Engineering management 8 (1) (2022) 9-23

Engineering management

ANALIZA MODELA UPRAVLJANJA RIZIKOM DRUŠTVENIH MEDIJA U ORGANIZACIONOM KONTEKSTU

Ana Milosavljević
Univerzitet u Beogradu, Tehnički fakultet u Boru, Odsek za inženjerski menadžment
Bor, Serbia

Izvod

Kroz brz protok i neograničenu dostupnost informacionih sadržaja i servisa, stvoreni su uslovi za kvalitativan iskorak čovečanstva u jedan potpuno novi svet. Društveni mediji kao produkti revolucionarnog razvoja, su neminovno postali sastavni deo života ljudi. Međutim, njihovom upotrebom, mogu se ispoljiti različite pretnje i rizici bezbednosti. Ovaj rad je prevashodno usmeren na rizike društvenih medija koji mogu naneti štetu organizacijama. Istraživanje bazirano na modelu upravljanja rizikom korišćenja društvenih medija, ima za cilj da pruži smernice organizacijama koje u svom poslovanju primenjuju društvene medije. Teorijski model podrazumeva četiri glavne komponente, čiji su međusobni uticaji i veze detaljno ispitani. Rezultati modelovanja su dobijeni uz pomoć softvera WrapPLS 7.0, dok je za deskriptivnu statistiku, faktorsku analizu i korelaciju, korišćen program SPSS Statistics 17.0.

Ključne reči: *Društveni mediji, Rizik upotrebe, Implementacija politike, Tehnička kontrola*

1. UVOD

Evidentno je da se društveni mediji, kao sredstva za interakciju, primenjuju u gotovo svim sferama života, kao i u mnogim privrednim granama (Ostojić et al., 2014). Kada se Internet društveni mediji koriste u poslovne svrhe, oni mogu doneti izuzetne poslovne efekte (Božić & Zubanov, 2018). Sa jedne strane društveni mediji olakšavaju komunikaciju sa korisnicima i dovode do jačanja konkurentske prednosti, a sa druge strane mogu doneti i brojne rizike (Stošić et al., 2015). Nove, ali i nedovoljno ispitane tehnologije donele su veliki broj opasnosti po bezbednost pojedinca i društvene zajednice (Slavković & Kršljanin, 2015). Kao uobičajeni rizici navode se uglavnom mogućnosti postavljanja neprikladnog sadržaja, zlonamerni programi koji nanose veliku štetu, gubitak i zloupotreba važnih poslovnih podataka (Stošić et al., 2015). Iako je reč o relativno novom načinu poslovanja, popularnost društvenih medija neminovno raste (Sarabdeen, 2014). Organizacije će sve više zaostajati za novim trendovima ukoliko su ograničene u pogledu primene društvenih medija ili iskazuju negodovanje prema ovakvom načinu poslovanja (Ćirić et al., 2015). Društvene mreže su dobile više od milijardu korisnika širom sveta za samo deset godina postojanja (Icha & Edwin, 2016). Internet zajednice pružaju mogućnost organizacijama da imaju bolji sistem upravljanja odnosima sa klijentima, što je dovelo do razvoja novog koncepta gde kompanije mogu poboljšati svoje performanse (Gupta & Dhami, 2015). Neminovno je da sa ekspanzijom korišćenja Interneta, primene i razvoja elektronskog poslovanja može doći do mnogih neželjenih pratećih pojava, odnosno rizika i opasnosti, ali pojavom Interneta i Internet aplikacija, svet je postao povezaniji nego ikada pre (Raičević et al., 2014; Khan et al., 2014). Izraz Web 2.0 definiše drugu generaciju

Internet aplikacija koje su uobičajeno poznate pod pojmom *društveni mediji* (Schluze et al., 2015). Na Slici 1 su prikazani društveni mediji koji danas zastupljeni.

Slika 1. Društveni mediji
Izvor: https://pixabay.com/illustrations/icon-social-networking-presentation-908163/

Tako se na primer, moć organizacije često ogleda u stepenu koji određuju pojedinci i mreža, u središtu odnosa trenutnog predmeta posla (Pajić, 2010). Većina razvijenih kompanija u globalnom kontekstu učestvovala je u pokretu „Dot-Com“ koji se dogodio krajem 90-ih i početkom 2000. godine. U ovom vremenskom periodu, kompanije su mnogo uložile u izradu web lokacija koje bi kupcima pružale ogromnu količinu informacija (Abuhashesh, 2014). Sasvim je očigledno da razvoj ovih društvenih medija čini relativno kratak vremenski period, ali izuzetno dinamičan i sa značajnim implikacijama u različitim sferama društvenog života (Khan et al., 2014). Podatak da se kapaciteti društvenih medija konstantno uvećavaju, govori činjenica da je 2010. godine postojalo čak 350 000 poslovnih stranica i naloga na društvenim mrežama (Hajli, 2013).

