FBIM Transactions
DOI 10.12709/fbim.03.03.02.08

UPRAVLJANJE RIZICIMA ELEKTRONSKOG POSLOVANJA

E-BUSINESS RISK MANAGEMENT

Milan Mihajlović
Fakultet za poslovno industrijski menadžment Beograd, Univerzitet „Union - Nikola Tesla“, Beograd, Srbija

Vlada Živanović
Državna revizorska institucija, sektor za reviziju budžeta lokalnih vlasti, Beograd, Srbija

Nedeljko Karakaš
Beogradska poslovna škola, Beograd, Srbija

JEL Category: **G32, M15, O33**

Apstrakt

Elektronsko poslovanje je, kao i svako drugo poslovanje, rizično. Prvi korak u upravljanju rizicima i njihovom smanjenju jeste saznanje da rizici postoje. U današnjem savremenom okruženju i Internet poslovanju, upravljanje rizicima ima ključnu ulogu u zaštiti organizacije. U ovom radu biće predstavljen proces upravljanja rizicima koji obuhvata proces identifikovanja rizika, analize i procene rizika, preduzimanje koraka za njegovo smanjenje (tretiranje rizika) i merenje rezultata. Identifikovanje rizika, kao prvi korak u procesu upravljanja rizicima ima za cilj da ustanovi koji su to faktori koji mogu ugroziti poslovanje kompanije, jer da bi se moglo upravljati rizicima, potrebno ih je prvo prepoznati. Analizom i procenom rizika se utvrđuje *kakav će negativan, a u nekom slučaju i pozitivan, uticaj identifikovani rizik imati na ostvarenje postavljenih ciljeva kompanije. Postupanje sa rizicima predstavlja proces selekcije i implementacije najbolje strategije tretiranja rizika, koja ima za cilj da smanji, ukloni, prihvati rizik ili ga prenese na neko treće lice. Merenje rezultata kao poslednji korak predstavlja proveru efikasnosti primenjene strategije tretiranja rizika.*

Ključne reči*: rizik, elektronsko poslovanje, upravljanje rizicima, strategija*

Adresa autora zaduženog za korespodenciju:
Milan Mihajlović
mihajlovicmilan89@gmail.com

Abstract

E-business is as risky as any other business. The first step in risk management and risk reduction is

awareness that risk exists. In today's modern environment and Internet operations, risk management plays a critical role in protection of organizations. This article deals with the risk management process which includes the process of identifying risk, risk assessment and analysis, risk response and evaluation of the results. Identifying risks, as a first step in risk management aims to recognize which factors may jeopardize the company's operations, because in order to manage risks, they need to be identified. Risk assessment and analysis should determine what kind of negative impact (in some cases positive impact) identified risk will have on achievement of the company's goals. Risk response is a process of selection and implementation of the best risk response strategy, which aims to reduce, remove, accept or transfer risk to a third party. Evaluation of the results as the last step in risk management needs to measure the efficiency of chosen risk response strategy.

***Keywords**: risk, e-business, risk management, strategy*

1. UVOD

Pod pojmom elektronsko poslovanje se podrazumeva poslovanje primenom računarskih tehnologija. Potrebno je istaći razliku između Internet poslovanja i elektronskog poslovanja. Internet poslovanje predstavlja kupovinu i prodaju putem Interneta. Elektronsko poslovanje obuhvata celu organizaciju poslovanja preduzeća u mrežnom okruženju, organizovanje poslovne komunikacije sa poslovnim partnerima i klijentima, kao i brigu o klijentima i poslovnim partnerima.(Čekerevac, 2015)

Elektronsko poslovanje jeste novi način poslovanja, omogućuje nove izvore prihoda, smanjenje troškova itd. Međutim, nije sve tako idealno, mnoge Internet kompanije su propale. Neke su bile dobro formirane u početku, ali nisu dovoljno brzo reagovale na promene, druge nisu investirale u razvoj, treće nisu predvidele buduće događaje, ili jednostavno: nisu dovoljno dobro upravljale rizicima poslovanja. Rizici se nalaze svuda, menadžeri imaju obavezu da prepoznaju, upravljaju i smanje te rizike.

