ELEMENTI I ANALIZA IT RIZIKA

ELEMENTS AND ANALYSIS OF IT RISK

Dr Branko Krsmanović, vanredni profesor
Fakultet spoljne trgovine u Bijeljini

Apstrakt. Analiza rizika se najčešće provodi korišćenjem univerzalne formule: Rizik = (vrijednost sredstava) x prijetnja x ranjivost. U radu se detaljno analizira svaki od elemenata u navedenoj formuli. Akcenat se stavlja na pitanja procjene sredstava, prijetnji i ranjivosti kao i na najčešće teškoće u vezi sa njihovom procjenom. Utvrđivanje IT rizika ima karakteristike životnog ciklusa sa prepoznatljivim fazama: identifikacija informacionih sredstava, kvantitativno i kvalitativno izražavanje prijetnji, procjena ranjivosti, otklanjanje nedostataka i kontrola i upravljanje tekućim rizikom.

Ključne riječi: IT, rizik, analiza, upravljanje rizikom

Abstract. Risk analysis is most often carried out by using an universal formula: Risk = (value of the resources) x threat x vulnerability. This paper thoroughly analyses each of the elements mentioned in the formula. The accent is on the issues of resources assessment, threats and vulnerability, as well as the most common difficulties in regard to their assessment. Determination of the IT risk has characteristics of the life cycle with the common phases: indetification of information resources, quantitative and qualitative expression of the threats, vulnerability assessment, removal of shortages and control and management of the current risk.

Key words: IT, risk, analysis, risk management

UVOD

Za ublažavanje IT rizika do nedavno su se koristili samo jednostavni softveri koji su se svodili na *firewall* i *antivirus softvere*. Sa porastom opasnosti prilikom korišćenja IT resursa, mnoge države su usvojile zakone u kojima se nalaže sprovođenje brojnih kontrola. Takav pristup rezultirao je potrebom da se upravlja i IT rizikom. Primjetno je da su i u našem okruženju mnoge organizacije povećale efektivnost svojih IT kontrola odnosno smanjile troškove time što su vršile dobre analize i upravljanje rizikom.

ELEMENTI I ANALIZA RIZIKA

Borba protiv rizika je u ne tako davnoj prošlosti izgledala sasvim drugačije od one koja je danas. Praktikovan je pristup izbjegavanja rizika (eng. Risk Avoidance). Ovakav pristup podrazumijevao je uglavnom prevenciju odnosno preduzimanje odgovarajućih mjera zaštite poslovanja od gubitaka ili šteta. Ovakav pristup nije vodio računa o stepenu izloženosti riziku te je zamijenjen novim pristupom - upravljanje rizicima.

Upravljanje rizicima je proces kojim organizacija otkriva, prepoznaje, umanjuje i nadzire potencijalne rizike i gubitke kojima je izložena. Suština je u pronalaženju prihvatljijvog nivoa rizika koji je povoljna kombinacija sigurnosti i troškova.

Analiza rizika se može provesti korišćenjem univerzalne formule : **Rizik** = (***vrijednost sredstava***) **x prijetnja x *ranjivost***.

Za procjenu rizika je od izuzetne važnosti relevantna procjena ovih elemenata. Rizik predstavlja vjerovatnoću dešavanja nekog neželjenog događaja (npr. gubitak novčanih sredstava, gubitak ugleda organizacije, gubitak informacija i sl) . Može se reći da je rizik funkcija vjerovatnoće dešavanja nekog neželjenog događaja i njegovih posledica.Vjerovatnoća da se desi neželjeni događaj zavisi od *prijetnji* i *ranjivosti*.

Sredstva se obično prikazuju u monetarnoj vrijednosti i mogu se definisati kao sve što posjeduje vrijednost za organizaciju a što se može oštetiti, ugroziti ili uništiti. To mogu biti zgrade, mašine, finansijska sredstva, informacije, ljudi, kompjuterski programi, znanja i sl. Obuhvata sve ono što treba organizaciji za ostvarenje

ciljeva koje je menadžment postavio. Vrijednost sredstava nije samo prost trošak zamjene nego sredstva treba vrednovati uzmajući u obzir osnovni trošak njegovog ugrožavanja. Ako su neka sredstva kritična za ostvarenje misije organizacije onda su veći i učinci i posledice njihovog oštećenja.

