VARSTVOSLOVJE,
let. 14
št. 3
str. 345-363

Informacijskovarnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji[1]

Branko Lobnikar, Kaja Prislan, Blaž Markelj, Emanuel Banutai

Namen prispevka:

S prispevkom prikazujemo vlogo varnostne ozaveščenosti v procesu vzpostavljanja informacijske varnosti in z vidika psihosocialnih dejavnikov predstavljamo pomen zaposlenih v tem procesu. Analiza, izvedena na vzorcu zaposlenih v javnem in zasebnem sektorju, prikazuje trenutno stanje ozaveščenosti v slovenskem okolju. Na podlagi rezultatov raziskave predlagamo priporočila za nadaljnje upravljanje vedenj zaposlenih pri varovanju informacijskega kapitala v podjetjih.

Metode:

Za potrebe prispevka je bila izvedena empirična raziskava med zaposlenimi v slovenskih podjetjih v javnem in zasebnem sektorju. Uporabljeno je bilo neeksperimentalno raziskovanje, za zbiranje podatkov pa je bil uporabljen anketni vprašalnik. Z njim smo merili stopnjo znanja, stališča in vedenje zaposlenih z vidika informacijske varnosti.

Ugotovitve:

Ozaveščenost uporabnikov informacijske tehnologije je ključnega pomena pri zagotavljanju učinkovitosti varnostnih procesov v organizacijskem okolju. Kljub dokazanemu pomenu preventivnih aktivnosti, se programi informacijskovarnostnega izobraževanja in usposabljanja zaposlenih še vedno v veliki meri nanašajo zgolj na usmerjene skupine znotraj organizacijske strukture, medtem ko je sodobna tehnologija vpletena v delo skoraj vsakega posameznika. Z raziskavo ugotavljamo, da je trenutno znanje zaposlenih o varnostni politiki pomanjkljivo. Ugotavljamo tudi, da obstaja zavedanje o prispevku informacijske varnosti k organizacijskemu uspehu in da zaposleni stremijo k dodatnim izobraževalnim procesom na tem področju. Zanimanje za dvig znanja in ozaveščenosti med zaposlenimi sicer obstaja, vendar so ti programi v največji meri odvisni od odločitev menedžerjev.

1 Avtorji se zahvaljujemo mag. Katji Rančigaj za pomoč pri pisanju teoretičnega dela članka ter za kritično branje prispevka.

Omejitve raziskave:

Raziskava je omejena na slovenski prostor, pri čemer udeleženci izhajajo iz različnih delovnih področij, kjer so tudi stanja informacijskovarnostne ozaveščenosti različna. Omejitve raziskave izhajajo tudi iz načina zbiranja podatkov, kjer je bila uporabljena metoda snežne kepe.

Praktična uporabnost:

Rezultati raziskave imajo uporabno vrednost, saj v splošnem predstavljajo vpogled v trenutno stanje ozaveščenosti uporabnikov informacijske tehnologije. Hkrati pa lahko sama struktura in vsebina raziskave poda smernice organizacijam pri merjenju lastnega indeksa ozaveščenosti.

Izvirnost:

Izvirnost prispevka se kaže v njegovi uporabni vrednosti za nadaljnje raziskave in ugotavljanje njenega vpliva na dejansko stanje informacijske varnosti. Ugotovitve raziskave predstavljajo izhodiščno točko za primerjave stanj ozaveščenosti v prihodnosti.

UDK: 004.056(497.4)

Ključne besede: Slovenija, podjetja, informacijska varnost, ozaveščenost

Information Security Awareness in Public and Private Sectors in Slovenia

Purpose:

The paper shows the importance of security awareness in the process of establishing information security and presents the importance of employees in this process from the prospective of psychosocial factors. Analysis that was carried out on a sample of employees in public and private sectors indicates the current state of security awareness in Slovenian environment. Based on the survey results some recommendations for future management of staff behavior are proposed in regard to the protection of information capital in companies.

Methods:

Empirical study was conducted among employees in Slovenian companies in public and private sectors for the purpose of this paper. We used non-experimental research and online questionnaire for data collecting. The latter measured the level of knowledge, attitudes and behavior of employees in terms of information security.

Findings:

The awareness of information technology users is crucial for ensuring the effectiveness of security processes in organizational environment. Despite the proven importance of preventive activities, information security programs of employees' education and training are still largely based on targeted groups within the organizational structure only, while the modern technology is involved in the working process of almost every individual working process of almost every individual. The results show, that the current employees knowledge about security policy is inadequate. Even more, there is awareness of the importance of information security for organizational success and employees seek for further

educational process in this area. Therefore, there is interest in rising the knowledge and awareness among the employees, but these programs largely depend on managers' decisions.

Research Limitations:

The research is limited to Slovenian area. The participants originate from different work environments that differ in the level of information security awareness.

Practical Implications:

The survey results have practical value, because they generally present the current state of information communication technology users' awareness. At the same time, the structure and the content of the survey provide guidance to organizations in measuring the self-awareness index.

Originality:

The originality of the paper is reflected in its use value for further research and in assessment of its impact on the actual state of information security. The survey findings represent a starting point, which can be compared in future with new researches' findings on information security awareness.

UDC: 004.056(497.4)

Keywords: Slovenia, companies, information security, awareness

1 UVOD – POSAMEZNIK KOT KLJUČNI DEJAVNIK ZAGOTAVLJANJA INFORMACIJSKE VARNOSTI

Zaradi tehnološke odvisnosti podjetij je način poslovanja organizacij v veliki meri opredeljen z razmerami v kibernetskem prostoru. Storilci kaznivih dejanj, ki pretijo informacijskemu kapitalu, so izkoristili prednosti sodobne tehnologije, kar je povečalo njihovo organiziranost, sofisticiranost in agresivnost. Stalna uporaba informacijsko-komunikacijske tehnologije (v nadaljevanju IKT) je informacijski varnosti pripisala kritičen pomen, saj so s tem različni načini kraje, okvare in zlorabe informacij postale lažji in hitrejši način doseganja ciljev različnih storilcev kibernetske kriminalitete. Dobovšek (2009) ugotavlja, da lahko kibernetsko kriminaliteto uvrstimo med najnevarnejše in družbi najškodljivejše oblike sodobnega kriminala. Agresivnost in nevarnost tovrstne grožnje pa se še posebej kaže v organizacijskem okolju, saj je glavna tarča ravno gospodarstvo, kjer je več kot 70 odstotkov organizacijskega kapitala shranjenega v obliki informacij, ki so danes povečini v elektronski obliki (Završnik, 2005). Po mnenju Bernika in Meška (2011) pa se zaradi specifične narave kibernetske kriminalitete (anonimnost, splošna dostopnost in razširjenost tehnologije ter možnost oddaljenega dostopa) preganja malo kaznivih dejanj povezanih s kibernetskim prostorom, zato je za odpravljanje tveganj potrebno ubrati drugačen, preventivno naravnan pristop.

Ob predpostavki, da za zagotavljanje informacijske varnosti razpolagamo s tehnološko dovršenimi orodji in da lahko na vplive iz zunanjega okolja vplivamo le v manjši meri, je posameznik in njegovo vedenje eden izmed ključnih dejavnikov tudi pri zagotavljanju varnosti (in s tem tudi informacijske varnosti) v podjetjih.