Dakle, koji su to rizici koje treba razmotriti kada se osniva e-organizacija? Dva očigledna rizika jesu pad računarskih sistema i pretnje od hakera koji pokušavaju da napadnu ove sisteme. Međutim, postoji i jedan širi skup rizika koje treba prepoznati. Pretnje mogu doći iz direktnih ili indirektnih izvora. Uzrok mogu biti ljudske greške (namerne ili nenamerne). Pretnje mogu doći iz okruženja, mogu nastati unutar organizacije ili izvan nje. Uticaj ovih rizika može biti privremen ili trajan, a njihova posledica može se odraziti na poverljivost, integritet, tačnost i pouzdanost informacija.

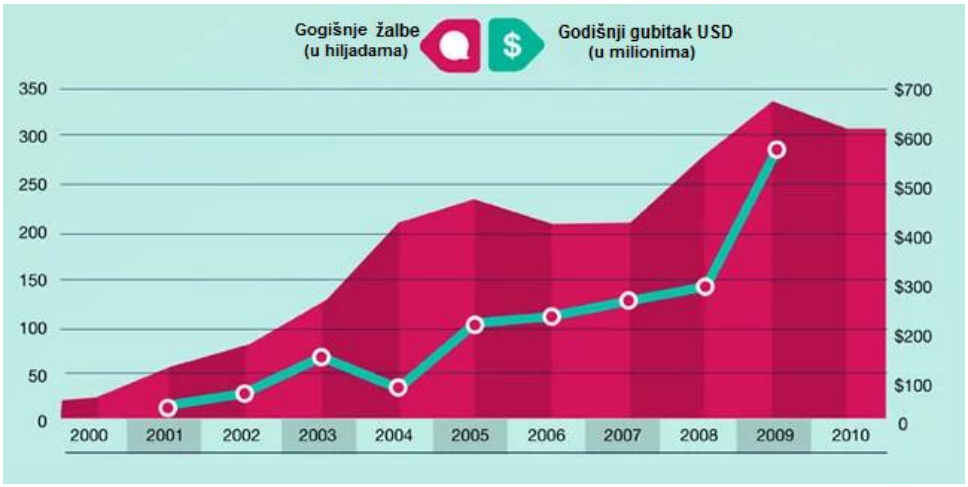
Da bi se tretirali rizici, tj. preduzeli koraci za njihovo smanjenje, potrebni su analiza identifikovanih rizika i procena njihovog uticaja na ostvarenje ciljeva kompanije. Postoji određen broj strategija koje se mogu primeniti u procesu upravljanja rizicima. Glavna pitanja koja se postavljaju jesu: koju strategiju primeniti, kada je primeniti i na koje rizike je primeniti? Odgovor na ova pitanja direktno utiče na efikasnost procesa upravljanja rizicima, kao i na ostvarenje ciljeva kompanije.

2. IDENTIFIKOVANJE RIZIKA

U elektronskom poslovanju mogu se razlikovati sedam vrsta rizika:

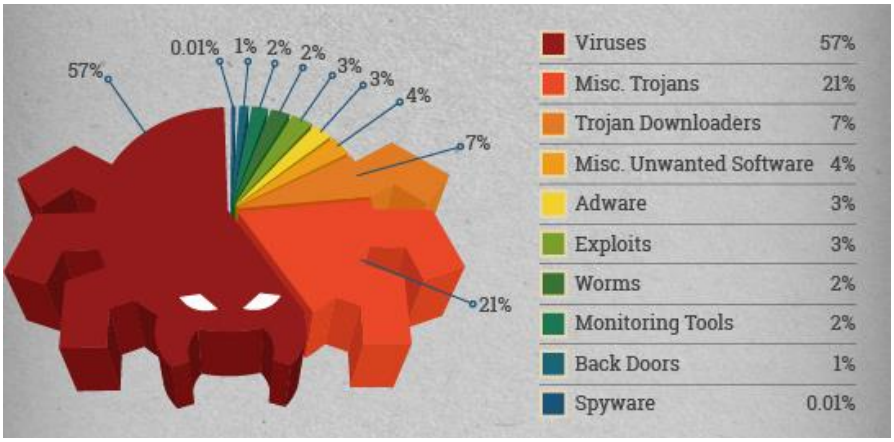
– ***Hakeri.*** *Ova* vrsta rizika dolazi od onih pojedinaca ili organizacija koje imaju nameru da se bave ilegalnim aktivnostima, kao što su prevare, infekcije, internet grafiti, „denial-of-service“ (onesposobljavanje veb stranice) itd. Online prevare su u sve većem porastu. Korišćenje Interneta svakog dana, čini se da je omogućilo povećanje sigurnosti i bezbednosti. Međutim, stvarnost je takva da su hakeri jednostavno postali bolji i lukaviji nego ranije, tako da je vođenje računa o prevarama na Internetu i dalje veoma značajno. Od 2005. do 2009. godine Internet prevare iz godine u godinu imaju konstantan porast. Novčani gubitak od primljenih i obrađenih žalbi od prevara je skoro 300 miliona dolara godišnje. Tri najčešće lokacije za internet prevare su SAD (65,9%), Velika Britanija (10,4%) i Kina (3,1%). (Wachs, Junger, & Sittichai, 2015)

