Godina VIII | Broj 16 | Sveska 2/2020 | ISSN 2334-816X

TRENDOVI U POSLOVANJU
NAUČNO-STRUČNI ČASOPIS

SAJBER BEZBEDNOST I POTREBA PROMENE MODELA PRAĆENJA PREVARA I FINANSIJSKOG KRIMINALA

CYBER SECURITY AND NEED TO CHANGE THE MODEL OF MONITORING FRAUD AND FINANCIAL CRIME

Radić Nikola | Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija | bra.radici@hotmail.com

UDK: 343.533::004
007:004.056
343.85:343.53
COBISS.SR-ID 26781193

Sažetak

Svet se menja iz osnova, što dovodi do dramatičnih promena prilika i rizika. U vezi s tim, banke su suočene sa tri međusobno povezane fundamentalne promene. Prvo, digitalna revolucija drastično povećava dostupnost i upotrebu podataka i brzinu donošenja odluka. Drugo, tehnološke inovacije ubrzavaju promene u konkurentskom i potrošačkom okruženju u kojem banke posluju. Konačno, hiperpovezanost višestruko povećava brzinu protoka informacija i preoblikuje način na koji ljudi misle i deluju, utičući na prirodu odnosa banke sa svojim klijentima i drugim zainteresovanim stranama. Brzina promena bez presedana i visok stepen neizvesnosti navode na potrebu uvođenja različitih pristupa rizicima. Za banke i druge finansijske institucije, pretnje se javljaju iznutra i spolja, koje se kreću od neprikladnog i ilegalnog ponašanja zaposlenih, do sofisticiranog sajber kriminala, trgovinskih ratova i klimatskih promena. Kao posledica toga, funkcije rizika moraju postati dinamičnije i fleksibilnije, moraju da pomognu u vođenju institucija kroz sloeni i promenljivo okruženje prilika i rizika, istovremeno ispunjavajući nova očekivanja ključnih aktera – regulatora, zakonodavaca, deoničara, klijenata i zajednice u celini. U radu je posebno apostrofirano pitanje prevara, raznih oblika finansijskog kriminala u odnosu na sajber bezbednost.

Abstract

The world is fundamentally changing , which leads to dramatic changes in opportunities and risks. In this regard, banks are facing three interrelated fundamental changes. First, the digital revolution has drastically increased the availability and use of data and the speed of decision-making. Second, technological innovation accelerates changes in the competitive and consumer environment in which banks operate. Finally, hyperconnection multiplies the speed of information flow and reshapes the way people think and act, influencing the nature of a bank's relationship with its customers and other stakeholders. The unprecedented speed of change and the high degree of uncertainty suggest the need to introduce different approaches to risk. For banks and other financial institutions, threats arise inside and out, ranging from inappropriate and illegal behavior by employees, to sophisticated cybercrime, trade wars and climate change. As a result, risk functions need to become more dynamic and flexible, they need to help guide institutions through a complex and changing environment of opportunities and risks, while meeting new expectations

key actors - regulators, legislators, shareholders, customers (clients) and the community as a whole. The paper especially emphasizes the issue of fraud, various forms of financial crime in relation to cyber security.

Ključne reči: *prevare, finansijski kriminal, sajber bezbednost, podaci, rizik, protivmere*

Keywords: *fraud, financial crime, cyber security, data, risk, countermeasures*

JEL klasifikacija*: G32*

1. Uvod

Svetski ekonomski forum (WEF) konstatovao je 2018. godine da su prevare i finansijski kriminal bili reda trilion (1000 milijardi) dolara, navodeći da su privatne kompanije u 2017. godini potrošile oko 8,2 milijardi dolara u borbi protiv pranja novca [1]. Kriminal, otkriven i neotkriven, postaje sve brojniji i skuplji nego ikad. Prema široko prihvaćenoj proceni, za svaki dolar prevare, institucije gube skoro tri dolara, nakon što se na povezane troškove doda i gubitak zbog prevare. Rizici za banke nastaju od različitih faktora, uključujući ranjivosti od prevara i finansijski kriminal (koji su svojstveni automatizaciji i digitalizaciji), masivan rast obima transakcija i veću integraciju finansijskih sistema unutar zemalja i na međunarodnom nivou. Takođe, pojačani su sajber kriminal i zlonamerno hakovanje [2]. U domenu finansijskog kriminala, u međuvremenu, regulatori kontinuirano revidiraju pravila, sve više uzimajući u obzir ilegalnu trgovinu i pranje novca, a vlade uvode ekonomske sankcije usmerene prema državama, javnim i privatnim entitetima, čak i pojedinacima. Institucije su ustanovile da njihovi trenutni pristupi borbi takvog kriminala ne mogu na zadovoljavajući način da se nose sa mnogim pretnjama i teretima. Iz ovog razloga su lideri transformisali svoje operativne modele kako bi stekli holistički pogled na razvoj finansijskog pejzaža (okruženja) kriminala. Ovaj pogled postaje polazna tačka efikasnog i efektivnog upravljanja rizikom od prevara [3].