Usmerjenost k zaposlenim oz. k socialnemu kapitalu v organizaciji predstavlja ločnico med »organizacijo včeraj« in »organizacijo jutri«. Slednja temelji na zavedanju, da je uspeh ali neuspeh organizacije v veliki meri odvisen od tega, kar zaposleni naredijo dobro oz. od tistega, kar je narejeno slabo. Če se je informacijska varnost pri upravljanju s tveganji še včeraj pretežno nanašala na tehnične rešitve, se je danes potrebno osredotočiti na bolj socialno-tehnične vidike in poudariti pomen vedenja zaposlenih tudi pri zagotavljanju varnosti (Dhillon in Backhouse, 2001).

1.1 Informacijska varnost – pomen informacijskovarnostne kulture

Zaščita sodobne IKT je večplasten postopek (Markelj in Bernik, 2011). Kot navajata Herath in Rao (2009) ustrezne informacijske varnosti ni mogoče doseči samo z uporabo tehničnih sredstev, saj je pozornost potrebno nameniti tudi procesom in ljudem v organizaciji.

Sistematično opredeljevanje postopkov, ki je v splošnem značilno za zagotavljanje informacijske varnosti, je pomembno z vidika preventive, saj prispeva k zmanjševanju, preprečevanju in izogibanju nevarnostim, ki so povezane z občutljivim področjem dela. Vendar pa to ni edini ter sam po sebi najbolj učinkovit način usmerjanja in spremljanja vedenja ljudi (European Network and Information Security Agency [ENISA], 2007). Določitev pravil vedenja je le nujni, a ni zadostni pogoj za končen uspeh.

Pri današnjem delu večina zlorab pravzaprav izhaja iz neznanja ali brezbrižnosti ljudi (McCullagh in Caelli, 2005), pri čemer ne smemo pozabiti tudi na njihovo malomarnost in priložnosti, ki jim jih ponuja njihov avtoriziran dostop do podatkov ali druge priložnosti nedovoljenih posegov v zaupne informacije. Ogroženost informacijskih sistemov v organizaciji je v veliki meri odvisna od vedenja zaposlenih pri uporabi tehnologije. Ljudje so najpomembnejši del varnostnega procesa, saj zaposleni, ki razumejo in spoštujejo informacijskovarnostno politiko, predstavljajo ključ do učinkovite stopnje informacijske varnosti v organizaciji. Za primer, Orgill in sodelavci (v Bakhshi, Papadaki in Furnell, 2009: 54) v raziskavi ugotavljajo, da bi kar 80 odstotkov zaposlenih zaupalo svoje uporabniško ime in 60 odstotkov svoje geslo osebi, ki bi se pretvarjala, da prihaja z oddelka za računalniško podporo. Podatki, da sta socialni inženiring in neprevidno vedenje ljudi odgovorna za več kot polovico vseh varnostih zlorab (Mackenzie, 2006), kažejo, da pravzaprav ni pomembno, kako učinkovite so oblike tehnične zaščite, saj je varnost navsezadnje odvisna od primernega vedenja končnih uporabnikov (Rhee, Cheongtag in Ryuc, 2009).

Iz tega sledi, da sta informacijska varnost in informacijskovarnostna ozaveščenost medsebojno povezana in soodvisna pojma. Ozaveščanje uporabnikov IKT je sestavni del procesa vzpostavljanja informacijske varnosti. S tem zagotovimo, da tehnologija služi svojemu namenu, implementacija tehničnih ukrepov pa na nedoslednost in malomarnost zaposlenih nima bistvenega učinka. V osnovi informacijska varnost pomeni zagotavljanje zaupnosti, integritete in dostopnosti informacij (University of Nevada Las Vegas, 2012), medtem ko informacijskovarnostno ozaveščenost definiramo kot vključenost posameznika

v procese vzpostavljanja informacijske varnosti in njegov interes za samo problematiko (Namjoo, Dan, Jahyun in Andy, 2008). Namen informacijskovarnostne ozaveščenosti je zagotoviti poznavanje in zavedanje zaposlenih o pravilih in postopkih varovanja informacijskega kapitala organizacije (Khan, Alghathbar, Nabi in Khurram, 2011).

V začetnem procesu uvajanja informacijskovarnostne politike je potrebno vedeti, kakšno stopnjo varnosti sploh želimo implementirati v delovni proces podjetja. Takšna odločitev naj bo podrejena zmožnostim kadrovskih, časovnih in finančnih virov, prav tako pa naj bo prilagojena obliki, velikosti in dejavnosti organizacij. Obenem je smiselno poznati in z merjenjem ugotoviti stanje znanja in ozaveščenosti zaposlenih na področju informacijske varnosti. Sprejem varnostnih pravil je najbolj učinkovit, kadar smo poučeni o zmogljivostih in možnostih tistih, ki naj bi pravila upoštevali. Ob implementaciji sprejete politike pa mora organizacija s pomočjo različnih izobraževalnih programov, tečajev, usposabljanj in testov poskrbeti za njeno razumevanje in dosledno upoštevanje. Tako kot je potrebno periodično ocenjevanje in posodabljanje tehnologije in varnostnih mehanizmov, je potrebno preverjati in dopolnjevati tudi znanje o informacijskovarnostnem vedenju.

Pri zagotavljanju ustrezne stopnje informacijske varnosti vseskozi iščemo ravnotežje med varnostjo in funkcionalnostjo sistemov in informacij. Ustrezno ravnotežje je mogoče doseči s potrebnimi tehničnimi ukrepi na najbolj ranljivih točkah informacijske infrastrukture v kombinaciji z usposobljenim, odgovornim in v proces zagotavljanja varnosti vključenim osebjem.

Vlogo ljudi in njihovega znanja pri zagotavljanju informacijske varnosti so potrdile različne raziskave. Spears in Barkhi (2010) sta ugotovila, da aktivna udeležba zaposlenih pri vzpostavljanju varnostnih ukrepov skupaj s programi ozaveščanja, pomembno vpliva na dvig dejanske stopnje informacijske varnosti. Tudi Saksida (2010) je v raziskavi informacijskovarnostne ozaveščenosti zaposlenih v Sloveniji ugotovil, da stanje ozaveščenosti zaposlenih vpliva na manjšo stopnjo informacijskih incidentov. Medtem so Talib, Clarke in Furnell (2010) s pomočjo raziskave prišli do ugotovitve, da ljudje večino znanja povezanega z varno uporabo tehnologije pridobimo ravno v delovnem okolju. Programi izobraževanja in usposabljanja so torej še toliko bolj pomembni, saj v delovnem okolju pridobljeno znanje prenašamo na druga okolja izven organizacije. Skoraj istočasno pa sta Bernik in Meško (2011) ob analizi zavedanja in dojemanja kibernetskih groženj med uporabniki tehnologije v Sloveniji ugotovila, da na splošno obstaja pomanjkanje ozaveščenosti o kibernetskih grožnjah in zakonodaji na tem področju.