Još jedna od ilegalnih aktivnosti hakera jesu infekcije. Mnoge velike kompanije su već preduzele korake za odbranu od infekcija. Međutim, male firme i domaćinstva nemaju adekvatne antiviruse i programe za odbranu od ove vrste napada, tako da su oni najviše zahvaćeni. Postoji veliki broj različitih infekcija, a neki od najznačajnijih su predstavljeni na slici 2.



Slika 1. Broj primljenih žalbi i novčanih gubitaka USD

Izvor:(Anson, 2012)



Slika 2. Različite vrste infekcija

Izvor: (Anon, 2014)

Posedovanje veb sajta jeste prilika da se reklamira kompanija govoreći svetu o svojim proizvodima, uslugama i mogućnostima. Ovo ima za pretpostavku da jedino kompanija može postavljati slike, tekst i drugo na svom veb sajtu. Ukoliko kompanija odluči da napravi pričaonicu („Internet chat room“), gde bilo ko može napisati šta želi, to otvara mogućnost još jednoj ilegalnoj aktivnosti, a to su Internet grafiti. Internet grafiti funkcionišu na isti način kao i klasični grafiti koje možemo videti na zidovima zgrada, a cilj im je da prenesu neku poruku ili neprijatnost. Kompanije često na svojim veb sajtu napišu “100% sigurno od napada”, što može izazvati i ohrabriti hakere da probiju tu zaštitu i naprave štetu. (Leukfeldt, 2014)

Kompanije koje u velikoj meri zavise da Internet trgovine, tzv. napad uskraćivanjem usluga („denial of service“) trebaju smatrati za veliki rizik. Ovo se odnosi na ometanje tehnologije na takav način da spreči kompaniju da vrši svoje aktivnosti zasnovane na Internetu. Najčešća posledica je gubitak veze između računarskih sistema kompanije i potencijalnih posetilaca sajta. Neke poznate Internet kompanije su bile zahvaćene ovim napadom, a to su Yahoo!, e-Bay, CNN.com, Amazon i E*Trade.

– ***Tržišno okruženje***. U okruženju postoje legalne aktivnosti i promene koje mogu pretiti kompaniji. Ponašanje potrošača, snaga dobavljača i kretanje kursa su primeri koji direktno mogu uticati na profitabilnost. Mnoge kompanije su pokazale veliko interesovanje za podršku i razvoj B2B trgovini, a u okviru toga najčešće postavljano pitanje jeste: kakav će efekat promena cena velikih kompanija imati na male, a cilj je jasan, osvojiti tržište. Sve kompanije u manjoj ili većoj meri zavise od svojih dobavljača.

Za e-poslovanje tri oblasti su veoma značajne: IT operacije, logistika i disintermedijacija. Na primer, ukoliko je sajt kompanije baziran na ISP, onda promocija proizvoda i prodaja direktno zavisi od sposobnosti ISP da održi veb sajt funkcionalan. Takođe, bitno je da proizvodi budu transportovani do svoje destinacije na vreme, samim tim logistika se mora pažljivo pratiti. U isto vreme treba imati rezervne planove, ukoliko dođe do nefunkcionalnosti IT tehnologije ili transporta. Poslovni rizik usled kretanja deviznog kursa najviše zavisi od iskustva kompanije.

– ***Pravna regulativa***. Postoji sve veći broj zakona i regulativa koje kompanija treba da ispoštuje. U većini zemalja zakonom su uključeni e-komunikacije, zaštitu Internet podataka, zaštitu ljudskih prava itd. Na primer, ukoliko kompanija namerava da čita mejlove svojih zaposlenih onda im mora to unapred objasniti, kao i staviti tu vrstu provere u ugovoru o radu. Pored ovih posebnih zakona i regulativa, za e-poslovanje važe i uobičajena pravila kao što su zakon o patentu, robne marke, autorska prava itd.

