.
- Prikupljanja dokaza: uključujući e-poštu, chatove, zapisnike, evidenciju transakcija, IP adrese, povijest web-preglednika, financijske evidencije i podatke iz oblaka iz širokog raspona izvora poput računala, pametnih telefona, tableta, poslužitelja i drugih. Istražitelji osiguravaju da se integritet dokaza čuva na ispravan način kroz lanac nadzora, uzimajući hashove digitalnih dokaza, čineći ih prihvatljivima na sudu.
- Oporavka podataka: U mnogim slučajevima digitalne prijevare, počinitelji često pokušavaju izbrisati ili šifrirati podatke. Kako bi kriptirali podatke, digitalni forenzičari koriste specijalizirane metode i alate za oporavak kriptiranih i izbrisanih podataka, a zatim daju dragocjene uvide u aktivnosti prevaranta.
- Poboljšanja kibernetičke sigurnosti: Nakon što se dogodi finansijska prevara, istražitelji identificiraju rupe u zakonu koje su počinitelji iskoristili. Kompanije koriste to znanje za prepoznavanje ranjivosti i slabosti u kibersigurnosnoj infrastrukturi organizacije kako bi poboljšale svoje sigurnosne procedure i spriječile buduće događaje.

ZAKLJUČAK

Ostvarenje profitabilnosti u uslovima povećane konkurencije kao i rasta rizika postaje izazov za savremeni menadžment. Kako preduzeća imaju sve veći broj informacija koji se treba pothraniti, načelo sigurnosti informacionog sistema je temelj poslovanja svakog preduzeća. Primjena sigurnosnih standarda u informacijskoj sigurnosti poboljšava smanjenje napada i incidenata, kao i eliminaciju postojećih grešaka u samom informacionom sistemu preduzeća. Kako bi se izbjegli napadi na informacioni sistem, upravljanje informacijskom sigurnošću je obaveza svakog preduzeća i društva, koju je neophodno stalno nadzirati i usavršavati. Prevara negativno utiče na preduzeća finansijski, reputacijom, kao i psihološkim i socijalnim implikacijama. Finansijski gubici uslijed prevare su vrlo značajni. Ukupan trošak prevare se ne može izmjeriti u smislu vremena, produktivnosti i reputacije preduzeća. U zavisnosti o ozbiljnosti gubitka, preduzeća mogu biti finansijski nepopravljivo oštećena uslijed uticaja finansijskih prevara. Zbog toga je za preduzeće od izuzetne važnosti uspostavljanje čvrstog programa prevencije i suzbijanja finansijskih prevara. Digitalna forenzika i istrage prevara bitne su komponente modernog poslovanja. Dok kriminalci nastavljaju razvijati nove načine za finansijske prevare koristeći digitalne uređaje i internet, digitalna forenzika istražiteljima pruža alate za pronalaženje i kazneni progon tih kriminalaca. Slijedeći najbolje prakse, kompanije mogu otkriti i spriječiti lažne aktivnosti i osigurati da se pravni postupci temelje na točnim i pouzdanim dokazima. Korištenje računalne forenzike važno je za forenzičko računovodstvenu praksu jer većina računovodstvenih informacije su danas u digitalnom obliku. Pristup dokazima je sve složeniji i daleko većih volumena nego u prethodnim desetljećima. Učinkovita i učinkovita sredstva za otkrivanje prijevare potrebna su za javnost kako bi održali svoje povjerenje u pouzdanost računovodstvene revizije i ugled računovodstvenih preduzeća. Softverski alati koje koristi forenzičko računovodstvo mogu se dovesti u pitanje. Mnogi izgledaju neadekvatni kad se suoče s njima sa složenošću prevare i potreban je razvoj automatiziranog i specijalističkog rješavanja problema forenzičkog softvera. Preporuka je usvajanje analize finansijskih pokazatelja kao osnove za poboljšani softver za otkrivanje prevara.

REFERENCE

[1] Ćosić J., Medić A., „Informacijska sigurnost, standardi i stanje u institucijama BIH“, dostupnonahttps://www.researchgate.net/publication/279174941_Informacijska_sigurnost_standardi_i_stanje_u_institucijama_BiH.
[2] Mijić, B. (2019) Informacijska sigurnost u BiH FBIM Transactions Vol. 7 No. 1 pp. 91-99 dostupno na https://fbim.meste.org/FBIM_1_2019/13_11.pdf.

[3] Atwood, B., CFE, CFF, CPA; Rainborn, C. A., CMA, CPA, CFE; Butler, J. B., (2012) CITP, CGMA, Illusions of Internal Controls, Strategic Finance, The Association of Accountants and Financial Professionals in Business, New Jersey, str. 34.
[4] Syed Zulfiqar, A., Safdar, B., Yasir, B. T.,(2011), Use or Abuse of Creative Accounting Techniques, International Journal of Trade, Economics and Finance, Vol. 2, No. 6.
[5] Gill, P., Oluić, A. (2010), Interna revizija i kontrola, Hrvatska zajednica računovođa i finansijskih djelatnika, sekcija internih revizora, Zagreb-Vodice, str. 179.
[6] Stanišić, M. (2011). Rukovođenje internom revizijom, Porezni savjetnik, broj 2., str. 77.
[7] Association of Certified Fraud Examiners, Fraud Tree, (online). ACFE, dostupno na: http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.
[8] Papić, M., Vudrić, N., Jerin, K (2017)., Benfordov zakon i njegova primjena u forenzičkom računovodstvu, Pregledni rad.