Dr. Alenka Rožanec, dr. Sebastijan Lahajnar

Kultura informacijske varnosti kot ključni dejavnik zagotavljanja ustrezne ravni informacijske varnosti

Znanstveni prispevek

UDK 004.056+008:004

KLJUČNE BESEDE: informacijska varnost, ravnanje uporabnikov, informacijska kultura, organizacije

POVZETEK - Raziskave ugotavljajo, da je bilo v zadnjem času največ varnostnih incidentov posledica neustreznega ravnanja uporabnikov in ne posledica vdorov s pomočjo naprednih orodij IT. V prispevku zato razložimo, zakaj orodja IT in postopki, ki se v praksi uporabljajo, že danes niso več dovolj učinkoviti, ter kako se mora upravljanje informacijske varnosti v prihodnosti spremeniti. Ravnanje uporabnikov v organizaciji je namreč poleg tega, da vodstvo podpira informacijsko varnost, izvaja varnostno politiko in postopke, odvisno predvsem od njihove varnostne ozaveščenosti, znanja, prepričanja in motivacije oziroma kulture informacijske varnosti. V prispevku predstavimo načela OECD, standarde, modele in raziskave tega področja ter principe upravljanja njenih sprememb. Samo s tehničnimi rešitvami, brez ustrezne kulture informacijske varnosti in varnega ravnanja uporabnikov, organizacije v prihodnosti ne bodo več mogle zagotavljati ustrezne ravni informacijske varnosti.

Scientific article

UDC 004.056+008:004

KEY WORDS: information security, human factors of information security, information security culture

ABSTRACT - Studies have shown that most recent information security incidents have been caused by improper user actions, and not by using IT hacking tools. The paper therefore explains why IT tools and procedures in nowadays use are no longer effective enough, and how should the information security management change in the future. Besides management support, security politics and procedures, user actions mainly depend on their security awareness, knowledge, beliefs and motivation, called the information security culture. In the paper, we present OECD's principles, standards, models, and research in the field of information security culture, as well as principles of managing its changes. Using only technical solutions, without implementing the proper information security culture, and consequently, secure behaviour of users, organisations will not be able to reach adequate information security levels anymore.

1 Uvod

Zagotavljanje ustrezne ravni informacijske varnosti v povezanem globalnem okolju postaja nepogrešljivo za dolgoročno uspešnost in ugled vsake organizacije. Kljub stalnemu vlaganju organizacij v informacijsko varnost se število varnostnih incidentov iz leta v leto povečuje. Raziskave ugotavljajo, da so organizacije večinoma že poskrbele za uvedbo tehničnih rešitev (npr. protivirusne programe, požarni zid, orodja za zaznavanje vdorov, orodja za izdelavo varnostnih kopij) in skrbijo za njihovo posodabljanje, da pa se premalo posvečajo zaposlenim, torej uporabnikom svojih informacijskih sredstev. En uporabnik pa lahko z enim nepremišljenim dejanjem izniči vse vlaganje v varnostno tehnologijo. Podatki kažejo, da sta socialni inženiring in nepazljivo ravnanje uporabnikov (torej človeški dejavnik) dandanes kriva za več kot 50 % varnostnih incidentov (Rančigaj in Lobnikar, 2012). Večina varnostnih inženirjev, ki

so sodelovali na delavnici o človeških dejavnikih informacijske varnosti, meni, da je obvladovanje človeških bolj problematično od tehničnih dejavnikov (CISO, 2011). Prislan in Bernik (2014) tudi ugotavljata, da zagotavljanje informacijske varnosti danes ni več samo tehnološki, ampak postaja tudi psihološki in družboslovni izziv.

Skozi kratko zgodovino razvoja rabe informacijske tehnologije ter napovedih sprememb za prihodnost v poglavju 2 prikažemo prednosti in tveganja prihajajočih tehnologij. V poglavju 3 predstavimo načela OECD in modele kulture informacijske varnosti (v nadaljevanju KIV), dejavnike vpliva nanjo ter principe obvladovanja njenih sprememb skozi čas. Ugotovimo, da med raziskovalci navedenih treh področij ne obstaja splošni konsenz, preseke med področji zato prikažemo v sliki 4. Iz nje lahko razberemo, da sta v raziskavah in modelih z vseh treh navedenih področij prisotna podpora vodstva in usposabljanje zaposlenih. Prav tako lahko vidimo, da je v presekih med dvema od področij od enega do pet dejavnikov. Organizacije brez ustrezne KIV v prihodnosti namreč ne bodo mogle več zagotavljati ustreznega nivoja informacijske varnosti, zato je dvig zavedanja o pomenu tega področja in pridobitev ustreznega znanja pri vodstvu in pri vsakem zaposlenem ključno za zagotavljanje uspešnosti vsake organizacije v prihodnosti.

2 Informacijska varnost

2.1 Osnovni pojmi informacijske varnosti

Informacijska varnost je zaščita računalniških sistemov proti kršitvam razpoložljivosti, celovitosti in zaupnosti. Z računalniškimi sistemi so mišljeni omrežja in računalnikiter informacije, ki jih ti vsebujejo. Informacijska varnost je proces, ki se zagotavlja z izvajanjem ustreznih kontrol, vključno s politikami, procesi, organizacijskimi strukturami in funkcijami programske in strojne opreme.

Ranljive točke (ang. vulnerabilities) so pomanjkljivosti v sistemih, ki jih napadalec lahko izkoristi. Ranljive točke so lahko tehnične narave (npr. napake v programski opremi) ali človeške narave (napake skrbnika sistema pri določanju pravic uporabnikov, nastavitev gesel, neustrezna varnostna pravila, neznanje uporabnikov). Število ranljivih točk se vsako leto povečuje, prav tako se povečuje število in kompleksnost groženj, ki pomenijo možnost uspešne zlorabe ranljivosti določenega sredstva. Najpogostejše grožnje so: zlonamerna programska oprema (npr. virusi, črvi), kraja mobilnih naprav, zloraba pooblastil zaposlenih, ribarjenje gesel (ang. phishing) in onemogočanje storitev (ang. denial of service). Ko določena grožnja izkoristi določeno ranljivost, govorimo o varnostnem incidentu (ang. security incident). Poznani so številni varnostni incidenti, katerih posledice so bile ustavljeno poslovanje, povzročena velika poslovna škoda in ogrožen ugled tudi najuglednejših organizacij, npr. Sony, Google, Yahoo, Verisign (Armerding, 2017).

2.2 Kakšne informacijske tehnologije in storitve bomo uporabljali?

V naslednjem desetletju lahko pričakujemo stalno povečevanje uporabe storitev preko mobilnih naprav, saj le-te postajajo vedno bolj zmogljive. Danes se preko mobilnih naprav še vedno izvede le okrog 10 % službenih opravil, vendar pa ta delež narašča. Mobilna omrežja dosegajo vedno višje hitrosti, boljšo odzivnost ter široko pokritost. Z rastjo uporabe mobilnih naprav in vedno večjim številom koristnih podatkov, ki jih vsebujejo, se pričakuje tudi selitev napadov na mobilne tehnologije. Te so zaradi svoje hitre rasti, manjše zrelosti in slabše standardiziranosti v primerjavi z osebnimi računalniki in strežniki ter njihovo programsko opremo namreč bistveno bolj ranljive.