– ***Ljudi***. Kada se kaže ljudi, tu se prvenstveno misli da menadžere i osoblje. Oni su ujedno jedan od rizika na koje kompanija najviše može da utiče. Glavni rizik ovde jeste problem u stavovima, smanjenje razumevanja, kao i mogućnost da neko od osoblja postane jedan od hakera. Korišćenje e-mejla i veb sajtova kao sredstva komunikacije je bio glavni razlog usvajanja Interneta za poslovanje. Ali potencijalna zloupotreba ovih medija predstavlja pretnju za elektronsko poslovanje. Kada kompanija poseduje lične i poverljive podatke o svojim kupcima, neophodno je da je osoblje upoznato i motivisano da izbegava zloupotrebu ovih podataka. Na primer, banka poseduje finansijske podatke neke firme, i ti podaci ne smeju biti dostupni nekoj drugoj firmi osim same banke. Isto tako podaci o kreditnoj kartici se nikada ne bi trebali slati e-mejlom, iz već navedenih razloga. Takvo poslovanje vodi u pad poverenja klijenata, a samim tim i pad poslovanja, a na kraju može dovesti i do likvidacije takve banke. Greške se mogu napraviti i u onlajn trgovini. Zaposleni trebaju voditi računa prilikom davanja informacija o ceni. Ukoliko se cena proizvoda pogrešno napiše, npr. da je 19,99 dolara umesto 1999 dolara, kupci u tom slučaju imaju prava da traže od kompanije da ispoštuje obavljenu transakciju.

– ***Poslovni procesi***. Efektivnost i efikasnost poslovnih procesa kompanije mogu dovesti do novog seta rizika. Znanje i informacije su postale važna poslovna imovina svih kompanija, kao i potreba njihove zaštite. Na primer, integritet podataka i intelektualna svojina trebaju biti zaštićeni putem ugovora. Poslovanje koje ne ispunjava očekivanja kupaca za posledicu može imati gubitak baze klijenata, na primer kašnjenje isporuke ili neodgovaranje na e-mejl kupaca. (Rotaru & Wilkin, 2011)

– ***Tehnologija***. Informacione i komunikacione tehnologije su glavni deo e-poslovanja. Ukoliko se njima pravilno upravlja, one mogu postati ključne za poslovni uspeh. S obzirom da su ključne, ukoliko zakažu onda će i kompanija biti u problemu. Prekid rada veb sajta je jedan od najvećih problema koji se mogu desiti u e-poslovanju. Utiče na smanjenje poslovanja, a samim tim i gubitak kupaca (zašto bi se kupac vratio na veb sajt koji ne radi). Kao što je u proizvodnim kompanijama proizvodni pogon ključna infrastruktura, tako su za e-kompanije softveri koji omogućavaju rad veb sajta, pa se u skladu sa tim moraju pažljivo i konstantno pratiti i unapređivati.

– ***Poslovna strategija***. Poslednji i možda najveći rizik jeste izbor poslovne strategije. Poslovna strategija treba biti logična, prihvatljiva i održiva. Strategija mora biti logična, tj. da ima smisla i da nudi proizvod ili uslugu koje tržište želi sada ili u budućnosti. Prihvatljivost se odnosi da reakcije drugih zainteresovanih strana. I na kraju, kompanija mora biti u mogućnosti da zaštiti svoj proizvod ili uslugu od imitacije. U svakom slučaju, inovacija je ta koja donosi velike nagrade i na šta poslovna strategija treba biti orjentisana. Međutim, ne treba zaboraviti da svaka inovacija, pored velike nagrade donosi i veliki rizik. (Živanović, 2014)

