Odnos organizacione kulture i bezbjednosti informacionog sistema organizacije

Bogdan Mirković
Fakultet za informacione tehnologije
Slobomir P Univerzitet
PF 70, Slobomir, 76300 Bijeljina, Republika Srpska, Bosna i Hercegovina
bogdanmirkovic@yahoo.com

Sadržaj—**U ovom radu se prikazuje priroda odnosa između organizacione kulture i informaciono-bezbjedonosne kulture. U radu su prikazani konceptualni okviri koji mogu pomoći organizacijama u određivanju do koje mjere informaciono-bezbjedonosnu kulturu mogu ugraditi u organizacionu kulturu. Okvir nudi preporuke organizacijama koje žele dostići određeni nivo informaciono-bezbjedonosne kulture u samoj organizaciji utičući na aktivnosti i ponašanja zaposlenih u organizaciji sa ciljem zaštite informacija u organizaciji na osnovu prioriteta koje organizacija definiše.**

Ključne riječi-organizaciona kultura; informacioni sistem; bezbjednost; (organizational culture; information system; security)

I. UVOD

Bezbjednost informacionog sistema obuhvata načela povjerljivosti, integriteta, raspoloživosti, autentičnosti, dokazivosti, neporecivosti i pouzdanosti. Jedno od najznačajnijih područja cjelokupnog upravljanja informacionim sistemom svakako je upravljanje bezbednošću tog sistema.

Kako bezbjednost informacionog sistema ne može nikada biti apsolutna, potrebno je obezbijediti postizanje i održavanje adekvatnog nivoa ove bezbjednosti. Koji je nivo adekvatan treba da procijeni svaka institucija, i to prevashodno na osnovu rezultata procjene rizika informacionog sistema, kao i obaveza koje proizlaze iz propisa, internih akata, ugovornih odnosa i sl. U tom smislu, upravljanje bezbjednošću informacionog sistema predstavlja kontinuiran proces identifikovanja i praćenja potreba za bezbjednošću informacionog sistema i postizanja i održavanja adekvatnog nivoa bezbjednosti uspostavljanjem i primjenom odgovarajućih kontrola. Prema načinu implementacije kontrole obuhvataju upravljačke, tehničke i fizičke, a prema namjeni mogu biti preventivne, detektivne i korektivne.

Različite organizacije iz različitih razloga treba da štite informacije. Za banke je od presudnog značaja integritet informacija, tj. neizmjenljivost novčanih transakcija, zbog finansijskog poslovanja. Za provajdere pristupa internetu i davaoce usluga najvažnije su raspoloživost i pouzdanost informacija u smislu dostupnosti i pouzdanog rada ključnih elemenata sistema, a sve zbog kontinuiteta pružanja usluga. Za privrednike je pak najvažnija povjerljivost informacija, zbog zahtjeva da informaciji pristupe samo ovlašćena lica, radi opstanka na tržištu i uspješnog poslovanja [1].

Kada je riječ o pojmu informacija i informacionoj bezbjednosti izuzetno je važno shvatiti i prihvatiti sljedeće činjenice:

1) Informacioni sistem nije isto što i kompjuterski sistem (informacioni sistem ≠ kompjuterski sistem)

2) Kompjuterski sistem je podsistem ili podskup informacionog sistema.

Informacioni sistem pored kompjuterskog sistema čine i papiri s podacima u registratorima na policama arhive, telefaks uređaji i kopije faksova, telefonske mreže, video i ostali oblici nadzora, zaposleni i poslovni partneri (odnosno ono što oni znaju o podacima), fizička zaštićenost objekata kao i drugi oblici informacija na različitim medijumima. Očito da je pojam zaštite informacionog sistema izuzetno širok i kompleksan i prelazi poimanje informatičara koji to svode u pravilu samo na kompjuterski sistem. No, u suštini nije cilj zaštita informacionog sistema, nego onoga što se kao osnovna vrijednosna jedinica nalazi u informacionom sistemu: informacija. Treba tako postaviti i organizovati informacioni sistem, te sveukupne aktivnosti oko njega da ne dođe do nekontroliranog odliva ili promjene informacija koje se čuvaju ili obrađuju u informacionom sistemu.

Poslovne informacije mogu oticati putem tehničkih kanala oticanja (koji je u literaturi najzastupljenije kroz razmatranje kompjuterskog kanala), ili putem tzv. unutrašnjih kanala, koji obuhvataju saradnike sa svojim motivima i radnim navikama. Posljedice neadekvatne zaštite informacija se ogledaju kao finansijski gubici, gubitak ugleda ili tržišnih pozicija i mogu imati katastrofalne posljedice. Očiglednost potrebe zaštite informacija je posebno izražena u različitim oblicima elektronskog poslovanja (e-bussines).