2. Evolucija prevara i finansijskog kriminala

Prevare i finansijski kriminal prilagođavaju se razvoju u domenima koje pljačkaju. Pojavom digitalizacije i automatizacije finansijskih sistema, ova krivična dela postaju sve više elektronski sofisticirana i bezlična [4].

U svrhe otkrivanja, zabrane i prevencije, mnoge institucije prave razliku između prevara i finansijskog kriminala. Sa porastom sajber pretnji, koje otkrivaju u kojoj meri su kriminalne aktivnosti postale složenije i međusobno povezane, nevidljive granice se brišu. Štaviše, razlika nije zasnovana na zakonu, a regulatori je ponekad vide kao rezultat organizacionih silosa. Ipak, finansijski kriminal generalno znači pranje novca i nekoliko drugih krivičnih dela, uključujući primanje mita i utaju poreza. S druge strane, prevara, uglavnom, označava mnoštvo krivičnih dela, poput falsifikovanja, kreditnih prevara i pretnji sa insajderskim podacima, koje uključuju obmanu finansijskog osoblja ili službi radi krađe. Finansijske institucije, koje su prevari uglavnom pristupale kao problemu gubitka, u poslednje vreme primenjuju naprednu analitiku za otkrivanje, pa čak i zabrane u realnom vremenu. Kako su razlike između ove tri kategorije krivičnih dela postale manje relevantne, finansijske institucije moraju da koriste mnoštvo alata kako bi zaštitile imovinu od svih njih [5].

Jedna serija krivičnih dela, tzv. napadi Carbanak, koji su započeli 2013. godine, dobro ilustruje sajber profil većeg dela današnjeg finansijskog kriminala i prevara. To su bile krađe banaka zasnovane na malveru (program sa virusom) u ukupnom iznosu većem od milijarde dolara. Napadači, koji su delovali kao banda organizovanog kriminala, pristupili su sistemima putem "fišinga" (phishing), a zatim na prevaru prebacili uvećani saldo na svoje račune i programirali bankomate kako bi izdavali gotovinu saučesnicima koji čekaju [6].

Ono što je značajno jeste da je ovo krivično delo bio simultani, koordinirani napad na mnoge banke. Napadači su pokazali sofisticirano znanje o sajber okruženju i verovatno su se razumeli u bankarske procese, kontrolu, pa čak i ranjivosti u organizacijama i upravljanju. Takođe su iskoristili nekoliko kanala, uključujući bankomate, kreditne i debitne kartice i bankovne transfere. Napadi su otkrili da nestaju značajne razlike između sajber napada, prevara i finansijskog kriminala.

Pristup tim međusobno povezanim rizicima postaje sve više neodrživ, pa je jasno da treba preispitati operativni model. Kako banke počinju da usklađuju poslovanje sa promenom profila finansijskog kriminala, suočavaju se sa sve dubljim vezama između narušavanja sajber bezbednosti i većine vrsta finansijskog kriminala. Na primer, donedavno se većina prevara zasnivala na transakcijama, a kriminalci su koristili slabosti u kontroli. Banke se takvoj prevari suprotstavljaju relativno direktnim kontrolama, tačno zasnovane kanalima. Međutim, u poslednje vreme, prevare zasnovane na identitetu postaju sve zastupljenije, jer prevaranti razvijaju aplikacije za eksploataciju podataka. Sajber napadi postaju sve ambiciozniji i sve prisutniji, narušavajući vrednost i značaj ličnih podataka i bezbednosne zaštite.

