Perica Miletić*

UDK 005.73
005.922.5:[007:004

DOI: 10.5937/MegRev2202183M
Pregledni naučni članak
Primljen 23.05.2022.
Odobren 12.06.2022.

MESTO INFORMACIONE BEZBEDNOSTI U VELIKIM ORGANIZACIJAMA**

Sažetak: *Potreba organizovanja poslova informacione bezbednosti u organizacijama nije više sporan koncept, posebno u doba digitalizacije. Kako organizovati ove poslove, koje mesto u organizaciji im opredeliti, kakva su dosadašnja iskustva primene pojedinih modela u praksi, pitanja su oko kojih diskusija treba da traje i da rezultira pružanjem različitih mogućnosti organizacijama da primene model koji im najviše odgovara u konkretnom trenutku, uvažavajući istovremeno postavljene poslovne ciljeve, osobine ambijenta u kojem posluju, kao i vrstu bezbednosnih pretnji sa kojima se suočavaju, te ukupne resurse sa kojima u tu svrhu raspolažu*

Ključne reči: *Zaštita informacija, bezbednost, organizacija, organizaciona kultura, poslovne funkcije*

* Docent, Pravni fakultet, Megatrend univerzitet, Beograd, Srbija; pmiletic011@gmail.com

** Rad je rezultat projekta FPBISD – Bezbednosni izazovi savremenog društva.

1. Uvod

Svedoci smo velikih promena koje karakterišu današnje društvo u različitim sferama života. Jedna od njih je svakako industrijska revolucija broj četiri, koja predstavlja kombinaciju tehnologije i digitalizacije, što posledično daje ekonomskim procesima sposobnosti i mogućnosti kojima nema premca u istoriji i koje doprinose stvaranju novog modela društva, te stvaranju nove socio-ekonomske paradigme.[1] Takav obrazac naglašava značaj koje imaju informacije (ukoliko je ovaj značaj ikada i bio upitan), posebno u poslovnom kontekstu. Informacije na ovaj način postaju strateški resurs, budući da svaka njihova kompromitacija donosi poteškoće u obavljanju poslovnih procesa, sa jedne strane, kao i polazeći od činjenice da se količina informacija umnožava dok se istovremeno zahteva sve brža obrada i veća dostupnost korisnicima. Iznete činjenice govore u prilog fundamentalnih potreba organizovanja zaštite informacija u privrednim organizacijama, ali u takvim okolnostima gde pretnje postaju sve učestalije, kao i da se javljaju u novim pojavnim oblicima.

U navedenim okolnostima i ukoliko smo saglasni da se ne diskutuje o samoj potrebi organizovanja bezbednosne poslovne funkcije u privrednim organizacijama, kojom prilikom smo svesni činjenice da zaštita informacija obuhvata samo jedan deo ovih (bezbednosnih) poslova, pažnju želimo da usmerimo ka načinu organizovanja informacione bezbednosti u privrednim organizacijama. Dakle pitanje više nije da li i koliko bezbednosti, već na koji način je organizovati.

Odgovor na postavljeno pitanje svakako bi uključivao zahteve za dodatnim određenjem konkretne organizacije za koju se uspostavlja sistem bezbednosti informacija. U tom smislu potrebno je uzeti u obzir brojne elemente koji karakterišu organizaciju, poput: vrste industrije, geografskog podneblja (usled povezanosti drugih brojnih elemenata poput klime, razvijenosti infrastrukture, ekonomske razvijenosti konkretnog regiona, pravnog ambijenta, nacionalne kulture i drugo) u kojem organizacija deluje, starosti organizacije, istorije bezbednosnih incidenata, raspoloživosti ljudskih i materijalnih resursa i drugo.

Neki domaći autori detaljno se bave pitanjem teorije organizacije, pa tako određuju pojam organizacionog dizajna kao (...) „proces u kome se obavlja set menadžerskih aktivnosti na stvaranju modela organizacione strukture koji je u skladu sa kontekstom organizacije".[2] Za potrebe pisanja ovog rada mi nećemo detaljnije ulaziti u ovu problematiku, već ćemo našu pažnju usmerili na organizacioni ambijent u kojem svoje uloge obavljaju poslovna funkcija bezbednosti, odnosno informaciona bezbednost kao njen integralni deo.