V prihodnosti se pričakuje vedno manjše ločevanje zasebne in poslovne rabe informacijske tehnologije in storitev, uveljavlja se koncept rabe lastnih naprav tudi v službene namene (koncept BYOD). Določeno storitev bomo uporabili, kjer koli in kadar koli jo bomo potrebovali (oblačne storitve, delo na daljavo), v poslovnem ali zasebnem življenju in s katere koli naprave. Inštitut SANS v svoji raziskavi navaja, da 75 % organizacij podpira ta trend in da odstotek še narašča. Žal pa ugotavlja, da kar 38 % organizacij lastne naprave dovoljuje brez ustrezne varnostne politike BYOD (Sans Institute, 2017), kar izrazito povečuje varnostno tveganje.

V internet se poleg računalnikov in mobilnih naprav v zadnjem času priključujejo tudi druge naprave (npr. gospodinjski aparati, TV, avtomobili), ki znajo komunicirati. S tem so tudi te naprave postale aktivne udeleženke najrazličnejših procesov. Že desetletje tako govorimo o internetu stvari (ang. internet of things), ki naj bi nam omogočil boljše in udobnejše življenje (transport, logistika, pametne hiše, pametna mesta), vendar še ni dosegel svojega vrhunca (Opcomm, 2013).

Poleg številnih prednosti bomo morali biti še bolj pozorni na ranljivost prihajajočih tehnologij. Spremembe namreč predstavljajo potrebo po novih pristopih za zagotovitev informacijske varnosti. Čeprav mlajši zaposleni to tehnologijo znajo uporabljati, so po navedbah raziskav zelo malo ozaveščeni o varnem ravnanju z njo. Večina se varne uporabe uči šele znotraj organizacije (Talib in sod., 2010). Ozaveščanju in izobraževanju uporabnikov o načinih varne rabe novih tehnologij bo zato treba posvetiti bistveno več pozornosti kot v preteklosti. Saj ne želimo, da bi kdo preko interneta vstopil v našo pametno hišo ali podjetje, ker smo zaradi svojega neznanja pustili priprta vrata?

3 Kultura informacijske varnosti in standardi

3.1 Kultura informacijske varnosti

Dhillon (1999) KIV definira kot skupek vseh vzorcev obnašanja, kot so vedenje, odnos in vrednote, ki prispevajo k zaščiti vseh vrst informacij v določeni organizaciji. Schlienger in Teufel (2003) trdita, da je KIV podkultura in da zajema vse družbeno-kulturne ukrepe, ki podpirajo tehnične ukrepe, da informacijska varnost postane na-

ravni način izvajanja vsakodnevnih aktivnosti vsakega zaposlenega. Da Veiga in Eloff (2010) pa menita, da KIV predstavlja odnos zaposlenih do organizacijskega sistema in postopkov v vsakem delu dneva, njihove predpostavke, prepričanja, vrednote in znanje . Odnos se kaže v sprejemljivem ali nesprejemljivem vedenju in postopanju pri zaščiti informacijskih virov. Kultura se sčasoma seveda tudi spreminja. KIV pomaga pri uveljavljanju informacijskih varnostnih politik in dobrih izkušenj v zvezi z informacijsko varnostjo organizacije (Da Veiga in sod., 2007).

3.2 Načela kulture informacijske varnosti in standardi

OECD (2002, str. 9-12) podaja devet načel KIV, ki usmerjajo vedenje in mišljenje ljudi pri rabi informacijskih sistemov:

1. *Zavedanje*. Uporabniki se zavedajo potrebe po varovanju informacijskih sistemov in omrežij ter se sprašujejo, kaj lahko storijo za povečanje varnosti.
2. *Odgovornost*. Vsi uporabniki so odgovorni za varnost informacijskih sistemov in omrežij.
3. *Dovzetnost*. Uporabniki ukrepajo pravočasno in kooperativno na način, da se preprečijo in odkrijejo varnostni incidenti oz. da se nanje primerno odzove.
4. *Etika*. Udeleženci spoštujejo legitimne interese drugih.
5. *Demokracija*. Varnost informacijskih sistemov in omrežij je v skladu s ključnimi vrednotami demokratične družbe.
6. *Ocena tveganj*. Uporabniki napravijo oceno tveganj, da se ugotovijo grožnje in ranljivosti, določijo tudi sprejemljivo raven tveganja, preden se vzpostavi nadzor.
7. *Varnostni načrt in implementacija*. Uporabniki vključujejo element varnosti kot ključni element informacijskih sistemov in omrežij, tako v tehnične kot netehnične ukrepe in rešitve.
8. *Upravljanje z varnostjo*. Udeleženci sprejmejo celovit pristop k upravljanju z varnostjo, vključno z varnostnimi politikami, praksami, ukrepi in postopki, ki so usklajeni in strnjeni z namenom, da se ustvari skladen varnostni sistem.
9. *Ponovna ocena*. Uporabniki pregledajo in ocenijo varnost informacijskih sistemov in omrežij ter poskrbijo za ustrezne spremembe varnostne politike, praks, ukrepov in postopkov.

Načela 6 do 9 so tudi sestavni del standardov za zagotavljanje informacijske varnosti, ki organizaciji pomagajo, da se na sistematičen način loti sprememb na tem področju. Najbolj uveljavljen pristop s področja informacijske varnosti predstavljajo standardi družine ISO 27000 (ISO/IEC 27001:2013, ISO/IEC 27002:2013).

3.3 Dimenzije kulture informacijske varnosti

S pregledom literature smo našli dvanajst dimenzij KIV, ki se nekatere bolj, druge manj pogosto pojavljajo v različnih raziskavah ter v predhodno navedenih načelih OECD in varnostnih standardih (tabela 1). Pri tem najskromnejši model obsega le dve dimenziji, medtem ko so drugi obsežnejši. V modelu Alnatheerja in sodelavcev (2012) KIV sestavljata: zavedanje o pomenu informacijske varnosti in lastništvo in-