2. TEORIJSKI OKVIR ISTRAŽIVANJA

2.1. Primena društvenih medija u poslovanju i upravljanje rizicima

Uspešno brendiranje danas zahteva angažovanje potrošača i lično, ali i putem digitalnih sredstava za efikasnu integrisanu promociju brenda (Scheinbaum, 2016). U tom smislu važno je da kompanija ima jasnu strategiju i bira prave medije u svoju svrhu, kako bi stvorila uspešnu komunikaciju i dostigla pravu ciljnu publiku (Greven & Sibring, 2013). ISACA, vodeća svetska organizacija znanja i obrazovanja o osiguranju i bezbednosti informacionih sistema, identifikovala je najdominantnije rizike izazvane upotrebom društvenih medijia, a to su: *virusi, zlonamerni softveri, gubitak brenda, nedostatak kontrole nad sadržajem, nerealna očekivanja korisnika na Internetu i neusklađenost sa propisima* (He, 2012). Pretnje se prenose putem Interneta sa jednog servera na drugi pod uslovom da je pojedinac ili kompanija povezana na Internet (Krubhala et al., 2015). Stoga se savetuje promišljeno postavljanje sadržaja, pri čemu je uzajamna korist pravilo, a ne izuzetak (Krstić & Lazarević, 2014). Institut za upravljanje rizicima, iz Londona, informatički rizik definiše *kao finansijsku štetu, gubitak ili narušavanje ugleda organizacije* (Jovanović, 2017). Najdominantniji informatički rizici, predstavljeni su u Tabeli 1 (He, 2012).

Tabela 1. Vrste izazova na društvenim medijima i rizici sigurnosti informacija

Vrsta izazova	Rizici informacione sigurnosti
Eksterni napadi na zaposlene i kompaniju	Zlonamerni softver, neželjena pošta, nepouzdane aplikacije, nesigurna internet veza.
Izazovi koji proističu iz radnji nesavesnih zaposlenih	Prevare, krađe identiteta, gubitak informacija, gubitak reputacije.
Izazovi vezani za usluge	Društveni mediji kao alat za umrežavanje (komunikacija sa klijentima, nedoumice oko privatnog i profesionalnog identiteta…)

2.1.1. Kategorizacija rizika na društvenim medijima

Od izuzetnog značaja je pravilno prepoznavanje rizika, koji se mogu javljati na najrazličitije načine (Tabela 2). Postojanjem rizika se svakako ne smanjuju prednosti i koristi društvenih medija, već je cilj korisnike upozoriti na moguće napade i posledice od upotrebe istih (Samčović, 2013). Pored toga, postoji i nekoliko dostupnih zakona o medijima, jer marketing društvenih mreža uključuje objavljivanje ili prenos *online* sadržaja. Prema tome, postoje i određene zakonske odredbe kada se radi o reklamiranju na nekoj društvenoj mreži (Assaad & Gomez, 2011). Prema mišljenju Vilson-a, postoji pet glavnih rizika koji mogu zadesiti organizaciju prilikom upotrebe društvenih mreža: smanjenje produktivnosti, curenje podataka, šteta reputaciji, sajber prevare i zastarele lozinke (Abuhashesh, 2014). Rizici su takođe ugrađeni u, čini se, bezazlene osobine mnogih alata društvenih medija (Andreesen & Slemp, 2011). Razvojem interaktivne komunikacije sa kupcima, menadžment kompanije se izlaže velikom riziku (Abuhashesh, 2014). Najčešći rizici u praksi sa kojima se organizacije mogu susresti tokom svog poslovanja su (Andreseen & Slemp, 2011):

- ***Transparentnost*** – kada kompanije postaju transparentne zbog društvenih medija, što znači da potrošačima omogućavaju uvid u poslovanje organizacije i;
- ***Zanimljiv sadržaj*** – može predstavljati rizik za kompanije koje žele da budu na društvenim mrežama, jer neuspeh u ažuriranju sadržaja može imati negativan uticaj na uspeh preduzeća (Greven & Sibring, 2013).

Treba naglasiti da bi trebalo da oni koji pohranjuju svoje podatke u *Cloud-u*, bolje kontrolišu rad onoga kod koga se podaci skladište (Pak, 2014). Često, određene organizacije, podatke sa svojih računara ne čuvaju na sopstvenim, već na serverima kompanija koje ih čini dostupnim putem Interneta (Outreville, 1998; Avakumović et al., 2013).

Tabela 2. Kategorizacija rizika na društvenim medijima

Rizik	Opis
Klasične i savremene pretnje	Klasične pretnje koriste se za izvlačenje ličnih podataka korisnika. Sa druge strane, obično je fokus savremenih pretnji na pribavljanju privatnih informacija korisnika i njihovih prijatelja. Na primer, kada napadač želi da sazna nešto o poslodavcu (Greven & Sibring, 2013).
Pravni aspekti	Prikriveni marketing poput blogova objavljenih tako da izgledaju kao preporuke korisnika nije zakonit (Greven & Sibring, 2013).
Kritike korisnika	Nezadovoljstvo i razočaranja lako se mogu izraziti na web lokacijama, što dugoročno može predstavljati opasnost za organizaciju (Greven & Sibring, 2013).
Nedostatak znanja	Prema mišljenju Carlsson-a, kompanije se mogu suzdržati od aktivnosti na društvenim medijima ukoliko nemaju dovoljno znanja o načinu njihove upotrebe (Greven & Sibring, 2013).
Agresivno	Ukoliko organizacije nisu pažljive sa agresivnim oglašavanjem, potrošači mogu napustiti