---

1 Instituto Espanol de Estudios Estrategikos (2022): „Industrial revolution 4.0!: A new century of revolts in the Mediterranean", Analysis Paper, https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA01_2022_PEDSAN_Revolucion_ENG.pdf (02.05.2022.)

2 Petković Mirjana, Janićijević Nebojša, Bogićević Biljana (2002): *„Organizacija"*, Ekonomski fakultet, Beograd, 53

Mišljenja smo da se po svom značaju za kreiranje sistema bezbednosti izdvajaju sledeći elementi, i to:
– organizaciona kultura,
– veličina organizacije, i
– budžet za potrebe bezbednosti.

2. Organizaciona kultura

Miletić navodi da je *organizaciona kultura* možda i najvažniji od navedenih elemenata, budući da ukoliko članovi organizacije ne smatraju da je zaštita informacija važna za ostvarenje ciljeva organizacije, onda će se informaciona bezbednost u praksi ostvarivati sa skromnim rezultatima, a sama organizacija će napore koje čini poslovna funkcija bezbednosti smatrati suprotni svojim interesima i uzaludnim trošenjem resursa. Brojni su teorijski radovi koji podržavaju ovu tvrdnju.[3]

Veličina organizacije, kao i resursi koji su na raspolaganju od velikog su značaja za zaštitu informacija. Organizacije sa velikim i zahtevnim IT sistemima, očekujuće, teže ka značajnijoj ulozi (podršci) od strane poslovne funkcije bezbednosti. Veliki sistemi mogu imati i posebne sektore (engl: *divisions*) koji su posvećeni navedenim poslovima. Često su u ovim slučajevima uspostavlja posebna menadžerska funkcija koja rukovodi poslovima zaštite informacija – CISO (engl: *Chief Information Security Officer*), kao i prateća stručna podrška od strane menadžera bezbednosti, administratora i drugog tehničkog osoblja. Razlike u veličini organizacije dovode do toga da je moguće da u malim organizacijama samo jedna osoba obavlja sve navedene poslovne bezbednosne funkcije.

Određivanje budžeta za informacionu bezbednost je različito od slučaja do slučaja, budući da za ove potrebe ne postoji standard koji bi pomogao ovu vrstu planiranja, ali može se lako dovesti u vezu sa veličinom organizacije (pretpostavka je da će veća organizacija imati potrebu i za većim budžetom). Ipak, kako bi se pomoglo planiranje ovih troškova, kao i poređenje (kako za interne potrebe tako i okviru celih industrija), ove veličine mogu biti iskazane kao odnos budžeta za zaštitu informacija prema ostvarenom prihodu organizacije; kao odnos broja zaposlenih na poslovima zaštite informacija prema ukupnom broju zaposlenih organizacije, odnosno na neki drugi način.

Sa druge strane, bez obzira na iznete elemente koji utiču na način osmišljavanja i funkcionisanja sistema bezbednosti u organizaciji, kako god bio uspostavljen taj sistem treba da ispunjava više funkcija. Vitman i Matord (engl: *Whitman and*

[3] Miletić, Perica (2020): „*Organizaciono i normativno uređenje zaštite informacija u funkciji bezbednosti poslovanja banaka i finansijskih institucija*", doktorska disertacija, Fakultet bezbednosti, Univerzitet u Beogradu, 115

Mattord) predlažu osnovne funkcije koje treba da obavlja organizacioni deo informacione bezbednosti i u tom smislu, kako tumači Miletić, navode sledeće poslove:[4]