U uslovima savremenog tržišta, poslovni uspjeh i ekonomska bezbjednost nezamislivi su bez informacione bezbjednosti. Informacije i informacioni resursi predstavljaju materijalna dobra i zbog toga je zaštita informacija neodvojivi dio poslovanja.

Činjenica je da je profil kompetentnosti specijaliste za informacionu bezbjednost ne samo tehnički kao kod IT menadžera, već on mora posjedovati i upravljačka (menadžment, ekonomija, privredno pravo) i specijalistička znanja (organizacija sistema informacione bezbjednosti, zaštita poslovnih tajni, specijalna psihologija, osnovi kriminalistike i industrijska špijunaža).

II. ORGANIZACIONA KULTURA

Šta je organizaciona kultura (OK)? U ovom poglavlju su date osnovne definicije OK date u različitim oblastima istraživanja koja su povezana sa djelovanjem organizacija. Termin ”organizaciona kultura” nastao je u Americi i veoma brzo se proširio na ostatak poslovnog sveta. Napisano je mnogo članaka i knjiga o kulturi u organizacijama. Ovu kulturu obično nazivaju i „korporativna kultura" ili „organizaciona kultura". Često se za kulturu kaže da su to: „moralne, socijalne i ponašajne norme jedne organizacije zasnovane na vjerovanjima, stavovima i prioritetima njenih članova" [2].

Kulturu možemo definisati kao karakteristična vjerovanja i ponašanja koja postoje u organizaciji. OK je skup formanih i neformalnih ponašanja koja je organizacija prihvatila kao svoj način obavljanja posla. Formalna strana obuhvata pisane izjave i šemu organizacione strukture. Neformalna strana bavi se time kako se posao obavlja - da li preko pisanih procedura ili putem direktne komunikacije, kako se zaposleni ponašaju jedni prema drugima, koliko su spremni da razmjenjuju ideje i informacije i kako hijerarhija dozvoljava zaposlenima da pređu granice „staze" da bi obavili posao [3].

U osnovi, ona je opisana kao osobenost, odnosno karakteristika jedne organizacije, ili jednostavno kao „način na koji su stvari uređene u organizaciji" [4]. Ona utiče na način na koji zaposleni misle, ponašaju se i osećaju. OK je širok termin koji se koristi za definisanje osobenosti ili karaktera posebne organizacije i uključuje elemente kao što su osnovne vrednosti i verovanja menadžmenta i ostalih zaposlenih, korporativna etika i pravila ponašanja. OK može biti izražena u misiji organizacije, u arhitektonskom stilu ili unutrašnjem dekoru kancelarija, zatim može biti iskazana načinom oblačenja zaposlenih na poslu, načinom na koji zaposleni oslovljavaju jedni druge i titulama koje su im date.

„Način na koji obavljamo stvari" je često navođena definicija kulture [5]. Međutim, ovo je suviše opšta definicija koja propušta da naglasi sljedeće:

- kulture su kolektivna vjerovanja koja oblikuju ponašanje;
- kulture su djelimično zasnovane na emocijama, koje su posebno uočijive kada se prijeti promjenom;
- kulture su zasnovane na istorijskom kontinuitetu; potencijalni gubitak kontinuiteta djelimično objašnjava otpor promjeni;
- iako se kulture protive promjeni, one se konstantno mijenjaju, itd.

Zapravo, gotovo svako ko govori ili piše na ovu temu ima sopstvenu definiciju. Neke od njih ukazuju na to da je OK:

- predispozicija da se ponašamo na određene načine [5];
- grupa ponašanja i kodova koje ljudi koriste za usmjeravanje interakcije ka drugima; ona uključuje formalne, pisane politike organizacije i neformalna pravila nastala sa iskustvom [6];
- način na koji preduzeće vidi sebe i svoje okruženje [3], itd.

Svaka organizacija ima svoju sopstvenu kulturu ili set vrijednosti. Najveći broj organizacija ne pokušava svjesno da kreira određenu kulturu, već se kultura organizacije uglavnom kreira nesvjesno i bazirana je na vrijednostima top menadžmenta ili osnivača organizacije. Ono čemu organizacija teži i koje vrijednosti se nada da će dostići, može se razlikovati od vrijednosti, vjerovanja i normi izraženih u tekućoj praksi i ponašanju.

