Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture

Katja Rančigaj, Max Planck Gesellschaft, Generalverwaltung, München, Nemčija
Branko Lobnikar, Fakulteta za varnostne vede, Univerza v Mariboru

Namen in cilj prispevka
Namen prispevka je analizirati vedenjske vidike zagotavljanja informacijske varnosti v sodobnem podjetju. Izkušnje in rezultati raziskav namreč dokazujejo, da za upravljanje s tveganji ni zadosti, da imajo podjetja vzpostavljeno strukturo za zagotavljanje varnosti (npr. sodobna strojna in programska oprema, predpisi in standardi …), temveč je končni rezultat odvisen predvsem od osebne zavzetosti zaposlenih, kako se bodo vedli. Prispevek tako kot ključni dejavnik za zagotavljanje varnosti izpostavi posameznikovo vedenje, ki pa ga je mogoče upravljati samo preko organizacijske (varnostne) kulture oziroma informacijske varnostne kulture. Cilj prispevka je prikazati, kako je mogoče z upravljanjem informacijske varnostne kulture doseči zaželene rezultate pri upravljanju z (informacijskimi) varnostnimi tveganji v podjetju.

Metodologija
Za potrebe priprave prispevka je bil opravljen pregled dosedanjih raziskav in objav na analiziranem področju. Pristop je po naravi kvalitativen.

Ugotovitve
Za uspešno upravljanje informacijske varnostne kulture je treba upravljati procese na treh nivojih: na nivoju organizacije, skupine in posameznika. Na organizacijskem nivoju so tako pomembne vzpostavljene politike in postopki, zelo pomembno je zgledovalno primerjanje (benchmarking), natančna analiza tveganj ter zagotavljanje primernega proračuna. Na skupinski ravni je ključno vedenje vodstva podjetja ter vzpostavitev zaupanja, na ravni posameznika pa sta pomembna dejavnika zagotavljanja informacijske varnostne kulture zavedanje pomena področja ter etičnost – pripravljenost vesti se v skladu s temi pravili. Informacijsko varnostno kulturo je tako mogoče upravljati v skladu s PCDA modelom: analiza trenutnega stanja, planiranje ukrepov, implementacija teh ukrepov ter ocenjevanje izvedenega. V zaključku so predstavljeni tudi dejavniki, ki na ravni posameznika vplivajo na njegovo pripravljenost vesti se v skladu s predpisanimi varnostnimi standardi: gre za posameznikove osebne vrednote, njegov občutek do odgovornosti do delodajalca, ter zaznane težave, s katerimi se zaposleni srečujejo pri upoštevanju varnostnih pravil.

Izvirnost
Prispevek je pripravljen kot pregledni znanstveni članek, kjer so na enem mestu zbrane ugotovitve z analiziranega področja.

Ključne besede: informacijska varnostna kultura, organizacijsko vedenje, varnostna kultura

1 UVOD - VEDENJE POSAMEZNIKA KOT DEJAVNIK ZAGOTAVLJANJA VARNOSTI

Ob predpostavki, da razpolagamo s tehnološko dovršenimi orodji in da lahko na inpute iz zunanjega okolja vplivamo le bolj ali manj uspešno, je posameznik in njegovo vedenje eden izmed ključnih dejavnikov tudi pri zagotavljanju varnosti (in s tem tudi informacijske varnosti) v podjetjih. Usmerjenost k posamezniku 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 bilo narejeno slabo. Če se je računalniška in 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).
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 s tako občutljivim področjem dela. Vendar pa to ni edini niti najbolj učinkovit način usmerjanja in spremljanja vedenja ljudi (ENISA - European Network and Information Security Agency, 2007). Določitev pravil vedenja je le nujni, a na zadostni pogoj za končen uspeh. Zaznavanje in interpretacija varnosti sta v veliki meri odvisna od splošne varnostne kulture. Za ponazoritev – če zapisana pravila ali postopki v določeni organizaciji štejejo za jalova in nepomembna, bo takšen tudi odnos do varnostnih pravil. V organizacijo se bo naselil negativen odnos do delovnih orodij, ki se najpogosteje kaže v obliki izgovorov, da določena stvar ni bila narejena zaradi tega, ker je pravila ne narekujejo (Guldenmund, 2000: 249). Aktiven odnos posameznika do zaščite in varovanja osebnih ter zaupnih podatkov, ki zajema celotno znanje o zaščiti in varovanju teh podatkov ter se manifestira z zavestnim vedenjem v konkretni situaciji, lahko opredelimo kot izraz visoke stopnje varnostne kulture. Ta ne predstavlja zgolj vedenja, ampak predvsem vsebino, globlje motive in vzroke, kjer je ogroženost vrednot glavni povod za njihovo zaščito (Košmrlj, 1982).
Pregled dosedanjih raziskav s področja informacijske varnosti kaže, da se relativno malo prispevkov nanaša na obravnavo informacijsko-varnostne ozaveščenosti in usposobljenosti, na odzivnost na incidente in človeški vidik informacijske varnosti (družbeni, kulturni in etični vidiki človeških virov in organizacijskih politik) (Dlamini, Eloff in Eloff, 2009). Kljub temu, da je zadosti že majhna napaka (npr. geslo za dostop v računalnik je shranjeno na vidnem mestu, vrata pisarne so odprta ali nezaklenjena in v njej osebni računalnik, manipulacija s pomočjo socialnega inženiringa …), da napredek sodobne tehnologije popolnoma zbledi, se organizacije še vedno premalo zavedajo, da so uporabniki z nizko stopnjo varnostne osveščenosti pravzaprav ena izmed najšibkejših vrzeli v organizaciji (Shaw in sod., 2009). Za primer, Orgill in sodelavci (2004; cit. v Bakhshi, Padaki in Furnell, 2009: 54) v raziskavi ugotavljajo, da bi kar 80% zaposlenih zaupalo svoje uporabniško ime in 60% 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).