oglašavanje	stranicu na određenoj društvenoj mreži (Greven & Sibring, 2013).
Računarska sabotaža	Ova pretnja se sastoji u uništenju ili oštećenju računara i drugih uređaja za obradu podataka u okviru kompjuterskih Sistema (Raičević et al., 2014).
Računarska špijunaža	Počinioci računarske špijunaže koriste različite maliciozne programe i tehnike u cilju infiltriranja u računarsku mrežu koja za njih predstavlja ciljnu metu (Raičević et al., 2014).
Sajber kriminal	Sajber (*cyber*) pretnje podrazumevaju uznemiravanje pojedinca ili grupe putem Interneta ili društvenih medija. Može se koristiti za nadgledanje, krađu identiteta, pretnje ili uznemiravanje (Siddiqui & Singh, 2016).
Računarski vrusi	Ovo su mali maliciozni programi, koji imaju sposobnost samoumnožavanja i prevashodni cilj im je da naprave štetu zaraženom računaru (Raičević et al., 2014).
Računarski crvi	Na primer crv, kao što je *Conficker*, uvek napada web lokacije koje nisu zaštićene od strane kompanije ili internim podešavanjima servera (Krubhala et al., 2015).
Računarske prevare	Računarske prevare predstavljaju najraširenij vid računarskog kriminaliteta, koji često može prouzorkovati enormne štetne posledice (Raičević et al., 2014).
Krađa identiteta	Krađa identiteta znači lažno predstavljanje nekog drugog na ilegalan način, obično u cilju pristupa resursima ili dobijanja kredita i drugih pogodnosti u ime druge osobe (Outreville, 1998).

2.2. Tehnike za upravljanje rizicima na društvenim medijima

Kako postoje mnogi sigurnosni rizici upotrebe društvenih medija u organizacijama, ključno je da organizacije budu svesne tih rizika i preduzmu korake za njihovo ublažavanje (He, 2012). Neophodno je identifikovati vrstu rizika koja se opaža prilikom korišćenja nekog društvenog medija, kako bi se definisao plan reagovanja (Šekarić & Kešetović, 2018). Kao što postoje ograničenja i smernice za druge oblike komunikacije, ni društvne medije ne bi trebalo tretirati kao izuzetak (Witzig et al., 2012). U mnogim preduzećima IT odeljenja često imaju malu kontrolu nad mobilnim uređajima zaposlenih zbog njihovog visokog stepena mobilnosti i drugih opravdanih razloga (Munnukka & Järvi, 2013). Istraživanje sporovedeno u SAD-u ukazuje da su približno 12% velikih i srednjih organizacija bile žrtve zlonamrnih softvera, dok je 9% organizacija izjavilo da su imale problem gubitka informacija zbog upotrebe društvenih medija i drugih Web 2.0 aplikacija (Savić, 2012). Virtualni svet postaje sve značajnije mesto za organizacije (Witzig et al., 2012). Pokušaji definisanja informatičkih rizika sveli su se na određivanje sadržine pretnje ili opasnosti koja u smislu osiguravajućih pokrića može prouzrokovati štetne posledice (Jovanović, 2017). Organizacije moraju biti oprezne prema etičnosti pitanja poput upada u privatnost korisnika, agresivnog oglašavanja i spamova, kao i zloupotrebe podataka (Bolotaeva & Cata, 2011). U Tabeli 3 su prikazane tehnike za upravljanje rizicima na društvenim medijima. U cilju što efikasnije upotrebe društvenih medija, organizacije često koriste društvene mreže u kombinaciji sa tradicionalnim medijima (Radenković et al., 2015). Holistički pristup integrisanju novih tehnologija pomaže da se organizacija osigura da se rizici razmatraju u kontekstu širih poslovnih ciljeva (Rico et al., 2010).

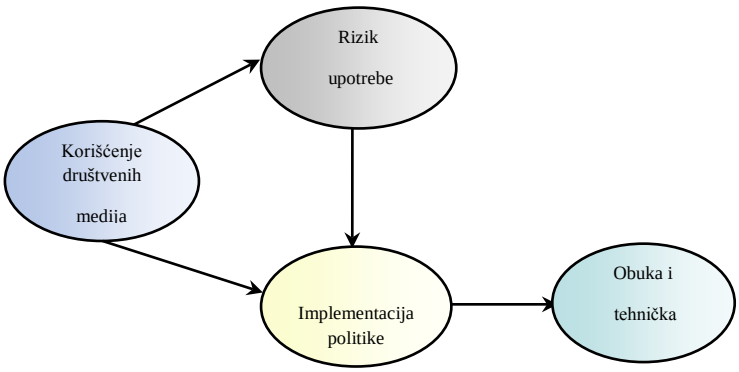
Tabela 3. Tehnike za upravljanje rizicima na društvenim medijima

Tehnike za upravljanje rizicima na društvenim medijima	
Politika	Formalna politika obično sadrži smernice koje određuju šta je prihvatljivo, a šta nije prihvatljivo prilikom njihove upotrebe, koje informacije zaposleni mogu da dele, a koje ne (He, 2012).
Pravilnik	Pažljivo kreirana politika koju svi razumeju i slede umanjiće rizike povezane sa korišćenjem društvenih medija pružajući neophodne smernice za iskorišćavanje mogućnosti, a izbegavajući opasnosti (Yehuda, 2012).
Obuka i obrazovanje	Zaposleni koji su učestvovali u nekom obliku obuka o bezbednosti u oblasti primene društvenih medija, manje je verovatno da će namerno otkriti potencijalne štetne informacije o svojoj kompaniji ili kolegama (Arnone & Deprince, 2016).