Potrjen vpliv ozaveščenosti na informacijsko varnost ob upoštevanju pomanjkanja zavedanja uporabnikov o kibernetskih grožnjah v slovenskem prostoru nakazuje na potrebo po izboljšanju trenutnega stanja v organizacijah in Sloveniji nasploh. Pri doseganju takšnega cilja se morajo izvajalci programov zavedati vpliva organizacijske kulture in njene dinamike na vedenje ljudi in njihovo uporabo tehnologije. Celovita informacijska varnost ne zajema samo znanj s področja tehnologije in tehnoloških procesov, temveč je potrebno razumeti tudi psihosocialne dejavnike, ki vplivajo na odnos človek – stroj. Čaleta, Rančigaj in Lobnikar (2011) ugotavljajo, da je ravno organizacijska dinamika najpomembnejši

dejavnik, ki vpliva na procese ponotranjenja pravil varnostnega vedenja in vedenjske vplive zaposlenih, ko se srečujejo z upravljanjem varnostnih podatkov. Tudi Kury, Meško, Mitar in Fields (2009) poudarjajo pomen organizacijske kulture na vedenje ljudi, saj je od same kulture ljudi odvisno dogajanje v nekem okolju. Ljudje pravzaprav sami ustvarjamo situacije, v katerih smo lahko oškodovani, zato je ustvarjanje varnostno pozitivnega okolja in kulture nujno potrebno za dosledno upoštevanje in izvajanje varnostnih ukrepov (Kreuger in Kerney, 2006).

Informacijskovarnostna kultura je sestavni del organizacijske kulture, saj slednja predstavlja prevladujočo kulturo v organizacijskem okolju, informacijska kultura pa je njena komponenta, kar potrjujejo tudi različne raziskave (Borck; Connolly; Le Grand in Ozier vsi v Da Veiga in Eloff 2010: 197). Informacijskovarnostno kulturo se lahko opredeli kot odnos, predpostavke, prepričanja, vrednote in znanje, ki ga imajo zaposleni v odnosu do organizacijskega sistema in postopkov v vsakem delu dneva. Odnos se kaže v sprejemljivem ali nesprejemljivem vedenju (nastanek napak) v obliki artefaktov (tj. vedenjskih vzorcev in načinov ravnanja) in postopanju, ki postane način za pravilno urejanje stvari v organizaciji z namenom, da se zaščitijo informacijske vrednosti (ibid.: 198). Podobno definirata informacijskovarnostno kulturo tudi Martins in Eloff (v Kuusisto in Ilvonen, 2003: 433), ki jo opisujeta kot predpostavko o sprejemljivem vedenju, ki je v skladu s pravili varovanja informacij in vključuje značilnosti, kot so celovitost in razpoložljivost informacij. Po njunem mnenju jo je mogoče oceniti na organizacijski, skupinski in individualni ravni.

Načela informacijskovarnostne kulture, ki usmerjajo vedenje in mišljenje ljudi, lahko strnemo v devet vsebinskih sklopov (Organization for economic co-operation and development [OECD], 2002, 9–12):

a) **Zavest**: uporabniki se zavedajo potrebe po varovanju informacijskih sistemov in omrežij ter se sprašujejo, kaj lahko storijo za povečanje varnosti.

b) **Odgovornost**: vsi uporabniki so odgovorni za varnost informacijskih sistemov in omrežij.

c) **Dovzetnost**: uporabniki ukrepajo pravočasno in kooperativno na način, da se preprečijo in odkrijejo varnostni incidenti oz. da se nanje primerno odreagira.

d) **Etika**: udeleženci spoštujejo legitimne interese drugih.

e) **Demokracija**: varnost informacijskih sistemov in omrežij je v skladu s ključnimi vrednotami demokratične družbe.

f) **Ocena tveganj**: udeleženci napravijo oceno tveganj, da se ugotovijo grožnje in slabosti, določijo tudi sprejemljivo raven tveganj, preden se vzpostavi nadzor.

g) **Varnostni načrt in implementacija**: uporabniki vključujejo element varnosti kot ključen element informacijskih sistemov in omrežij, tako v tehnične kot netehnične ukrepe in rešitve.

h) **Upravljanje z varnostjo (varnostni menedžment)**: udeleženci sprejmejo celovit pristop zagotavljanja varnosti, vključno z varnostnimi politikami, praksami, ukrepi in postopki, ki so usklajeni in strjeni z namenom, da se ustvari skladen varnostni sistem.

i) **Ponovna ocena**: udeleženci pregledajo in ocenijo varnost informacijskih sistemov in omrežij ter poskrbijo za ustrezne spremembe varnostne politike, praks, ukrepov in postopkov.

Omenjena načela informacijskovarnostne ozaveščenosti dokazujejo, da so varnostna politika, neformalna pravila vedenja, medsebojni odnosi, zgled nadrejenih, praksa nadziranja ter (ne)doslednost pri nagrajevanju in sankcioniranju tisti elementi, ki jih je smiselno upoštevati pri oblikovanju in izvajanju programa informacijskovarnostnega ozaveščanja.

1.2 Programi informacijskovarnostnega ozaveščanja in merjenje njihove učinkovitosti

Za uspešen proces vzpostavljanja informacijskovarnostne ozaveščenosti mora imeti organizacija določeno informacijskovarnostno politiko, ki je prilagojena potrebam in sposobnostim organizacije ter njenim zaposlenim. Ob tem je potrebno določiti postopke ocenjevanja, merjenja in nadziranja varnostnega obnašanja, saj brez ocene stanja pred in po uvedbi programa ne moremo soditi o njegovi uspešnosti. Izvajalci in uporabniki programov ozaveščanja se morajo zavedati, da gre za dinamičen proces, ki ga je zaradi nenehnih sprememb potrebno stalno obnavljati, spreminjati in posodabljati.

Pri oblikovanju programa je potrebno upoštevati zahteve po natančnosti, jasnosti, razumljivosti, predvsem pa doslednosti in zanimivosti, z namenom, da vzbudimo interes pri udeležencih (Kreuger in Kerney, 2006). Ugotovljeno je bilo, da je za ponotranjenje nekega vedenja potrebno pri ljudeh dvigniti znanje, občutek nadzora nad svojimi dejanji in ozaveščenost. Tudi znanje o posledicah in verjetnostih informacijskih incidentov vpliva na pripravljenost zaposlenih upoštevati pravila (Huang, Rau, Salvendy, Gao in Zhou, 2011). Vendar znanje samo po sebi še ne povzroči spremembe v obnašanju, temveč so premiki odvisni od motivacije in namenov ljudi.

Odnos posameznika do neke situacije pogojuje njegov odziv na dogajanje. Če bi se tega zavedali vsi izvajalci programov informacijske varnosti in bi poskrbeli za ustrezno motiviranost ter znanje uporabnikov tehnologije, bi se ogrožanje oz. tveganja informacijskega kapitala organizacij močno zmanjšalo. Teorije motiviranja zaposlenih in pripadnosti organizaciji, ki jih menedžerji uporabljajo pri vodenju zaposlenih so velikokrat spregledane, še posebej kadar je govora o informacijski varnosti, saj se le-ta še vedno v večini organizacij ločuje od drugih organizacijskih področij in razume kot sistem zase, večinoma pa izhaja iz tehničnega in ne vedenjsko-upravljavskega pristopa. Kar je napačno in predstavlja tveganje za varno vedenje. Takšno razumevanje in ločevanje je mogoče odpraviti s programi informacijskovarnostnega ozaveščanja, ki upoštevajo organizacijske, psihološke in sociološke procese v organizaciji.

