Šeme prevara koje dovode do bankrotstva

Posmatrajući finansijske lomove koji su zadesili velike korporacije u poslednje dve decenije zbog prevare, korupcije ili nekog drugog oblika zloupotrebe, jasno je da se radi o riziku koji ostavlja ozbiljne posledice po organizacije i da *ad hoc* postupanje ne može da dovede do trajnog rešenja problema, već naprotiv može samo trajno da ugrozi poslovanje kompanije. Kako se zaštititi i ko vam u tome može pomoći

Piše:
Marija Kušić Radovanović,
sertifikovan istražitelj prevara (CFE), član Odbora Udruženja sertifikovanih istražitelja prevara Srbije (ACFE Srbija) i član globalne asocijacije ACFE

Finansijski kriminal je posebna vrsta rizika s kojima se privredna društva susreću. Ova vrsta rizika dugo se nije prepoznavala kao takva već su se finansijski gubici zbog prevara posmatrali kao neželjene situacije u kojima je trebalo gledati da se gubici minimiziraju, a počinici krivičnog dela izvedu pred lice pravde. Organizacije nisu preduzimale dodatne mere zaštite od budućih nepoželjnih „napada" izvršilaca kriminalnih dela. Nije bilo sistemskog planiranja u procesu prevencije, detekcije i istrage s ciljem prevencije rizika zloupotreba. Posmatrajući finansijske lomove koji su zadesili velike korporacije u poslednje dve decenije zbog prevare, korupcije ili nekog drugog oblika zloupotrebe, jasno je da se radi o riziku koji ostavlja ozbiljne posledice po organizacije i da *ad hoc* postupanje ne može dovesti do trajnog rešenja problema, već naprotiv može samo trajno da ugrozi poslovanje kompanije.

Mnoge prevarne radnje mogu da ugroze poslovanje – kako ih sprečiti

Sajber napadi, zloupotrebe insajderskih informacija, falsifikovanje ličnih dokumenata vlasnika firmi i potencijalne zloupotrebe koje mogu da nastanu po tom osnovu, rizik manipulacije s finansijskim izveštajima, samo su neki od oblika prevarnih radnji. Poseban rizik prevare predstavljaju tzv. „fiktivne firme" koje ne obavljaju delatnost zbog koje su osnovane. Najčešći vlasnici ovih kompanija su lica s veoma lošom reputacijom. Ove firme postoje „samo na papiru", a osnovane su s namerom da se ostvari ekonomska dobit dovođenjem u zabludu ostalih učesnika na tržištu lažnim prikazivanjem ili prikrivanjem činjenica. Na ovaj način oštećena pravna

lica trpe ozbiljne posledice jer su dovedena u zabludu.

U finansijskoj forenzici poznat je i vid prevare pod nazivom „CEO fraud". U pitanju je šema prevare gde se koriste javni podaci o direktorima i vlasnicima firmi kako bi se „presrela" komunikacija direktora i/ili vlasnika firme s ostalim zaposlenima, a kako bi se napravila šteta za kompaniju. Nije neobično da se falsifikuju lična dokumenta direktora ili članova izvršnog odbora kompanije kako bi se pokušala prevara dovođenje u zabludu radi činjenja ili nečinjenja neke aktivnosti, a koja bi u slučaju izvršenja dovela do štete po kompaniju.

Postoje brojni „alati" koje kompanije i njihove stručne službe za prevenciju rizika zloupotreba u okviru kompanija, mogu da primene s namerom da se spreči rizični događaj ili makar da se minimiziraju posledice istog. Primeri nekih od alata su: primena internih procedura, uspostavljanje pravila o usklađenosti u poslovanju (eng. compliance), proklamovanje „tone at the tope" atmosfere u organizaciji gde menadžmet kompanije šalje poruku zaposlenima koji je to model ponašanja poželjan, odnosno koji su to standardi ponašanja koji se očekuju od svih zaposlenih u domenu odgovornog ponašanja. Tu su i funkcije kojima je u nadležnosti da primenjuju, ali i da proveravaju da li se uspostavljena pravila ponašanja poštuju. U te funkcije spadaju: službe za usklađenost u poslovanju, službe bezbednosti, službe za prevenciju rizika zloupotreba. Efikasno upravljanje rizicima zloupotreba podrazumeva da se prepoznaju tri linije odbrane od rizika prevara. Prvu liniju čine same poslovne funkcije koje u sklopu svojih svakodnevnih aktivnosti treba da budu svesne i rizika zloupotreba koje mogu da se pojave u toku poslovanja/obavljanja dnevnih aktivnosti i ako prepoznaju navedeni rizik, blagovremeno i na propisan način da obaveste funkcije koje čine drugu liniju odbrane. To su funkcije koje smo već spomenuli: službe za usklađenost u poslovanju, službe bezbednosti, službe za prevenciju rizika zloupotreba. Interna revizija predstavlja treću liniju odbrane od rizika zloupotreba. Nadležnost ove funkcije ogleda se u proveri da li se poslovne aktivnosti odvijaju na način propisan procedurama, podrazumevajući i proveru primene procedure upravljanja rizicima zloupotreba.