Prijetnja se može defnisati kao potencijalni događaj koji bi svojim dešavanjem izazvao neželjeni uticaj. Neželjeni uticaj i pored različitih formi u kojima se može pojaviti, najčešće rezultira finansijskim gubicima. Uobičajeno je da se prijetnje izražavaju u procentima pri čemu dva faktora determinišu ozbiljnost prijetnje: stepen gubitka i vjerovatnoća pojave. Stepen gubitka se najčešće predstavlja faktorom izloženosti koji predstavlja procjenu gubitka vrijednosti sredstva izraženu u procentima do koga će doći ako se prijetnja realizuje.

Ranjivost se najčešće definiše kao slabost kumulativnih kontrola kojima se štiti određeno sredstvo. Ranjivost se, takođe, procjenjuje procentualno na osnovu nivoa slabosti kontrola. Nedostatak kontrole se izračunava tako što se od vrijednost 1 ili 100% oduzima efektivnost kontrole. Stepen ranjivosti odnosno nivo rizika mogu se smanjiti osmišljavanjem, izborom i provođenjem odgovarajućih sigurnosnih protivmjera.

U praksi se rijetko vrši izračunavanje rizika za svaku prijetnju, mada se treba potruditi da se otkriju sve prijetnje za organizaciju. Kada se jednom utvrde, identifikovanje novih prijetnji nije velika obaveza i treba je kontinuirano provoditi.

Za ***prijetnju*** je specifično da se uvijek izvodi iz samo jedne vrijednosti. Na primjer, IT rizik može podrazumijevati hakerske pokušaje. Kombinovanje ove prijetnje sa nekom drugom, recimo, prijetnjom da se zloupotrebe privilegije pristupa dobila bi se pogrešna procjena rizika. Nadalje, druga vrsta grešaka koja se pojavljuje odnosi se na propuste pri ocjenjivanju i ugrađivanju faktora izloženosti u vrijednost prijetnje. To za posledicu ima pogrešnu (veću) procjenu rizika. Tačna vrijednost prijetnje uobzirila bi i faktor izloženosti i godišnju stopu pojave.

Da bi se identifikovala ***ranjivost*** mora se razumjeti jačina kontrola. Česta greška u analizi rizika je upravo zbog toga što jačina kontrola nije adekvatno ocijenjena.

POSTUPAK UTVRĐIVANJA IT RIZIKA

Upravljanje IT rizikom ima karakteristike životnog ciklusa:[1]

- identifikacija informacionih sredstava,
- kvantitativno i kvalitativno izražavanje prijetnji,
- procjena ranjivosti,
- otklanjanje nedostataka kontrola
- upravljanje tekućim rizikom.

Najvažniji postupci u **fazi identifikacije informacionih sredstava** su: definisanje značaja informacija, identifikovanje poslovnih funkcija, mapiranje informacionih procesa, identifikovanje informacionih sredstava i dodjeljivanje značaja informacionim sredstvima.
Ova faza obuhvata identifikovanje informacionih sredstava i pripisivanje značaja svakom informacionom sredstvu (veliki, srednji ili mali) u pogledu povjerljivosti, integriteta i raspoloživosti. Jedan od najčešće korišćenih metoda za identifikaciju informacionih sredstava je tzv. *silazni pristup*, pri kome se počinje od funkcija organizacije, identifikuju se procesi koji pružaju podršku tim poslovnim funkcijama i tako redom na niže sve do informacionih sredstava koja se obrađuju.

Prije nego što se priđe identifikaciji informacionih sredstava potrebno je znati koje su informacije velikog, srednjeg i malog značaja za poslovanje. Veoma problematičan aspekt upravljanja rizikom odnosi se na identifikovanje lokacije na kojoj se nalaze informaciona sredstva, a potom i sredstva koja su posebno važna za poslovanje. U praksi, ovo se rješava korišćenjem organizacionih šema preduzeća (ako su preduzeća

[1] Prema : Chris Davis, Mike Schiller and Kevin Wheeler, IT Auditing : Using Controls to Protect Information. Assets, Mc Graw Hill, 2007.

organizovana prema funkcijama) na osnovu kojih se dolazi do njima pripadajućih poslovnih funkcija. Nakon identifikovanja poslovnih funkcija pripisuje im se odgovarajući značaj.

Mapiranje informacionih procesa je važno da bi se uspostavila veza informacionih sredstava i procesa, potom da se otkriju tačke procesa koje zahtijevaju manuelni unos kao i da se stekne razumijevanje kojim informacionim sistemima je potrebna zaštita. Kada se identifikuju najvažnije poslovne funkcije započinje se sa identifikacijom procesa koji su podrška poslovnim funkcijama i informacionih sredstava koja porolaze kroz proces. Tokom tog procesa ne obraća se pažnja na tehniku koja se koristi za obradu informacija, već sam tok procesa. Kada se mapiraju informacioni procesi moguće je identifikovati informaciona sredstva i dodijeliti im određeni značaj. Pri tome treba voditi računa o povjerljivosti, integritetu i raspoloživosti sredstava.