Večina programov ozaveščanja zaposlenih temelji na t. i. KAB[2] teoriji, ki v ospredje postavlja pomen znanja. Dvig znanja naj bi sprožil spremembe v vedenju vendar takšne spremembe po mnenju Khana et al. (2011) niso dolgoročne. Če želimo sprožiti trajne spremembe v posameznikovem vedenju, je potrebno razumeti tudi teorijo razumskosti,[3] ki velik pomen pripisuje tudi odnosu in namenu posameznika. Kadar ima le-ta pozitiven odnos do nekega dogajanja, bo to hitreje ponotranjil in posledično spremenil svoje vedenje.

Iz tega sledi, da mora proces učenja vsebovati tri elemente (Peltier, 2005): ozaveščenost (motiviranje, stimuliranje), usposobljenost (pravilna uporaba tehnologije) in znanje (o tehnoloških procesih, grožnjah). V nadaljevanju mora biti posamezniku jasno predstavljena meja med dovoljenim in nedovoljenim in mu dana možnost, da sam izbere pravo pot (Peršak, 2009), saj se s tem izognemo občutku prisile in grožnje. Seveda mora ob tem informacijskovarnostna politika jasno opredeliti, kako se ukrepa, če nekdo v podjetju namerno ali po pomoti krši postavljena pravila. Izjemno pomemben je tudi odnos vodstva podjetja, ki mora za varnostno pozitivno okolje postaviti zgled za celotno organizacijo in poskrbeti za kontinuiranost ter razvijanje procesa. Cilj razvoja znanja in usposobljenosti zaposlenih pri ravnanju z IKT je mogoče doseči zgolj s stalnim ocenjevanjem in primerjanjem trenutnega stanja. S tem lahko identificiramo dosedanje dosežke in ugotovimo potrebe po izboljšanju v prihodnosti.

Kruger in Kerney (2006) sta razvila model za merjenje informacijskovarnostne ozaveščenosti zaposlenih, v katerega sta vključila predpostavke o znanju, odnosu in obnašanju zaposlenih z vidika informacijske varnosti. Zanimalo ju je, kaj zaposleni vedo, kaj si mislijo in kako se obnašajo pri uporabi tehnologije in v primerih informacijskih incidentov. Na podlagi rezultatov sta izmerila indeks ozaveščenosti v različnih oddelkih, naredila mapo stanja ozaveščenosti in predlagala smernice za izboljšanje stanja varnosti v organizaciji.

Celoviti programi informacijskovarnostnega ozaveščanja, ki bi upoštevali vse vidike vedenja ljudi, so v slovenskem organizacijskem okolju še vedno redkost. Sicer veliko organizacij posveča pozornost izobraževanju zaposlenih, vendar navadno le tistih, ki imajo opravka z vzpostavljanjem in ohranjanjem informacijskih sistemov, medtem ko so ostali zaposleni prepuščeni sami sebi, lastnemu nadgrajevanju obstoječega znanja in organizacijski politiki. Iz tega sledi, da so tudi programi merjenja informacijskovarnostne ozaveščenosti še vedno v povojih, kljub temu, da naj bi bila začetna faza v procesu ozaveščanja ljudi. Z namenom spodbujanja razvoja tovrstnih programov smo razvili merski inštrument za merjenja informacijskovarnostne ozaveščenosti in izvedli pilotsko študijo med zaposlenimi v slovenskih organizacijah.

2 *Knowledge-attitude-behaviour.*

3 *TRA-theory of reasonable action.*

2 OPIS UPORABLJENE METODE IN VZORCA

Za merjenje stopnje informacijskovarnostne ozaveščenosti smo uporabili neeksperimentalno raziskovanje družboslovnih pojavov. Tehnika zbiranja podatkov je temeljila na metodi snežne kepe z uporabo socialnih omrežij, raziskavo pa smo izvedli s pomočjo anketnega vprašalnika, objavljenega na internetni strani. Pri tem smo si pomagali s spletnim orodjem 1ka (http://www.1ka.si/).

Iz načina zbiranja podatkov (ne gre za enostavni naključni vzorec) izhajajo tudi omejitve te raziskave, ki jih je treba upoštevati pri posploševanju podatkov na celotno slovensko okolje. Za tovrstno anketiranje pa smo se odločili zaradi predpostavke, da želimo anketirati uporabnike IKT v podjetjih, ki jih je mogoče najlažje doseči tako, da jih nagovoriš s pomočjo uporabe informacijske tehnologije.

Anketiranje je potekalo v februarju 2012. Sodelovanje v raziskavi je bilo prostovoljno, uporabnikom pa je bila zagotovljena anonimnost in zaupnost njihovih odgovorov. Zbrane podatke smo obdelali s pomočjo licenčnega statističnega programskega orodja SPSS, za prikaz ugotovitev pa so bile uporabljene metode opisne statistike in multivariatne statistične metode.

V raziskavi je sodelovalo 498 zaposlenih v slovenskih podjetjih, pri tem jih je 64 % zaposlenih v javnem sektorju in 56 % v zasebnem sektorju. 14 % anketirancev prihaja iz mikro podjetja, 20 % jih je zaposlenih v majhnem podjetju, 24 % anketirancev je del srednje velikega podjetja, preostalih 42 % pa jih prihaja iz velikega podjetja. Velika večina udeležencev raziskave, 89 %, pri svojem delu zelo pogosto uporablja računalnike, 10 % jih le-te uporablja pogosto, 1 % pa zgolj občasno.

Namen raziskave je bil najprej izdelati celovit inštrument za merjenje informacijskovarnostne ozaveščenosti v slovenskem delovnem okolju ter ga testirati na zadosti velikem vzorcu zaposlenih. Anketni vprašalnik je poleg splošnih demografskih podatkov anketirancev meril tri vsebinske sklope: (a) znanje o informacijskovarnostnem vedenju, (b) vedenje uporabnikov IKT ter (c) odnos uporabnikov do informacijskovarnostnih ukrepov/procesov v organizaciji (v skladu s prej omenjeno KAB teorijo). Vsebinski del, ki se je nanašal na znanje o področju informatike in uporabe IKT v organizaciji/podjetju, je sestavljalo deset trditev, ki so jih anketiranci ovrednotili z vidika ne/strinjanja. Drugi del vprašalnika je bil sestavljen iz devetih trditev, s katerimi smo merili informacijskovarnostno vedenje anketirancev, pri čemer smo za merjenje odgovorov uporabili petstopenjsko Likertovo lestvico. Zadnji del vprašalnika je sestavljalo deset trditev, s katerimi smo merili odnos uporabnikov do informacijskovarnostnih ukrepov/procesov v organizaciji; za označevanje odgovorov pa smo uporabili štiristopenjsko lestvico Likertovega tipa (Crombach α koeficient notranje konsistentnosti vprašalnika je bil 0,842).

3 PREDSTAVITEV IN INTERPRETACIJA REZULTATOV RAZISKAVE

V nadaljevanju so prikazani rezultati analize zbranih podatkov. Pri predstavitvi rezultatov smo kot izhodišče uporabili strukturo znanje-vedenje-odnos, da bi

ugotovili medsebojni vpliv na celovito stanje informacijskovarnostne ozaveščenosti. V nadaljevanju smo s pomočjo korelacijske analize analizirali tudi povezavo med temi proučevanimi vsebinskimi sklopi.