Procjena kulture može da obezbedi realne podatke o stvarnim vrijednostima i normama organizacije. Kultura je "kolektivno programiranje uma koje pravi različitosti ljudi iz različitih zemalja, u skladu s socijalno-antropološkom teorijom" [7]. Na osnovu ovoga, OK se definiše kao niz osobina na koje utiče to kako zaposleni vidi organizaciju [8].

U [8] definisana je OK: "To je kolektivni fenomen koji raste i mijenja se s vremenom i, u određenoj mjeri, na njega se može uticati ili čak i kreirati od strane upravnih organa organizacije". Osnovne pretpostavke koje određena grupa zaposlenih izumi, otkrije ili razvije u procesu učenja i nošenja sa svojim problemima eksterne adaptacije i interne integracije, i ako to rade dovoljno dobro da se smatra ispravnim mogu poslužiti i kao osnov za definisanje OK novih zaposlenih da i oni na isti način misle i osjećaju u vezi sa istim ili sličnim problemima. Posebno se ovo može odnositi na IBK. Za neke autore, kultura je najvažniji faktor u objašnjavanju uspjeha ili neuspjeha u organizaciji [9]. Međutim, ranijim studijama utvrđeno je da je samo 5% organizacija ima definisanu kulturu, gdje viši menadžment uzima aktivnu ulogu u oblikovanju OK [10]. Ako menadžment ne razumije kulturu organizacije, to bi se moglo pokazati kao fatalno [11]. Ipak, OK svake organizacije određuje ponašanje svojih zaposlenih i utiče na one stvari kojima se zaposlenim određuju prihvatljiva ponašanja unutar organizacije [12].

III. POJAM INFORMACIONO-BEZBJEDONOSNE KULTURE

Informaciona bezbjednost, kao jedan od novijih pravaca istraživanja u sferi bezbjednosti, posljedica je tehnološkog razvoja i odraz je novog pogleda na svijet. Ona se javlja ne samo kao jedan od vidova (oblika) bezbjednosti, već i kao presjek svih drugih vidova bezbjednosti u kojima informacione tehnologije zauzimaju važno mesto. O značaju informacione bezbjednosti govori i činjenica da je ona postala jedna od osnovnih komponenata nacionalne bezbjednosti.

Informaciono-bezbjedonosna kultura (IBK), koja je sastavni dio OK ima veze s ponašanjem zaposlenih [13]. Načini na koji zaposleni obavljaju svoje poslove temelje se na kolektivnim vrijednostima, normama i znanjima i imaju presudan uticaj na uspjeh cijele organizacije. Veoma je mali broj istraživanja o IBK koja bi dala jasniju sliku o definiciji IBK, niti postoje jasni stavovi o tome kako stvoriti OK za podršku IBK [14]. Takođe, u [14] tvrdi se da je veoma važno razumjeti OK koja će dovesti do odgovarajućeg načina upravljanja IBK-om.

OK ima značajan uticaj na sigurnost podataka, a to bi može biti negativno ili pozitivno [15]. Važno je da OK odražava pozitivan stav prema informacionoj bezbjednosti kroz cijelu organizaciju a to je važno za obavljanje poslova organizacije i treba biti u skladu s dobrom praksom IBK. Bezbjedonosna

kultura "temelji se na interakciji zaposlenih s podacima i sigurnosno ponašanje pokazuju u kontekstu OK organizacije" [16].

Da bi se razumio uticaj OK na bezbjedonosnu kulturu, u [14] je predložen organizacioni model kulture baziran na modelu OK definisanog u [17], koji se koristi u literaturi o bezbjedonosnoj kulturi i primjenjiv je na svakoj dimenziji bezbjednosti u organizaciji. Nakon toga je razvijen istraživački model za vrednovanje IBK. Međutim, u [18] je utvrđeno da samo posvećivanje pažnje na OK nije dovoljno za razumijevanje svih faktora koji utiču na IBK. Svaki pojedinac u svakoj organizaciji je pod uticajem nekoliko etičkih, nacionalnih i organizacionih kultura koje utiču na način na koje taj pojedinac tumači značenje i važnost informacione bezbjednosti. Kao rezultat toga, važno je razumjeti složenost OK koja ima uticaja na bezbjedonosnu kulturu.