Realizacija prijetnji uzrokuje troškove koji su obično veoma visoki. Za organizaciju to obično znači gubitak posla, gubitak resursa, troškovi sudskih procesa, kazna i sl. Sledeći korak upravljanja rizikom je **kvantitativno i kvalitativno izražavanje prijetnji**. Kod identifikacije opasnosti, takođe se najčešće koristi silazni pristup. Počinje se sa poslovnim opasnostima a zatim sa tehničkim. U ovoj fazi zahtijevaju se sledeći postupci:

- procjena poslovnih prijetnji,
- identifikaciju tehničkih, fizičkih i administrativnih opasnosti,
- identifikaciju opasnosti komponente procesa,
- kvalitativno izražavanje opasnosti.

Poslovne prijetnje obuhvataju finansijske prijetnje, zakonske i regulatorne prijetnje. U krajnjoj liniji sve su informacione prijetnje finansijske jer se svode na novčani gubitak ako se realizuju. Ipak pod finansijskom prijetnjom se podrazumijeva prijetnja koja bi, ako bi se realizovala, dovela do gubitka sredstava, narušavanja reputacije, operativne efektivnosti ili konkurentne prednosti, a krajnji ishod je novčani gubitak. Najčešće obuhvataju finansijske kriminalne radnje, gubitak vlasničkih informacija i gubitak produktivnosti. Nakon identifikacije informacionih sredstava finansijske prijetnje postaju vidljivije. Takođe, potrebno je utvrditi kolika je potencijalna izloženost zakonskim mjerama povezana sa realizacijom prijetnji (zakonska prijetnja). Tačna procjena poslovnih prijetnji podrazumijeva identifikovanje potencijalne izloženosti zakonskim mjerama u slučaju narušavanja zaštite informacija. Uporedo sa razmatranjem finansijskih i zakonskih prijetnji razmatraju se i regulatorne prijetnje. Za identifikovanje regulatornih prijetnji potrebno je dobro razumijevanje zakona ili obavezujućih standarda koji regulišu informacije koje organizacija obrađuje. Nakon identifikacije svih poslovnih prijetnji prelazi se na identifikaciju tehničkih, fizičkih i administrativnih prijetnji. Realizacija neke od ovih prijetnji će uzrokovati jednu od poslovnih prijetnji koja je identifikovana.

Tehničke prijetnje su uvijek povezane sa sistemom i utiču na informacije koje se skladište ili prenose. Primjeri tehničkih prijetnji su: upadi u sistem, razni virusi, otkazivanje sistema i sl. Za razliku od tehničkih prijetnji, fizičke prijetnje se odnose na objekte i najčešće su vezane za prirodne događaje ili mehaničke kvarove. Obuhvataju: fizički upad, prirodne nepogode, požar, poplave i sl. Realizacija ovih prijetnji dovodi, često, do gubitka informacija.

Administrativne prijetnje su uvijek u vezi sa ljudima i zaštita je često ugrožena zbog „ljudskog faktora“. To može biti slučajno objelodanjivanje povjerljivih podataka, privredna špijunaža, uništavanje informacija, falsifikovanje informacija.

Nakon identifikovanja prijetnji potrebno je procijeniti vjerovatnoću da će se prijetnja realizovati odnosno potrebno ih je kvantitativno izraziti. Tokom analize prijetnje naročito su bitna dva faktora:

- stepen gubitka sredstava,
- vjerovatnoća pojave.

Predstavljanje stepena gubitka može se izvršiti preko faktora izloženosti a predstavljanje vjerovatnoće može izvršiti korišćenjem godišnje stope pojave.

Poslije identifikovanja informacionih sredstava i opasnosti za svako sredstvo slijedi **faza procjene ranjivosti**. Svaka prijetnja povezana je informacionim sredstvom i to je zajednički imenilac za sve ispitivane

prijetnje. Kod procjenjivanja ranjivosti uvijek se posmatra informacioni proces. Metodološki, prvo se identifikuju ranjivosti po komponentama procesa a zatim se vrši njihovo kombinovanje radi utvrđivanja ranjivosti cjelokupnog procesa. Sada se koristi tzv. *uzlazni pristup*. Koriste se sledeći postupci:[2]

- identifikovanje kontrola u vezi sa opasnostima,
- utvrđivanje nedostataka kontrola komponenti procesa,
- kombinovanje nedostataka kontrola u procesima,
- kategorizacija nedostataka kontrola prema ozbiljnosti,
- ocjena rizika.