formacijske varnosti s strani vseh zaposlenih. Podpora in vključenost najvišjega vodstva, usposabljanje in izvajanje varnostne politike pa so v tem modelu predstavljeni kot dejavniki, ki vplivajo na informacijsko varnostno kulturo. Da je zavedanje vseh zaposlenih o pomenu informacijske varnosti potrebno za varno ravnanje, je bilo že izpostavljeno v več starejših raziskavah oziroma modelih, npr. Van Niekerk in Von Solms (2005) ter Martins in Eloff (2002). Lastništvo informacijske varnosti pomeni, da vsi zaposleni razumejo svojo vlogo in odgovornost pri zagotavljanju informacijske varnosti ter poznajo varnostna tveganja, povezana z nalogami, ki jih vsakodnevno opravljajo. Alnatheer v svojem prispevku (2014) razširi seznam KIV na sedem dimenzij: podpora najvišjega vodstva, zavedanje, varnostna politika, usposabljanje, analiza tveganj, varnostna skladnost in etičnost. Primerjava s predhodno opisanim modelom pokaže, da so zadnje štiri dimenzije nove, manjka dimenzija lastništva. Varnostne politike morajo biti pripravljene za vsako organizacijo unikatno na podlagi predhodno opravljene analize tveganj. V analizi tveganj ocenimo ranljivost informacijskih sredstev organizacije, grožnje in vrednost sredstev. Šele ko tveganja za posamezna sredstva poznamo, lahko vzpostavimo ustrezne varnostne ukrepe, da le-ta zmanjšamo na sprejemljivo raven (ISO 27001; OECD, 2012). Proces preverjanja skladnosti organizaciji omogoča, da preveri svoje dejanske varnostne postopke in kontrole z zahtevami mednarodnih varnostnih standardov (Alnatheer in Nelson, 2009), kar omogoča kakovostnejše upravljanje informacijske varnosti, vpliva pa tudi na večje zaupanje v organizacijo in povečanje njenega ugleda.

Bolj strukturiran trinivojski model, ki KIV obravnava trinivojsko, najdemo v Martins in Eloff (2002):

- *Nivo organizacije* obsega definirane varnostne politike in postopke, ki uporabnikom povedo, kako lahko varno ravnajo z informacijskimi sredstvi, in temeljijo na predhodno opravljeni analizi tveganj. Pomemben je primerno visok proračun, namenjen informacijski varnosti, avtor pa priporoča tudi primerjavo s podobnimi organizacijami in mednarodnimi standardi (npr. ISO 27001).
- *Na nivoju skupine* je zelo pomembno zaupanje med zaposlenimi in vodstvom. Ker ima vodstvo ključno vlogo pri udejanjanju informacijske varnosti, mora skozi svoja dejanja kazati svojo zavezanost in vključenost ter biti zgled drugim zaposlenim pri spoštovanju varnostne politike in postopkov.
- *Na nivoju posameznika* je treba dvigniti zavedanje o pomenu informacijske varnosti. Prav tako je pomembna etičnost pri ravnanju z intelektualno lastnino organizacije.

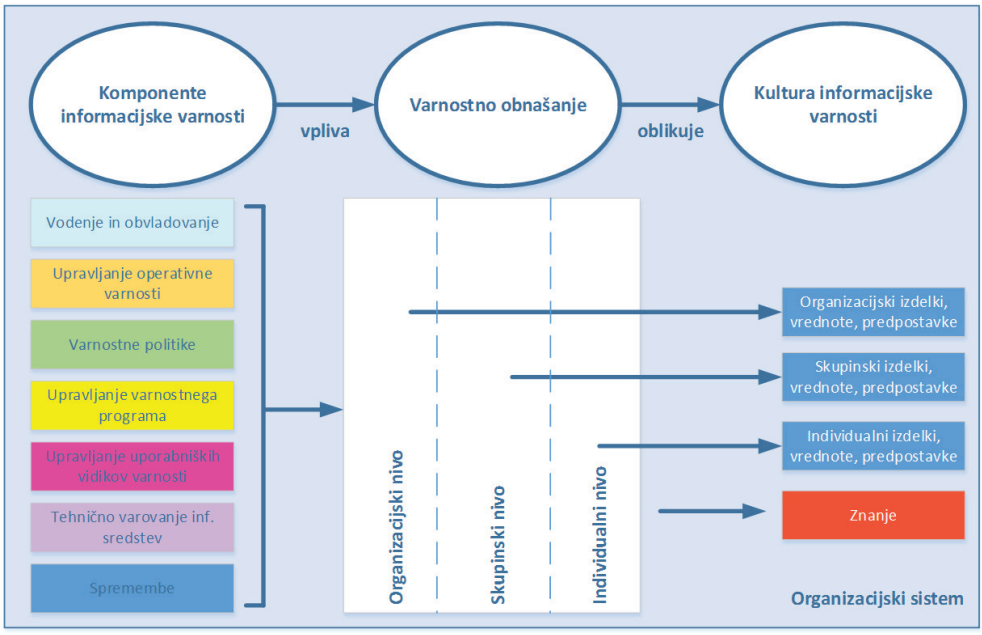
Vse tri ravní kulture informacijske varnosti so seveda medsebojno odvisne, zato je pomembno usklajeno izboljševanje njihovih faktorjev.

3.4 Dejavniki vpliva na kulturo informacijske varnosti

V Da Veiga in Eloff (2010) najdemo celovito ogrodje KIV, ki izhaja iz predhodno navedenega trinivojskega modela (Martins in Eloff, 2002). V ogrodju so obravnavane komponente informacijske varnosti, ki so razvrščene v sedem kategorij. Komponente nadalje usmerjajo aktivnosti varovanja informacijskih sredstev na različnih nivojih

(organizacijskem, skupinskem, individualnem) oziroma določajo načine varnostnega obnašanja zaposlenih ter tako sčasoma oblikujejo želeno KIV organizacije (slika 1). Rezultat varnostnih aktivnosti je oblikovana KIV, ki jo sestavljajo izdelki, vrednote in predpostavke, izpeljane iz modela organizacijske kulture. V prispevku Van Niekerk in Von Solms (2010) pa je dodano še znanje o informacijski varnosti, brez katere ne moremo pričakovati ustrezne KIV.

Slika 1: Vpliv komponent informacijske varnosti na varnostno obnašanje in KIV



Vir: Povzeto po Da Veiga, A. in Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, Vol. 29, št. 2, str. 196 – 207; Van Niekerk, J. F. in Von Solms, R. (2010). Information Security Culture: A management perspective. Computers & Security, 29, št. 4, str. 476-486.

Tabela 1 poleg dimenzij KIV prikazuje tudi dejavnike, ki nanjo vplivajo. Prvih šest navedenih postavk tabele (podpora vodstva, zavedanje o pomenu informacijske varnosti, varnostna politika, usposabljanja, varnostna skladnost, zaupanje in znanje) smo identificirali kot dimenzije KIV in opisali že v predhodnem poglavju. Tako ugotovimo, da med znanstveno in strokovno javnostjo ni jasne razmejitve, kaj so dimenzije KIV in kaj dejavniki, ki nanjo vplivajo. Največje število, devet dejavnikov, ki vplivajo na KIV, najdemo v Hasan in sod. (2015). To so: podpora najvišjega vodstva, zavedanje, varnostna politika, znanje, kulturne razlike, zaupanje, deljenje informacij, prepričanje in varno obnašanje. Vidimo, da prve tri dejavnike iz navedene raziskave najdemo tudi v mnogih drugih raziskavah (Knapp in sod., 2006b; Alnatheer in Nelson, 2009; Gebrasilase in Lessa, 2011; Martins in Da Veiga, 2015), prav tako se v številnih raziskavah (Alnatheer in Nelson, 2009); Da Veiga in Eloff, 2010; Alnatheer in sod.,

2012) nahaja dejavnik usposabljanja, ki pa ga v raziskavi Hasan in sod. (2015) ne najdemo.