U svetu u kome kupci retko kontaktiraju bankarsko osoblje i u potpunosti komuniciraju sa digitalnim kanalima, "digitalno poverenje" je brzo postalo značajan diferencijator korisničkog iskustva. Banke koje nude siguran i brz digitalni interfejs uvideće pozitivan uticaj na prihod, dok one koje to ne učine, erodiraju svoju vrednost i potencijalno gube posao. Savremeno bankarstvo zahteva brže odluke o riziku (kao što su plaćanja u realnom vremenu), tako da banke moraju postići pravi balans između upravljanja prevarama i trenutnog rukovanja sa autorizovanim transakcijama.

Rastući troškovi finansijskog kriminala i rizika od prevare takođe su nadmašili očekivanja. Pošto se banke usko fokusiraju na smanjenje obaveza i troškova efikasnosti, propuštaju se gubici u oblastima poput korisničkog iskustva, prihoda, reputacije, pa čak i usklađenosti sa propisima.

3. Objedinjavanje operacija praćenja finansijskog kriminala i prevara i sajber bezbednosti

Niko ne može sa sigurnošću predvideti kako će banke funkcionisati 2030. godine, ili tačno predvideti moguće poremećaje, bilo da je reč o tehnološkom napretku, makroekonomskim šokovima ili bankarskim skandalima. Ali, osnovni trendovi omogućavaju širok opis onoga što će biti potrebno od funkcije rizika u budućnosti. Trendovi, nadalje, sugerišu da banke sada mogu preduzeti neke inicijative za postizanje kratkoročnih rezultata dok se pripremaju za predstojeće promene. Funkciju rizika u budućnosti oblikovaće sledeći trendovi [7]:

- propisi će se i dalje proširivati i produbljavati,
- očekivanja klijenata rastu u skladu sa promenama tehnologija,
- dalji razvoj tehnologije i napredne analitike,
- pojavljuju se novi rizici,
- funkcija rizika može pomoći bankama da se reše nekih predrasuda,
- pritisak na smanjenje troškova će se nastaviti.

Iako veličina i brzina regulatornih promena verovatno neće biti ujednačene u svim zemljama, budućnost će nesumnjivo doneti više propisa – finansijskih i nefinansijskih – čak i za banke koje posluju u ekonomijama u razvoju. Reakcije banaka na veća očekivanja klijenata biće automatizovane: npr. trenutni odgovor na odluke o kreditima za stanovništvo i preduzeća, i jednostavan, brz proces otvaranja računa na mreži. Da bi banke mogle da isporučuju usluge na ovom nivou, moraće da budu redizajnirane iz perspektive korisničkog iskustva, a zatim digitalizovane. Tehnološke inovacije se kontinuirano pojavljuju, omogućavajući nove tehnike upravljanja rizikom i pomažući funkciji rizika da donosi bolje odluke o riziku po nižim troškovima. Big Data, mašinsko učenje i crowdsourcing ilustruju taj potencijalni uticaj. Neizbežno će funkcija rizika morati da otkriva i upravlja novim i nepoznatim rizicima tokom sledeće decenije. Primeri koji su se pojavili su rizik od modela praćenja, rizik od sajber bezbednosti i rizik od malicioznih programa

(virusa). Bihevioralna ekonomija napravila je velike korake u razumevanju načina na koji ljudi donose odluke vođeni svesnim ili nesvesnim predrasudama. Funkcija rizika mora imati važnu ulogu u smanjenju troškova tako što će omogućiti smanjenje rizika. Pošto će pritisak na smanjenje troškova i dalje trajati, funkcija rizika će morati da nađe dodatne mogućnosti uštede troškova u digitalizaciji i automatizaciji, istovremeno isporučujući "mnogo više za mnogo manje".

U vodećim institucijama radi se na tome da se objedine napori u pogledu finansijskog kriminala, prevara i sajber kriminala. U mnogim bankama frontline i back-office operacije orijentisane su u ovom pravcu. Funkcije rizika i regulatori se takođe razumeju. Sprečavanje pranja novca, iako se sada uglavnom rešava kao regulatorno pitanje, smatra se sledećim horizontom za integraciju. Važni početni koraci za institucije koje ulažu napore u integraciju su precizno definisanje prirode svih povezanih aktivnosti upravljanja rizikom i definisanje uloga i odgovornosti na linijama "odbrane". Ovi koraci će obezbediti potpunu, jasno razgraničenu pokrivenost – poslovnim i preduzetničkim funkcijama (prva linija odbrane) i funkcijom rizika, uključujući finansijske kriminalne radnje, prevare i operacije sajber-bezbednosti (druga linija) – istovremeno eliminišući dupliranje napora.