Pored već spomenutih načina da se rizici zloupotreba minimiziraju, postoje i mnogi drugi, ali ovom prilikom treba naglasiti da se rizik zloupotreba ne može potpuno neutralisati. U pitanju je rezidualni rizik koji je uvek prisutan, a u kojoj meri će se ispoljiti zavisi od menadžmenta i ostalih zaposlenih, kao i njihove svesti o mogućnostima rizika prevare i posledicama ukoliko se ne posluje u skladu s etičkim standardima. U tom smislu, pored formalnog dela, koji podrazumeva da postoje procedure i propisi poželjnog ponašanja, odnosno koje su posledice nesavesnog ponašanja, neophodna je i suštinska primena preporuka u prevenciji rizika prevara.

Nije moguće predvideti sve rizike zloupotreba koji mogu da se dese jer kompanije posluju u dinamičnom okruženju, a to znači da se menjaju i rizici kojima kompanije mogu biti izložene. Međutim, savesno i odgovorno ponašanje menadžmenta kompanije i samih zaposlenih može da pomogne da se rizici svedu na najmanju moguću meru. Dodatno je poželjno da pored internih službi i internih procedura postoje i eksterne organizacije koje mogu da pomognu u umanjenju štete koja može nastati po osnovu rizika finansijskog kriminala. Napomenuli smo da je u pitanju rezidualni rizik koji jedino može da pokaže različitu amplitudu ponavljanja, svaki put s različitim posledicama/iznosima gubitaka, ali eksterne organizacije, kao što su osiguravajuća društva, mogu da pomognu da rizici gubitaka po osnovu zloupotreba ostave najmanje moguće posledice po kompaniju.

> **Samo stručna ekspertiza u prevenciji, detekciji i istrazi rizika zloupotreba može da pomogne da se identifikuju prevarni događaji i da se utvrde obim i posledice istog. Finansijski forenzičari su lica koja imaju set znanja iz oblasti finansijske forenzike**

Prepoznavanje rizika i uloga osiguranja

Da bi došli do momenta u kome će se organizacije osigurati od rizika finansijskog kriminala, prvi korak jeste da se prepoznaju navedeni rizici. To znači da treba sprovesti, na redovnoj osnovi (godišnje, polugodišnje ili češće) tzv. risk assessment-e. Pod ovim se podrazumeva procena rizika u najširem smislu (opis scenarija rizika, procena izloženosti, frekvencije ponavljanja, centri koji nose trošak i dr.). Kada se urade procene, na bazi istorijskih i očekivanih budućih rizika kojima je organizacija bila izložena ili će biti posmatrajući trendove promene npr. zakonskih propisa, promena u tehnologijama i na tržištu, onda se kroz assessment predlaže plan oporavka.

Tada nastupaju osiguravajuće kuće! Koje sve vrste rizika zloupotreba će biti „pokrivene" osiguranjem, do kog iznosa ili preko kog iznosa gubitka će biti moguće aktivirati polisu osiguranja, ko će raditi procenu gubitaka, ovlašćena lica iz osiguravajućih kuća ili će se procena bazirati na izveštaju stručnih lica u samoj organizaciji, kao što su na primer sertifikovani istražitelji prevara skraćeno CFE ili neka treća lica, ostaje da se definiše planom oporavka. Ovo su samo neka od pitanja koja će osiguranik uputiti osiguravajućim društvima.

Kao primer dobre prakse navešćemo lizing kuća koje već dugi niz godina osiguranje od rizika krađe sredstava lizinga koriste kao instrument za minimiziranje gubitaka od prevara/utaje.

U eri digitalizacije, najviše se spominju sajber napadi i to jeste rizik kom su kompanije možda i najviše izložene u ovom trenutku. Nameće se pitanje, da li prilikom procene rizika zloupotreba postoji svest i/ili saznanje o mogućnosti da se kompanije osiguraju od ove vrste rizika.

Osiguranje i moguće zloupotrebe

Pored rizika zloupotreba koji se može pojaviti kod osiguranika, treba imati u vidu da se rizici finansijskog kriminala mogu prepoznati i kod samih osiguravajućih kuća. Finansijska forenzika prepoznaje nekoliko tipova zloupotreba. Neki slučajevi rizika zloupotreba se odnose na prevarne šeme gde se na primer pokušava aktiviranje premije osiguranja, iako se osigurani događaj realno nije dogodio, dok se određeni tipovi rizika zloupotreba odnose na rizike pranja novca koji opet u krajnjoj instanci imaju za cilj neosnovano bogaćenje. Nekada je vrlo teško dokazati da iza određenog osiguranog događaja postoji krivično delo. Da bi se isto dokazalo potrebno je da istragu sprovodi lice koje ima specifična znanja i veštine u oblasti finansijske forenzike. Samo stručna ekspertiza u prevenciji, detekciji i istrazi rizika zloupotreba može da pomogne da se identifikuju prevarni događaji i da se utvrdi obim i posledice istog. Finansijski forenzičari su lica koja imaju set znanja iz oblasti finansijske forenzike. U ta znanja spada poznavanje pravnog okvira u kojem kompanija posluje, specifičnosti poslovanja same kompanije, svih alata koji se mogu primeniti u prevenciji i istrazi, praćenje trendova na tržištu, sticanje novih znanja i veština, a sve s ciljem da se kontinuirano i na sistematski način radi na prevenciji finansijskog kriminala.

Oblast finansijske forenzike je široka, sveobuhvatna i tema kojom ćemo se sve više baviti u budućnosti jer iskustvo je pokazalo da se radi o vrsti rizika koja je ozbiljna pretnja za kompanije i da uticaj na profitabilnost, možda i na opstanak same organizacije, može ozbiljno biti doveden u pitanje, ako se ovoj problematici ne pristupi na celishodan način. ■