IV. Odnos organizacione i informaciono-bezbjedonosne kulture

Kultura je set shvatanja i pretpostavki u određenoj grupi, na primjer u etničkoj grupi ili zemlji. OK sastoji se iz glavnih shvatanja i pretpostavki o poslovanju, korporaciji ili organizaciji. Shvatanja uključuju zajednička vjerovanja i ubjeđenja, vrijednosti, pristup odlučivanju i najčešće nisu dokumentovani kao ciljevi u formalnim politikama organizacija. Može se npr. očekivati od zaposlenih da budu uredno podašišani, da nose konzervativna odijela i da budu ljubazni s korisnicima. OK formira se u toku dužeg vremenskog perioda, koje može da traje i nekoliko godina. Kao i organizaciona struktura, tako i OK može uticati na razvoj i korišćenje informacionih sistema u organizacijama. Npr., procedura povezana s novim informacionim sistemom može biti u koliziji s nekim neformalnim proceduralnim pravilima koja su dio organizacione kulture.

Odnos između OK i ponašanja zaposlenih treba uzeti u obzir pri provođenju bezbjedonosne prakse, jer to utiče na način na koji se zaposleni ponašaju u organizacijama [19].

U radu [20] je dodatno naglašeno da, ako sigurnosna kultura ne prevladava u organizacijama, te će organizacije biti u problemima za održavanje integriteta organizacija i zaštitite tehničkih sistema organizacije. Od 1996.godine, mnogi autori su predložili da IBK mora biti integrisana sa OK kao uputstvo o ponašanju zaposlenih u održavanju informacione bezbjednosti [20]-[24]. U istraživanju grupe autora [25], takođe je prepoznata IBK kao skup uvjerenja zaposlenih, njihovih poštovanja određenih vrijednosti, koje se manifestuju u postupcima i ponašanju zaposlenih u zaštiti podataka organizacije.

Kroz ispitivanje definicija OK i IBK, postoje argumenti koji pojmove IBK i OK povezuju. Godinama unazad, IBK ostaje kao jedan od najviše rangiranih oblasti rada akademskih istraživača i praktičara. Na primjer, Vijeće Organizacije za ekonomsku saradnju i razvoj (OECD) posebno je definisalo smjernice za postizanje željenog stepena IBK u organizacijama [26]-[28]. Nakon toga, mnogi naučni radnici predložili se da IBK treba biti dio OK i podržavati sve aktivnosti koje se bave informacijama u organizacijama [13], [24]. Drugi autori tvrde da bi se slučajevi gdje zaposleni u organizaciji poštuju pravila organizacije dobrovoljno kao dio OK mogli smatrati utopijom [19], [24].

U literaturi su definisane tri vrste (tipa) odnosa između OK i IBK. Tip 1: IBK je odvojena od OK; Tip 2: IBK je subkultura OK; i Tip 3: IBK je ugrađena u OK.

Tip 1 odnosi se na situacije u kojima informaciona bezbjednost nije sastavni dio većine OK [14]. Često, članovi organizacije ne učestvuju ili učestvuju vrlo malo u provođenju bezbjednosti u organizacijama [14]. Članovi organizacije imaju vrlo malo znanja i ne osjećaju da je njihova odgovornost u bezbjedonosnim problemima. Organizacije često imaju tendenciju da vide troškove (posebno finansijske) u vezi sa bezbjednošću kao nepotrebni trošak, a često se bore da smanje sredstva koje se izdvajaju za bezbjedonosne inicijative [29]. Takođe, česta je situacija u kojoj IBK organizacije je potpuno odvojena od OK a svijest o organizacionoj sigurnosti je niska. To je situacija u kojoj se aktivnosti koje se tiču informacione bezbjednosti odnose samo na zaposlene u IT sektoru organizacije.

Organizacije u tipu 2 veza između IBK i OK predstavljaju situaciju u kojoj članovi organizacija unutar svog odjeljenja ili drugog nižeg oblika organizavanja poslova u organizaciji su više svjesni sigurnosnih zahtjeva; povremena obuka za sigurnost se provodi kao poštovanje zahtjeva za upravljanje. Uprava počinje više obraćati pažnju na primjeni informaciono-bezbjedonosne prakse.

U ovakvom tipu organizacija još uvijek je u manjem stepenu zastupljena međuresorna koordinacija u rukovanju informacionom bezbjednošću organizacije. Samo mala grupa ljudi učestvuje ili se uključuje u razvijanje i sprodođenje mjera iz oblasti bezbjednosti informacija i njihovo sprovođenje u organizacijama ovog tipa [14]. IBK organizacija ovog tipa je mješavina bezbjedonosnih subkultura, u kojoj svaka subkultura smiješta svoje potrebe povezane s odgovornostima i radnim zadacima pojedinih profesionalnih grupa [25]. IBK je subkultura OK. Ovakva situacija je gdje su određene vrijednosti prihvaćene od strane određene grupe, kao što je računovodstveni sektor ili sektor upravljanja ljudskim resursima.