- procenu rizika (engl: *Risk Assessment*), gde se procenjuje prisutan rizik u IT-u, a gde se identifikuju izvori rizika i gde se predlažu mere za njihovo smanjenje;
- upravljanje rizikom (engl: *Risk Management*), gde se sprovode odgovarajuće kontrole u cilju smanjenja rizika. Obično se obavlja zajedno sa prethodno navedenom *risk assessmentom*;
- testiranja (engl: *System Testing*), u kojima se ocenjuje ranjivost postojećih softvera i proverava da li su novi programi usklađeni sa usvojenim bezbednosnim politikama. Često predstavlja deo funkcija odgovora na incidente i/ili upravljanja rizikom;
- kreiranje politika (engl: *Policy*), gde se podrazumeva osmišljavanje i promocija odgovarajućih pravila. Potrebno je da ona budu usaglašena sa drugim pravilima organizacije;
- usklađenost prakse i politika sa zakonima i drugim propisima (engl: *Legal Assessment*). Gotovo uvek se nalazi van odeljenja za informacionu bezbednost (engl: *Information Security – IS*) ili IT-a;
- odgovor na incidente (engl: *Incident Response*), gde je suština pružanje najranijeg odgovora na sve vrste incidenata i umanjenje njihovih negativnih efekata. Podrazumeva se da uključuje aktivnosti srednjeg menadžmenta iz drugih poslovnih funkcija, kako bi i tokom incidenata bilo omogućeno upravljanje organizacijom;
- planiranje (engl: *Planning*), gde se podrazumeva istraživanje i stvaranje planova u oblasti bezbednosti informacija, što često podrazumeva učestvovanje u projektima koji su strateški za celu organizaciju. Potrebno je da koordinira sa drugim procesima i politikama u organizaciji;
- merenje (engl: *Measurement*) svih aspekata informacione bezbednosti, koristeći postojeći sistem kontrola. Kontrole dakle treba da budu merljive, a podaci koji se dobijaju ovim procesom blagovremeni i tačni;
- kontrola usaglašenosti (engl: *Compliance*) proverava da li sistem i mrežni administratori popravljaju uočene slabosti brzo i pravilno. U praksi predstavlja izazov, budući da se odnosi na korisnički servis, koji je istovremeno usmeren na klijente (korisnike) i ispunjava navedene obaveze;
- kontrola autentifikacije (engl: *Centralized Authentication*) predstavlja upravljanje mrežnim i sistemskim akreditacijama za celu organizaciju i obično se delegira u servis koji pruža pomoć korisnicima (engl: *Help Desk*);
- administracija i konfiguracija računara (engl: *Systems Security Administration*). Mnoge organizacije upravo u ovu poslovnu funkciju delegiraju funkciju zaštite informacija (gde je reč o očiglednom sukobu interesa, *prim. aut.*);

[4] Whitman, M., Mattord, H. J. (2008): *Management of Information security*, Course Technology Cengage Learning, second edition, Boston, USA, 161-162

- obuke za informacionu bezbednost (engl: *Information Security Training*) podrazumevaju obučavanje svih zaposlenih za zaštitu informacija i nekada mogu da se izvode u saradnji sa poslovnom funkcijom koja izvodi obuke (to su uglavnom IT i HR (funkcija ljudskih resursa), a retko i uglavnom u velikim sistemima – funkcija informacione bezbednosti, *prim. aut.*);
- administriranje mreže (engl: *Network Security Administration*), gde organizacije takođe često delegiraju funkciju zaštite informacija (i takođe predstavlja sukob interesa, *prim. aut.*), i
- procena ranjivosti (engl: *Vulnerability Assessment*), gde se lociraju uočene ranjivosti informacionih resursa. Često se ovu svrhu koriste testovi mogućnosti upada u sistem (engl: *Penetration Testing*), a radi dobijanja realnog i nezavisnog izveštavanja, te zbog izbegavanja sukoba interesa sa funkcijom IT-a. Obično ih izvode spoljni saradnici (engl: *outsorcing*).

Naša kritika je da se predloženom metodologijom uzimaju u obzir samo poslovi koji su u najužoj vezi sa IT sferom poslova, zbog čega se u praksi (a što se inače često događa) zapostavljaju netehnički aspekti zaštite informacija, poput organizacionih, normativnih, kadrovskih i drugih sličnih oblasti bez kojih nije moguće konstituisati funkcionalan sistem bezbednosti. Moguće je da je u tom smislu najbolji primer fenomen razvoja svesti o bezbednosti zaposlenih organizacije (engl: *security awareness*), budući da se na njega utiče pretežno netehničkim merama, a što je datom metodologijom izostavljeno kao potrebna aktivnost.