3.1 Znanje o informacijskovarnostnem vedenju

V tabeli 1 so prikazani odgovori na trditve, s katerimi smo želeli ugotoviti, ali imajo uporabniki dovolj znanja o varni uporabi IKT pri njihovem vsakdanjem delu. Trditve so bile oblikovane tako, da odsevajo standarde varne uporabe IKT pri delu v podjetjih/organizaciji, anketiranci pa so pri vsaki trditvi lahko izbrali med odgovorom »da« ali »ne«, pri čemer so se vsa vprašanja nanašala na področje uporabe tehnologije izključno v delovnem okolju.

Tabela 1: Znanje o varni uporabi IKT

Trditev	Da %	Ne %
Ali ste previdni pri ravnanju z e-pošto, še posebej tako, da nikoli ne odpirate priponk, če niste popolnoma prepričani o njihovem izvoru?	90,7	9,3
Ali uporabljate posodobljene anti-virusne programe na vseh računalnikih, ki jih uporabljate?	86,9	13,1
Poznam posameznika (ali skupino), ki je zadolžen za varnost informacijsko-komunikacijske tehnologije v naši organizaciji in skrbi za nadgradnjo varnostnih programov na mojem računalniku.	85,3	14,7
Moji računalniški računi so zaščiteni z močnim geslom.	72,2	27,8
Ali ste previdni pri brskanju po internetu, zlasti z uporabo varnejših brskalnikov, imate npr. izklopljen Active X in ste previdni pri klikanju na nove povezave?	70,9	29,1
Gesla, ki ga uporabljam na svojih računalnikih v službi, nimam nikjer zapisanega in ga nisem nikoli povedal komu drugemu.	65,5	34,5
Če pustim svoj računalnik nevarovan (na primer, ko odidem iz nezaklenjene pisarne), je ta zavarovan z geslom, ko se (v nekaj minutah) vključi ohranjevalnik zaslona.	62,7	37,3
Dobro poznam pravila s področja informacijske varnosti v svoji organizaciji.	54,3	45,7
Ali veste, kaj morate narediti, če se pri delu z računalnikom zgodi nekaj, kar bi lahko opisali kot (informacijski) varnostni incident?	51,7	48,3
Poznam postopek varnostnega kopiranja vseh podatkov, za katere sem odgovoren v organizaciji in sem že preizkusil obnoviti podatke (datoteke), ki sem jih shranil s pomočjo varnostnega kopiranja.	36,3	63,7

Iz prikazanih odgovorov lahko ugotovimo, da so šibke točke v znanju o varnem vedenju pri delu povezanem z IKT predvsem naslednje: (a) uporabniki slabo poznajo pravila s področja informacijske varnosti v svoji organizaciji; (b) uporabniki ne poznajo pravil/postopkov varnostnega kopiranja podatkov in so pri tem delu zelo neizkušeni; ter (c) uporabniki ne vedo, kaj naj naredijo, če se jim pri delu z IT tehnologijo zgodi nekaj, kar bi lahko opisali kot varnostni incident.

Iz odgovorov smo lahko izračunali tudi stopnjo znanja o informacijskovarnostnem vedenju (sešteli smo odgovore »da« pri vsakem anketirancu – posameznik je tako lahko dobil minimalno 0 in maksimalno 10 točk). Rezultati so predstavljeni v nadaljevanju (tabela 2). Vidimo lahko, da je 29 odstotkov udeležencev raziskave zbralo manj kot 6 točk (če za kriterij uporabimo visokošolsko ocenjevanje in za stopnjo zadostnosti znanja določimo 60 odstotkov). Pri tem smo ugotovili, da med zaposlenimi v javnem in zasebnem sektorju ne prihaja do statistično značilnih razlik.

Tabela 2: Porazdelitev stopnje znanja o uporabi IKT

Vrednost	Frekvenca	Odstotek	Kumulativni odstotek
,00	2	,4	,4
1,00	3	,6	1,0
2,00	12	2,4	3,5
3,00	27	5,5	9,0
4,00	37	7,6	16,5
5,00	61	12,4	29,0
6,00	71	14,5	43,5
7,00	75	15,3	58,8
8,00	79	16,1	74,9
9,00	58	11,8	86,7
10,00	65	13,3	100,0
Skupaj	490	100,0	

Povprečna vrednost/ocena znanja o informacijskovarnostnem vedenju znaša 6,77, kar pomeni, stopnjo znanja lahko ocenimo z oceno »dobro«, saj je več kot polovica udeležencev raziskave zbrala vsaj sedem od skupaj deset možnih točk glede znanja o varnem vedenju pri uporabi IKT v službi.

3.2 Vedenje uporabnikov informacijsko-komunikacijske tehnologije

Naslednji vsebinski sklop zajema oceno dejanskega vedenja uporabnikov IKT z vidika informacijske varnosti. Namen je bilo ugotoviti, kako se zaposleni vedejo pri uporabi delovne tehnologije. Ločeno merjenje znanja in vedenja izhaja iz domnev, da uporabniki tehnologije največkrat vedo, kako se je potrebno obnašati pri uporabi tehnologije, vendar pa se iz različnih vzrokov ne vedejo tako, kot bi bilo prav oz. zaželeno.

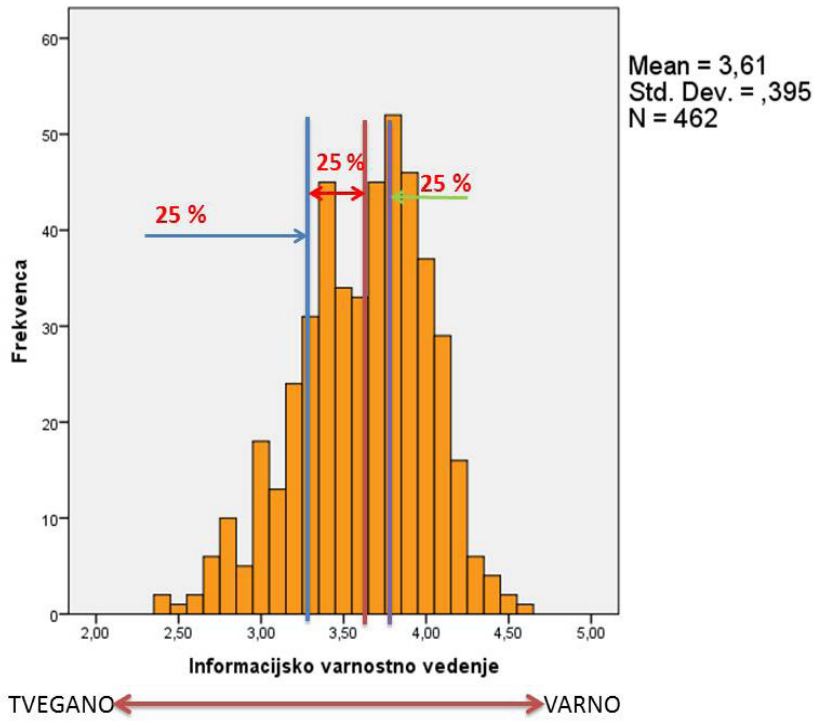
V tabeli 3 so prikazani odgovori na devet trditev o varnem ravnanju anketirancev pri uporabi IKT, prav tako so predstavljeni rezultati opisne statistike, za podrobnejšo analizo pa poleg povprečne vrednosti vključujemo tudi rezultate za modus (najbolj pogost odgovor) ter mediano (središčnica). Za merjenje vedenja je bila uporabljena pet stopenjska lestvica, pri čemer je izbira višje vrednosti na lestvici pomenila tudi bolj varno vedenje pri uporabi IKT.