Tabela 1: Dimenzije KIV in dejavniki vpliva na KIV

Dimenzija KIV/ dejavnik	*Opis*	*Reference dimenzije KIV*	*Reference dejavnika vpliva na KIV*
1. Podpora vodstva	Vodstvo podpira in je aktivno vključeno v pripravo, sporočanje, spremljanje izvajanja varnostne politike. Zagotavlja sredstva in določa odgovornosti za informacijsko varnost.	Martins in Eloff (2002), Alnatheer (2014)	Van Niekerk in Von Solms (2005), Knapp in sod. (2006b), Alnatheer in Nelson (2009), Gebrasilase in Lessa (2011), Alnatheer in sod. (2012), Hassan in sod. (2015), Martins in Da Veiga (2015)
2. Zavedanje	Zaposleni se zavedajo svojega varnostnega poslanstva.	OECD (2002), Van Niekerk in Von Solms (2005), Martins in Eloff (2002), Alnatheer in sod. (2012), Alnatheer (2014)	Alnatheer in Nelson (2009), Da Veiga in Eloff (2010), Gebrasilase in Lessa (2011), Alnatheer in sod. (2012), Hassan in Ismail (2012), Da Veiga in Martins (2014), Martins in Da Veiga (2014, 2015), Hassan in sod. (2015)
3. Varnostna politika	Priprava varnostnih politik in spremljanje njihovega spoštovanja s strani zaposlenih.	OECD (2002), Martins in Eloff (2002), Alnatheer (2014)	Alnatheer in Nelson (2009), Da Veiga in Eloff (2010), Gebrasilase in Lessa (2011), Alnatheer in sod. (2012), Da Veiga in Martins (2014), Martins in Da Veiga (2014, 2015), Hassan in sod. (2015)
4. Usposabljanja	Usposabljanja s področja informacijske varnosti, ki uporabnikom omogočajo delo, skladno z zastavljenimi varnostnimi politikami.	Alnatheer (2014)	Van Niekerk in Von Solms (2005), Alnatheer in Nelson (2009), Da Veiga in Eloff (2010), Gebrasilase in Lessa (2011), Alnatheer in sod. (2012), Da Veiga in Martins (2014), Martins in Da Veiga (2014, 2015)
5. Varnostna skladnost	Skladnost z informacijskimi varnostnimi standardi in dobrimi praksami.	Alnatheer (2014)	Alnatheer in Nelson (2009), Da Veiga in Eloff (2010), Da Veiga in Martins (2014), Martins in Da Veiga (2014, (2015)
6. Zaupanje	Medsebojno zaupanje med vodstvom in zaposlenimi, zaposlenimi in strankami.	Martins in Eloff (2002)	Da Veiga in Eloff (2010), Martins in Da Veiga (2014), Da Veiga in Martins (2014)
7. Znanje	Znanje uporabe varnostnih rešitev in poznavanje varnostnih postopkov.	Van Niekerk in Von Solms (2010)	Van Niekerk in Von Solms (2005), Hassan in Ismail (2012), Hassan in sod. (2015)
8. Analiza in ocena tveganj	Postopek, s katerim ocenimo ranljivost organizacije in grožnje, ki lahko to ranljivost izkoristijo, ter vrednost sredstev.	OECD (2002), Martins in Eloff (2002), Alnatheer (2014), ISO 27001	/

Dimenzija KIV/ dejavnik	*Opis*	*Reference dimenzije KIV*	*Reference dejavnika vpliva na KIV*
9. Etičnost	Zagotavljanje etičnega ravnanja z intelektualno in drugo lastnino organizacije.	OECD (2002), Martins in Eloff (2002), Alnatheer (2014)	/
10. Lastništvo	Vsi zaposleni razumejo svojo vlogo in odgovornost pri zagotavljanju informacijske varnosti ter poznajo varnostno tveganje, povezano z nalogami, ki jih opravljajo.	OECD (2002), Alnatheer in sod. (2012)	/
11. Proračun	Ustrezno visok proračun namenjen informacijski varnosti.	Martins in Eloff (2002)	/
12. Primerjava	Primerjava varnostnih praks organizacije z drugimi podobnimi organizacijami in mednarodnimi standardi.	Martins in Eloff (2002)	/
13. Kulturne razlike	Kulturne razlike, ki izhajajo iz razlik v nacionalni in organizacijski kulturi.	/	Alnatheer in Nelson (2009), Da Veiga in Eloff (2010), Van Niekerk in Von Solms (2010), Hassan in Ismail (2012), Hassan in sod. (2015), Ifinedo (2014)
14. Varno obnašanje	Ravnanje z informacijskimi sredstvi in vsebovanimi informacijami, da je zagotovljena njihova zaupnost, celovitost in razpoložljivost, kot jo zahteva varnostna politika.	/	Da Veiga in Eloff (2010), Van Niekerk in Von Solms (2010), Hassan in Ismail (2012), Hassan in sod. (2015)
15. Prepričanje in odnos	Prepričanje in odnos do varovanja informacijskih sredstev.	/	Van Niekerk in Von Solms (2010), Hassan in sod. (2015)
16. Vodenje in obvladovanje inf. varnosti	Vodenje, obvladovanje, strategije, upravljanje tveganj.	/	Da Veiga in Eloff (2010), Martins in Da Veiga (2014), Da Veiga in Martins (2014)
17. Upravljanje inf. sredstev	Upravljanje sredstev, tehnično varovanje, upravljanje incidentov.	/	Da Veiga in Eloff (2010), Martins in Da Veiga (2014), Da Veiga in Martins (2014)
18. Zasebnost	Percepcija zaposlenih glede varstva njihovih osebnih in podatkov strank organizacije.	/	Da Veiga in Eloff (2010), Martins in Da Veiga (2014), Da Veiga in Martins (2014)
19. Upravljanje sprememb	Pogosto posodabljanje aplikacij, sistemov in infrastrukture povečuje varnost in zanesljivost.	/	Martins in Eloff (2002), Da Veiga in Eloff (2010), Hassan in Ismail (2012), Martins in Da Veiga (2014), Da Veiga in Martins (2014)

Vir: Lastni vir, 2017.