Svi rizici povezani sa finansijskim kriminalom uključuju tri vrste protivmera (tabela 1):

- identifikovanje i autentifikacija kupca,
- praćenje (nadzor) i otkrivanje anomalija u transakcijama i ponašanju, i
- odgovor na ublažavanje rizika i problema [8].

Svaka od ovih aktivnosti, bilo da je preduzeta kao odgovor na prevaru, narušavanje ili napad na sajber bezbednost ili drugi finansijski kriminal, podržana je mnogim sličnim podacima i procesima. Povezivanje ovih izvora podataka sa analitikom značajno poboljšava vidljivost, a istovremeno pruža mnogo dublji uvid u poboljšanje sposobnosti otkrivanja. U mnogim slučajevima to, takođe, omogućava preventivne mere.

Zauzimajući holistički pogled na osnovne procese, banke mogu usmeriti poslovnu i tehnološku arhitekturu na bolje korisničko iskustvo, bolje donošenje odluka o riziku i veću troškovnu efikasnost. Tada se, po potrebi, može rekonfigurisati i organizaciona struktura.

Za analizu su važna tri modela za rešavanje finansijskog kriminala, koji se odlikuju stepenom njihove integracije u procesima i operacijama za različite vrste krivičnih dela. Uopšteno govoreći, iskustvo pokazuje da su upravljanje i organizacioni dizajn glavna tema za razvoj operativnog modela. Bez obzira na određeni izbor, institucije treba da okupe prave ljude u agilnim timovima, zauzimajući holističkiji pristup zajedničkim procesima i tehnologijama i udvostruče analitiku kako bi se razvila sofisticiranija rešenja. Uobičajeno je da institucija započne sa kolaborativnim modelom i postepeno se kreće ka većoj integraciji, u zavisnosti od dizajnerskih rešenja [9].

Tabela 1. Osnovne protivmere u otkrivanju finansijskog kriminala i prevara

	Identifikacija Ko je moj kupac?	**Nadzor** Koje transakcije su zakonite?	**Odgovor** Kako da reagujem na pretnju?
Finansijski kriminal	• ocena rizika klijenta • pažnja prema klijentu	• nadzor transakcija • skrining imena • skrining plaćanja	• nadzor sumnjivih aktivnosti • finansijska obaveštajna jedinica • upravljanje spiskom • ne preko banke
Prevara	• verifikacija identiteta, uključujući digitalno i nedigitalno prisustvo	• nadzor transakcija i donošenje odluka • analitika pomoću uređaja i glasa	• istražni i timovi za rešavanje
Sajber bezbednost	• upravljanje akreditivima	• centar za bezbednost informacija i mrežni operativni centar	• centar za bezbednost informacija • forenzika • timovi za rešavanje
Sinergija među funkcijama	• određivanje pokazatelja rizika korišćenjem zajednilkih ili sličnih podataka, kao što su finansijski, digitalni otisak i nedigitalni snimci	• određivanje pokazatelja transakcija korišćenjem slične analitike i zajednička upotreba slučajeva zasnovanih na vremenu, destinaciji, izvoru, vrednosti, frekvenciji, sredstvu i geolokacionim informacijama	• zajednička povratna sprega za razvoj holističkog pogleda na načine rada i podsticanje razvoja slučajeva odozgo nadole • udruživanje resursa i mogućnosti

3.1. Kolaborativni model

U kolaborativnom modelu, koji predstavlja status quo za većinu banaka, svaki od domena – finansijski kriminal, prevara i sajber bezbednost – zadržava svoje nezavisne uloge, odgovornosti i izveštavanje. Svaka jedinica gradi svoj nezavisni okvir, sarađujući na taksonomiji rizika, podacima i analitici za praćenje transakcija, prevara i kršenja. Pristup je poznat regulatorima, ali malim bankama pruža neophodnu transparentnost za razvijanje holističnijeg pogleda na rizik od finansijskog kriminala. Pored toga, kolaboracioni model često dovodi do praznina ili preklapanja među odvojenim grupama i ne uspeva da ostvari koristi koje dolaze sa većom funkcionalnom integracijom. Oslanjanje modela na male, diskretne jedinice, takođe, znači da će banke biti manje sposobne da privuku najviše rukovodstvo.