2 VARNOSTNA KULTURA

Raven varnostne kulture kot dela organizacijske kulture tako postaja vse pomembnejši parameter t. i. skrite vrednosti organizacije in skrbi za vzpostavljanje učinkovitih mehanizmov obvladovanja in upravljanja z občutljivimi podatki. Varnostno (samo)zavedanje namreč predstavlja segment, ki si ga vodstveno osebje prizadeva doseči preko različnih pristopov zavednega in nezavednega vplivanja na zaposlene. Predpisi, varnostne politike, protokoli in standardi sami po sebi za varno vedenje še niso zadosti, saj na ravnanje z občutljivimi podatki vplivajo tudi osebne predpostavke o varnosti, ki so odraz posameznikovega zaznavanja oz. razumevanja tako varnostnih predpisov, kot tudi dejanskih groženj (Zakaria, 2006). Zhang in sodelavci (2002) so pri pregledu različnih definicij varnostne kulture ugotovili, da je kljub številnim poskusom opredelitve, mogoče izločiti nekaj skupnih značilnosti. Varnostna kultura:

a. je koncept, ki je definiran na ravni skupine ali višje in se nanaša na skupne vrednote celotne skupine oz. članov organizacije;
b. se ukvarja s formalnimi varnostnimi zadevami v organizaciji in je ozko povezana, a ne omejena, z menedžerskim in nadzorstvenim sistemom;
c. poudarja prispevek vsakogar na vseh ravneh organizacije;
d. organizacije ima vpliv na vedenje ljudi pri delu varnostna kultura se navadno odraža v nepredvidljivostih med sistemom nagrajevanja in varnim postopanjem;
e. se odraža v organizacijski pripravljenosti, da se razvija in uči iz napak, incidentov in nezgod;
f. je relativno trajna, stabilna in odporna na spremembe.

Varnostna kultura je torej odraz usklajenih organizacijskih prizadevanj, da se elemente (organizacijske) kulture usmeri k doseganju varnostnih ciljev, vključujoč člane organizacije, sisteme in delovno aktivnost (Cooper, 2000). Pri tem gre za prehod splošnega varnostnega zavedanja v varnostno kulturo, kar se zgodi v tistem trenutku, ko prične skupina kot celota varnostne kršitve socialno in moralno dojemati kot nesprejemljive za okolje, v katerem delujejo (Lobnikar in sod., 2009: 47) in se začne (samo)varnostno tudi obnašati.

3 INFORMACIJSKA VARNOSTNA KULTURA

Wagner in Brooke (2007) pravita, da sta zaznavanje potencialnih groženj in prepoznavanje lastnih ranljivosti ključna za vsako uspešno podjetje in institucijo, saj so dokumenti v smeteh pogosto več vredni, kot isti dokumenti v računalniku. Zato vloga človeškega dejavnika postaja pri zagotavljanju varnosti vse bolj prepoznavna, poleg tega pa vsaj toliko pomembna kot je pomemben sam tehnološki dejavnik. Glede na to, da je delo zaposlenih v obdobju razvitega IKT-ja povezano z visoko stopnjo odgovornosti, integritete, zaupanja in možnostjo razmeroma lahkega dostopanja do informacij, je za vsako podjetje izredno pomembno, da njeni zaposleni z njo delijo enake poglede na varnost, da razumejo svoje naloge in vlogo, ki jo imajo. Znanje o tem, kakšna je vloga posameznika v organizaciji in kaj se od njega pričakuje, prispeva k zagotavljanju informacijske varnosti ter predstavlja prvo izmed dveh dimenzij človeškega dejavnika pri zagotavljanju varnosti (van Niekerk in von Solms, 2006). Poleg znanja vpliva na posameznikovo varno delo z občutljivimi podatki tudi njegovo lastno vedenje. Kajti povsem mogoče je, da zaposleni svoje vloge in naloge razumejo pravilno (imajo primerno znanje), a se kljub temu ne držijo varnostnih pravil, ker ta niso v skladu z njihovimi prepričanji in vrednotami (Schlienger in Teufel, 2003; cit. v van Niekerk in von Solms, 2006: 2). Zaradi tega je vzpostavitev primerne informacijsko varnostne kulture, ki združuje obe dimenziji, nujna za zagotovitev učinkovite informacijske varnosti.

Informacijska varnostna kultura je produkt organizacijske kulture, saj slednja predstavlja prevladujočo kulturo v organizacijskem okolju, informacijska kultura pa je njena komponenta, kar potrjujejo tudi različne raziskave (Borck, 2000; Connolly, 2000; Le Grand in Ozier, 2000; cit. v Da Vaiga in Eloff 2010: 197). Pojem informacijske varnostne kulture se je razvil iz pojma varnostne kulture in pravzaprav nakazuje vrsto varnostne kulture v okolju z določenimi značilnostmi. Na odnos med varnostno in informacijsko varnostno kulturo je mogoče gledati tudi z vidika dopolnitve, saj se značilnosti varnostne kulture odražajo v informacijski varnostni kulturi, le da so te nekoliko bolj usmerjene v ustvarjanje okoliščin, ki so naklonjene varovanju občutljivih podatkov. Informacijska varnostna kultura se razvije na podlagi informacijsko-varnostnega vedenja (torej vedenja, ki je povezano s skrbjo za varovanje informacij oz. podatkov) na enak način, kot se razvije organizacijska kultura na podlagi vedenja zaposlenih v organizaciji (ibid: 198).

Informacijsko varnostno 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 informacijsko varnostno kulturo tudi Martins in Eloff (2002, cit. 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 s pomočjo organizacijskih, skupinskih in individualnih ravni. Načela informacijske varnostne kulture, ki usmerjajo vedenje in mišljenje ljudi, lahko strnemo v devet vsebinskih sklopov:

1. Zavest: 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 odreagira.
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 slabosti, določijo tudi sprejemljivo raven tveganj, preden se vzpostavi nadzor.
7. Varnostni načrt in implementacija: Uporabniki vključujejo element varnosti kot ključen element informacijskih sistemov in omrežij, tako v tehnične kot netehnične ukrepe in rešitve.
8. Upravljanje z varnostjo (varnostni menedžment): Udeleženci sprejmejo celovit pristop k upravljanju z varnostjo, vključno z varnostnimi politikami, praksami, ukrepi in postopki, ki so usklajeni in strjeni 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 (OECD 2002, 9–12).

3.1 Stopnje informacijske varnostne kulture

Pregled obstoječe literature kaže, da obstajajo v organizacijah različne stopnje povezanosti med organizacijsko kulturo in informacijsko varnostno kulturo. Ločimo med (Lim in sod. 2009: 91):

1. organizacijami 1. tipa: informacijska varnostna kultura je ločena od organizacijske kulture;
2. organizacijami 2. tipa: informacijska varnostna kultura je subkultura organizacijske kulture, in
3. organizacijami 3. tipa: informacijska varnostna kultura je vključena oziroma je del organizacijske kulture.