Raziskave ugotavljajo, da navedeni dejavniki v tabeli 1 niso neodvisni. Raziskava Martins in Da Veiga (2015) na primer pokaže pozitiven in močan vpliv podpore vodstva na varnostno politiko. Jasno napisana in zaposlenim predstavljena varnostna politika in njihovo usposabljanje pa povečujeta zavedanje in znanje uporabnikov (Martins in Da Veiga, 2014; 2015). Povečanje zavedanja in znanja ob drugih primernih dimenzijah varnostne kulture v organizaciji (npr. zaupanje vodstvu, etičnost, prepričanje) vodijo k bolj varni rabi informacijskih sredstev oziroma k bolj varnemu obnašanju uporabnikov (Da Veiga in Eloff, 2010; AlHogail, 2015a). Če ostale dimenzije KIV niso ustrezne, pa se kljub visokemu zavedanju o varnostnem tveganju in ustreznem znanju uporabniki vseeno lahko vedejo neustrezno (Van Niekerk in von Solms, 2010), npr. ne pazijo pri odpiranju priponk ali izdajajo svoja gesla drugim uporabnikom. Prislan in Bernik (2014) ugotavljata, da se je ozaveščenost v zadnjih letih sicer izboljšala, vendar se uporabniki varnostne politike in pravil pogosto ne držijo, kar predstavlja izziv za prihodnost. Vzporednice bi lahko iskali na področju prometa, kjer vsi poznamo prometna pravila in omejitve, pa jih vseeno pogosto kršimo, saj v nacionalni kulturi takšno obnašanje ni nesprejemljivo. Dejavnik kulturne razlike kaže, da mora biti KIV ustrezno prilagojena organizacijskemu in nacionalnemu kontekstu (Alnatheer in Nelson, 2009; Da Veiga in Eloff, 2010; Van Niekerk in Von Solms, 2010; Alnatheer, 2014), kar prikazuje tudi slika 2.

Nacionalna kultura je kultura, ki jo gojijo pripadniki določenega naroda in je z vidika informacijske varnosti pomembna, saj kulturne norme lahko bistveno vplivajo na kršitve pri rabi informacijskih sredstev (kot v prej navedenem primeru prometa). Organizacijska kultura je vzorec vrednot, norm, prepričanj, odnosov in predpostavk, ki niso nujno zapisane, a oblikujejo obnašanje in načine dela v organizaciji (Armstrong, 2006, str. 384). Eno najbolj uveljavljenih klasifikacij organizacijske kulture (Handy in Harrison, v: Cadle in Yeates, 2001, str. 6-7) obsega štiri skupine: močna, birokratska, individualistična in matrična kultura.

Slika 2: Kontekst kulture informacijske varnosti

Vir: Povzeto po Alnatheer, M. (2014). A conceptual model to understand Information Security Culture. International Journal of Social Science and Humanity, Vol. 4, No. 2, str. 104–107.

Pri močni kulturi je za izvajanje vseh sprememb najpomembnejše vodstvo, napisanih pravil in predpisov je malo. Za uspešnost KIV je najpomembnejša zavezanost vodstva. Za birokratski tip kulture je značilno, da so opisi del in pravila jasno zapisani in se jih zaposleni večinoma držijo.

Značilna je za javno upravo in banke. Pri tej vrsti kulture so jasno zapisna vloga informacijske varnosti, pravila in njihovo spoštovanje s strani uporabnikov pričakovani in, če so ustrezno predstavljeni, tudi upoštevani. Za različne strokovne organizacije, npr. odvetniške pisarne ali raziskovalne organizacije, ki zaposlujejo visoko usposobljene posameznike, pa je značilna individualistična kultura, saj niso vajeni formaliziranih pravil.

V takšnih tipih organizacij so zato potrebni posamezniki, ki imajo znanje in prepričajo še druge zaposlene, da skupaj določijo in implementirajo varnostna pravila. Zadnjo skupino predstavljajo proizvodna podjetja, za katera je značilna matrična kultura. V tovrstnih organizacijah motiviranje uporabnikov za zavezanost in spoštovanje informacijskih varnostnih politik ni tako zahtevno kot pri predhodno opisani individualistični kulturi (Da Veiga in Eloff, 2010).

3.5 Spremembe kulture informacijske varnosti

Uveljavljanje načel KIV pomeni za organizacijo veliko spremembo, ki mora biti načrtovana premišljeno in izvedena po majhnih korakih, saj v nasprotnem primeru lahko pričakujemo neuspešnost in odpor zaposlenih.

Organizacijam zato svetujemo uporabo uveljavljenih ogrodij obvladovanja sprememb, npr. Kotterjev model osmih korakov ali Cameronov ciklični model sprememb (Cameron in Green, 2015). V Alhogail in Mirza (2014) najdemo opis načel in ogrodje, prilagojeno obvladovanju sprememb KIV. S slike 3 vidimo, da načela sprememb KIV izhajajo iz splošnih načel obvladovanja sprememb.

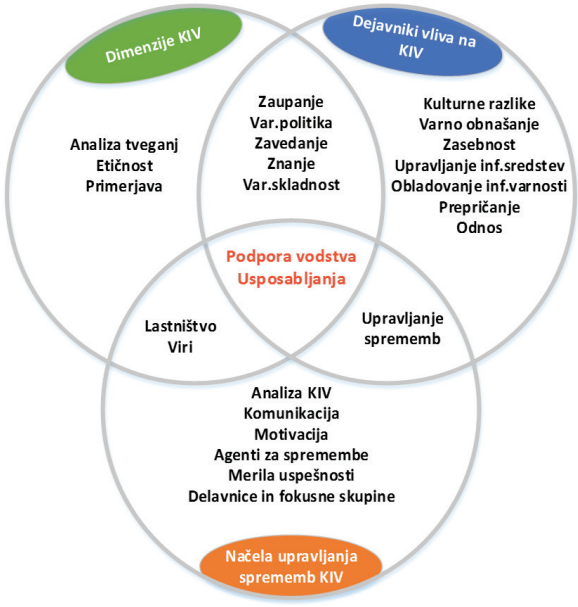
V raziskavi (AlHogail, 2015) se je kot najpomembnejše načelo izkazala podpora vodstva, sledila so sredstva in drugi viri, komunikacija, vključenost in lastništvo ter delavnice in fokusne skupine. Alhogail (2015a) ugotavlja tudi pozitiven odnos med nivojem KIV in uporabo načel obvladovanja njenih sprememb, kar še dodatno poudarja vlogo ustreznega upravljanja sprememb za implementacijo učinkovite KIV.

Slika 3: Načela obvladovanja sprememb KIV

Vir: Alhogail, A. in Mirza, A. (2014). A framework of information security culture change. Journal of Theoretical and Applied Information Technology, Vol. 64, No. 2, str. 540–549.

S sliko 4, ki prikazuje dimenzije KIV, dejavnike vpliva nanjo in načela upravljanja sprememb KIV, jasno pokažemo, da se veliko število elementov pojavi v modelih in raziskavah dveh ali celo vseh treh navedenih področij.

Slika 4: Presek področij kulture informacijske varnosti (KIV)



Vir: Lastni vir, 2017.

V središču, torej v preseku vseh treh področij najdemo podporo vodstva in usposabljanja, kar sta tudi po našem mnenju najpomembnejša dejavnika za zagotovitev takšne kulture informacijske varnosti organizacije, v kateri se bo vsak zaposleni čutil odgovornega in imel znanje za varno ravnanje z informacijskimi sredstvi ter ne bo predstavljal vedno večje varnostne ranljivosti organizacije, ki jo nepridipravi lahko hitro izkoristijo.