3. ANALIZA I PROCENA RIZIKA

Analiza i procena rizika je sistemski proces za identifikaciju i vrednovanje događaja koji mogu uticati na ostvarenje ciljeva, pozitivno ili negativno. Kada ovi događaji počnu da utiču ili se predvidi da će uticati na poslovanje oni postaju rizik. Analiza i procena rizika se vrši po zahtevu regulatornih organa ili ako kompanija proceni da je potrebno. Razumevanje ciljeva organizacije i vrste mogućih rizika je ključna determinanta

procene rizika. Ciljevi mogu biti široki (npr. strateški ili operativni) i uski (koji se odnose na proizvod, proces, funkciju itd.). Isto tako mogući rizici mogu da se odnose na velike kategorije (tržište, kredit, likvidnost itd.) ili na tačno određene, kao što je na primer rizik dobavljača. Na kraju treba definisati obim procene, kojim se može obuhvatati cela organizacija ili samo neki njeni delovi. Kada se obim definiše, rizici koji mogu nastati se rangiraju po uticaju ili verovatnoći nastanka. Na osnovu dobijenih rezultata se sastavlja grafički prikaz uticaja rizika ili verovatnoće njihovog nastanka. Ovo omogućava kompanijama da razviju strategije odgovora i odrede pravilnu alokaciju resursa. Na primer, takozvana „*heat map",* koja prikazuje mogućnost kompanije da preuzme rizik, kao i kakav će uticaj on imati na poslovanje kompanije. „*Heat map"* prikazuje podatke u dvodimenzionalnoj mapi predstavljeni bojama. Zbog toga ima bolji vizuelni prikaz od nekih drugih grafičkih prikaza. (Nastase, Nastase, & Sova, 2007)

Kvalitativne procene su najosnovniji oblik procene rizika, i one klasifikuju potencijalne rizike na osnovu uticaja i verovatnoće njihovog nastanka. Nešto složeniji oblik procene rizika su kvantitativne metode. Kako podaci sve više postaju dostupni iz internih dešavanja (transakcijskih grešaka, žalbe potrošača) i eksternih dešavanja (praćenje statusa kompanije od strane neke eksterne firme) tako se i vrši konstantna procena rizika. Ovakvi detaljniji podaci omogućavaju bolju analizu izloženosti potencijalnim rizicima i brži i efikasniji odgovor na rizične situacije. Oslanjajući se na kvalitativne i kvantitativne procene, putem benčmarkinga se može izvršiti upoređivanje rizika sa drugim sličnim organizacijama unutar industrijske grane. (Chaffey, 2009)

Bord direktora često traži široku procenu rizika da bi se ključni rizici identifikovali i sprečili. Međutim, pored ove široke procene, ne bi trebalo isključiti druge, uže procene. Funkcija interne revizije na primer, treba proceniti rizik da bi planirali reviziju sledeće godine, poslovne jedinice trebaju vršiti procene rizika za poslovno planiranje itd. Ove individualne procene treba uskladiti sa ključnim ciljevima kompanije i integrisati ih sa širokom procenom rizika. Primeri čestih procena rizika su:

- Strateška procena rizika: odnosi se na analizu organizacijske misije, vizije i ciljeve koju obično obavlja rukovodstvo kompanije.
- Operativna procena rizika: odnosi se na analizu rizika koji utiče na smanjenje rezultata putem neuspelih procesa, ljudi, sistema ili eksternih događaja.
- Procena rizika usklađenosti: procena faktora rizika koji se odnose na usklađenosti sa pravnom regulativom, politikama, procedurama, etike, poslovnih standarda itd.
- Procena rizika finansijskih izveštaja: odnosi se na rizike vezane za greške u izveštajima pri ulazu i izlazu robe u organizaciji.
- Procena rizika od prevara: odnosi se na procenu potencijalnih slučajeva prevara koji mogu uticati na usklađenosti sa standardima, poslovnom praksom, integritet finansijskih izveštaja itd.
- Procena tržišnih rizika: procena kretanja na tržištu koji mogu uticati na performanse kompanije, na primer porast kamatne stope.
- Procena kreditnog rizika: odnosi se na procenu da li će dužnik ispuniti svoje obaveze u skladu sa dogovorenim uslovima.
- Procena rizika kupaca: odnosi se na procene profila kupaca koji bi potencijalno mogli uticati na reputaciju organizacije, kao što je kreditna sposobnost, namere kupaca itd.
- Procena rizika lanca snabdevanja: procena rizika koji su povezani sa identifikovanjem inputa i logistike potrebne za stvaranje proizvoda ili usluge.
- Procena rizika proizvoda: procena faktora povezanih sa proizvodom organizacije, od dizajna i razvoja, kroz proizvodnju i distribuciju, do upotrebe.
- Procena rizika sigurnosti: procene potencijalnih povreda imovine kompanije i zaštite sigurnosti informacija.
- Procena rizika informacione tehnologije: procena mogućih kvarova tehnologije i sistemskih grešaka.
- Procena rizika projekta: odnosi se na procenu rizika implementacije projekta, rokova izrade, visine troškova itd. (Atkinson & Jourdan, 2008)

Svi gore navedeni primeri su sveobuhvatni, tako da svaka organizacija treba da sama odredi koje

će procene rizika vršiti, u zavisnosti od sopstvenih ciljeva.