Sigurnosni softver	Zaposleni takođe moraju redovno ažurirati softver i aplikacije trećih strana na uređajima kako bi minimizirali rizike (Munnukka & Järvi, 2013)..
Sigurni protok	Napadi kao što su prevare i krađa podataka mogu se kontrolisati kada je mrežni IP postavljen na podrazumevane vrednosti kako bi se sakrio identitet korisnika od mogućih hakera (Krubhala et al., 2015).
Nadgledanje i kontrola	Na primer, organizacije bi trebalo da redovno skeniraju Internet u cilju uočavanja zloupotrebe korporativnog Brenda (He, 2012)..
Praćenje aktivnosti	Ukoliko zaposleni suviše vremena na radnom mestu provode na društvenim mrežama, to će direktno uticati na smanjenu produktvinost i utrošeno vreme (Väyrynen et al., 2012).
Arhiviranje	Automatizovani alati, poput Symantec-ovog *Enterprise Vault* softvera za arhiviranje, stvoreni su da pomognu organizacijama sačuvaju informacije o društvenim medijima koje objavljuju zaposleni (He, 2012).
Polise osiguranja	Na savremenom tržištu osiguranja postoje različite Internet polise koje pokrivaju sve štete prouzrokovane nestankom, oštećenjem ili manipilacijom podataka čak i onda kada hardver nije oštećen (Radenković et al. 2015).

3. METODOLOGIJA ISTRAŽIVANJA

Za potrebe istraživanja koje je prikazano u ovom radu primenjena je metodologija anonimnog upitnika za prikupljanje podataka. Cilj ove istraživačke studije je identifikovanje i razumevanje opsega i obima rizika povezanih sa korišćenjem društvenih medija od strane organizacija. Za dobijanje deskriptivne statistike, faktorske analize i korelacije primenjen je SPSS Statistics 17.0, a za testiranje modela, softver - WrapPLS 7.0. Zbog prirode korišćenja društvenih medija, pretpostavlja se da organizacije preduzimaju reaktivan pristup upravljanju rizikom na društvenim medijima. Dalje, ovo sugeriše na razvijanje teorijskog modela koji je predstavljen na Slici 2, a ima za cilj razumevanje međusobnog uticaja i veza između sve četiri grupe pitanja iz upitnika.



Slika 2. Teorijski model

4. ANALIZA I REZULTATI

4.1. Analiza pouzdanosti indikatora

Da bi se podaci obradili na najkvalitetniji način, neophodna je ocena njihove pouzdanosti i validnosti. Za ocenu interne konzistentnosti korišćen je *Cronbach alpha test*. Test služi za proračun prosečnih vrednosti korelacija među stavkama mernog instrumenta – *alpha koeficijent* (Manasijević, 2016). U skladu sa ovim testom, vrednosti koeficijenata alpha (α)

veće od 0.70 predstavljaju dobar potencijal za modelovanje rezultata ankete razmatrane populacije. Na osnovu dobijenih vrednosti *Cronbach* koeficijenata prikazanih u Tabeli 4, dokazana je validnost upitnika, čime se mogu očekivati pouzdani rezultati sprovedenog istraživanja.

Tabela 4. Koeficijenti interne konzistentnosti grupacija pitanja u upitniku

Grupa pitanja	**Broj stavki u okviru grupe**	**Cronbach alpha koeficijent**
KDM	6	0.752
RU	6	0.753
IP_L	2	0.776
IP_RM	2	0.773
IP_LJR	2	0.776
OTK	2	0.748

4.2. Deskriptivna statistika ispitivanog uzorka

Rezultati iz programa SPSS Statistics pokazuju osnovne parametre deskriptivne statistike. Dakle, reč je o pojedninačnim odgovorima iz ukupno četiri grupe pitanja: korišćenje društvenih medija (KDM), rizik upotrebe društvenih medija (RU), implementacija politike društvenih medija (IP), koja uključuje odgovore na pitanja vezana za politiku/smernice koje se odnose na ličnu upotrebu društvenih medija (IP_L), upotrebu društvenih medija na radnom mestu (IP_RM) i upotrebu društvenih medija od strane službe za ljudske resurse (IP_LJR). Na samom kraju, poslednju grupu pitanja čine obuka i tehnička kontrola (OTK).

Tabela 5. Deskriptivna statistika ispitivanog uzorka

Promenljiva	**Srednja vrednost**	**Medijana**	**Modus**	**Standardna devijacija**	**Varijansa**
KDM_1	3.77	4.00	4.00	1.137	1.293
KDM_2	3.45	4.00	5.00	1.323	1.750
KDM_3	3.66	4.00	5.00	1.167	1.362
KDM_4	3.05	3.00	3.00	1.311	1.719
KDM_5	2.98	3.00	2.00	1.400	1.961
KDM_6	3.30	3.00	5.00	1.379	1.902
RU_1	3.25	3.00	3.00	1.277	1.630
RU_2	2.96	3.00	3.00	1.244	1.499
RU_3	3.01	3.00	3.00	1.319	1.740
RU_4	2.85	3.00	3.00	1.099	1.207
RU_5	2.66	3.00	3.00	1.175	1.381
RU_6	3.50	4.00	4.00	1.226	1.502
IP_L_1	1.72	2.00	2.00	0.449	0.202
IP_L_2	1.80	2.00	2.00	0.402	0.162
IP_RM_1	1.80	2.00	2.00	0.402	0.162
IP_RM_2	1.70	2.00	2.00	0.458	0.210

IP_LJR_1	1.70	2.00	2.00	0.458	0.210
IP_LJR_2	1.76	2.00	2.00	0.428	1.183
OTK_1	2.51	2.00	1.00	1.279	1.637
OTK_2	2.62	3.00	3.00	1.236	1.527

Kao najzanačajni parametri posmatraju se aritmetička sredina i modus. Modus pokazuje vrednost obeležja koja u posmatranom uzorku ima najveću frekvenciju, odnosno najčešće se javlja i zato je najtipičnija vrednost u ispitivanom uzorku. Kada je u jednoj seriji samo jedna vrednost obeležja sa najvećom frekvencijom kaže se da je unimodalna, a ukoliko postoje dve ili više takvih vrednosti, serija je bimodalna, odnosno multimodalna, što i jeste slučaj sa ovim uzorkom ispitanika (Manasijević, 2016).