Za organizacije 1. tipa je značilno, da varovanje informacij še ni sestaven del organizacijske kulture. Večina zaposlenih ni vključena ali pa ima zelo slabo vlogo pri izvajanju varnostnih pravil, kar je povezano z njihovim slabim znanjem in pomanjkanjem odgovornosti za razvijanje informacijske varnosti. Organizacija sama, na drugi strani, gleda na varnost z vidika dodatnega stroška, se izogiba investicijam in je prepričana, da je informacijska varnost izključno naloga IKT- oddelka. Nasprotno se pri organizacijah 2. tipa že kaže večja varnostna osveščenost, saj se občasna usposabljanja s tega področja izvajajo kot upoštevanje navodil menedžmenta. Zaposleni se bolje zavedajo varnostnih zahtev, kljub temu pa je medresorsko (ali med-oddelčno) usklajevanje še vedno nezadovoljivo, saj so vrednote informacijske varnosti pretežno vezane na majhno skupino ljudi (npr. finančni oddelek, kadrovski oddelek) in ne prežemajo celotne organizacije. Najbolj zaželene organizacije so seveda organizacije 3. tipa, kjer so varnostne prakse odgovornost vseh zaposlenih. Organizacija redno posodablja in prilagaja varnostno politiko ter zagovarja visoko stopnjo vključevanja v te procese. To vpliva na oblikovanje občutka, da so informacije last zaposlenih in povečuje motivacijo za spoštovanje varnostnih predpisov (Lim et.al. 2009: 91–92).

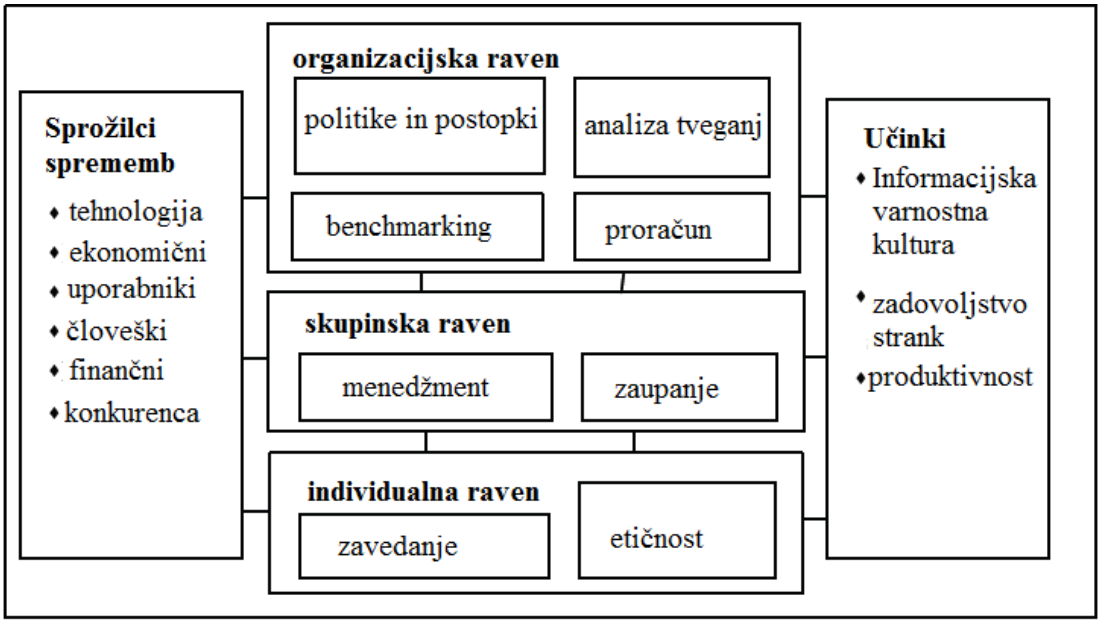
Ko govorimo o različnih stopnjah informacijske varnostne kulture v organizacijah, je potrebno omeniti tudi t. i. valove razvoja informacijske varnosti. Kot pravi von Solms (2000, cit. v Kuusisto in Ilvonen 2003: 432–433) je prvi val informacijske varnosti, ki je trajal približno do začetka 80. let, zaobjel tehnični vidik varnosti in obravnaval varovanje informacij z vidika zmogljivosti IKT-ja (npr. preverjanje pristnosti, storitve nadzora dostopa). Drugi val, t. i. menedžerski val, se je pojavil z začetkom vključevanja organizacij v mrežne aktivnosti, torej s prihodom interneta v zgodnjih 80. letih in zajema pripravo varnostnih politik, postopkov, metod in varnostnega osebja. Tretji val, t. i. institucializacijski val pa gradi na informacijski varnosti kulturi na takšen način, da postane informacijska varnost normalen element vsakodnevnih dejavnosti in o njem govorimo v obdobju od zadnjih let 90. let do danes.

3.2 Ključni indikatorji informacijske varnostne kulture

Za ohranjanje sprejemljive ravni informacijske varnosti morajo podjetja del svoje pozornosti nameniti tudi implementaciji obširnih in ustreznih indikatorjev, ki so v pomoč pri iskanju odgovorov na številne grožnje, ki ogrožajo varnost posameznikov, delovnih procesov in tehničnih pripomočkov. Indikatorji se odražajo na ravni posameznikov, skupin in celotne organizacije. Individualna raven se nanaša na značilnosti, ki vplivajo na posameznikovo vedenje na delu in vključujejo demografske podatke kot sta starost in stan, osebnostne značilnosti, emocionalne značilnosti, vrednote, prepričanja in osnovne predpostavke (Robbins, 2001; cit. v Da Veiga in Eloff, 2010: 201). Skupinska raven se povezuje z vedenjem ljudi v skupinah in raziskuje vpliv skupin (skupinsko mišljenje) na vedenje posameznikov.

Organizacijska raven pa vpliva na vedenje posameznikov zlasti preko različnih varnostnih politik in pravil (ibid.).

Na Sliki št. 1 so predstavljene tri ravni organizacijskega vedenja, izmed katerih je vsaka raven podlaga drugi. Na ravneh se nahajajo določene postavke, ki morajo biti ustrezno izpolnjene, da lahko spodbujajo krepitev kulture z visoko stopnjo naklonjenosti k udejanjanju informacijske varnosti. Te postavke bodo v nadaljevanju poimenovane indikatorji informacijske varnostne kulture.