Tabela 3: **Vedenje pri uporabi IKT**

Trditev	Povpr.	St.od.	Me	Mo
Svoja gesla intervalno (po določenem času) menjam.	4,37	1,01	5	5
Zgodi se, da kdaj zaradi radovednosti odprem kakšno od priponk ali povezav, ki jo dobim z elektronsko pošto, čeprav ne vem natančno, kdo mi je to pošto poslal.	4,34	,76	4	5
Uporabljam staro verzijo anti-virusnega programa.	4,22	,99	5	5
Redno varnostno kopiram svoje podatke oz. datoteke.	4,14	,81	4	4
Če se mi pri delu z računalnikom zgodi varnostni incident, tega ne povem nikomur, ampak sam popravim škodo.	3,97	1,14	4	5
Ko menjam računalniško geslo, uporabim kakšno svoje staro geslo.	3,96	1,11	4	5
Zaradi narave svojega dela sem svoje računalniško geslo že zaupal kateremu od svojih sodelavcev.	3,91	1,21	4	5
Zgodi se, da pustim svoj računalnik nezavarovan ali nezaščiten.	3,64	1,35	4	5
Ko v službi brskam po internetu, si ogledujem tudi strani, za katere bi lahko trdili, da so z vidika varnosti neprimerne.	3,01	1,37	3	4

Najšibkejšo točko pri (ne)varnem vedenju ob uporabi tehnologije v analiziranih organizacijah, lahko identificiramo na področju brskanja po nedovoljenih spletnih vsebinah v delovnem času. Z vidika nesprejemljivosti varnega vedenja pa lahko nekaj težav opazimo tudi pri dostopu do računalniške opreme, ki jo uporabniki kar pogosto pustijo nezaščiteno in tako ranljivo tudi za zlorabe.

Iz odgovorov smo izračunali tudi stopnjo varnega vedenja pri uporabi informacijske tehnologije v slovenskih podjetjih, ki je predstavljena na Grafu 1 v nadaljevanju. Tako kot pri znanju, lahko ugotovimo, da je povprečna vrednost 3,61, kar pomeni oceno varnostnega vedenja nekje med »dobro« in »prav dobro«. V grafu lahko tudi vidimo porazdelitev po kvartilih, pri čemer ugotovimo, da se najvišja frekvenca začne v zadnjem, zgornjem, kvartilu.



Graf 1: Stopnja informacijsko-varnostnega vedenja v slovenskih podjetjih

3.3 Odnos do varne uporabe informacijsko-komunikacijske tehnologije

V zadnjem vsebinskem sklopu smo ugotavljali še odnos uporabnikov do uporabe tehnologije. Rezultati odgovorov na deset trditev povezanih z odnosom anketirancev so prikazani v tabeli 4. Ugotovimo lahko, da se anketiranci najmanj strinjajo s trditvijo, da so spremembe, ki poskušajo izboljšati informacijsko varnost v organizaciji sprejete pozitivno, hkrati pa se anketiranci v manjši meri počutijo odgovorne za vzdrževanje visoke stopnje informacijske varnosti v podjetju, v katerem so zaposleni. V splošnem so anketiranci na štiri stopenjski lestvici[4] (kjer 4 pomeni varno) dosegli povprečno vrednost 3,21. Rezultat je podoben tistemu, ki smo ga dobili pri analiziranju anketirančevega vedenja in znanja.

4 *Za štiristopenjsko lestvico smo se odločili, ker nismo želeli vključiti možnosti »niti se ne strinjam, niti se strinjam«; tako smo merili samo različne nivoje (ne)strinjanja s postavljenimi trditvami.*

Tabela 4: Odnos do informacijske varnosti v slovenskih podjetjih

Trditev	Povpr.	St. odklon
Menim, da je izobraževanje s področja informacijske varnosti za zaposlene potrebno.	3,44	,57
Menim, da bi vsaka organizacija morala imeti natančno določen postopek prijave varnostnih incidentov.	3,40	,52
Menim, da je vedno pomembno upoštevati pravila, ki se nanašajo na prenos informacij z interneta, npr. priponke v e-pošti, software itd.	3,36	,52
V vsaki organizaciji bi morali imeti zapisana pravila o tem, kako poročati o nezgodah, ki so v povezavi z informacijsko varnostjo.	3,33	,55
V mojem interesu je, da prijavim in tudi razrešim varnostni incident, vezan na rabo informacijsko-komunikacijske tehnologije.	3,25	,59
Pripravljen/a sem spremeniti svoje delovne navade, če bi se s tem zagotovila večja varnost informacij, s katerimi imamo opravka v organizaciji.	3,22	,52
Visoka informacijska varnost je ključnega pomena za uspešnost in učinkovitost moje organizacije.	3,21	,70
Menim, da bi moral biti vsak posameznik osebno odgovoren za neupoštevanje/zlorabo pravil o varovanju informacij v naši organizaciji.	3,12	,67
Počutim se odgovornega za vzdrževanje visoke stopnje informacijske varnosti v naši organizaciji.	2,94	,76
Spremembe, ki poskušajo izboljšati informacijsko varnost, so znotraj moje organizacije sprejete pozitivno (npr. urejeno delovno okolje, uporaba enkripcije, vsakodnevno ustvarjanje varnostnih kopij itd.).	2,83	,69

Legenda: 1 - sploh se ne strinjam 2 - se ne strinjam 3 - se strinjam 4 - močno se strinjam

Šibke točke v odnosu do zagotavljanja informacijsko varnostnega vedenja v analiziranih podjetjih lahko najdemo predvsem v dejstvu, da spremembe, ki bi poskušale izboljšati informacijsko varnost v podjetjih, niso dojete kot nekaj pozitivnega in pomembnega tako za zaposlene kot za podjetje kot celoto, hkrati pa lahko ugotovimo, da se posamezniki ne počutijo odgovorne za vzdrževanje visoke informacijske varnosti v njihovi organizaciji. Kot kaže, zaposleni še vedno verjamejo, da morajo informacijsko varnost zagotavljati predvsem drugi (na primer sistemski inženirji), kar z vidika varnostnega ozaveščanja predstavlja pomembno tveganje.

3.4 Povezave med znanjem, vedenjem in odnosom do zagotavljanja informacijskovarnostnega vedenja

V nadaljevanju smo izvedli korelacijsko analizo (uporabili smo Pearsonov korelacijski koeficient) povezanosti med znanjem, vedenjem ter odnosom do

informacijskovarnostnega vedenja. Izvedli smo tudi primerjavo rezultatov med zaposlenimi v javnem in v zasebnem sektorju.