3. Sadržaj poslova

Ipak, ovako data metodologija u mnogome približava sadržaj poslova koje je potrebno uspostaviti „negde" u organizaciji (i ako ih ne iscrpljuje i zapostavlja netehničke aktivnosti zaštite informacija). Miletić navodi da ovi autori smatraju da nije obavezujuće navedene funkcije razvijati u okviru poslova bezbednosti (ili funkcije zaštite informacija), ali da one svakako treba da budu uspostavljene.[5] Upravo ova konstatacija nas dovodi do diskusije o mogućim rešenjima organizovanja poslova zaštite informacija u organizacijama, gde ne pretendujemo da predložimo konačno i najbolje rešenje (jer ono i nije moguće izložiti, polazeći od brojnih činilaca koji utiču na način organizovanja poslova zaštite informacija, o čemu je bilo reči prethodno u ovom radu, *prim. aut.*), ali želimo da sagledamo osnovne prednosti i nedostatke pojedinih modela organizovanja predmetnih poslova. Navedeni autor prenosi i stavove Vitmana i Matorda, da je u cilju uspostavljanja većine funkcija zaštite informacija koju smo naveli u ovom radu, moguće organizovati i onda kada ne postoje resursi (i razlozi, *prim. aut.*) da se organizuju u okviru poslovne funkcije zaštite informacija (ili bezbednosti), koju

[5] Miletić Perica, 116.

ipak treba podrazumevati (sa pitanjem o resursima i obimom poslova koje će obavljati, *prim. aut.*). U tom smislu funkcije zaštite informacija je moguće podeliti u grupe poslova (veća organizacija podrazumeva i veći broj grupa), i to prema sledećem:[6]

1. funkcije koje obavljaju netehničke poslovne jedinice izvan IT poslova, kao što su grupe pravnih poslova ili ljudskih resursa (u vezi sa izvođenjem treninga);
2. funkcije koje obavljaju IT grupe, ali izvan područja informacione bezbednosti, kao što su:
   a. poslovi administracije i konfiguracije računara;
   b. administracija mrežne bezbednosti, i
   c. centralizovana administracija bezbednosti.
3. funkcije koje se obavljaju u organizaciji informacione bezbednosti, kao što su:
   a. procena rizika;
   b. testiranje sistema;
   c. odgovor na incident;
   d. planiranje;
   e. merenje, i
   f. procena ranjivosti.
4. funkcije koje se obavljaju u organizaciji informacione bezbednosti a proizilaze iz zakonskih obaveza organizacije, kao što su:
   a. pisanje bezbednosnih politika;
   b. usklađenost za zakonskim obavezama i revizija (engl: *Audit*), i
   c. upravljanje rizikom.

Miletić prenosi da Vitman i Matord, radi lakše sistematizacije i određivanja veličine organizacije, kao referentnu vrednost uzimaju broj radnih stanica koje organizacija koristi. Tako za velike organizacije uzimaju one koje imaju više od hiljadu radnih stanica, za one srednje veličine uzimaju organizacije sa brojem radnih stanica od stotinu do hiljadu, a one koje imaju ispod stotinu radnih stanica smatraju malim organizacijama.[7] S tim u vezi, ovi autori navode da velike organizacije obično imaju sopstvene kadrove za ostvarivanje programa zaštite informacija, a da njihov broj zavisi od konkretnih uslova, te da se on kreće i do dvadesetak administratora/tehničara koji su posvećeni poslovima zaštite informacija (kojom prilikom nisu svi sa punim radnim vremenom, *prim. aut.*). Zadatak rukovodioca informacione bezbednosti, nevezano za veličinu organizacije, jeste da organizuje „negde" potrebne funkcionalnosti, te da ih koordinira i kontroliše. Kako smo prethodno napomenuli, pojedine poslove (funkcije) zaštite informacija mogu da obavljaju i zaposleni koji prioritetno imaju druga zaduženja u organizaciji (i oni ne ulaze u brojno stanje prethodno navedenih zaposlenih

[6] *Ibid.*

[7] *Ibid*, 118.