Slika 1: Model informacijske varnostne kulture (Vir: Martins, 2002)

Nepredvidljiv razvoj IKT-ja pospešuje potrebo po proaktivnemu prilagajanju informacijske varnosti na spremembe, ki jih s sabo prinašajo tehnološke novosti, tekmovalnost med organizacijami, razvoj ekonomije, posledice človeškega dejavnika, pričakovanja uporabnikov (strank) in finančni vložki. T. i. sprožilci sprememb so v okviru proučevanja informacijske varnostne kulture izredno pomemben dejavnik, saj vplivajo na dogajanje znotraj organizacije in se odražajo na spremembah na organizacijski, skupinski in individualni ravni (Martins, 2002).

(a) Organizacijska raven

Organizacijska raven predstavlja krovno raven v organizaciji, saj kot dežnik zaobjema vse, kar se dogaja na skupinski in individualni ravni. Preko oblikovanja in izvajanja politik in postopkov daje organizaciji značilno strukturo ter vpliva na oblikovanje delovnih procesov in uporabo tehnologije (Martins, 2002). Na organizacijski ravni so pomembni naslednji štirje indikatorji:

1. Politike in postopki: usmerjajo vedenje ljudi in določajo, kaj se pričakuje od njih. Preko njih se kaže tudi naklonjenost menedžmenta informacijski varnosti, saj ta težko pričakuje, da bodo zaposleni opravljali naloge na določen način, če nimajo na voljo ustreznih sredstev in navodil. Varnostni dokumenti morajo biti pripravljeni na podlagi specifičnih potreb in ciljev organizacije ter morajo obravnavati postavke, ki jih zahteva informacijska varnost;
2. Benchmarking ali zgledovalno primerjanje: je pomembno z vidika primerjave organizacije z drugimi podobnimi organizacijami in mednarodnimi standardi. Poleg tega prinaša tudi usmeritve, kako primerno ravnati z informacijsko lastnino in jo ob enem varovati pred nevarnostmi. Organizacije lahko npr. napravijo zgledovalno primerjanje s pomočjo standardov družine ISO, ki predstavljajo referenčni dokument z vsemi nadzornimi mehanizmi, ki so potrebni v večini situacij ne glede na velikost organizacije;
3. Analiza tveganj: služi identifikaciji pomanjkljivosti v organizacijskem sistemu in grožnjam, ki lahko izkoristijo te pomanjkljivosti. V okviru IKT-okolja obstajajo številne priložnosti za

računalniški kriminal in zaradi tega je potrebno, da se analizirajo grožnje, ki ogrožajo varnost informacij in posledično implementirajo primerni kontrolni mehanizmi oz. ukrepi;

4. Proračun: predstavlja del sredstev organizacije, ki so namenjena za zagotavljanje varovanja informacij. Redno načrtovanje stroškov za potrebe informacijske varnosti postane s sčasoma sprejemljivo in ne predstavlja več dodatnega stroška, temveč investicijo oziroma obogatitev organizacije. Poraba sredstev v namene višje informacijske varnosti je tako lahko potencialni generator prihodkov (Martins, 2002: 74–80).

(b) Skupinska raven

Na skupinski ravni igra izrazito vlogo menedžment, ki daje pomen varnostnim politikam s predanostjo in rednim vključevanjem v njihove izboljšave. Menedžment ustvarja s podpiranjem in upoštevanjem varnostnih predpisov okolje v katerem igra zaupanje pomembno vlogo. Na skupinski ravni je pomembna vloga dveh indikatorjev:

1. Menedžment: menedžment igra ključno vlogo pri procesu udejanjanja informacijske varnosti, saj je odgovoren prepoznati varnostna tveganja in zagotoviti primerne zaščitne ukrepe. Poleg tega se njegova odgovornost povezuje tudi z vsakodnevno predanostjo, usmerjanjem in podporo pri implementaciji informacijske varnosti;
2. Zaupanje: izvajanje varnostnih predpisov in spreminjanje vedenja zaposlenih v skladu z načeli informacijske varnosti je lažje, če menedžment zaupa svojim zaposlenim in ti zaupajo svojim nadrejenim (Martins, 2002: 82–86).

(c) Individualna raven

Vsak izmed posameznikov v organizaciji ima svoja prepričanja, ki se odražajo v njegovem vedenju. Ustrezno vedenje je povezano s poznavanjem procesov, ki so definirani na organizacijski ravni, in vpliva na uspešno realizacijo postavk na organizacijski in skupinski ravni. Kajti če se posameznike ne usmerja in opozarja na stvari, se ti ne morejo vesti v skladu s pričakovanji vodstva. Na individualni ravni so pomembni naslednji indikatorji:

1. Zavedanje: pomeni pritegniti pozornost ljudi, zakaj je področje informacijske varnosti pomembno in poteka preko usposabljanja in izobraževanja na takšen način, da pričakovano vedenje vpliva na gradnjo kulture. V organizaciji, kjer posamezniki ne razumejo in se težko vedejo na način, da ne bi povzročali groženj varnosti, je informacijska varnostna kultura še toliko bolj potrebna;
2. Etičnost: se povezuje z odnosom do intelektualne lastnine, na katero je potrebno gledati kot na premoženje organizacije in se jo lahko uporablja preudarno ter le v skladu z obstoječimi predpisi. Zaposleni morajo takšen odnos spoštovati in ocenjevati svoje delo kot prispevek k rasti organizacijske intelektualne lastnine. Seveda pa mora tudi organizacija spoštovati pravico zaposlenih do zasebnosti (Martins, 2002: 88–93).

4 UPRAVLJANJE INFORMACIJSKE VARNOSTNE KULTURE

Kako se ljudje v organizacijah vedejo, na kakšen način se odzivajo na dogodke in incidente, ter kaj se jim zdi pomembno, je odvisno od vpliva treh dejavnikov. Te dejavnike, ki so med sabo dinamično povezani (moč vsakega je povezana z močjo ostalih dveh) in skupaj tvorijo okvir v katerem se oblikuje vedenje, predstavljajo struktura, procesi in kultura[1] (Guldenmund, 2007). Raziskave kažejo, da so netehnični vidiki prav tako pomembni kot tehnični vidiki pri varovanju občutljivih ali zaupnih informacij v organizaciji (Dhillon in Torkzadeh, 2006; Siponen in Oinas-Kukkonen, 2007; cit. v Alfawaz, Karen in Kavoos, 2010: 2) oz., da informacijske varnosti ni mogoče doseči le z uporabo tehničnih sredstev in je treba pozornost nameniti tudi ljudem in procesom v organizaciji (Herath in Rao, 2009: 154).