Kada se analizira ranjivost prvo se razmatraju prijetnje i evidentiraju postojeće kontrole koje ublažavaju te prijetnje. Radi boljeg razumijevanja rizika iz ugla organizacije, važno je identifikovati sve kontrole koje su primijenjene. Kontrole (kao i prijetnje) mogu biti tehničke, fizičke ili administrativne. Poslije toga sagledavaju se kontrole sa aspekta njihove efektivnosti. Zadatak u ovom koraku je i da se sagledaju nedostaci primijenjenih kontrola i da se odmjeri efektivnost postojećih kontrola. Da bi se došlo do nivoa rizika u informacionom procesu potrebno je izvršiti kombinovanje nedostataka kontrola za komponente procesa a potom i procese kako bi se uvidio nivo rizika svake poslovne funkcije. Razmatranjem nivoa rizika svih poslovnih funkcija dolazi se do nivoa rizika cijele organizacije. Kada se stekne uvid u rizik organizacije, neki od rizika su ozbiljniji od drugih jer imaju uticaj na informaciona sredstva ili nisu ublaženi. Sada je na redu utvrđivanje kvalitativne ocjene rizika poslovnih funkcija, informacionih procesa i komponenti procesa. Najčšće se ovi rizici opisuju kao veliki, srednji ili mali. Daljom analizom utvrđuju se njihova kvantitativna vrijednost koja treba da bude glavni pokazatelj za dodatna ulaganja u kontrole.

U **fazi otklanjanja nedostataka kontrole** potrebno je obratiti pažnju na najozbiljnije rizike kao i na načine njihovog ublažavanja. Uobičajeno se koriste sledeći postupci: odabir kontrola, implementiranje kontrola, provjera novih kontrola i ponovna ocjena rizika.

Poslednja faza (peta) odnosi se na **upravljanje tekućim rizikom**. Komponenta rizika koja se odnosi na prijetnje je naročito dinamična i potrebno je kontinuirano odmjeravati rizik. To podrazumijeva utvrđivanje repera rizika i ponovno procjenjivanje rizika. Nakon nove procjene rizika ustanovljava se reper rizika. On će se koristiti za mjerenje promjena nivoa rizika i određivanje trendova tokom ciklusa upravljanja rizikom. Obuhvata ocjene rizika cijele organizacije, poslovnih funkcija i procesa.

ZAKLJUČAK

Dinamika u pogledu strukture i prirode IT rizika i uticaj na poslovne funkcije uslovila je potrebu stalnog upravljanja, nadzora i kontrole od strane najviših korporativnih tijela (uprava, nadzorni odbor, odbor za upravljanje IT resursima i dr.). Sem aktivnosti u vezi s upravljanjem IT rizicima, na korporativnom nivou trebaju da se donose i odluke u vezi sa usklađivanjem sa regulatornim odredbama. Pitanja IT rizika protežu se ne samo na organizaciju nego i na sve druge organizacije sa kojima organizacija ima poslovne veze. Zbog toga je od posebne važnosti podizanje svijesti o potrebi upravljanja IT rizicima, što zahtijeva, prije svega, detaljnu analizu komponenti rizika.

LITERATURA:

1. Andrić, M., Krsmanović, B., Jakšić, D., *Revizija, teorija i praksa*, Ekonomski fakultet Subotica, 2004.
2. Davis, Ch., Schiller, M. and Wheeler, K., *IT Auditing : Using controls to Protect Information Assets*, Mc Graw Hill, 2007.
3. Krsmanović, B., Polić, S., *Informacione tehnologije u računovodstvu i reviziji*, Finrar i Fakultet spoljne trgovine, Banja Luka - Bijeljina, 2008.
4. Panian, Ž., Spremić, M. i saradnici, *Korporativno upravljanje i revizija informacionih sistema*, Zgombić & Partneri / nakladništvo i informatika d.o.o., Zagreb, 2007.
5. Seen, J. A, *Information technology: principles, practices, oportunities*; Copyright 2004, by Pearson Prentice Hall.

[2] Prema : Chris Davis, Mike Schiller and Kevin Wheeler, IT Auditing : Using Controls to Protect Information Assets, Mc Graw Hill, 2007.