koji su posvećeni poslovima zaštite informacija, *prim. aut.*). Primer za to su IT administratori, koji su zaduženi za funkcionisanje pojedinih servera i servisa, od čije funkcionalnosti zavisi poslovanje cele organizacije, pa oni tom prilikom održavaju i pripadajuće bezbednosne aplikacije. Ovakva praksa takođe otvara pitanja sukoba interesa ovih zaposlenih, kao i bezbednosnog pitanja „ko kontroliše kontrolore", ali polazeći od predmeta istraživanja ovog rada nećemo ga posebno razmatrati. Organizacije sa srednjom veličinom, imaju manje namenskih grupa i više dodeljenih funkcija u okviru svake grupe. Karakteristično je da se ovde mnoge bezbednosne funkcije dodeljuju IT-u, kao i da se neke bezbednosne funkcije (prethodno navedene, *prim. aut.*) ignorišu, budući da poslovna funkcija bezbednosti nije u prilici da obavlja pojedine aktivnosti. U ovakvim situacijama rukovodilac bezbednosti treba da pronađe raspoložive resurse unutar organizacije i da poboljša saradnju između grupa zaduženih za obavljanje pojedinih funkcija. U malim organizacijama, bezbednosne funkcije svedene su na minimum, a one koje postoje obično se organizuju u različitim organizacionim delovima. U njima se često angažuju spoljni saradnici, za pitanja koje organizacije ne mogu same da reše, a lokalni administratori informacionog sistema pridruženo obavljaju poslove zaštite informacija (za koja imaju potrebna znanja, *prim. aut.*). Male organizacije ipak obično imaju potrebne politike zaštite informacija, a spoljni saradnici svoje aktivnosti obavljaju preko veba. Ipak, one imaju i određe prednosti u odnosu na veće organizacije, budući da je u njima moguće trening za povećanje bezbednosne svesti obavljati pojedinačno, a zaposlenima je uvek na raspolaganju IT administrator za pružanje potrebne pomoći. Treba napomenuti i da manji broj zaposlenih podrazumeva da se članovi organizacije obično međusobno poznaju, odakle se lakše uspostavlja odgovarajuća bezbednosna kultura te organizacije.

U velikim organizacijama je čest slučaj da se informaciona bezbednost organizuje u okviru IT poslova. Prema Vitmanu i Matordu, formalna nezavisnost bezbednosne funkcije postiže se dvostrukom linijom raportiranja.[8] U okviru IT-a (u organizacionom smislu, *prim. aut.*), kao i prema Odboru za bezbednost (u funkcionalnom smislu, *prim. aut.*). Očigledna prednost ovakvog rešenja je olakšana komunikacija bezbednosne i IT poslovne funkcije, odakle se postiže bolja koordinacija rada i brže rešavanje operativnih pitanja. Rukovodilac za informacionu bezbednost raportira izvršnom direktoru zaduženom za IT. Ovakva organizacija podrazumeva da su njihovi poslovni ciljevi usaglašeni, što u praksi zna da predstavlja problem. Rukovodilac IT-a zadužen je za efikasno funkcionisanje informacionog sistema, a svako usporavanje procesa ga ograničava da bude uspešan u obavljanju svoje poslovne funkcije. Rukovodilac informacione bezbednosti je tada često u ulozi revizora, jer se bavi otkrivanjem nedostataka u informacionoj tehnologiji, softveru i aktivnostima i procesima zaposlenih. Ono što za IT mora da se obavi sada i odmah, za funkciju bezbednosti ne mora da

[8] *Ibid,* 121.

znači, jer je prioritet u zaštiti analitičnost i sagledavanje mogućih rizika neke operacije. Poslovi bezbednosti u navedenom smislu ne smeju da prave kompromise, već potencijalne pretnje treba da se sagledaju i da se u zavisnosti od ustanovljenog rizika o njima odmah obaveste najviši organi upravljanja. Iz navedenih razloga razumljiva je argumentacija da se u velikim organizacijama razdvoje poslovi bezbednosti i IT-a, budući da se ovde lako javlja sukob interesa. Miletić navodi da se i pored očigledne argumentacije koju smo naveli, ova transformacija odvija sporo, o čemu postoje brojne studije. Izuzetak su banke i finansijske institucije, budući da nadležni regulatori prepoznaju ovaj sukob interesa, te funkciju bezbednosti informacija organizuju često u poslovnoj funkciji koja se bavi rizikom, a često i raportiraju direktno generalnom direktoru (engl: C*hief executive officer – CEO*).[9]