Ugotovili smo, da je znanje povezano s pogostostjo uporabe IKT; tisti, ki računalnike uporabljajo zelo pogosto, imajo tudi več znanja o varnem vedenju ($r = 0,129$; $p = 0,005$). Prav tako ugotavljamo, da je znanje pozitivno povezano z varno uporabo IKT; tisti z več znanja se tudi pri uporabi računalnika vedejo manj tvegano ($r = 0,460$; $p = 0,000$). Ta rezultat kaže, da naša predpostavka, da med znanjem in vedenjem ni nujne povezanosti, v analiziranem primeru ne drži. Več kot je znanja, pogostejše je tudi dejansko varno vedenje pri uporabi IKT tehnologij v podjetjih.

Zanimiv je tudi rezultat, da se anketiranci z več znanja počutijo bolj odgovorne za vzdrževanje visoke varnostne kulture, naklonjeni so upoštevanju pravil ter so pripravljeni spremeniti svoje vedenje, da bi dosegli višji nivo informacijskovarnostnega vedenja. Če se spomnimo rezultata, da je prav občutek neodgovornosti za varno vedenje pri uporabi informacijske tehnologije v organizacijah ena od šibkih točk, ki so se pokazale v naši analizi, lahko zaključimo, da bi bilo mogoče s krepitvijo znanja krepiti tudi zaposlenčevo odgovornost za informacijskovarnostno vedenje.

Hkrati pa ugotavljamo, da je varno vedenje bolj pogosto v večjih podjetjih ($r = 0,114$; $p = 0,015$). Statistično značilnih razlik pa nismo potrdili med javnim in zasebnim sektorjem na področju znanja in vedenja pri uporabi IKT.

4 RAZPRAVA

Informacijskovarnostna ozaveščenost zaposlenih za organizacijo predstavlja ključni člen v verigi vzpostavljanja celovite informacijske varnosti. Da bi zagotovili ustrezno stopnjo varnosti informacijskega kapitala, je zato potrebno poskrbeti tudi za ustrezen nivo uporabniške informacijske varnosti, ki se uresničuje skozi ozaveščenost uporabnikov tehnologije. Naša analiza je ugotovila povezavo korelacij med znanjem, vedenjem in odnosom zaposlenih. Kot najpomembnejši dejavnik ozaveščenosti se je izkazalo znanje, ki pogojuje tako vedenje kot odnos uporabnikov do varne uporabe informacijske tehnologije v organizacijah. Rezultati raziskave so pokazali, da se s povečevanjem znanja povečuje pozitivno varnostno vedenje in pozitiven odnos uporabnikov. Iz tega izhaja tudi potreba po krepitvi znanja o informacijskovarnostnem vedenju, saj so anketiranci v tem segmentu našega proučevanja dosegli najnižje vrednosti – kar 29 odstotkov udeležencev raziskave zbralo manj kot 6 točk na indeksu znanja o informacijskovarnostnem vedenju, kar za podjetja predstavlja relativno visoko stopnjo tveganja na tem področju. Ugotovili smo, da je najšibkejše poznavanje informacijskovarnostnih pravil, kar se posledično odraža tudi na področju njihovega vedenja. Znanje je namreč nujni (a ne zadostni) pogoj za informacijskovarnostno vedenje, zato velja v podjetjih še več časa posvetiti prav temu področju.

Vedenje anketirancev ob uporabi tehnologije je sicer v povprečju doseglo boljše rezultate kot njihovo znanje, največje pomanjkljivosti pa se kažejo ravno v odsotnosti upoštevanja osnovnih informacijskovarnostnih pravil. Tudi odnos zaposlenih do informacijske varnosti in tehnologije je v splošnem dober. Najšibkejši točki na tem

področju sta negativen odnos zaposlenih do sprememb v informacijskovarnostnih postopkih in pomanjkanje občutka odgovornosti v primeru uresničenih varnostih incidentov.

Z raziskavo smo poskušali identificirati še dejavnike, ki vplivajo na stanje informacijskovarnostne ozaveščenosti. Ugotavljamo, da takšno stanje ni odvisno od sektorja organizacije, kar je logično, saj so v sodobnem času vse organizacije vpete v kibernetski prostor, zato je informacijska varnost enako pomembna v vseh poslovnih okoljih. Smo pa ugotovili pozitivno in statistično značilno povezavo stanja ozaveščenosti zaposlenih z velikostjo organizacije. Takšna ugotovitev je prav tako razumljiva, saj se z večanjem organizacijske strukture povečuje njen zaupen informacijski kapital, večja je vpetost v kibernetsko okolje, hkrati pa je večja tudi odvisnost od sodobne tehnologije, posledično pa je več tudi ranljivosti. Zato lahko sklepamo, da je zavedanje o pomenu uporabniškega nivoja informacijske varnosti višje v večjih organizacijah, kjer so kibernetske grožnje pogostejše in bolj nevarne.

V splošnem smo največje pomanjkljivosti v stanju informacijskovarnostne ozaveščenosti zaposlenih identificirali na ravni znanja uporabnikov, obenem pa ugotavljamo, da so anketiranci motivirani za dodatno izobraževanje in imajo željo po izboljšanju znanja o varni uporabi tehnologije. Enako v raziskavi kibernetske kriminalitete ugotavljata tudi Bernik in Meško (2011), ki sta zaključila, da je poznavanje kibernetskih groženj nasploh v Sloveniji šibko, vendar obstaja tendenca po izboljšanju obstoječega znanja. Iz tega sledi, da je nadaljnje postopanje za dvig informacijskovarnostne ozaveščenosti zaposlenih v domeni organizacij/podjetij, ki naj poskrbijo za ustrezno informacijskovarnostno izobraževanje vseh zaposlenih, in ne zgolj specializiranih skupin, kot je v navadi. Ob tem morajo organizacije najprej identificirati stopnjo obstoječega znanja, da bodo le-to lahko tudi izboljšale.

5 SKLEP

Ugotovitve raziskave so pokazale, da je stanje informacijskovarnostne ozaveščenosti v Sloveniji močno odvisno od zavedanja in naklonjenosti organizacij nuditi zaposlenim ustrezno izobraževanje o postopkih varne uporabe tehnologije. Zaradi komplementarnega odnosa vseh treh proučevanih vsebinskih sklopov informacijskovarnostne ozaveščenosti pa se morajo organizacije zavedati, da je za dolgoročne spremembe v posameznikovem vedenju potrebno vplivati tudi na njegov odnos oz. pripravljenost upoštevati pravila varnega vedenja. Učinkovitost informacijske varnosti je odvisna od osebne zavzetosti zaposlenih, da ponotranjijo vrednote in pravila informacijskovarnostne kulture. Tako Leach (2003) navaja, da na posameznikov odnos vplivajo trije pomembni dejavniki: občutek odgovornosti, osebne in skupinske vrednote ter težave pri uresničevanju zahtevanih postopkov. Prav občutek osebne neodgovornosti za zagotavljanje informacijske varnosti pa je tisti, ki smo ga ugotovili v naši raziskavi in smo ga opredelili kot eno izmed možnih točk povečanega tveganja. Iz tega sledi, da stanje ozaveščenosti ni samo v domeni znanja in poznavanja pravil, temveč je v kontekstu celotne varnostne kulture v organizaciji. Občutek odgovornosti je v veliki meri pogojen z osebno pripadnostjo organizaciji, poznavanjem varnostnih pravil in postopkov ter doslednostjo

pri nadziranju in sankcioniranju kršitev. Poudariti velja tudi pomen primerne zasnove informacijskovarnostne politike v podjetjih, ki mora biti jasna, predvsem pa razumljiva za vse zaposlene, obenem pa jim mora biti predstavljen tudi način reševanja varnostnih incidentov, s čimer se odpravijo težave pri izpolnjevanju zahtevanih postopkov.