[1] Organizacijska struktura prikazuje podobo organizacije in porazdelitev centrov moči in odgovornosti (horizontalno in vertikalno razlikovanje) ter mehanizme komunikacije, koordinacije in nadzora (npr. število kontrolorjev dela in njihovo delovno mesto). Kultura zajema osnovne predpostavke, ki oblikujejo prepričanja (npr. »Potrebujemo veliko kontrolorjev dela, ker moramo stalno nadzorovati zaposlene.«). Procesi pa so vsi osnovni in podporni procesi, ki potekajo v celotni organizaciji (npr. proces nadzorovanja, ki stremi k večji predanosti in manjšim napakam pri delu) (Guldenmund, 2007: 737).

Ob številnih ukrepih in trudu organizacij so zaposleni še vedno tisti, ki zaradi svoje nepazljivosti, prenizke osveščenosti in znanja, povzročajo največ varnostnih incidentov in posledično velike finančne izgube podjetjem. Workman, Bommer in Straub (2008) ugotavljajo, da kljub številnim ukrepom, kako izboljšati varnostno vedenje ljudi, le ti v praksi niso prinesli pričakovanih uspehov. Analiza obstoječih raziskav, ki so jo opravili, kaže, da so le-te predlagale že celo kopico različnih ukrepov, od kaznovanja, navodil o delovni etiki, višanju varnostne osveščenosti, večanja števila varnostnih postopkov, obravnavanja konkretnih situacijskih dejavnikov, izboljšanja kvalitete obstoječih politik, izboljšanja povezanosti med organizacijskimi cilji in praksami do izboljšav s strani razvijalcev programske opreme. A vendar se zdi, da teorija vse premalokrat prehaja tudi v prakso. Zaradi tega je vprašanje, kako zmanjšati občutno razliko med osveščenostjo oz. poznavanjem informacijskih groženj in dejanskim ukrepanjem ali spremembo vedenja, vse pogostejša tema razprav o informacijski varnosti. Raziskovalci namreč opažajo, da čeprav se je razumevanje varnostnega vedenja v zadnjih letih izboljšalo, obstaja »vem kako, a ne delam tako« eden izmed temeljnih raziskovalnih in praktičnih vprašanj, ki še niso bili v celoti obravnavani (Workman in sod., 2008).
Raziskave kažejo, da je kljub razumevanju pomena varnostih groženj in zavedanju, da je potrebno tveganja resno obravnavati, med zaposlenimi pogosto premalo prepoznavanja lastne vloge pri varovanju informacij in prispevanju k varni drži organizacije (SecureInfo Corporation, 2007). Na področju varovanja različnih vrst tajnosti se celo dogaja, da zaposleni dejansko predstavljajo večje tveganje, kot pa grožnje izven sistema organizacije (Federal Bureau of Investigation, 2007; cit. v Lobnikar in sod., 2008: 50). Podobno kažejo tudi rezultati raziskave, ki je v vzorec zajela 443 ameriških strokovnjakov s področja informacijske varnosti, saj kar 25 odstotkov vprašanih meni, da je več kot 60 odstotkov finančnih izgub posledica dejanj zaposlenih, ki pa v osnovi niso zlonamerna. Večina vprašanih je tudi mnenja, da so usposabljanja s področja varnostne ozaveščenosti nezadostna, medtem ko navajajo, da so naložbe v ostala področja zadostne (Computer Security Institute, 2009).

4.1Kako upravljati informacijsko varnostno kulturo?

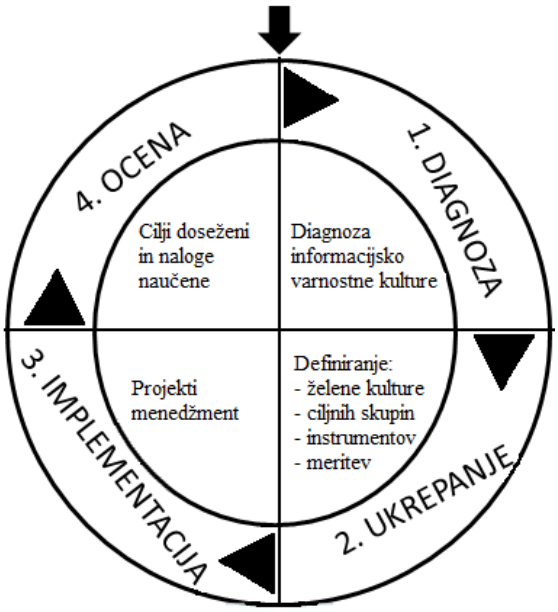
Informacijska varnostna kultura se nenehno spreminja zaradi številnih dejavnikov, ki vplivajo na njo. To pomeni, da je v organizaciji ni mogoče preprosto ustvariti ter nato pozabiti nanjo. Tako kot splošna organizacijska kultura zahteva konstantno upravljanje oz. vplivanje nanjo, da se ohrani želena stopnja. Zaradi tega lahko proces upravljanja z informacijsko varnostno kulturo poimenujemo tudi kot proces, ki nima konca oz. kot neprekinjen krog analiz in posledičnih sprememb (Schlienger in Teufel, 2005). Načela pri obvladovanju tveganj pravijo, da je potrebno razpršiti odgovornost za njeno upravljanje, in sicer tako, da skrb za upravljanje ne zadeva le vodstvenih kadrov, temveč postane naloga vseh zaposlenih v organizaciji, element vsakodnevnih aktivnosti in praks, tudi tistih, ki se zdijo nepovezane z varnostjo, ter je posledica učenja in prioritetnega položaja, ki ga ima področje varnosti (Chevreau, 2006).
Struktura, procesi in ljudje oziroma kultura, ki jo ti ustvarjajo, predstavljajo pomembno postat za varno delovanje IKT-ja oz. poslovanje organizacij nasploh, česar pa se strokovnjaki pogosto premalo zavedajo. Najučinkovitejši pristop k zmanjševanju potencialnih nesreč tako ni povezan z brezhibno delujočo tehnično opremo, ampak z usmerjanjem pozornosti na socialne in organizacijske dejavnike v organizaciji (Fleming in Lardner, 1999).
Kot je razvidno iz Slike št. 2, zajema proces upravljanja po Schliengerju in Teufelu (2005: 66–69)[2] štiri različne faze:

1. Analiza trenutnega stanja ali diagnoza; prikaže dejansko stanje kulture in njene pomanjkljivosti. Najpogosteje vključuje kombinacijo različnih merskih pripomočkov in metod, pogosto je narejena analiza specifičnih dokumentov, anketiranje zaposlenih, intervjuvanje ali anketiranje oseb, ki neposredno skrbijo za varnost, npr. varnostnikov ter metoda opazovanja.
2. Planiranje ukrepov; je odvisno od rezultatov analize, saj so za ohranjanje določene stopnje kulture potrebni milejši ukrepi kot pri spreminjanju slabe ali nizke kulture. Pri pripravi ukrepov je potrebno upoštevati obstoječe varnostne politike in predpise, ki predstavljajo

[2] Proces upravljanja s kulturo sta avtorja večkrat preverila, tudi s pomočjo delovne skupine predstavnikov Information Security Society Switzerland, ki je bila poimenovana »Informacijska varnostna kultura«.

definicijo kulture. Poleg tega je v pomoč pri določitvi pravilnih ukrepov tudi jasna odločitev o tem, na koga želimo vplivati. Pogosto uporabljen pristop zajema tri ključne skupine ljudi, tj. osebje, ki se ukvarja z IKT-jem, vodstvo in ostale zaposlene ali podporno osebje. Sprejeti ukrepi so različni, vključujejo pa določanje odgovornosti, interno komunikacijo (programe osveščanja), usposabljanje, izobraževanje in poudarek na zglednem vedenju menedžerjev.

3. Implementacija ali realizacija izbranih ukrepov; vključuje podrobno določitev aktivnosti, odgovornosti, časovno premico in finančna sredstva.
4. Ocenjevanje: poda dragocene podatke o učinkovitosti uporabljenih ukrepov in morebitnih izboljšavah v prihodnosti. Poleg tega se v tej fazi predvidijo tudi nadaljnji ukrepi, ki vplivajo na planiranje letnih finančnih sredstev in organizacijsko učenje. Zaposleni namreč vidijo, da je bila uvedba ukrepov mišljena resno ter da se njihovi učinki ocenjujejo preko vedenja ljudi, kar posledično prinese tudi hitrejše prilagajanje vedenja.



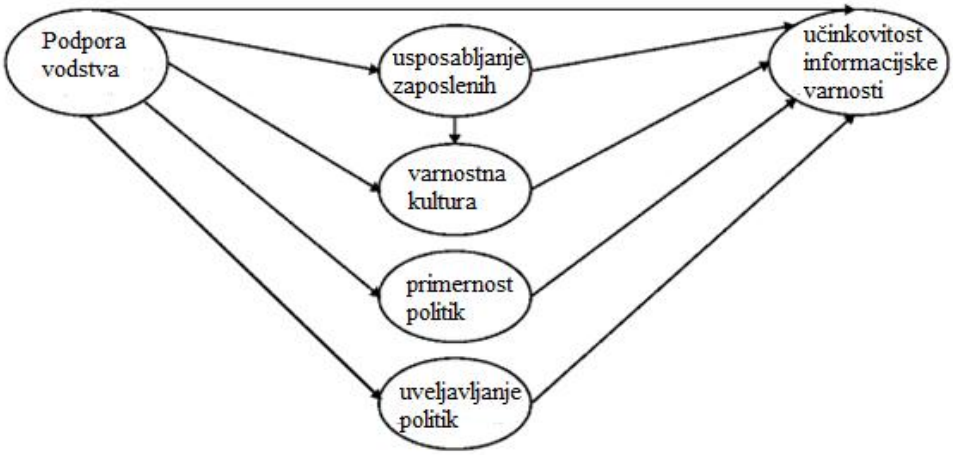
Slika 2: Proces upravljanja z informacijsko varnostno kulturo (vir: Schlienger in Teufel, 2005: 67)

(a) Vloga vodstva podjetja

Čeprav v prispevku zagovarjava stališče, da je skrb za visoko stopnjo informacijske varnostne kulture, naloga celotne organizacije (tako strokovnjakov, ki se neposredno ukvarjajo z IKT-jem, kot vodstva in t. i. »end users« oz. ostalih zaposlenih v organizaciji), se nama zdi potrebno posebej izpostaviti vlogo vodstva oz. menedžmenta in jo nadgraditi s priporočili, kako lahko prispevajo k spreminjanju varnostnega vedenja ljudi. Vodje so namreč v prvi vrsti odgovorni za delovanje organizacije in zaradi ogromnih zneskov, ki jih lahko povzroči že dokaj nedolžno razkritje zaupnih podatkov, tudi prvi zainteresirani (ali bi vsaj morali biti) za vlaganje časa, sredstev in dobre volje v izgradnjo informacijske varnosti. Zaradi tega področje informacijske varnosti najprej zadeva vodstveni nivo oz. je v splošnem problem vodstvenih struktur v podjetju, informacijska varnostna kultura pa je le odsev tega, kako dobro se upravlja s področjem varnosti (Ruighaver, Maynard in Chan, 2007). Knapp in sodelavci (2006, cit. v Ruighaver, Maynard in Chan, 2007: 61) celo ugotavljajo, da je podpora najvišjega menedžmenta bistven napovedovalec tako stopnje organizacijske varnostne kulture kot tudi stopnje do katere se sprejete varnostne politike še dejansko uresničujejo.

Vloga vodstvenih struktur je pomembna tudi zaradi tega, ker je nemalokrat zanemarjena ali celo podcenjena pri vplivu na varnostno kulturo organizacije. Čeprav je razvoj IKT-ja že sam po sebi prinesel določene spremembe, ki učinkujejo na večje zavedanje ranljivosti informacijsko komunikacijskih sistemov in k osveščenosti močno prispevajo tudi svetovni mediji, raziskave ocenjujejo, da je prispevek vodstva k višji stopnji varnosti še vedno nezadosten. Npr. 874 sodelujočih strokovnjakov s področja informacijske varnosti je v spletni raziskavi iz leta 2004 na