4. Zaštita informacija

U teoriji, nema spora da poslovi zaštite informacija pripadaju grupi poslova bezbednosti. Uobičajeno je da ova poslovna funkcija obavlja i druge aktivnosti koje se odnose na sprečavanje različitih oblika ugrožavanja imovine, zaposlenih i poslovanja, pa se tako javljaju grupe poslova kao što su: bezbednost zaposlenih, zaštita od požara, bezbednost i zdravlje na radu, fizička bezbednost, zaštita životne sredine i drugo. Polazeći od prirode navedenih aktivnosti, očigledna je prednost ukoliko organizacija ima mogućnosti da ih sve poveže u okviru iste poslovne funkcije – funkcije bezbednosti. Reč je o tome da se različiti poslovi bezbednosti međusobno prožimaju, usled čega njihovo organizovanje u jednu poslovnu funkciju olakšava koordinaciju aktivnosti i manje zavisi od aktivnosti drugih poslovnih funkcija, u situacijama kada su ove funkcije rasute na drugim mestima u organizaciji. Takođe, ovakvom organizacijom izbegava se izvesni sukob interesa, koji se javlja kada je funkcija zaštite informacija (i inače bezbednosti) organizovana po drugim poslovnim funkcijama, o čemu smo već izneli odgovarajuće primedbe.

Izbegavanje sukoba interesa prilikom organizovanja poslova bezbednosti, princip je koji treba imati u vidu kada se planiraju ovi poslovi unutar organizacije, kojom prilikom smo svesni principa ekonomičnosti organizacije, koji nalaže prihvatanje određenih kompromisa i odstupanje od idealnih modela. U slučaju bezbednosne poslovne funkcije, idealni model bi predstavljao samostalnu poslovnu funkciju koja objedinjava sve poslove koji se obavljaju u organizaciji u cilju njene zaštite, sa direktnom linijom raportiranja najvišem menadžmentu. Svaki drugačiji način, spajanje bezbednosne funkcije sa drugim poslovima, dovodi do sukoba interesa koji je posledica zakonitosti ponašanja ljudi u organizaciji. Rukovodilac koji je zadužen za poslovanje određenog organizacionog

[9] *Ibid*, 120.

dela, u koji je iz razloga ekonomičnosti organizacije smeštena i funkcija bezbednosti, naći će se u situaciji izbora između aktuelizacije nastalih incidenata, otkrivenih pretnji i rizika i promocije rezultata matične poslovne funkcije, ukoliko su propusti koji su doveli do ugrožavanja bezbednosti nastali u njegovoj zoni odgovornosti. Druga strana ovakve organizacije poslova bezbednosti, može samo da unapredi njenu funkcionalnost, budući da će se zaposleni u okviru istog organizacionog dela bolje poznavati, deliti slične vrednosti i uspešnije koordinirati međusobne aktivnosti – posebno kada dele srodne poslovne zadatke.

Organizovanje poslova bezbednosti i HR poslovne funkcije u okviru iste celine može da donese određene prednosti (što ne znači da se i ovde radi o pristajanju na kompromis sukoba interesa). To se posebno ogleda u sprovođenju obuka za podizanje bezbednosne svesti, budući da je upravo HR odgovoran za organizovanje treninga u okviru organizacije. Takođe, od značaja je i stepen poverljivosti koji se javlja u ovakvim organizacijama između HR i bezbednosne poslovne funkcije, posebno kada su u pitanju radne pozicije sa posebnim bezbednosnim odgovornostima u organizaciji (što obuhvata ne samo najviši menadžment, već i radna mesta kritična sa aspekta bezbednosti poslovanja, po svim nivoima organizacije). Tako će biti olakšana, na primer, bezbednosna provera zaposlenih i kandidata za posao koji obavljaju poslove sa visokim nivoom potrebnih privilegija u informacionom sistemu.

Sličan primer je i organizovanje poslova bezbednosti u okviru funkcije opštih i administrativnih poslova, budući da se ovi poslovi odnose na svakodnevni život organizacije (što savršeno pogoduje filozofiji bezbednosti). Kada god je reč o organizovanju poslova bezbednosti unutar neke druge poslovne funkcije, različiti aspekti bezbednosti delegiraju se različitim rukovodiocima, a njihove aktivnosti koordinira i kontroliše nadležni rukovodilac poslovne funkcije u koju je smeštena bezbednost. Na ovaj način dobija se dodatni nivo u rukovođenju poslova bezbednosti, što nije slučaj kada rukovodilac bezbednosti samostalno koordinira aktivnosti poslovnih funkcija koje organizuje. Slabost ovakvog rešenja može da bude i izbor menadžera koji rukovodi poslovnom funkcijom gde je prinudno smeštena bezbednost, u ovom slučaju izbor rukovodioca opštih i administrativnih poslova, budući da njegovo rukovođenje u mnogome zavisi od njegovih sklonosti i vrste obrazovanja koje ima. Menadžeri sa tehničkom osnovom obrazovanja preferiraće ovakav isti pristup poslovima bezbednosti, a oni drugi, sa netehničkim obrazovanjem težiće oblastima koje su im bliske, kao što je bezbednost kadrova, fizička bezbednost, bezbednost i zdravlje na radu i slično. Problem nije u favorizovanju segmenata bezbednosti koje su bliske rukovodiocu „centralne" poslovne funkcije, već u činjenice da će se u ovakvim slučajevima često zanemariti deo bezbednosti koji ne pripada ovoj prvoj grupi. Posebnost administrativnih poslova, sa aspekta bezbednosti, jeste upravljanje dokumentacijom organizacije (oblasti čuvanja i arhiviranja dokumenata, dakle informacija), odakle se ovakva organizaciona rešenja zaštite informacija