3.2. Delimično integrisani model za sajber bezbednost i prevare

Mnoge institucije sada rade na modelu delimične integracije, u kojem su sajber bezbednost i prevare delimično integrisani kao druga linija odbrane. U ovom modelu svaka jedinica zadržava nezavisnost, radi iz konzistentnog okvira i taksonomije, ali sledi obostrano prihvaćena pravila i odgovornosti. Tako konzistentna arhitektura za prevenciju (kao što je autentifikacija kupaca) se usvaja, dele se procesi identifikacije i procene (uključujući taksonomiju) i primenjuju se slični procesi zabrane. Dublje prevladavaju integralne prednosti, uključujući konzistentnost u nadzoru i otkrivanju pretnji i manji rizik od praznina i preklapanja. Međutim, pristup ostaje dosledan postojećoj organizacionoj strukturi i malo remeti tekuće poslovanje. Stoga se transparentnost ne povećava, jer se održava odvojeno izveštavanje.

3.3. Objedinjeni model

U potpuno integrisanom pristupu, operacije finansijskog kriminala, prevara i sajber bezbednosti objedinjene su u jedinstveni okvir, sa zajedničkom imovinom i sistemima koji se koriste za upravljanje rizikom u celoj organizaciji. Model ima jedinstven pogled na kupca i deli analitiku. Konvergencijom rizika poboljšava se transparentnost pretnji u celoj organizaciji, čime se bolje otkrivaju najvažniji osnovni rizici. Nedostatak ovog modela je što podrazumeva značajne organizacione promene. Međutim, čak i sa organizacionim promenama i konvergencijom rizika, rizici ostaju diferencirani.

4. Imperativ integracije

Integracija operacija identifikacije prevara i sajber bezbednosti sada je imperativ, jer su ta krivična dela već duboko povezana. Poboljšane mogućnosti analitike podataka sada su ključni alati za sprečavanje, otkrivanje i ublažavanje pretnji. Većina naprednih institucija radi na takvoj integraciji, kreirajući ujednačeniji model zasnovan na uobičajenim procesima, alatima i analitici. Aktivnosti na sprečavanju pranja novca takođe se mogu integrisati, ali sporijim tempom, sa posebnim fokusom na preklapajuća područja.

Polazna tačka za većinu banaka bio je model saradnje, ali keke banke sada prelaze sa ovog modela na model koji integriše sajber bezbednost i prevare. U sledećem horizontu, potpuno integrisani model omogućava sveobuhvatan tretman sajber bezbednosti i finansijskog kriminala, uključujući borbu protiv pranja novca. Povećana integracija može postepeno poboljšati kvalitet upravljanja rizikom, jer poboljšava osnovnu efektivnost i efikasnost u svim kanalima, tržištima i linijama poslovanja.

4.1. Strateška prevencija: Pretnje, predviđanje i kontrole

Ideja strateške prevencije je da se predvidi rizik, a ne samo da se na njega reaguje. Da bi predvidele gde će se pojaviti pretnje, banke treba da redizajniraju operacije sa klijentima i interne operacije i procese na osnovu kontinuirane procene stvarnih slučajeva prevara, finansijskog kriminala i sajber pretnji. Pogled na njih razvija se prema kupcu. Kontrole su dizajnirane holistički, oko procesa, a ne tačaka. Takav pristup može značajno poboljšati zaštitu banke i njenih klijenata (tabela 2).

Tabela 2. Primer potencijalne prevare

	Otvaranje računa	**Promena računa**	**Izvrešenje uplate**	**Uplata depozita**
Aktivnost koju pokreće klijentc	Klijent otvara novi račun ili dodaje novi račun preko mobilne mreže, bankomata ili filijale	Ažuriranje postojećeg korisničkog računa (npr. dodavanje korisnika ili promena adrese)	Klijent plaća sebi ili trećoj strani preko platne, kreditne ili debitne kartice ili putem mrežne transakcije	Klijent vrši prenos ili depozit na svoj račun
Kanal napada				
Bankomati	• Krađa identiteta • Veštački ID • Račun koji generiše zaposleni • Malver (program sa virusom)	• Malver (program sa virusom)	• Skimming kartice (lažni čitač kartica koji služi za očitavanje podataa sa platne kartice) • Lažni PIN kod • Zadržavanje novčanica • Duplikat kartice • Storniranje transakcije • Malver (program sa virusom)	• Pranje novca ili finansiranje terorizma
Kartica ili e-trgovina		• Preuzimanje računa • Promena adrese • Druga kartica • Malver (program sa virusom	• Prevara bez kartice • Skimming kartice • Sajber napad • Malver (program sa virusom)	
e-banking ili mobilna mreža		• Dodavanje lažnog korisnika • Preuzimanje računa • Malver (program sa virusom)	• Sajber napad • Malver (program sa virusom) • Transakcija koju izvršava zaposleni	
Filijala		• Preuzimanje računa	• Nepoznato	