prvo mesto izmed 25 najbolj perečih varnostnih vprašanjih s katerimi se srečujejo sodobne organizacije, postavilo prav pomanjkljivo podporo vodstva. Na drugo mesto so uvrstili programe usposabljanj in izobraževanj za osveščanje uporabnikov, na sedmo pa organizacijsko kulturo (Knapp in Marshall, 2007).
Vodstvo ima pomembno vlogo pri vplivanju na upravljanje z varnostno kulturo. Seveda pa je potrebno pri tem poudariti, kateri so tisti segmenti organizacijskega življenja, ki so še posebej dojemljivi za vplive s strani vodstva oz. odgovoriti, na kaj se mora vodstvo osredotočiti, če želi izboljšati področje varnosti v organizaciji. Kot je razvidno iz slike št. 3, vodstvo neposredno vpliva na učinkovitost informacijske varnosti, a samo njegov vpliv ne zadostuje. Avtorja diagrama, Knapp in Marshall (2007), poudarjata, da se dejavnik podpore vodstva povezuje še s štirimi drugimi dejavniki in sicer z dejavnikom usposabljanja zaposlenih, varnostne kulture, primernih politik in dejavnikom udejanjanja teh politik. Osredotočenost na ta področja prinaša največ možnosti za spreminjanje obstoječega stanja.
Model tako nakazuje, da si je potrebno zastaviti zgolj eno vprašanje, da lahko v splošnem ocenimo »zdravje« organizacije z vidika z varnosti, in sicer, ali vodstvo vidno in aktivno podpira aktivnosti, ki so v povezavi z informacijsko varnostjo oz. s programi, ki so namenjeni njeni krepitvi. Odgovor na vprašanje je namreč močen pokazatelj in napovedovalec varnostnega stanja oz. učinkovitosti zastavljenih programov. In če je odgovor pritrdilen, potem obstaja velika verjetnost, da je organizacija na dobri poti za dosego zastavljenih ciljev. V primeru negativnega odgovora, pa je verjetnost za dosego želenih ciljev sorazmerno manjša. Podpora vodstva je tako v vsaki organizaciji ključna in bistvena za udejanjanje sprememb. Posamezniki bodo sami in brez nje le težko kaj spremenili na bolje oz. bo njihov trud v primerjavi s končnim uspehom nesorazmerno večji (ibid.).



Slika 3: Konceptualna povezanost med podporo vodstva in ostalih dejavnikov na učinkovitost informacijske varnosti Vir: Knapp in Marshall, 2007: 54

(b) Priporočila za izboljšanje varnostnega vedenja ljudi
Pomemben dejavnik, ki vpliva na izboljšanje izboljšanju varnostnega vedenja ljudi in s tem tudi na izgradnjo informacijske varnostne kulture, je usposabljanje. Čeprav se na usposabljanje pogosto gleda z vidika dodatnega stroška za organizacijo, je investicija v strokovno usmerjanje varnostnega vedenja ljudi, pravzaprav vložek v njeno dolgoročno uspešnost. Ne glede na to, kako podrobne in natančne so sprejete politike in predpisi, življenje je preveč dinamično, da bi bilo mogoče predvideti vse situacije, ki bodo zahtevale hitro in ustrezno ukrepanje zaposlenih. Poleg tega vodstvo ni sposobno nadzirati vseh delovnih procesov in mora marsikatero odločitev, ki vključuje tudi varnostne dimenzije, prepustiti ostalim zaposlenim.
V nadaljevanju bodo v dveh skupinah predstavljeni dejavniki, ki imajo močan vpliv na varnostno vedenje ljudi, izpostavljeni pa bodo tisti trije, preko katerih lahko organizacija najbolj vpliva na svoje zaposlene. Prva skupina vključuje dejavnike, ki predstavljajo posameznikovo razumevanje tega, kar organizacija pričakuje od njih, in zajema tisto, kar:

- je posameznikom povedano: sem spadajo vsi t. i. varnostni dokumenti, ki predstavljajo znanje organizacije in so učinkoviti glede na to, kako enostavno se jih pridobi, kako dovršeni in jasno so ter kako enotne so varnostne vrednote, ki jih sporočajo;
- kar posamezniki vidijo, da počnejo drugi; vedenje drugih, ki ga posamezniki opazujejo okoli sebe, ima nanje močnejši vpliv, kot sama navodila o tem, kako se morajo vesti. Pri tem so posebej izrazite vrednote in odnos do varnosti, ki ga ima vodstvo, konsistentnost med zapisanimi vrednotami in tistimi, ki so vidne iz opazovanega vedenja ter zrcaljenje varnostnih vrednot v vseh organizacijskih dejavnostih;
- kar se posamezniki naučijo iz svojih preteklih izkušenj: ker je večina varnostnih odločitev, ki jih sprejmejo posamezniki, sprejeta v nekritičnih situacijah in v okviru normalnih okoliščin, so osebne izkušnje bogata zakladnica znanja za učenje kako pravilno ukrepati oz. se vesti (Leach, 2003: 586–687).

Druga skupina vključuje dejavnike, ki vplivajo na posameznikovo osebno pripravljenost za upoštevanje predpisanih norm in pravil ter zajemajo:

- osebne vrednote in načine vedenja: večina posameznikov verjame v pomembnost skupnih vrednost in navadno hitro prevzema organizacijski sistem vrednot, saj jim je lažje delati v skladu z dogovornimi pravili kot brez njih. Težje je seveda v primeru, ko se vrednote posameznikov razlikujejo od tistih, ki jih goji organizacija;
- občutek odgovornosti do delodajalca: je posledica psihološkega pritiska, ki ga čutijo posamezniki in zajema prostovoljno upoštevanje pričakovanj organizacije; lahko se ga opiše s pojmom psihološke pogodbe.
- težave, s katerimi se srečujejo pri upoštevanju predpisanih postopkov: v primeru nerazumljivih ali težko izvedljivih varnostnih mehanizmov, kjer njihovo upoštevanje nima vidnih učinkov, imajo zaposleni izredno nizko stopnjo tolerance za vedenje v skladu z njimi (Leach, 2003: 588–689).

Leach (2003) pravi, da ima organizacija največ pristojnosti in potenciala za spremembe, ki se nanašajo na vedenje vodstva in ostalih zaposlenih (2. dejavnik 1. skupine), na uporabo znanja, ki izvira iz preteklih izkušenj (3. dejavnik 1. skupine) in na moč psihološke pogodbe (2. dejavnik 2. skupine). Spremembe je mogoče doseči preko procesa povratne komunikacije, kjer zaposleni opozarjajo na pomanjkljivosti v sistemu, preko opozarjanja na napake in skupnega iskanja boljših rešitev do nagrajevanja dobrih odločitev. Za spodbujanje psihološke pogodbe pa je dobrodošlo vpletanje varnostnih tem v vsakodnevne pogovore in sestanke, ki morajo biti vidno, da postane varnost normalna tema pogovorov.