4.3. Mere adekvatnosti uzorka i validacije strukture

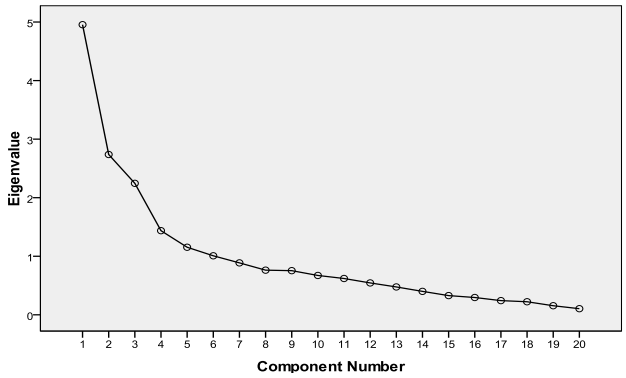
Merenje adekvatnosti uzorkovanja je izvršeno primenom *Kaiser–Meyer–Olkin* (KMO) testa. Minimalno prihvatljiva vrednost *Kaiser–Meyer–Olkin* indikatora jeste 0.6, a njegova vrednost na razmatranom uzorku iznosi 0.713, što pokazuje da podaci prikupljeni u ovom istraživanju jesu adekvatni i kao takvi su pogodni za primenu faktorske analize. Takođe, *Barttlett-ov test* sferičnosti je statistički značajan (χ^2 = 893.681, Sig. = 0.000), što ukazuje da postoje određene korelacije između grupa pitanja u okviru upitnika i da korelaciona matrica nije jedinična (Manasijević, 2016). Kako bi se moglo odrediti koliko komponenti, odnosno faktora treba izdvojiti, razmatra se deo rezultata. Po Kajzerovom kriterijumu, u obzir se moraju uzeti samo one komponente čija je karakteristična vrednost 1 ili više. Da bi se stekao uvid u to koliko komponenata zadovoljava taj kriterijum, posmatra se Tabela 6 u kojoj je prikazana ukupna objašnja varijansa.

Tabela 6. Total Variance Explained

Component	**Initial Eigenvalues**			**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings[a]**
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	4.955	24.773	24.773	4.955	24.773	24.773	3.453
2	2.738	13.688	38.461	2.738	13.688	38.461	3.078
3	2.245	11.226	49.687	2.245	11.226	49.687	2.689
4	1.437	7.184	56.871	1.437	7.184	56.871	1.686
5	1.154	5.769	62.640	1.154	5.769	62.640	2.328
6	1.008	5.039	67.680	1.008	5.039	67.680	2.533
7	.887	4.434	72.114				
8	.762	3.812	75.926				
9	.754	3.769	79.696				

10	.672	3.360	83.056				
11	.620	3.100	86.156				
12	.544	2.722	88.878				
13	.476	2.379	91.257				
14	.400	2.001	93.258				
15	.328	1.640	94.898				
16	.295	1.477	96.376				
17	.242	1.212	97.588				
18	.223	1.114	98.702				
19	.155	.775	99.478				
20	.104	.522	100.000				

Od ukupno 20 komponenti, samo prvih šest komponenti imaju karakteristične vrednosti preko 1. (4.955, 2.738, 2.245, 1.437, 1.154, 1.008), respektivno. Ovih šest komponenti objašnjavaju ukupno 67.68% varijabiliteta kao i što je prikazano u koloni *Cumulative* %. Broj komponenti koje zadovoljavaju Kajzerov kriterijum je često prevelik, pa obavezno treba pogledati i dijagram prevoja (*Screeplot*) koji se kreira SPSS-u. Na dijagramu prevoja (Slika 3) se zadržavaju se samo one komponente iznad prevojne tačke. U ovom primeru je uočen lom dijagrama na spoju sedme i osme komponente.



Slika 3. Dijagram prevoja

Pre sprovođenja PCA (*Principal Component Analysis*), bila je ocenjena prikladnost podataka za faktorsku analizu. Pregledom korelacione matrice uočeno je mnogo koeficijenata vrednosti 0.3 i više. Vrednost *Kajzer-Meyer Olkinovog* pokazatelja bila je 0.713, što premašuje preporučenu vrednost 0.6. *Bartletov test* sferičnosti dostigao je statističku značajnost, što dalje ukazuje na faktorabilnost korelacione matrice. Analiza glavnih komponenata otkrila je prisustvo šest komponenti sa karakterističnim vrednostima preko 1, koje objašnjavaju ukupno 67.68 procenata varijabiliteta. Pregledom dijagrama prevoja utvrđeno je postojanje jasne tačke loma iza šeste komponente.