4 Razprava in sklep

Število in raznovrstnost naprav, ki jih uporabljamo v zasebni in poslovni sferi, narašča. Uporabniki imajo vedno večjo izbiro storitev in lokacij uporabe. Prihajajo tudi nove naprave - internet stvari. Pri heterogenosti naprav in storitev, ki jih uporabljamo kjer koli in kadar koli, tako ne moremo več pričakovati, da bo oddelek IT sam zagotavljal ustrezno raven informacijske varnosti, kot jo je v preteklosti, ko je imel popoln nadzor nad vsemi napravami in storitvami. Obvladovanje človeških dejavnikov pri informacijski varnosti oziroma implementacija ustrezne informacijske varnostne kulture zato dandanes postaja nuja za zagotavljanje ustrezne ravni informacijske varnosti. Vsaka organizacija pa bo morala z uporabo dobrih praks, standardov, modelov, ogrodij in študij primerov izbrati zase najprimernejši način za vzpostavitev dobre kulture informacijske varnosti.

Pregled raziskav in modelov KIV pokaže, da gre za kompleksno področje, na katerega uspešnost vpliva veliko število dejavnikov. Ugotavljamo, da med znanstveno in strokovno javnostjo ni poenotenega mnenja, kaj so dimenzije KIV in kaj dejavniki, ki nanjo vplivajo. Obstaja tudi presek z načeli obvladovanja sprememb KIV skozi čas, kar nazorno pokaže slika 4. Iz nje lahko razberemo tudi, da sta podpora vodstva in usposabljanje zaposlenih prisotna v raziskavah in modelih z vseh treh navedenih področij.

Model, ki so ga zasnovali Knapp in sod. (2006b) kaže, da podpora vodstva vpliva na številne druge dimenzije informacijske varnosti. Raziskava Knapp in sod. (2006a), v kateri so sodelovala podjetja najrazličnejših panog, pokaže, da je to tudi najpomembnejši med 25 ocenjevanimi dejavniki informacijske varnosti. Študija primera (Gebrasilase in Lessa, 2011) pokaže tudi nasprotni primer, kjer zaradi pomanjkanja podpore s strani vodstva bolnišnica nima zapisanih varnostne politike, zavedanje med uporabniki je nizko, imajo slabo znanje. V študiji primera finančne inštitucije, ki so jo spremljali osem let, Da Veiga in Martins (2014) ugotavljata, da je izvajanje varnostnih aktivnosti vplivalo na izboljšanje vseh dimenzij KIV ter da so imeli največji vpliv upravljanje informacijskih sredstev, obvladovanje informacijske varnosti, varnostna politika in upravljanje uporabnikov (zavedanje, usposabljanje). Značilne razlike v višji KIV tistih uporabnikov, ki so se usposabljali, v primerjavi z ostalimi, jasno kaže na pomembnost in koristnost usposabljanja ter se predlaga kot ključna aktivnost za izboljšavo KIV. Raziskava s področja zdravstva (v: Hassan, 2015) pa je pokazala, da je najpomembnejši dejavnik za zagotovitev informacijske varnosti zavedanje uporab-

nikov, ki ga usposabljanje prav tako povečuje. Dhillon tudi poroča (v: Gebrasilase, 2011), da je dvig zavedanja o pomembnosti varovanja s strani vsakega uporabnika, ki se izvede preko ustreznega usposabljanja, najučinkovitejši ukrep za izboljšanje KIV.

Kot smo predstavili v poglavju 3.4 na KIV močno vpliva kontekst nacionalne in organizacijske kulture, zato ga je treba skrbno analizirati in upoštevati pri načrtovanju sprememb. Glede na slovensko nacionalno kulturo je pričakovati, da bo za doseganje dobre kulture informacijske varnosti težja in daljša pot kot v zahodnoevropskih in skandinavskih državah, kjer se zakoni, predpisi in pravila bolj dosledno spoštujejo. Težje delo je tako na primer pričakovati na elementu motivacije zaposlenih za spoštovanje varnostne politike, kjer je treba dobro razmisliti, kakšno razmerje negativnih in pozitivnih spodbud bo v določeni organizaciji najučinkovitejše. Pri tem želimo spomniti, da je pohvala veliko premalo uporabljana vzpodbuda glede na njene pozitivne učinke. Predlagamo, da se s pohvalo vzpodbudi vsakega zaposlenega, ki prijavi varnostni incident takoj, ko opazi kar koli neobičajnega, saj s tem prepreči njegovo širitev in povečanje škode. Organizacijam z birokratsko in matrično organizacijsko kulturo (praviloma večje organizacije, npr. javna uprava, večja podjetja, banke) svetujemo, da se naslonijo na standarde družine ISO 27000 ter postopoma zagotovijo tehnologijo, uredijo postopke in usposobijo zaposlene za varno ravnanje ter si za dolgoročni cilj postavijo pridobitev certifikata informacijske varnosti ISO 27001. Manjšim organizacijam z močno ali individualistično kulturo pa svetujemo, da se sprememb lotijo pri dovolj vplivnih posameznikih, ki morajo s pomočjo usposabljanja pridobiti ustrezno zavedanje in znanje s področja varnosti, da bodo skupaj z drugimi zaposlenimi na manj formalen način določili varnostna pravila in njihovo spoštovanje, temelječe na zaupanju in etičnosti. Ne glede na vrsto organizacije je potrebno najprej zagotoviti podporo vodstva, ki bo omogočilo vire za stalna vlaganja v informacijsko varnost. Tukaj je zelo pomembna proaktivna vloga osebja IT v organizaciji, ki mora na ustrezen način vodstvu predstaviti pomen navedenega področja. Nadalje je treba vzpostaviti skupino za informacijsko varnost z ustreznimi kompetencami, ki bo zagotovila stalno upravljanje in izboljševanje varnostnih aktivnosti. Med pomembnejše aktivnosti sodijo: analiza obstoječe kulture informacijske varnosti in trenutnega znanja zaposlenih (strokovnjakov IT in uporabnikov), analiza tveganj, priprava varnostne politike ob upoštevanju rezultatov predhodno navedenih analiz, predstavitev varnostne politike zaposlenim in stalno usposabljanje za varno ravnanje z novimi tehnologijami (e-gradiva, delavnice).

Alenka Rožanec, PhD, Sebastijan Lahajnar, PhD

Information security culture as the key factor in ensuring an adequate level of information security

Ensuring an appropriate level of the organisation's information security in the interconnected, global environment is becoming indispensable for the long-term su-

ccess and reputation. In spite of regular investments into the information security, the number of security incidents is increasing every year. Studies have shown, that organisations mainly use technological safeguards (e.g. antivirus software, firewalls, intrusion detection systems, backup tools), but devote too little attention to employees, i.e. users of their information assets, making social engineering and improper behaviour the culprits for over 50% of security incidents (Rančigaj and Lobnikar, 2012). Prislan and Bernik (2014) stated that ensuring a proper information security is thus not only a technological, but in great part also a psychological and social issue. Organisations will have to pay more attention to human factors in the future, if they wish to ensure an appropriate level of information security. The behaviour of users namely depend on security procedures, management commitment and support, awareness, knowledge, beliefs and motivation.