Da bi došle do realnog pogleda na ove prestupe, institucije treba da razmišljaju poput kriminalaca. Kriminalac koristi slabe tačke sistema. Trenutna odbrana od sajber kriminala i prevara fokusirana je na kontrolne tačke ili silose, ali zapravo nije zasnovana na razumevanju kako se kriminalci ponašaju. Na primer, ako banke poboljšaju tehnologiju odbrane, kriminalac će migrirati negde drugde - u kol centre, filijale ili kupce. Usvajanjem ovog načina razmišljanja, banke će moći da prate migracioni tok kriminalba, sagledavajući određenu vrstu krivičnog dela od nastanka do izvršenja, mapirajući sve mogućnosti. Dizajnirajući kontrole oko ovog principa, banke su primorane da objedine discipline (poput autentifikacije i analize glasovnog stresa), što poboljšava efektivnost i efikasnost [10].

Efikasnost obima i procesa integrisane funkcije prevara i sajber rizika mogu poboljšati otkrivanje i predviđanje pretnji i eliminisati dupliranje napora i resursa. Uloge i odgovornosti mogu se razjasniti tako da ne ostanu praznine između funkcija ili unutar druge linije odbrane u celini. Konzistentne metodologije i procesi (uključujući taksonomiju i identifikaciju rizika) mogu biti usmereni ka izgradnji razumevanja i upravljanja rizicima. Integrisanje operativnih procesa i kontinuirano ažuriranje procena rizika omogućavaju institucijama da dinamički ažuriraju svoje stavove o rizičnosti klijenata i transakcija [11].

Kroz integraciju, potencijal prevara sa podacima, automatizacijom i analitikom banke može se potpunije ostvariti. Integrišući podatke o odvojenim funkcijama, kako iz internih tako i iz eksternih

izvora, banke mogu poboljšati identifikaciju i verifikaciju klijenata. Veštačka inteligencija i mašinsko učenje, takođe, mogu da podrže prediktivnu analitiku kada je podržana agregatnim izvorima informacija. Moguće je brže generisati uvide – da bi se, na primer, utvrdila povezanost između napada na akreditive, verovatnoću preuzimanja računa i kriminalno kretanja novca. Preklapanjem takvih uvida u rešenja zasnovana na pravilima, banke mogu smanjiti stope lažnih pozitivnih rezultata u algoritmima detekcije. To smanjuje troškove i pomaže istražiteljima da ostanu usredsređeni na stvarne incidente [12].

Integrisani pristup riziku od prevare, takođe, može rezultirati optimizovanim korisničkim iskustvom. Očigledno je da znatna poboljšanja u zadovoljstvu kupaca pomažu u oblikovanju njihovog ponašanja i poboljšavaju poslovne rezultate. U kontekstu modela upravljanja rizikom, ciljevi uključuju segmentaciju prevara i bezbednosnih kontrola u skladu sa iskustvom i potrebama kupaca, kao i upotrebu automatizacije i digitalizacije [13], [14].

Objedinjeno upravljanje rizikom od prevara i finansijskog kriminala podiže poverenje u digitalne sajber pretnje, koncept koji se banke oblikuju u diferencijaciji klijenata. Bezbednost je očigledno u središtu ovog koncepta i njegov je najvažniji činilac. Međutim, faktori poput pogodnosti, transparentnosti i kontrole takođe su važne komponente digitalnog poverenja. "Težine" atributa poverenja koje kupci dodeljuju variraju prema segmentu, ali vrlo često su prednosti kao što je provera autentičnosti bez problema ili brzo rešavanje sporova neophodni graditelji digitalnog poverenja.