Organizacije u tipu 3 odnosa IBK i OK ukazuju na situaciju u kojoj organizaciona bezbjedonosna praksa je odgovornost svih članova organizacije. Sprovođenje mjera bezbjednosti je uvedeno na holistički način i ima relativno visok nivo uključenosti članova.

Osim toga, u organizacijama ovog tipa se vodi računa i o ažuriranju bezbjedonosne politike. Članovi organizacije osjećaju određeni tip vlasništva nad informacijama i oni su motivisani da se pridržavaju bezbjedonosne politike. IBK je ugrađena u OK. Ovakva priroda odnosa je situacija u kojoj postoji razvijena svijest o važnosti zaštite podataka i ona nesvjesno postaje dio dnevnih poslova zaposlenih kao dio njihove rutine [19], [24]. Svi članovi organizacije prihvataju važnost IBK koja omogućuje organizacijama donošenje boljih odluka u vezi sa bezbjednosti informacija.

Ovakva klasifikacija organizacija na osnovu tipa odnosa IBK i OK odgovara klasifikaciji organizacija na osnovu kulturoloških stavova prema informacionoj bezbjednosti koju

je predložio Fitzgerald [30]. On je istakao da organizacioni kulturološki stavovi prema informacionoj bezbjednosti mogu biti, pojednostavljeno rečeno, visoki, umjereni i niski. Oni su ukratko opisani u nastavku:

- *Visoki.* Viši nivoi mendžmenta stalno vode računa o informacionoj bezbjednosti u svakom novom projektu koji se implementira u organizaciji. Periodično se vrši ažuriranje akata iz oblasti informacione bezbjednosti na visokom nivou odlučivanja. Zaposleni su svjesni važnosti informacione bezbjednosti i oni znaju kako i kome se trebaju prijaviti bezbjedonosni incidenti kada god do incidenata dođe. Godišnji budžet se postavljaju na takav nivo da je obezbiježeno finansiranje programa bezbjednosti. Viši menadžment tretira bezbjednost kao reduktor poslovnog rizika i traži od ostalih zaposlenih stalne napore na povećanju informacione bezbjednosti kroz učestovanje u aktivnostima za povećanje bezbjednosti i njihovo finansiranje .
- *Umjereni*. Zaposleni imaju određeni nivo obuke o informacionoj bezbjednosti. Uloga nadzornika informacione bezbjednosti je dodijeljena određenoj osobi kao regulatoru ili revizoru. Bezbjedonosna pravila su kreirana od strane IT odjeljenja ili sektora, ali to ne znači da se za sprovođenje ovakvih mjera ima snažna podrška. Zaposleni ne znaju gdje se pravila nalaze. Viši menadžment je obično dodijelio poslove vezane za informacionu bezbjednost zaposlenom u IT odjeljenju ili sektoru. Pojedincu su dodjeljena prava za operativne aktivnosti veznae za bezbjednost (lozinke i kreiranje novih naloga za novozaposlene).
- *Niski*. Informaciono-bezbjedonosna politika u organizaciji može biti izrađena (najčešće samo prekopirana od slične organizacije), ali organizacije ne sprovodi ili nema ozbiljne namjere za njihovo sprovođenje. Obično, mjere previđene informaciono-bezbjedonosnom politikom se upotrebljavaju u slučajevima kada je došlo do incidenata koji utiču na bezbjednost kao što je razmjena lozinki za pristup podacima. Iako viši menadžment zna da je pitanje informacione bezbjednosti važno, ipak se ovakvim pitanjima dodjeljuje niži nivo važnosti u praksi. Nema posebnog fonda za informacionu bezbjednost i obično se ovaj dio aktivnosti finansira iz predviđenih troškova za IT podršku.

Važnost IBK i dalje raste, sve više i više organizacija oslanjaju se na podatke da dobiju prednost u odnosu na konkurenciju u dinamičnom okruženju. Dakle, organizaciji je potrebna IBK da vodi postupke i ponašanje zaposlenih u zaštiti podataka organizacije. Veza između klasifikacija organizacija koje su do sada predstavljene data je u tabeli I.