Tabela 7. Pattern Matrix

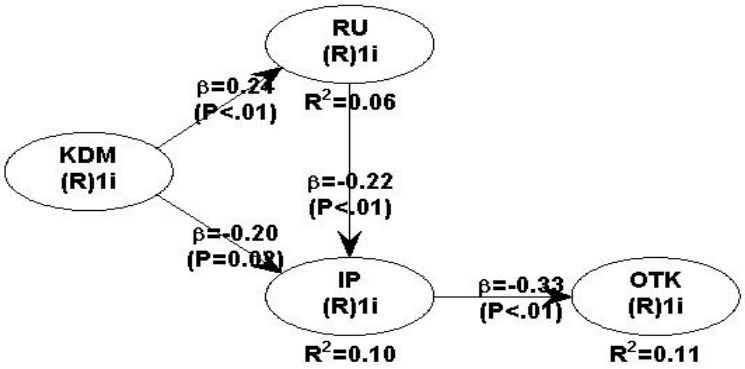
	Component					
	1	**2**	**3**	**4**	**5**	**6**
KDM 2	.882					
KDM 3	.831					
KDM 1	.830					
KDM 4	.670					-.414
RU 4		-.812				
RU 6		-.768				
RU 5		-.679				
RU 3		-.629				
IP LJR 2			.815			
IP LJR 1			.755			
OTK 1	.319		-.441		-.426	-.341
KDM 6	.361		-.402			
IP RM 1				.703		
IP L 1				.685		
IP RM 2			.394	.554		
RU 1					-.786	
RU 2					-.701	
OTK 2	.303		-.385		-.444	-.350
IP L 2						-684
KDM 5		-.429				-.603

Da bi se lakše protumačile komponente sprovedena je *oblimin* rotacija (Tabela 7). Rotirano rešenje je otkrilo postojanje jednostavne strukture, pri čemu sve komponente imaju ne tako veliki broj faktorskih težina gde sve promenljive daju znatne težine samo po jednoj od komponenata. A kada je reč o korelaciji među komponetama, ne uočava se niti preterano snažna niti slaba međusobna korelacija, o čemu će biti nešto više reči u nastavku rada.

4.4. Testiranje modela uz pomoć softvera WrapPLS 7.0

Program WrapPLS 7.0. je softver koji je razvio Ned Kock, koristeći MATLAB, C++ i Javu. Softver pomaže da se sprovede modeliranje pomoću različitih metoda na bazi kompozita i faktora, koristeći metod parcijalnih najmanjih kvadrata (*engl. PLS – Partial Least Squares*). Kako bi se testirao uticaj grupe pitanja iz modela predstavljenog na Slici 1, primenjen je WrapPLS 7.0. Obzirom da je KDM nezavisna varijabla (prediktor), najpre je utvrđeno kako ona utiče na rizik upotrebe društvenih medija (RU) i na implemantaciju politike (IP). Potom kako rizik upotrebe utiče na implementaciju politike

i na kraju pod kakvim je uticajem obuka i tehnička kontrola (OTK) u odnosu na implementiranu politiku (IP). Primenom ovog softvera, dobijeni su rezultati tri koeficijenta determinacije, nivoi statističke značajnosti, kao i standardizovani regresioni beta koeficijenti (β), a izlazni rezultat je prikazan na Slici 3.



Slika 4. Istraživački model i PLS rezultati

Testiran je model istraživanja sa Slike 2 pomoću programa WarpPLS 7.0. koji omogućava upotrebu dihotomskih mera. Budući da koristi tehniku *bootstrappin* za modelovanje parametara i *p*-vrednosti, mere ne moraju da zadovolje parametarska očekivanja. Koeficijent determinacije (R^2) je relativna mera reprezentativnosti regresione linije i ona na taj način pokazuje učešće (*procenat*) objašnjenog varijabiliteta. Njegove vrednosti se kreću od 0 (0%) do 1 (100%). Što je vrednost koeficijenta determinacije bliža jedinici to je regresioni model bolji, odnosno reprezentativniji. Najpre je ispitano kako korišćenje društvenih medija (KDM) utiče na rizik upotrebe društvenih medija (RU) i na implementaciju politike (IP). Rezultati iz softvera WrapPLS 7.0 ukazuju da je procenat varijabilnosti zavisne promenljive RU koji je objašnjen nezavisnom promenljivom KDM, izuzetno nizak i iznosi R^2=0.06 (6% varijabiliteta). Sa Slike 4 se može videti i da postoji statistička značajnost između ove dve varijablie, obzirom da je $p<0.01$ što se kod ovog programa definiše kao standardno utvrđeni nivo značajnosti. Kada je reč o uticaju korišćenja društvenih medija (KDM) i rizika upotrebe (RU) na implementaciju politike (IP), koeficijent determinacije R^2=0.10 (10% varijabiliteta) ukazuje na neznatno viši procenat varijabilnosti. Ali ne postoji statistička značajnost između grupa pitanja KDM i IP, jer je u ovom slučaju (p=0.02), što ukazuje na nepostojanje statističke značajnosti. Međutim kada govorimo o odnosu RU i IP, zaključujemo da postoji statistička značajnost ($p<0.01$). Na kraju je razmatran uticaj koji implementacija politike (IP) ostvaruje na obuku i tehničku kontrolu (OTK). Procenat varijabiliteta koji promenljiva (IP) ostvaruje na (OTK) je R^2=0.11 (11% varijabiliteta), a analiza ukazuje i da postoji statistička značajnost između implementacije politike i obuke i tehničke kontrole. Beta koeficijenti pokazuju intenzitet pedikcije odnosno objašnjavanja između promenljivih. U tom smislu se uočava da IP najviše doprinosi objašnjavanju poslednje grupe pitanja (OTK), jer je na liniji između ove dve varijable prikazan najveći beta koeficijent (β=0.33). Odnosno, OTK pod uticajem IP i RU, u ovom modelu najviše doprinosi objašnjavanju nezavisne promenljive KDM.