5. Zaključak

Cilj transformisanog operativnog modela je holistički pogled na evolutivni pejsaž finansijskog kriminala. Ovo je neophodno stanovište efektivnosg i efikasnog upravljanja rizikom od prevara, koje ističe značaj nezavisnog nadzora i izazove kroz dužnosti jasno naznačene u tri linije odbrane. Na kraju, institucije će morati da integrišu poslovne, operativne, bezbednosne i timove za rizik radi efikasne razmene obaveštajnih podataka i pravovremene reakcije na pretnje.

Kada banke kreiraju put ka jedinstvenom operativnom modelu za finansijski kriminal, prevare i sajber bezbednost, moraju jasno postavljati pitanja o procesima i aktivnostima, ljudima i podacima u organizaciji, alatima i tehnologijama i upravljanju.

Većina banaka to započinje uskom integracijom svojih jedinica za sajber bezbednost i prevare. Kako poboljšavaju razmenu informacija i koordinaciju, postaje sve efikasnost i efektivnije u identifikaciji i rešavanju rizika. Državne banke redefinišu organizacione "linije i okvire" i, što je još važnije, uloge, odgovornosti, aktivnosti i sposobnosti potrebne za svaku liniju odbrane.

Većina banaka nije uspela da u potpunosti objedini funkcije rizika povezane sa finansijskim kriminalom, mada su nekoliko njih ostvarile dublju integraciju. Jedna vodeća američka banka uspostavila je holistički ”centar izvrsnosti” kako bi omogućila donošenje odluka ”od početka do kraja”, u vezi sa prevarama i sajber bezbednošću. Od prevencije do istrage i oporavka, banka može ukazati na značajan napredak u efikasnosti. Kombinujući sve operacije povezane sa finansijskim kriminalom, uključujući prevare i borbu protiv pranja novca, u jednu globalnu uslužnu službu, banka je stekla holistički pogled na rizik klijenta i smanjila operativne troškove za približno 100 miliona dolara.

Kako kriminalni prekršaj u sektoru finansijskih usluga postaje sve sofisticiraniji i probija se kroz tradicionalne granice rizika, banke shvataju da njihove različite funkcije rizika postaju skuplje i manje efikasne. Stoga lideri preispituju svoje pristupe kako bi iskoristili sinergiju dostupnu u integraciji. Konačno, prevara, sajber kriminal i sprečavanje pranja novca mogu se konsolidovati u okviru holističkog pristupa zasnovanog na istim podacima i procesima. Većina pogodnosti dostupna je u kratkom roku, ali kroz integraciju operacija prevara i sajber bezbednosti.

6. Bibliografija

[1] Craig D., Why we need to talk about financial crime, World Economic Forum, Geneva, 2018.
[2] Härle P., Havas A., Samandari H., The future of bank risk management, McKinsey, New York, 2016.
[3] Mikkelsen D., Pravdic A., Richardson, B., Flushing out the money launderers with better customer risk-rating models, McKinsey, New York, 2019.
[4] Crespo I., Kumar P., Noteboom, P., Taymans, M., The evolution of model risk management, McKinsey, New York, 2017.
[5] Boehm J., Curcio N., Merrath P., Shenton L., Stähle T., The risk-based approach to cybersecurity, McKinsey, New York, 2019.
[6] Europol, Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain, Hague, 2018.
[7] KPMG, Emerging trends in risk management, London, 2017.
[8] Bevan O., Boehm J., Manocaran M., Riemenschnitter R., Cybersecurity and the risk function, McKinsey, New York, 2018.
[9] Wallace T., Raggl A., Tejada M., Agarwal R., Model Risk Management, Global Update, McKinsey, New York, 2019.
[10] Brand A., Risk in Financial Services, Chartered Institute for Securities & Investment, London, 2016.
[11 Helbekkmo H., Levy C., White O., Creating the bank enterprise risk management function of the future, Journal of Risk Management in Financial Institutions, Henry Stewart Publications, 2019, 12(4): pp. 26-31.
[12] Garcia F. J., Financial Risk Management, Palgrave McMillan, Cham, 2017.
[13] Tomas-Miskin S., Vitomir J., International Review, 2019, No.1-2: pp. 101-109.
[14] Rabrenovic M., Mitrovic R., Kovacevic B., The Relationship Between Strategic Management and Public Relationsand their Implications for Financial Operations, International Review, 2020, No. 1-2: pp. 89-93.