mogu potražiti kod subjekata čija se delatnost zasniva na obimnoj proizvodnji dokumentacije. Digitalizacija donosi sa sobom brojne prednosti za poslovanje, ali dovodi i do favorizovanja digitalne sfere, što u poslovima bezbednosti (zaštite informacija) rezultira fokusiranjem na IT od strane bezbednosnih stručnjaka, te dovodi do zanemarivanja netehničkih oblasti bezbednosti (dakle dovodi do njene nekompletnosti). Organizacije i dalje imaju ogroman broj dokumenata na papiru, što u slučaju objedinjavanja funkcija opštih i administrativnih poslova i funkcije bezbednosti olakšava zaštitu informacija u procesima: organizovanja arhivskih poslova; fizičkog čuvanja dokumentacije; uništavanja dokumentacije; digitalizacije dokumentacije; upravljanja digitalnom dokumentacijom i njenom skladištenju.[10]

Priroda poslova osiguranja i upravljanja rizikom u organizacijama bliska je poslovima bezbednosti, budući da ove funkcije dele zainteresovanost za bliske teme. Odatle ovakva saradnja predstavlja još jedan mogući model organizovanja poslova bezbednosti (zaštite informacija) u velikim organizacijama. Sa jedne strane imamo bezbednosne rizike, dok sa druge strane stoji grupa rizika koji se eksplicitno, u užem smislu odnose na poslovanje. Zbog svog značaja za poslovanje organizacije, poslovna funkcija upravljanja rizikom zauzima u njoj centralno mesto, budući da je usredsređena na posmatranje cele organizacije i deljenje informacija sa svim poslovnim funkcijama, što pogoduje poslovima bezbednosti i u tom smislu odražava istu ambiciju. Ne manje važno je da ovde dve poslovne funkcije na sličan način posmatraju rizik kao pojavu. To podrazumeva da je potrebno iz grupe prepoznatih rizika izdvojiti one koji su od značaja za poslovnu funkcionalnost organizacije, sistematizovati ih, proceniti njihov uticaj na organizaciju, odrediti njihove ključne pokazatelje (kako bi se rizici pratili), odrediti mere zaštite od njihovog delovanja i obavljati njihovu redovnu evaluaciju.[11]

Ilustrativan primer u smislu prethodno navedenog predstavlja određenje pojma operativnog rizika u bankarskom poslovanju, kao jedne od kategorija rizika koje je odredila Narodna banka Srbije, u svojstvu nacionalnog regulatora u ovom sektoru. Naime, operativni rizik je određen kao mogućnost koja se odnosi na ostvarivanje negativnih poslovnih rezultata banke, a koji su nastali kao (...) „posledica propusta (namernih i nenamernih) u radu zaposlenih, neodgovarajućih internih procedura i propisa, neadekvatnog upravljanja informacionim i drugim sistemima, kao i usled nepredviđenih eksternih događaja".[12]

Još jedan pokazatelj koji upućuje na bliskost i prirodnu povezanost poslovnih funkcija osiguranja i upravljanja rizikom i funkcije zaštite informacija je podatak da se u toku 2020. godine u svetu predviđala potrošnja od oko osam

[10] *Ibid,* 132.

[11] *Ibid,* 136.