U prvoj koloni tabele I prikazane su tipovi veza i kultoroloških stavova a njihv odnos može se smatrati kontinuitet u rasponu od IBK nije dio OK do IBK je ugrađena u potpunosti u OK.

Druga kolona tabele I prikazuje odnos organizacione kulture prema informaciono-bezbjedonosnoj praksi u organizacijama. Nivo učestvovanja menadžmenta i njehovo podržavanje u smislu uspostave bezbjedonosne strategije, raspored odgovornosti, učestvovanje, pružanje ogućnosti obuke, obrazovanja i treninga, kao i obezbjeđivanje finansijskih sredstava za njegovo sprovođenje može biti u rasponu od niskog do visokog.

Treća kolona pokazuje djelovanje i ponašanje zaposlenih u odnosu na informaciono-bezbjedonsnu praksu. Na novou gdje je IBK odvojena od OK, zaposleni ne brinu o odgovornosti prema bezbjedonosnim pitanjima. Zaposleni ne učestvuju u bezbjedonosnim pitanjima, a ta pitanja su ostavljena za IT sektor. Oni ne znaju kako i šta učiniti kada se suočave sa bezbjedonosnim pitanjima. Na suprotnoj kraju odnosa, gdje IBK u potpunosti je ugrađen u OK, ponašanje i rad zaposlenih su uvijek u skladu sa informaciono-bezbjednosnom politikom i definisanim procedurama. Zaposleni periodično prolaze programe o bezbjednosti. Oni osjećaju odgovornost i vlasništvo nad informacijama i prema bezbjedonosnim pitanjima. Oni znaju šta treba učiniti i kome prijaviti kada se suoče sa bezbjedonosnim problemima.

Četvrta kolona pokazuje moguće posljedice koje organizacija može imati sa bezbjedonosnim pitanjima, zavisno o njihovom trenutnom položaju u tabeli. Organizacije u kojoj je IBK je odvojena od OK mogu imati najniže troškove u sprovođenju mjera bezbjednosti, ali u isto vrijeme oni se suočavaju s najviše ranjivost. S druge strane, organizacije u kojoj je IBK u potpunosti ugrađen u OK mogu imati najniži rizik, ali s druge strane, to uključuje visoke troškove u sprovođenju mjera bezbjednosti.

V. ZAKLJUČAK

Teorijski posmatrano, da bi IBK uključili u OK, svi članovi organizacije moraju prihvatiti važnost IBK. U [31] takođe se tvrdi da se pravim fokusom, organizacije mogu kretati brže od niskog do visokog nivo informacione bezbjednosti.

Pitanje ostaje zašto IBK još uvijek nije u potpunosti ugrađen u organizacijama. U ovom radu je predstavljen okvir za bolje razumijevanje uticaja OK na bezbjednost informacija u organizaciji, kao i veze između IBK u organizaciji kao cjelini i pojedinaca koji čine tu organizacije (menadžment, ostali zaposleni) i OK. Takođe, predstavljeni okvir daje određene smjernice organiazcijama i njihovom menadžmentu ka boljoj organizovanju obuka i treninga za poboljšavanje stanja informacione bezbjednosti u organizaciji. Osnovni nedostatak predloženog okvira je njegov izvor koji se nalazi u pregledanoj literatiru iz ove oblasti a koji još nije ispitan u praktičnom djelovanju. Okvirom nisu obuhvaćene konkretne mjere koje se mogu realizovati u svakoj specifičnoj organizaciji.