4. TRETIRANJE RIZIKA I MERENJE REZULTATA

Pre bilo kakvih koraka treba utvrditi da li su izvršeni pravilna identifikacija, analiza i procena rizika. Ukoliko bilo koji od ovih preduslova nedostaje, efikasnost postupanja sa rizicima (tretiranja rizika)[1] će verovatno biti ugrožen. Najosnovnije je znati na koje se rizike treba fokusirati. Pored toga potrebno je odrediti i koji deo organizacije je ugrožen tim rizicima. Konačno potrebno je utvrditi koji rizik predstavlja prioritet za delovanje ka njegovom smanjenju. Da bi tretiranje rizika bilo efikasno, moraju se ispuniti određeni kriterijumi. Svako tretiranje rizika treba biti:

- *Prikladno* – na osnovu uticaja rizika, nivo tretiranja treba biti tačno određen. Raspon može biti od velike krize, gde kompanija ne može nastaviti sa poslovanjem dok se rizik ne ukloni ili smanji, do malih rizika gde se vrše mala smanjenja ili tretiranja uopšte nema.
- *Isplativo* – troškovi tretiranja trebaju biti utvrđeni, tako da količina utrošenog vremena, truda i novca ne bude veća od samog rizika.
- *Delotvorno* – obim i vreme delovanja trebaju biti utvrđeni. Neki rizik će zahtevati neposredno delovanje, a neki mogu biti ostavljeni za kasnije delovanje.
- *Ostvarljivo* – nema smisla definisati tretiranje rizika ukoliko to tretiranje nije realistično ili izvodljivo, bilo zbog tehničkih ili ljudskih faktora.
- *Merljivo* – sva predložena tretiranja trebaju imati mogućnost merenja njihove efikasnosti delovanja.
- *Odobreno* – svako tretiranje mora biti unapred odobreno od strane borda direktora ili top menadžmenta. (Hillson, 2009)

Postoji više strategija tretiranja rizika, u zavisnosti da li su to rizici sa negativnim uticajem ili pozitivnim uticajem (šanse). Postoje četiri strategije tretiranja rizika sa negativnim uticajem, to su izbegavanje, transfer, smanjenje i prihvatanje. Strategije za tretiranje rizika sa pozitivnim uticajem su: iskorišćenje, povećanje i prihvatanje.

Izbegavanje rizika je strategija koja nastoji da eliminiše neizvesnost. Ona se može ostvariti na dva načina, direktno i indirektno. Kada je rizik nastao zbog nedostatka znanja, on se može tretirati direktno. Takva tretiranja obuhvataju povećanje komunikacije, definisanje ciljeva, dobijanje informacija, učenje, sprovođenje istraživanja, razvoj itd. Alternativni način direktnog tretiranja obuhvata uklanjanje izvora rizika, čime se direktno eliminiše neizvesnost. Indirektna izbegavanja obuhvataju promenu okolnosti pod kojim je rizik nastao. Na primer, ukoliko je rizik nastao zbog zastarelosti tehnologije, nabavkom nove tehnologije i sam rizik se uklanja.

Strategija transfera ima cilj da kompanija odgovornost sa sebe prenese na neko treće lice. Sposobnost da se prenese odgovornost za određeni rizik je atraktivan za mnoge organizacije, i mnoge pokušavaju da koriste ovu strategiju kad god je to moguće. Njegova glavna primena je ograničena na finansijski rizik, tj. prenos odgovornost na drugu stranu da izvrši plaćanje ukoliko rizik nastane. Treba imati u vidu da strategija transfera uvek nosi sa sobom i plaćanje premije rizika. Transfer rizika uključuje osiguranje, gde plaćanje premije omogućuje isplatu određene sume novca ukoliko osigurani rizik nastane. Pored osiguranja postoje i drugi finansijski derivati za transfer rizika. Alternativne strategije transfera jesu korišćenje ugovora kao sredstva za prenos odgovornosti. Za bilo koji tip strategije transfera rizika važno je da se rizik prenosi kao deo aranžmana, gde pored prenosa odgovornosti, prenosi se i vlasništvo rizika. Ali treba napomenuti da ovom strategijom rizik ne nestaje, već se jednostavno prenosi na treće lice.