Rezultati naše raziskave potrjujejo ugotovitve, da je za vzdrževanje varnostne kondicije in krepitve nivoja znanja s tega področja potrebno oblikovati celovite programe varnostnega ozaveščanja, ki morajo biti kontinuirani in predstavljati sestavni del organizacijske (varnostne) kulture vsakega podjetja. Schlienger in Teufel (2003) navajata, da morajo biti programi usposabljanja s področja varnostnega ozaveščanja zasnovani tako, da vodijo od stopnje „postati ozaveščen", k stopnji „ostati ozaveščen" , da bi dosegli stopnjo „biti ozaveščen", s čimer se trajno spremeni varnostna kultura v podjetju.

Predvsem pa se je potrebno zavedati, da je varnostna kultura, katere del je tudi varnostna ozaveščenost, dodana vrednost organizacije, od katere je odvisno, ali bodo postavljene varnostne zahteve, pravila in tehnični postopki zaživeli in prispevali k razvoju organizacije ali pa bodo predstavljali največjo oviro pri doseganju zastavljene vizije. Kot navaja Hinson (2009) so zaposleni lahko najšibkejša (mi dodajamo, da so ključna) točka varnostne strukture, lahko pa po drugi strani predstavljajo največji organizacijski kapital. Glavni problem informacijskih incidentov pravzaprav nikoli ni bil v tehnologiji, temveč v ljudeh, ki z njo upravljajo. Najboljša obramba pred kibernetskimi grožnjami je zato vsekakor pozitivna varnostna klima v organizaciji. Naloga menedžerjev je, da hočejo in znajo upravljati organizacijsko varnostno kulturo ter krepiti varnostno klimo v podjetju, ki ga vodijo.

LITERATURA

Bakhshi, T., Papadaki, M. in Furnell S. (2009). Social engineering: Assessing vulnerabilities in practice. *Information Management & Computer Security, 17*(1), 53-63.

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, *62*(3), 242-252.

Čaleta, D., Rančigaj, K. in Lobnikar, B. (2011). The nature of security culture in a military organization: A case study of the Slovenian Armed Forces. *Varstvoslovje, 13*(2), 222-239.

Da Veiga, A. in Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

Dhillon, G. in Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Info Systems, 11*(2), 127-153.

Dobovšek, B. (2009). *Transnacionalna kriminaliteta*. Ljubljana: Fakulteta za varnostne vede.

European Network and Information Security Agency [ENISA]. (2007). *Pobude za ozaveščanje o varnosti informacij: sedanja praksa in merjenje uspeha.* Pridobljeno na http://www.enisa.europa.eu/act/ar/deliverables/2007

Herath, T. in Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hinson, G. (2009). Information security awareness. V M. Gupta in R. Sharman (ur.), *Social and organizational liabilities in information security* (str. 307-324). New York: Information science reference.

Huang, D. L., Rau, P. L. P., Salvendy, G., Gao, F. in Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies, 69*(12), 870-883.

Khan, B., Alghathbar, K. S., Nabi, S. I. in Khurram, M. (2011). Effectiveness of information security awareness method based on psychological theories. *African Journal of Business Management, 26*(5), 10862-10868.

Kreuger, H. A. in Kerney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Kury, H., Meško, G., Mitar, M. in Fields, C. (2009). Slovenian police officers attitudes towards contemporary sucurity threats and punishment. *Policing: An International Jourmal of Police Strategies & Management, 32*(3), 415-429.

Kuusisto, T. in Ilvonen, I. (2003). Information security culture in small and medium size enterprises. V M. Hannula, A. M. Järvelin in M. Seppä (ur.), *Frontiers of e-business research* (str. 431-439). Tampere: University of technology & University of Tampere.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685-692.

Mackenzie, K. (30. 5. 2006). Employees may be opening the door to criminals. *Financial Times.* Pridobljeno na http://www.ft.com/cms/s/458807fe-efec-11da-b80e-0000779e2340.html

Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. V *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. konferenca Dnevi slovenske informatike.* Ljubljana: Slovensko društvo Informatika.

McCullagh, A. in Caelli, W. (2005). Who goes there?: Internet banking: A matter of risk and reward. V C. Boyd in J. M. Nieto Gonzalez (ur.), *Information security and privacy: 10th Australasian conference, ACISP 2005* (str. 336–357). Berlin Heidelberg: Springer-Verlag.

Namjoo C., Dan K., Jahyun G. in Andy W. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management and Computer Security, 16*(5), 484–501.

Organization for economic co-operation and development [OECD]. (2002). *Guidelines for the security of information systems and networks.* Pridobljeno na http://www.oecd.org/dataoecd/16/22/15582260.pdf

Peltier, T. R. (2005). Implementing an information security awareness program. *The EDP Audit, Control, and Security Newsletter, 33*(1), 1-18.

Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo*, *60*(3), 191–198.

Rhee, H.-S., Cheongtag, K. in Ryuc, Y. U. (2009). Self-efficacy in information security: Its influence on end users information security practice behavior. *Computers & Security*, *28*(8), 816-826.

Saksida, M. (2010). *Politika varovanja informacij s poudarkom na upravljanju s človeškimi viri* (Magistrsko delo). Ljubljana: Fakulteta za varnostne vede.

Schlienger, T. in Teufel, S. (2005). Tool supported management of information security culture. V R. Sasaki, S. Qing in H. Yoshiura (ur.), 65 *security and privacy in the age of ubiquitous computing* (str. 65-77), Boston: Springer.

Spears, J. L. in Barkhi, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522.

Talib, S., Clarke, N. L. in Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. V *5th International Conference on Availability, Reliability and Security: ARES 2010*, 15.-18. 2. 2010 (str. 196-203). Cracow: IEEE computer soc.

University of Nevada Las Vegas [UNLV]. (2012). *Definition of information security*. Office of information technology. Pridobljeno na http://oit.unlv.edu/network-and-security/definition-information-security

Završnik, A. (2005). Kibernetična kriminaliteta – (kiber)kriminološke in (kiber) viktimološke posebnosti »informacijske avtoceste«. *Revija za kriminalistiko in kriminologijo*, *56*(3), 248–260.

O avtorjih:

Dr. Branko Lobnikar, izredni profesor za področje upravljanja varnostnih organizacij, Fakulteta za varnostne vede, Univerza v Mariboru.

Kaja Prislan, mag. var., Fakulteta za varnostne vede, Univerza v Mariboru.

Blaž Markelj, asistent, Fakulteta za varnostne vede, Univerza v Mariboru.

Emanuel Banutai, mag. var., doktorski študent in mladi raziskovalec, Fakulteta za varnostne vede, Univerza v Mariboru.