[12] Izvor: Narodna banka Srbije, https://nbs.rs/sr/finansijske-institucije/banke/upravljanje-rizicima/ (15.05.2022.)

milijardi dolara za potrebe pokrivanja polisa osiguranja (nasuprot pet milijardi dolara godinu dana ranije), koje su plaćale organizacije kako bi ublažile eventualne gubitke koji nastaju ugrožavanjem informacija. Reč je, prema tadašnjim podacima, od oko šest i po procenata godišnjih budžeta koje su trošile organizacije na svetskom nivou, upravo za potrebe zaštite informacija.[13]

Tome treba dodati i traumatično iskustvo koje je svet od tada imao sa pandemijom, odnosno sa porastom napada na informacione sisteme privrednih organizacija, a posebno kada se uzme u obzir nepripremljenost organizacija za masovni daljinski rad svojih zaposlenih, naročito u pogledu bezbednosnih propusta u njihovoj opremljenosti i pripremljenosti za nove rizike kojima su izloženi, a koji se prvenstveno odnose na oblast zaštite informacija. Posledica – sa velikom izvesnošću može se predvideti dalji rast budžeta koje će organizacije da izdvajaju za ublažavanje posledica koje su proizvod narušavanja bezbednosti informacija.

5. Zaključak

Ne treba da bude presudno, ali iznete činjenice mogu da opredele neke organizacije da primene upravo model organizovanja poslova zaštite informacija gde je bezbednost, odnosno zaštita informacija organizovana unutar poslova osiguranja i upravljanja rizikom, budući da se na taj način postiže bolja koordinacija obe poslovne funkcije i uspostavlja efektivnija kontrola troškova koji će za ove potrebe biti izdvojene.

Pored ovde navedenih (osnovnih) modela organizovanja poslova zaštite informacija u velikim organizacijama, postoje i druge brojne forme kako se ovi poslovi mogu organizovati, a stalno se pojavljuju i istražuju nove. Mišljenja smo da bezbednost ne treba posmatrati kao gotov proizvod, već kao proces koji zavisi od brojnih činilaca. Odatle i organizovanje poslova bezbednosti nije forma koja je data jednom za uvek, čak i u okviru jedne iste organizacije. Na izbor odgovarajućeg modela, kako smo prethodno istakli, utiču brojni činioci, a neki od njih su: vrsta industrije kojoj pripada organizacija, nacionalna kultura, bezbednosna kultura, geografski prostor sa svojim osobinama tržišta, normativni okvir u kojem posluje organizacija, starost organizacije, stepen kriminaliteta poslovnog okruženja, organizaciona kultura, raspoloživi ljudski resursi, poslovni ciljevi organizacije, budžet koji se određuje za ove potrebe i drugi.

[13] Izvor: https://www.statista.com/statistics/387868/it-cyber-securiy-budget/ (15.05.2022.)

Literatura:

- Miletić Perica (2020): *Organizaciono i normativno uređenje zaštite informacija u funkciji bezbednosti poslovanja banaka i finansijskih institucija*, doktorska disertacija, Fakultet bezbednosti, Univerzitet u Beogradu,
- Petković Mirjana, Janićijević Nebojša, Bogićević Biljana (2002): *„Organizacija"*, Ekonomski fakultet, Beograd
- Whitman, M., Mattord, H. J. (2008): *Management of Information security*, Course Technology Cengage Learning, second edition, Boston, USA

Elektronska literatura:

- Instituto Espanol de Estudios Estrategikos (2022): „Industrial revolution 4.0!: „A new century of revolts in the Mediterranean", Analysis Paper, https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA01_2022_PEDSAN_Revolucion_ENG.pdf (02.05.2022.)
- Narodna banka Srbije, https://nbs.rs/sr/finansijske-institucije/banke/upravljanje-rizicima/ (15.05.2022.)
- https://www.statista.com/statistics/387868/it-cyber-securiy-budget/ (15.05.2022.)

Perica Miletić

UDC 005.73
005.922.5:[007:004

DOI: 10.5937/MegRev2202183M
Review scientific article
Received 23.05.2022.
Approved 12.06.2022.

THE PLACE OF INFORMATION SECURITY IN LARGE ORGANIZATIONS

Abstract: *The need to organize information security work in organizations is no longer a controversial concept, especially in the age of digitalization.How to organize these jobs, what place in the organization to determine, what are the previous experiences of applying certain models in practice, are issues that should be discussed and result in providing different opportunities for organizations to apply the model that suits them best at the same time.set business goals, characteristics of the environment in which they operate, as well as the type of security threats they face, and the total resources at their disposal for this purpose.*

Keywords: *Information protection, security, organization, organizational culture, business functions*