Smanjenje rizika je strategija koja se može upotrebiti za većinu rizika, za razliku od strategija transfera i izbegavanja. Svrha strategije smanjenja je, kao što i sam naziv kaže, da se smanji uticaj rizika do nivoa koji je prihvatljiv. Da bi se strategija smanjenja rizika upotrebila, pre svega je potrebno da se odredi nivo prihvatljivog

[1]Postupanje sa rizicima (tretiranje rizika, engl. risk response)(SRPS ISO 31000:2010, 2010)

rizika. Nivo prihvatljivog rizika može biti visok, srednji, nizak ili po nekom drugom sistemu vrednovanja. Ova strategija se koristi da se smanji verovatnoća nastanka rizika, da se smanji uticaj rizika ukoliko on nastane, ili i jedno i drugo. Preventivna tretiranja rizika su bolja od tretiranja kada rizik nastane, jer ukoliko su uspešna, dovode do izbegavanja rizika. Preventivna tretiranja se bave uzrocima nastanka rizika, tj. traže se šanse za njegovo smanjenje. Ukoliko se uzrok nastanka identifikuje, on se može tretirati u cilju smanjenja verovatnoće njegove pojave. Tamo gde nije moguće smanjiti verovatnoću nastanka rizika, strategija smanjenja se fokusira na smanjenje njegovog uticaja. Rano delovanje na zaštitu od najgorih efekata rizika može učiniti taj rizik prihvatljivim.(Heldman, 2013)

Prihvatanje *(negativni uticaj rizika)* je strategija gde menadžment kompanije odlučuje da prihvati rizik i ne čini ništa dok rizik ne nastane. Ova strategija se koristi kada nije moguće tretirati rizik na drugi način.

Iskorišćenje je strategija koja se koristi kod rizika sa pozitivnim uticajem gde organizacija želi da bude sigurna da će se šanse iskoristiti. Ova strategija teži da otkloni nesigurnosti povezane sa mogućim pratećim rizikom pri korišćenju šansi. ***Povećanje*** je strategija koja se koristi da se poveća verovatnoća iskorišćenja šansi i njihovog pozitivnog uticaja. ***Prihvatanje*** *(pozitivni uticaj rizika)* jeste strategija gde se šanse ne traže, već se jednostavno prihvate ukoliko se pojave. (PMI, 2013)

Nakon primene odgovarajuće strategije, merenje rezultata je konačan korak u procesu upravljanja rizicima. Ovaj proces sprovodi kontrolne aktivnosti uključujući ponovne procene rizika nakon sprovedene strategije. Konstantno praćenje politika, procedura i poslovnih procesa omogućuje menadžmentu da sagleda efikasnost primenjenih strategija za tretiranje rizika.

5. ZAKLJUČAK

Klasifikacija rizika koja je prezentovana ovde može da predstavlja polaznu osnovu za upravljanje rizicima u elektronskom poslovanju. Sedam tipova rizika koji su predstavljeni mogu biti iskorišćeni kao jedan model mogućih rizika koje kompanija treba da uzme u obzir. Buduća istraživanja se mogu fokusirati na neke nove tipove rizika i proširiti postavljenu klasifikaciju.

Nakon identifikacije rizika efikasna analiza istih je logičan sled događaja. Da bi se analiza izvršila, potrebno je najpre utvrditi ciljeve takve analize, kao i sam obim analize, da li će on obuhvatiti celu organizaciju ili samo neke njene delove. Što se tiče predstavljene klasifikacije mogućih procena rizika, ona predstavlja samo jedan sveobuhvatan primer mogućih procena, a sama kompanija treba odlučiti koje će procene vršiti u zavisnosti od identifikovanih rizika.