Odgovor na vprašanje, kako upravljati z organizacijskimi značilnostmi, da postane komponenta varnosti del prepričanj, dejanj in vedenj zaposlenih in kaj je tisto, kar je potrebno dodati številnim predpisom, paleti postopkov evidentiranja in odpravljanja napak, vključno s pravili sankcioniranja kršitev in nenehnega usposabljanja, da bo stopnja informacijske varnosti večja, ni preprost. Zagotovo pa ga lahko iščemo v smeri ponotranjenega zavedanja, kako potrebno je varno vedenje v okviru določene dejavnosti, ki jo posameznik opravlja. Tisto, kar najpogosteje manjka črkam na papirju, je izkustvo – najbolj vplivne (ne)formalne norme in pravila je treba čutiti in ponotranjiti, ni jih mogoče enostavno zapakirati v obliko priročnika in servirati kot sredstvo za hitre spremembe (Rao, 2007: 731). Zato se je mogoče strinjati s trditvijo, da Ahilovo peto vsakega podjetja na področju zagotavljanja informacijske varnosti v največji meri predstavljajo predvsem njeni zaposleni (Gonzales, 2002; Zegers, 2000: cit. v Wager in Brooke 2007: 118).

VIRI

Alfawaz, S., Karen, N. in Kavooks M. (2010). *Information security culture: a behaviour compliance conceptual framework.* Prispevek predstavljen na Australasian Information Security Conference, 18.-21. januarja, v Brisbane, Avstralija.

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

Chevreau, F. (2006). Dafety culture as a rational myth: why developing safety culture implies engineering resilience? V E. Hollnagel in E. Rigaud (ur.), Proceedings of the second resilience

engineering symposium (str. 63-73), Antibes, Juan-les-Pins, Paris: Mines Paris, Les Presses. Pridobljeno 10.6.2010 na http://www.resilience-engineering.org/REPapers/Chevreau_R.pdf
Cooper, M. D. (2000). Towards a model of safety culture. Safety Science, 36 (2), 111-136.
Computer Security Institute. (2009). CSI Computer Crime and Security Survey. Pridobljeno 21.1.2010 na http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey09_Executive-Summary.pdf
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 soxio-organizational perspectives. Info Systems 11(2), 127-153.
Dlamini, M.T., Eloff, J.H.P. in Eloff M. M. (2009). Information security: The moving target. Computers & Security 28 (3-4), 189-198.
ENISA, European Network and Information Security Agency. (2007). Pobude za ozaveščanje o varnosti informacij: Sedanja praksa in merjenje uspeha. Heraklion: ENISA, European Network and Information Security Agency. Pridobljeno 19.1.2010 na: http://www.enisa.europa.eu/act/ar/deliverables/2007
Fleming, M. in Lardner, R. (1999). Safety culture – the way forward. The Chemical Engineer. Pridobljeno 1. 1. 2010 na /www.keilcentre.co.uk/Data/Sites/1/Culture.pdf.
Guldenmund, F. W. (2007). The use of questionnaires in safety culture research – an evaluation. Safety Science, 45 (6), 723-743.
Guldenmund, F. W. (2000). The nature of safety culture: a review of theory and research. Safety Science 34(1-3): 215-257.
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.
Knapp, K. J. in Marshall, T. E. (2007). Top management support Essential for effective information security. V H. F. Tipton in M. Krause (ur.), Information Security Management Handbook, Sixth Edition (str. 51-58), Boca Raton: Auerbach Publications.
Košmrlj, R. (1982). Varnostna kultura v sistemu družbene samozaščite. Diplomska naloga. Ljubljana: Fakulteta za družbene vede.
Kuusisto, T. in Ilvonen, I. (2003). Information security culture in small and medium size enterprises. Frontiers of e-business research, 431-439. Pridobljeno 15.5.2010 na http://www.ebrc.info/kuvat/431-439.pdf
Mackenzie, K. (2006). Employees may be opening the door to criminals. Financial Times Limited. Pridobljeno 20.5.2010 na http://www.ft.com/cms/s/458807fe-efec-11da-b80e-0000779e2340.html
Martins, A. (2002). Information Security Culture. Master's dissertation. Johannesburg: Rand Afrikaans University.
Leach, J. (2003). Improving user security behaviour. Computers & Security, 22 (8), 685-692.
Lim, J.-S., Shanton C., Maynard, S. in Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. Prispevek predstavljen na 7th Australian Information Security Management Conference, 1.-3. decembra, v Perthu, Zahodna Avstralija.
Lobnikar, B., Čaleta, D., Žaberl M., Anžič, A. in Rančigaj, K. (2009). Varnostna in organizacijska kultura v Slovenski vojski z vidika upravljanja s tajnimi podatki : končno poročilo raziskovalne skupine Fakultete za varnostne vede. Ljubljana: Fakulteta za varnostne vede.
OECD - Organizacija za gospodarsko sodelovanje in razvoj. (2002). Guidelines for the Security of Information Systems and Networks. Pridobljeno 30.5.2010 na http://www.oecd.org/dataoecd/16/22/15582260.pdf
Rao, S. (2007). Safety culture and accident analysis - A socio-manage,ent approac based on organizational safety social capital. Journal of Hazardous Materials 142 (3), 730- 740.
Rheea, 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.
Ruighaver, A. B., Maynard, S. B. in Chang, S. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security, 26 (1), 56-62.

Shaw, R. S., Charlie Charlie C. C., Harris, A. L. in. Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52 (1), 92-100.

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.

SecureInfo Corporation. (2007). Information Security Awareness Report. The Government Workers' perspective. Pridobljeno 15.6.2010 na http://www.secureinfo.com/downloads/reports/SecureInfo-InfoSec-Report-Dec-2007.pdf

van Niekerk, J. in von Solms, R. (2006). Understanding information security culture. A conceptual framework. Johanesburg: Information Security South Africa (ISSA). Pridobljeno 25.5.2010 na *icsa.cs.up.ac.za/issa/2006/Proceedings/Full/21_Paper.pdf*

Wagner, A. in Brooke, C. (2007). Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches. The Electronic Journal of Business Research Methods, 5 (2), 117-124.

Workman, M., Bommer, W. H. in Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers and Human Behavior, 24 (6), 2799-2816.

Zakaria, O. (2006). Employee Security Perception in Cultivating Information Security Culture. V S. Furnell, B. Thuraisingham, X. S. Wang in P. Dowland (ur.), Security Management, Integrity, and International Control in Information Systems (str. 83-92), Boston: Springer.

Zhang, H., Wiegmann, D. A., Von Thaden, T. L., Sharma, G. in Mitchell, A. A. (2002). Safety culture: a concept in chaos? The Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society. Pridobljena 25.2.2010 na http://www.humanfactors.illinois.edu/Reports&PapersPDFs/humfac02/zhawiegvonshamithf02.pdf