Depending only on technological security safeguards is not sufficient anymore due to changes in the use of information assets. The first major change was the connection of users to the internet. The second major change is the use of private devices (e.g. mobile, laptops) for business work, named Bring your own device. The latter brings many risks, especially if the BYOD privacy policy is not defined, and if the users do not have knowledge to secure their private devices (Sans Institute, 2017). The third novelty is cloud computing, allowing companies to hire hardware and software instead of owning it. For about a decade, we have also been talking about the internet of things, various devices for better and more comfortable life (e.g. transport, logistics, smart houses, smart cities, wearables) (Opcomm, 2013). Along with the benefits (e.g. savings, greater flexibility) of listed new devices and services connected to internet, we must also expect many security incidents, as new immature technologies (e.g. mobile or things) are much more vulnerable than the mature ones and thus could be easier exposed. Younger employees use information technology on a daily basis, but have very poor awareness and knowledge about the information security. Therefore, most of them learn how to securely use IT only within the organisation (Talib et al., 2010). Information security awareness and training programs will thus require a lot more attention than they had in the past.

To avoid the increase of security incidents due to improper actions of users, constant information security culture improvements are required. The information security culture can be defined as the attitude, assumptions, beliefs, values and knowledge that employees have in relation to the organisation and procedures during each part of the day. The attitude is shown in the acceptable and unacceptable behaviour and deviations in the protection of information assets (Da Veiga and Eloff, 2010). OECD (2002, pp. 9-12) provides nine principles of information security culture:

Awareness: users should be aware of the need for security of information systems and networks, and ask themselves what they can do to enhance security.

Responsibility: all users are responsible for information systems and network security.

Response: users should take actions on time and cooperatively to detect, prevent and respond to security incidents.

Ethics: participants should respect legitimate interests of others.

Democracy: security of information systems and networks should be compatible with key values of a democratic society.

Risk assessment: users conduct risk assessments to identify threats and vulnerabilities, and define the acceptable risk levels before supervision is established.

Security design and implementation: users should incorporate security as a key element of information systems and networks, both technical and non-technical safeguards and solutions are required.

Security management: participants should adopt a comprehensive approach to security management, including security policies, practices, measures and procedures, which are coordinated and integrated to create a coherent security system.

Reassessment: users should review and reassess the security of information systems and networks, and ensure that suitable changes to security policies, practices, measures and procedures are made.

Principles 6 to 9 are integral parts of the information security standards. The fundamental standard ISO/IEC 27001 (ISO/IEC 27001:2013) specifies the requirements for establishing, implementing, maintaining and continually improving the information security management system within the context of an organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. More thorough advice and best practices for establishing controls enabling the risks are reduced to the acceptable level can be found in the standard ISO/IEC 27002 (ISO/IEC 27002:2013).

The modest model of information security culture consists of two dimensions, security awareness and ownership (Alnatheer et al., 2012), while others are more extensive (Van Niekerk and Von Solms, 2005; Alnatheer, 2014). The most comprehensive model where information security culture is considered on three levels (organisational, group, individual) was developed by Martins and Eloff (2002). During the review of models, OECD principles and security standards, we identified the following twelve dimensions forming the information security culture: management support, security awareness, security policy, training, security compliance, trust, knowledge, risk analysis, ethics, ownership, budget, and benchmarking.

Furthermore, we reviewed the research of factors influencing the information security culture. Among the fourteen identified factors, seven factors are the same as information security culture dimensions (management support, security awareness, security policy, training, security compliance, trust and knowledge). Others are: cultural differences (Hassan et al., 2015; Ifinedo, 2014), security behaviour (Da Veiga and Eloff, 2010; Van Niekerk and Von Solms, 2010; Hassan and Ismail, 2012), belief and attitude (Van Niekerk and Von Solms, 2010; Hassan et al., 2015), security leadership and governance, security management and operations, privacy and change management (Da Veiga and Eloff, 2010; Martins and Da Veiga, 2014; Da Veiga and Martins, 2014). We could state that researches and practitioners do not share a common view of what dimensions that constitute information security culture are, and

which factors are influencing it. The research of Knapp et al. (2006a) shows that the most important factor is management support; the healthcare study (in: Hassan et al., 2015) found the security awareness as the most important one.

Research showed that dimensions or factors are not independent but influence each other. The model of Knapp et al. (2006b) shows that the management support influences all other information security items. Martins and Da Veiga (2015) show positive influence of management support on security policies. Clearly written and communicated policies and trainings raise security awareness and knowledge (Martins and Da Veiga, 2014; 2015).

Higher awareness and better knowledge along with other appropriate factors of the security culture (e.g. trust, ethics, attitudes, beliefs) lead to a more secure behaviour of users (Da Veiga and Eloff, 2010; Martins and Da Veiga, 2015). On the other hand, if the listed cultural factors are inappropriate, users still behave unsecure (Van Niekerk and Von Solms, 2010). Prislan and Bernik (2014) found out that security awareness has increased in the recent years, but often users still do not respect the privacy policies, which is definitely a challenge for the future. Parallels could be found in the field of transport in Slovenia, where drivers are familiar with traffic rules and restrictions, but they are often violated, since such behaviour is not unacceptable in the national culture.

The implementation of good information security culture, ISO/IEC 27001 standard or OECD principles means a huge change and requires a lot of effort of all employees. To avoid resistance and achieve success, it is very important that the change is carefully planned and carried out in a way that suits the characteristics of the organisation. For the best possible success in the information security field, we advise the use of general change management models, e.g. Kotter's Eight-Step model, Ulrich's Seven-Step model (Cameron and Green, 2015), or the specific information security culture change management framework (Alhogail and Mirza, 2014). The framework provides description of ten important principles, e.g. culture analysis, communication, motivation, management support, sufficiency of resources, change agents team.

According the research of Alhogail (2015), the most important principle is the top management support, followed by sufficiency of resources.

Very important are also workshops and focus groups. Participation of key users allows the exchange of knowledge, raises awareness and achieves better understandability of security policies, which also affects their better compliance. Following the security culture change management principles enables the cultivation of the information security culture, where users do not relay on the IT department's technological safeguards but are aware of their own responsibility.

Considering previously described changes in the information technology field, the only possible way for ensuring a suitable level of information security in the future is the motivation of all users to constantly learn and self-educate themselves regarding the information security, and compliance with security policies of the organisation.