TABELA I. ODNOS OK, IBK I MOGUĆIH POSLJEDICA PO BEZBJEDNOST

Priroda veze / Kulturni stavovi	Organizaciona kultura	Uvjerenja zaposlenih, akcije i ponašanje (IBK)	Moguće posljedice po bezbjednost
Tip 3 veze: IBK je obuhvaćena OK. [13], [19], [24] Visoki stavovi [30]	Uključenost menadžmenta: Menadžment se bavi bezbjedonosnim pitanjima i strategijama na visokom nivou. Odgovornost: upravljanje bezbjednosti uključuje svakog člana organizacije. Informaciono-bezbjedonosna politika: Objavljene na holistički načine. Osim toga, tu su i redovne obavijesti o bezbjedonosnoj politici. Obrazovanje / Obuka: Menadžment redovno pravi programe i treninge koji su obvezni za sve zaposlene. Finansiranje: Menadžment obezbjeđuje finansijska sredstava za pitanja bezbjednosti	Odgovornost: Uvijek se pridržavaju sigurnosnih procedura i uputstava Učestvovanje: Zaposleni prolaze periodično organizovane trening programe za podizanje nivoa bezbjednosti Predanost: Zaposleni osjećaju odgovornost i vlasništvo nad podacima. Motivacija: Motivisani i angaživani prema sigurnosnim pitanjima Svijest / Znanje: Znaj kako i kome se obratiti u vezi sa bezbjedonosnim pitanjima i problemima	Rizik: mali Svijest: Zaposlenici su vrlo svjesni i vode računa o bezbjedonosnim pitanjima u organizaciji. Odgovornost: Bezbjednost je obaveza svakog zaposlenog Bezbjedonosna praksa: Holistički način. Nesvjesno postaje svakodnevna rutina Investiranje u bezbjedonosnu praksu: Visoki troškovi u sprovođenju bezbjedonosnih aktivnosti
Tip 2 veze: IBK je subkultura OK [25] Umjereni stavovi [30]	Uključenost menadžmenta: Menadžment obično delegira pitanja bezbjednosti na IT sektor Odgovornost: Menadžment preusmjerava bezbjedonosna pitanja na rukovodioce sektora. Informaciono-bezbjedonosna politika: Stvorena u IT sektoru i nema široku podršku Obrazovanje / Obuka: Menadžment obraća pažnju na svijest. Zaposleni dobijaju neku obuku o informacionoj bezbjednosti Finansiranje: Menadžment djeluje promptno prema troškovima koji se odnose na bezbjedonosne aktivnosti	Odgovornost: Pridržavaju se bezbjedonosnih pitanja kao uslov za upravljanje Učestvovanje: Zaposleni su uključeni oko bezbjedonosnim pitanjima u njihovom sektoru. Manje je izražena međuresorna koordinacija. Predanost: Odgovoran i počinio u sigurnosnim pitanjima za vlastite odjelu. Motivacija: Zaposlenici su motivisani u vezi sa bezbjedonosnim pitanjima u njihovom sketoru. Svijest: Znaju kako i ko se bavi bezbjedonosnim pitanjima kada se suočavaju sa ovom vrstom problema u sektoru.	Rizik: Srednji Svijest: Zaposleni su svjesni bezbjedonosnih pitanjaa u njihovom sektoru Odgovornost: Zaposleni su odgovorni za pitanja bezbjednosti u njihovom sektoru Bezbjedonosna praksa: Bezbjednost je rutinska aktivnosti zaposlenog u njegovom sektoru. Investiranje u bezbjedonosnu praksu: Srednja veličina troškova u sprovođenju bezbjedonosnih aktivnosti
Tip 1 veza: IBK odvojena od OK [14], [29] Niski stavovi [30]	Uključenost menadžmenta: Menadžment zna važnost informacione bezbjednosti, ali joj dodjeljuje niži nivo važnosti Odgovornosti: Menadžment dodjeljuje svu bezbjedonosnu odgovornost IT sektoru. Informaciono-bezbjedonosna politika: Postoji deifinisana politika ali se ne sprovodi. Obrazovanje / obuka: Niska svijest. Menadžment ne obraća pažnju na obuku i treninge. Finansiranje: Obično dio sredstava za IT podršku.	Odgovornost: Ne brinu, i neodgovorne se ponašaju prema bezbjedonosnim pitanjima Učestvovanje: Zaposleni nisu uključeni u aktivnosti vezane za bezbjedonosna pitanja Obaveze: Bezbjedonosna pitanja se prepuštaju IT sektoru. Uvijek se nastoje zaobići bezbjedonosne procedure. Motivacija: Zaposlenici nisu motivisani za rad sa bezbjedonosnim pitanjima Svijest: Ne znaju šta učiniti kada se suočavaju sa bezbjedonosnim problemima	Rizik: Visok Svijest: Bez svijesti oko bezbjedonosnih pitanja Odgovornost: Samo IT sektor je odgovoran za pitanja bezbjednosti Bezbjedonosna praksa: Nerutinska aktivnost zaposlenih Investiranje u bezbjedonosnu praksu: Nisko investiranje u sprovođenje bezbjedonosnih aktivnosti

LITERATURA

[1] L. Prodanović, "Informaciona bezbednost u savremenom svetu", Okrugli sto Digitalna forenzika i IT veštačenje u funkciji borbe protiv visoko tehnološkog kriminala, IT Veštak, 2007.

[2] J. Duffy, Harvesting experience: reaping the benefits of knowledge, ARMA International, Kansas, USA, 1999.

[3] P. Guptara, "Lessons of experience – learning from others", D. Lock (ed.) Handbook of Quality Management, Gower, Aldershot, 1994.