4.5. Korelacija

Nakon ispitivanja korelacije pomoću programa SPPS Statistics 17.0, između sve četiri grupe pitanja, iz Tabele 8, može se videti da ne postoje jake veze, osim između grupe pitanja KDM i OTK, gde je uočena jaka pozitivna korelacija i iznosi r=0.551, uz postojanje statističke značajnosti (Sig=0.031).

Tabela 8. Korelacija

		KDM	RU	OTK	IP
KDM	Pearson Correlation	1	.211*	.551**	-.190
	Sig. (2-tailed)		.031	.000	.052
	N	105	105	105	105
RU	Pearson Correlation	.211*	1	.314**	-.173
	Sig. (2-tailed)	.031		.001	.077
	N	105	105	105	105
OTK	Pearson Correlation	.551**	.314**	1	-.319**
	Sig. (2-tailed)	.000	.001		.001
	N	105	105	105	105
IP	Pearson Correlation	-.190	-.173	-.319**	1
	Sig. (2-tailed)	.052	.077	.001	
	N	105	105	105	105

Između rizika upotrebe (RU) i obuke i tehničke kontrole (OTK), je Pirsonov koeficijent korelacije umeren i iznosi r=0.314 i kao takav jeste statistički značajan (Sig=0.001). Izuzetno mala, ali pozitivna korelacija postoji između RU i KDM, gde je koeficijent korelacije r=0.211 i jeste statistički značajan. Postojanje negativnih veza između grupa pitanja IP sa jedne strane i preostale tri grupe sa druge, pokazuje da će implementacijom politike doći do smanjenja korišćenja društvenih medija, rizika upotrebe i obuke i tehničke kontrole.

5. ZAKLJUČAK

Merenje adekvatnosti uzorkovanja je izvršeno primenom (KMO) testa koji je pokazao da su podaci prikupljeni u ovom istraživanju adekvatni i kao takvi pogodni za primenu faktorske analize. Takođe, *Barttlett-ov test* sferičnosti je statistički značajan što ukazuje da postoje određene korelacije između grupa pitanja u okviru upitnika i da korelaciona matrica nije jedinična. Testiranje modela programom WrapPLS 7.0, je dalo rezultate koji su pokazali da model ima umerenu moć objašnjavanja, odnosno nije najreprezentativniji, obzirom na to da su koeficijenti determinacije izuzetno niski i da je standardizovani β keoficijent najznačajniji između poslednje dve grupe pitanja. Kada je reč o korelaciji koja je ispitana uz pomoć programa SPSS Statistic 17.0, utvrđeno je da između grupa pitanja postoji korelacija koja je uglavnom slaba, ali najznačajnija između grupe pitanja koja se odnosi na korišćenje društvenih medija (KDM) i obuku i tehničku kontrolu (OTK), ali ona kao takva i jeste statistički značajna. Društveni mediji su doslovno promenili način funkcionisanja ljudi bilo u privatnom ili u poslovnom smislu. Međusobni odnos ljudi i kompanija je danas baziran na mogućnostima digitalnog sveta koji uključuje društvene medije kao neizostavan alat komunikacije. Iz svega predstavljenog, može se zaključiti da bi neracionalna upotreba društvenih medija u poslovanju mogla usloviti postojanje velikog broja rizika koji mogu doprineti nastanku drastičnih gubitaka. Neminovno je da razultati ispitivanja ukazuju na to da su mnoge organizacije u svim svojim sistemima nedovoljno

usvojile strategije upravljanja rizicima. Organizacije bi trebalo da najpre sprovedu formalnu procenu rizika koja identifikuje i procenjuje rizike korišćenja društvenih medija, a zatim da odrede odgovarajuće odgovore na te rizike. Apsolutno je neophodno da menadžeri i zaposleni na svim nivoima u organizaciji u potpunosti shvate i razumeju važnost i mogućnosti upotrebe tehnologija 21. veka.

ANALYSIS OF SOCIAL MEDIA RISK MANAGEMENT MODELS IN ORGANIZATIONAL CONTEXT

Ana Milosavljević
University of Belgrade, Technical Faculty in Bor, Engineering Management Department Bor, Serbia

Abstract

Through the rapid flow and unlimited availability of information content and services, the conditions have been created for a qualitative step forward of humanity into a completely new world. Social media, as products of revolutionary development, have inevitably become an integral part of people's lives. However, their use can pose various security threats and risks. This paper is primarily focused on the risks of social media that can harm organizations. The research, based on the social media risk management model, aims to provide guidance to organizations that apply social media in their business. The theoretical model includes four main components, whose mutual influences and connections have been examined in detail. Modeling results were obtained with the help of WrapPLS 7.0 software, while for descriptive statistics, factor analysis and correlation, the program SPSS Statistics 17.0 was used.

Keywords: *Social media, Usage risk, Policy implementation, Technical control*

LITERATURA / REFERENCES

Abuhashesh, Y.M. (2014). Integration of Social Media Businesses. International Journal of Business and Social Science, 5(8), 202-209.

Andreesen, T., Slemp, C. (2011). Managing Risk in a Social Media-Criven Society. Knowledge Leader, 1-8.

Arnone, L., Deprince, E. (2016). Small Firms Internationalization: Reducing the Psychic Distance Using Social Networks. Global Journal of Business Research, 10(1), 55-63.

Assaad, W., Gomez Marx, J. (2011). Social Network in marketing (Social Media Marketing) Opportunities and Risks. International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT), 2(1), 13-22.

Avakumović, J., Avakumović, Č., Avakumović, J. (2013). Upravljanje rizikom u poslovanju poslovnih proizvodnih sistema, FBIM Transactions, 1(1), 92-100.