LITERATURA

1. AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, No. 49, pp. 567–575.
2. AlHogail, A. (2015a). Cultivating and assessing an organizational information security culture. International Journal of Security and Its Applications, 9, No. 7, pp.163–178.
3. Alhogail, A. and Mirza, A. (2014). A framework of information security culture change. Jour-nal of Theoretical and Applied Information Technology, 64, No. 2, pp. 540–549.
4. Alnatheer, M. (2014). A conceptual model to understand Information Security Culture. International Journal of Social Science and Humanity, 4, No. 2, pp. 104–107.
5. Alnatheer, M. and Nelson, K. (2009). Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. Retrieved on 6/29/2017 from the Inter-net: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001 &context=ism.
6. Alnatheer, M. et al. (2012). Understanding and measuring Information Security Culture. Re-trieved on 8/25/2017 from the Internet: http://aisel.aisnet.org/cgi/viewcontent.cgi ?article=119&context=pacis 2012.
7. Armerding, T. (2017). The 15 worst data security breaches of the 21st century. Retrieved on 1/22/2017 from the Internet: http://www.csoonline.com/article/2130877/data-protection/data-protection-html.
8. Armstrong, M. (2006). A Handbook of Human Resource Management Practice. 11th ed., London and Philadelphia: Kogan Page.
9. Cadle, Y. and Yeates, D. (2001). Project management for information systems. London: Pear-son Education.
10. Cameron, E. and Green, M. (2015). Making sense of change management: a complete guide to the models, tools and techniques of organizational change. London: Kogan Page.
11. CISO (2011). Human behaviour and security culture. Retrieved on 8/30/2017 from the Inter-net: http://exec.tuck.dartmouth.edu/downloads/623/human_behavior_and_security_ cultu-re_ciso_ workshop_overview.pdf.
12. Da Veiga, A. and Eloff, J. H. P. (2010). A framework and assessment instrument for infor-mation security culture. Computers & Security, 29, No. 2, pp. 196–207.
13. Da Veiga, A. and Martins, N. (2014). Information Security Culture: A Comparative Analysis of Four Assessments. Retrieved on 8/15/2017 from the Internet: http://uir.unisa.ac.za/bitstream/handle/10500/18734/Information%20Security%20Culture%20A%20Comparative%20Analysis%20of%20Four%20Assessments%202014.pdf?sequence=1&isAllowed=y.
14. Da Veiga, A. et al. (2007). Information security culture – validation of an assessment instru-ment. Southern African Business Review, 11, No. 1, pp. 147–166.
15. Dhillon, G. (1999). Managing and controlling computer misuse, Information Management & Computer Security, 7, No. 4, pp. 171–175.
16. Gebrasilase, T. in Lessa, L. F. (2011). Information Security Culture in Public Hospitals. The Xase of Hawasa Referral Hospital. The African Journal of Information Systems, 3, No. 3, pp. 72–86.
17. Hassan, N. H. and Ismail, Z. (2012). A conceptual model for investigating factors influencing information security culture in healthcare environment. Retrieved on 6/27/2017 from the In-ternet: http://www.sciencedirect.com/science/article/pii/S1877042812052196.
18. Hassan, N. H. et al. (2015). Information Security Culture: A systematic literature review. Re-trieved on 8/24/2017 from the Internet: http://www.icoci.cms.net.my/proceedings/2015/PDF/PID205.pdf.
19. Ifinedo, P. (2014).The effects of national culture on the assessment of information security threats and controls in financial services industry. International journal of electronic business management, 12, No. 2, pp. 75–89.
20. International Organisation for Standardization. ISO/IEC: 27001:2013, Information technolo-gy -- Security techniques -- Information security management systems – Requirements. Re-trieved on 2/3/2017 from the Internet: http://www.iso.org/iso /catalogue_detail?csnumber=54534.

21. International Organisation for Standardization. ISO/IEC: 27002:2013, Information technolo-gy -- Security techniques -- Code of practice for information security controls. Retrieved on 2/3/2017 from the Internet: http://www.iso.org/iso/catalogue _detail?csnumber=54533.
22. IT Governance Institute (2007). CobiT 4.1. Rolling Meadows: IT Governance Institute.
23. Knapp, K. J. et al. (2006a). The top information security issues facing organizations: What can government do to help? Information Security And Risk Management, 15, No. 4. pp. 51–58.
24. Knapp, K. J. et al. (2006b), Information security: management's effect on culture and policy, Information Management and Computer Security, 14, No. 1, pp. 24–36.
25. Martins, A. in Eloff, J. (2002). Information security culture. Retrieved on 8/26/2017 from the Internet https://link.springer.com/content/pdf/10.1007%2F978-0-387-35586-3_16.pdf.
26. Martins, N. and Da Veiga, A (2015). An information security culture model validated with structural Equitation modelling. Retrieved on 8/30/2017 from the Internet: http://uir.unisa.ac.za/bitstream/handle/10500/19061/CSCAN-OA-254%20Inf%20Sec%20 Cul%20Model%20with%20SEM%20HAISA%202015.pdf?sequence=1&isAllowed=y.
27. Martins, N. and Da Veiga, A. (2014). The value of using a validated information security cul-ture assessment instrument. Retrieved on 8/30/2017 from the Internet: http://uir.unisa.ac.za/bitstream/handle/10500/14350/Martins%20Da%20Veiga_The%20Value%20of%20Using%20a%20Validated%20Information%20Security%20Culture%20Instrument.pdf?sequence=2.
28. OECD (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Retrieved on 1/5/2017 from the Internet: http://www.oecd.org/sti/ieconomy/15582260.pdf.
29. Opcomm (2013). Pridobljeno dne 3. 2. 2017 s svetovnega spleta: http://www.opcomm.eu/sl/medijsko-sredisce/blog/139-zakaj-postaja-internet-stvari-najveja-globalna-panoga.
30. Prislan, K. in Bernik, I. (2014). Trendi informacijske varnosti v sodobni organizaciji. Uporabna informatika, 22, št. 1, str. 25–37.
31. Rančigaj, K. in Lobnikar, B. (2012). Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture. Pridobljeno dne 20. 1. 2017 s svetovnega spleta: http://www.fvv.um.si/konferencaiv/zbornik/Rancigaj_Lobnikar.pdf.
32. Sans Institute (2017). Pridobljeno dne 22. 1. 2017 s svetovnega spleta: https://www.sans.org/reading-room/whitepapers/analyst/survey-mobility-byod-security-policies-practices-35175.
33. Schlienger, T. and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. Retrieved on 8/22/2017 from the Internet: http://ieeexplore.ieee.org/abstract/document/1232055/.
34. Talib, S. et al. (2010). An analysis of information security awareness within home and work environments. Retrieved on 2/1/2017 from the Internet: http://ro.ecu.edu.au/cgi/ viewcon-tent.cgi?article=7348&context=ecuworks.
35. Van Niekerk, J. F. and Von Solms, R. (2010). Information Security Culture: A management perspective. Computers & Security, 29, No. 4, pp. 476–486.
36. Van Niekerk, J. F. and Von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. Retrieved on 8/30/2017 from the Internet: https://www.researchgate.net/profile/Johan_Van_Niekerk2/publication/220803201 _A_holistic_framework_for_the_fostering_of_an_information_security_sub-culture_in_organizations/links/0deec519093063e1f2000000.pdf.

Dr. Alenka Rožanec, višja predavateljica na Fakulteti za upravljanje, poslovanje in informatiko Novo mesto.
E-naslov: alenka.rozanec@guest.arnes.si

Dr. Sebastian Lahajnar, BPNLAB Ljubljana.
E-naslov: sebastian.lahajnar@siol.net