Efikasno tretiranje rizika je od vitalnog značaja za upravljanje rizicima. Posedovanje pravih informacija i primene prave strategije pored toga što omogućava dobro poslovanje, ima svoj doprinos i u povećanju poverenja stejkholdera u menadžment kompanije. Proces upravljanja rizicima nikada neće doneti prave rezultate ukoliko je tretiranje rizika neefikasno. Rizici koji su identifikovani i procenjeni će i dalje predstavljati pretnju kompaniji ukoliko se ne tretiraju pravom strategijom. Naravno, merenje rezultata predstavlja poslednji i nezaobilazan korak, koji treba da verifikuje efikasnost primenjenih strategija.

Ovde prikazana klasifikacija rizika odnosi se na kompanije koje posluju u Internet okruženju. Analiza i procena rizika, kao i tretiranje rizika i merenje rezultata su jedinstveni za sve kompanije u poslovnom okruženju. Proces upravljanja rizicima, koji je ovde predstavljen, pored primene u elektronskom poslovanju može naći primenu i u drugim kompanijama.

CITIRANI RADOVI

Anon. (2014, Apr 11). *Cloud Infographic: Computer Virus Facts And Stats*. Preuzeto sa CloudTweaks: http://cloudtweaks.com/2014/04/cloud-infographic-computer-virus-facts-stats/

Anson, A. (2012, Jun 12). *Internet Scam Statistics 2012 [Infographic]*. Retrieved from ansonalex.com: http://ansonalex.com/infographics/internet-scam-statistics-2012-infographic

Atkinson, J., & Jourdan, C. (2008). A practical guide to risk assessment. *Sustainable Forestry Initiative*.

Chaffey, D. (2009). E-business and e-commerce management. *Prentice Hall*.

Čekerevac, Z. (2015). *Elektronsko poslovanje.* Beograd: Fakultet za poslovno industrijski menadžment.

Heldman, K. (2013). *Project management jump start, third edition.* Indiana: Wiley Publishing.

Hillson, D. (2009). Developing Effective Risk Responses. *Project Management Institute*.

Leukfeldt, R. (2014). Cybercrime and social ties. *Springer Science+Business Media New York*.

Nastase, F., Nastase, P., & Sova, R. (2007). Information Security Audit in e-business applications. U *Informatica Economica* (str. 79-86). Bucharest: Academy of economic studies.

PMI. (2013). *A Guide to the Project Management Body of Knowledge (Pmbok Guide) – fifth edition.* USA: Project management insitute.

Rotaru, K., & Wilkin, C. (2011). Formalizing process-based risk. *Inf Syst E-Bus Manage*.

SRPS ISO 31000:2010. (2010, Jul 30). *SRPS ISO 31000:2010*. Retrieved from ISS Institut za standardizaciju Srbije: http://www.iss.rs/standard/?natstandard_document_id=25496

Wachs, S., Junger, M., & Sittichai, R. (2015). Traditional, Cyber and Combined Bullying Roles: Differences in Risky Online and Offline Activities. *Open acess societies*.

Živanović, N. (2014). *Strategijski menadžment.* Beograd: Fakultet za poslovno industrijski menadžment.

Datum prve prijave: 03.03.2015.
Datum prijema korigovanog članka: 27.05.2015.
Datum prihvatanja članka: 21.06.2015.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Mihajlović, M., Živanović, V., & Karakaš, N. (2015, jul 15). Upravljanje rizicima elektronskog poslovanja. (Z. Čekerevac, Ed.) *FBIM Transactions, 3*(2), 67-74. doi:10.12709/fbim.03.03.02.08

*Style – **Chicago** Sixteenth Edition:*

Mihajlović, Milan, Vlada Živanović, and Nedeljko Karakaš. 2015. "Upravljanje rizicima elektronskog poslovanja." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 3 (2): 67-74. doi:10.12709/fbim.03.03.02.08.

*Style – **GOST** Name Sort:*

Mihajlović Milan, Živanović Vlada and Karakaš Nedeljko Upravljanje rizicima elektronskog poslovanja [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, jul 15, 2015. - 2 : Vol. 3. - pp. 67-74.

*Style – **Harvard** Anglia:*

Mihajlović, M., Živanović, V. & Karakaš, N., 2015. Upravljanje rizicima elektronskog poslovanja. *FBIM Transactions,* 15 jul, 3(2), pp. 67-74.

Style – **ISO 690** Numerical Reference:

Upravljanje rizicima elektronskog poslovanja. **Mihajlović, Milan, Živanović, Vlada and Karakaš, Nedeljko.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, jul 15, 2015, FBIM Transactions, Vol. 3, pp. 67-74.