Bolotaeva, V., Cata, T. (2011). Marketing Opportunities with Social Networks. Journal of Internet Social Networking and Virtual Communities, 1-8.

Božić, A., Zubanov, V. (2018). Društvene mreže u modernom restoraterstvu, Tims Acta, (12), 25-35.

Ćirić, Z., Ćirić, I., Seldak, O., Ivanišević, S. (2015). Društvene mreže, nezaobilazni alat savremenog poslovanja Infoteh-Jahorina, 14, 350-354.

Greven, A., Sibring, S. (2013). What risks are you taking with Social Media? A qualitative study about risks with Social Media communication, 1-74.

Gupta, A., Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. Journal of Direct, Data and Digital Marketing Practice, 17(1), 43-53.

Hajli, M.N. (2013). A study of the impact of social media on consumers. International Journal of Market Research, 56(3), 387-404.

He, W. (2012). A review of social media security risks and mitigation techniques. Journal of Systems and Information Technology, 14(2), 171-180.

Icha, O., Edwin, A. (2016). Effectiveness of Social Media Networks as a Strategic Tool for Organizational Marketing Management. Journal of Internet Banking and Commerce 21(S2), 1-19.

Jovanović, S. (2017). Osiguranje od informatičkih rizika, Udruženje za pravno osiguranje Srbije, Teme, 3, 823-837.

Khan Feroz, G., Swar, B., Lee Kon, S. (2014). Social Media Risks and Benefits: A Public Sector Perspective. Social Science Computer Review, 32(5), 606-627.

Krstić, A., Lazarević, S. (2014). Primena društvenih mreža u savremenom poslovanju. Impact of the Internet on Bussines Activities in Serbia and Worldwide, 221-226.

Krubhala, P., Niranjana, P., Sindhu Priya, G. (2015). Online Social Network - A Threat to Privacy and Security of Human Society. International Journal of Scientific and Research Publications, 5(4), 1-6.

Manasijević, D. (2016). Teorijske osnove za izradu master rada, Beograd, 31-165.

Munnukka, J., Järvi, P. (2013). Perceived risks and risk management of social media in an organizational context. Electronic Markets, 24(3), 219-229.

Ostojić, S., Ilić, D., Damnjanović, N. (2014). Važnost društvenih mreža za promociju malih i srednjih preduzeća, Trendovi u poslovanju, 1(3), 23-28.

Outreville, J.F. (1998). Theory and Practice of Insurance, France, 1-12.

Pajić, B. (2010). Društveni mediji kao marketinški alat, Novi Sad, 1-68.

Pak, J. (2014). Osiguranje internet rizika, Zbornik radova, Beograd, 71-76.

Radenković, B., Despotović Zrakić, M., Bogdanović, Z., Barać, D., Labus, A. (2015). Elektronsko poslovanje, Beograd, 185-196.

Raičević, M.V., Matijašević-Obradović, D.J., Kovačević, S.M. (2014). Pravni i etički aspekti rizika poslovanja putem interneta, 94-100.

Rico, S., Bradley, B., Raine, M., Kiefer, M. (2010). Social Media: Business Benefits and Security, Governance and Assurance Perspectives, An ISACA Emerging Technology White Paper, 1-10.

Samčović, A. (2013). Bezbednost društvenih mreža sa osvrtom na Twitter, Infoteh-Jahorina, 12, 1-4.

Sarabdeen, J. (2014). Legal Risks in Social Media Marketing, International Journal of e-Education, e-Business, e-Management and e-Learning, 4(3), 218-223.

Savić, Z. (2012). Bezbednosni aspekti poslovne primene internet društvenih mreža, Konferencija o bezbednosti informacija Bices, Univerzitet Metropolitan, 6-10.

Scheinbaum, C.A. (2016). Digital Engagement: Opportunities and Risks for Sponsors: Consumer-Viewpoint and Practical Considerations For Marketing via Mobile and Digital Platforms, Journal of Advertising Research, 56(4), 341-345.

Schulze Horn, I., Taros, T., Dirkes, S., Huer, L., Rose, M., Tietmeyer, R., Constantinides, E. (2015). Business Reputation and Social Media: A Primer on Threats and Responses, IDM Journal of Direct, Data and Digital Marketing Practice, 16(3), 1-13.

Šekarić, N., Kešetović, Ž. (2018). Uloga društvenih mreža u upravljanju vanrednim situacijama, Originalni naučni rad, 23(2), 113-130.

Siddiqui, S., Singh, T. (2016). Social Media its Impact with Positive and Negative Aspects, International Journal of Computer Applications Technology and Research, 5(2), 71-75.

Slavković, V.R., Kršljanin, V.D. (2015). Uticaj operativnog okruženja na sajber pretnje, Vojno delo, 5, 333-356.

Stošić, B., Petrović, N., Antić, S. (2015). Inovativna rešenja operacionog menadžmenta za revitalizaciju privrede Srbije, Beograd, 495-501.

Väyrynen, K., Hekkala, R., Wiander, T. (2012). Information Security Challenges of Social Media for Companies, ECIS Proceedings 56, 1-12.

Witzig, L., Spencer, J., Galvin, M. (2012). Organizations' use LinkedIn: An Analysis Of Nonprofits, Large Corporations And Small Business. Marketing Management Journal, 22(1), 113-121.

Yehuda, G.B. (2012). Road Hazards: Recognizing the Risks of Social Media, Viewpoints, 68-70.