[4] P.M. Wright, W.R. Boswell, "Desegregating HRM: A review and syntehesis of micro and macro human resource management", Journal of Management, 28(3), 2002.

[5] D. Jakovljević, V. Grujić, Menadžment u zdravstvenim ustanovama, ECPD, 1998.

[6] M.C. Stoppler, Corporate Culture, 2002.

[7] G. Hofstede, Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations. Thousand Oaks, Calif: Sage Publications, Inc., 2001.

[8] E.H. Schein, Organizational Culture and Leadership: San Francisco: Jossey-Bass, 1992.

[9] T.E. Deal, A.A. Kennedy, Organization cultures: the rites and rituals of organisation life. Reading, UK: Addison-Wesley, 1982.

[10] P. Atkinson, Creating culture change – strategies for success. Bedfordshire, England: Rushmere Wynne, 1997.

[11] Hagberg Consulting Group, Corporate culture/organisational culture: understanding and assessment, 2009.

[12] L.R. Beach, Making the right decision. Organizational culture, vision and planning. Eaglewood Cliffs, New Jersey: Prentice Hall, 1993.

[13] T. Schlienger, S. Teufel, "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture", DEXA Workshops, 2003.

[14] P. Chia, S. Maynard, A.B. Ruighaver, "Exploring Organizational Security Culture: developing a comprehensive research model", IS ONE World Conference, Las Vegas, Nevada USA, 2002.

[15] S.E. Chang, C. Lin, "Exploring organisational culture for information security management", Industrial Management & Data Systems, 107(3), 2007, pp. 438-458

[16] A. Da Veiga, J.H.P. Eloff, "A framework and assessment instrument for information security culture", Computer & Security, 29, 2010, pp.196-207.

[17] J. R. Detert, R.G. Schroeder, J.I. Mauriel, "A Framework for Linking Culture and Improvement in Organizations", Academy of Management Review, 25(4), 2000., pp. 850-863

[18] T. Helokunnas, R. Kuusisto, "Information Security Culture in a Value Net", IEEE International Engineering Management Conference, 2003.

[19] K. Thomson, R. von Solms, L. Louw, Cultivating an Organizational Information Security Culture. Computer, Fraud & Security, 2006(10), 2006., pp. 7-11

[20] G. Dhillon, Managing Information System Security, Houndmills, Basingstoke, Hampshire: Macmillan Press LTD, 1997.

[21] H.L. James, Managing Information Systems Security: A Soft Approach. IEEE, 1996.

[22] M. Andress, N. Fonseca, "Manage People to Protect Data", Infoworld, 22(46), 48, 2000.

[23] S. Breidenbach, "How Secure Are You", Information Week 2000;800:71-8, 2000.

[24] B. Von Solms, "Information Security - the Third Wave? ", Computers & Security, 19(7), 2000., pp. 615-620

[25] S. Ramachandran, V.R. Srinivasan, G. Tim, "Information Security Cultures of Four Professions: A Comparative Study", Proceedings of the 41st Hawaii International Conference on System Sciences - 2008, Hawaii, 2008.

[26] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, Recommendation of the OECD Council, 1037th Session on 25 July 2002., 2002.

[27] OECD, Implementation Plan for OECD Guides for the Security of Information Systems and Networks: Towards a Culture of Security, 2003.

[28] OECD, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, 2005.

[29] P. Shedden, A Ahmad, A.B. Ruighaver, "Risk Management Standard-the Perception of Ease of Use", Proceedings of the fifth annual security conference, Las Vegas, Nevada, USA, 2006.

[30] T. Fitzgerald, "Building Management Commitment through Security Councils, or Security Council Critical Success Factors", H. F. Tipton (Ed.), Information Security Management Handbook, Hoboken: Auerbach Publications, 2007., pp. 105-121

[31] H.F. Tipton, Information Security Management Handbook Hoboken Auerbach Publications, 2007.

ABSTRACT

This paper presents the nature of the relationship between organizational culture and information-security culture. The paper introduce a different conceptual frameworks which could assist organizations in determining the level of incorporation a information-security culture into the organizational culture. The framework provides recommendations for organizations which have intention to reach a certain level of information-security culture in their organization by influencing the actions and behavior of employees, with the aim of protecting information based on the organizational defined priorities.

THE REALATIONSHIP OF ORGANIZATIONAL CULTURE AND INFORMATION SYSTEM SECURITY IN ORGANIZATIONS

Bogdan Mirković