VARSTVOSLOVJE,
let. 16
št. 1
str. 50–67

Dejavniki sprejemanja odločitev pri urejanju učinkovite informacijske varnosti v organizacijah

Kaja Prislan, Igor Bernik

Namen prispevka:

V preglednem znanstvenem prispevku analiziramo aktualne varnostne trende in sociološke ter psihološke ovire, s katerimi se sooča varnostni management, z namenom pojasniti dileme pri zagotavljanju informacijske varnosti. V času negotovih razmer v poslovnem okolju postaja informacijska varnost vse pomembnejši poslovni proces. Učinkovitost je pogojena z različnimi okoljskimi, strukturnimi in osebnostnimi dejavniki, ki jih je potrebno upravljati, če se želi ustrezno obvladovati tveganja, ki ogrožajo obstoj organizacij.

Metode:

Analiza varnostnih trendov je izvedena s pregledom aktualnih mednarodnih raziskav o trenutnem stanju informacijske varnosti. Prav tako je bil izveden pregled teorij, ki pojasnjujejo vpliv psiholoških dejavnikov na odločitvene procese. S sintezo ugotovitev smo izoblikovali predpostavke o vzrokih neracionalnih odločitev, teoretične pristope pa smo nadgradili z njihovo umestitvijo v organizacijsko in varnostno področje.

Ugotovitve:

Ugotavljamo, da organizacije funkcije informacijske varnosti ne razvijajo ustrezno. Pregled aktualnih raziskav je pokazal, da se organizacije pogosto neučinkovito odzivajo na povečana varnostna tveganja, saj jim to onemogočajo neugodne poslovne razmere, strokovna nepodkovanost in tradicionalna vodstvena mentaliteta, spremembe na področju varnostnih rešitev in kognitivne pristranskosti pri odločevalcih. Prav tako ugotavljamo, da je učinkovitost informacijske varnosti vse bolj pogojena z netehničnimi ukrepi, pri čemer največjo vlogo odigra usposobljen, dobro razvit in strateško naravnan varnostni management.

Praktična uporabnost:

Varnostni trendi, ki jih predstavljamo v prispevku, za večino sodobnih organizacij predstavljajo velik izziv pri doseganju poslovne uspešnosti. S prispevkom želimo opozoriti na sodobne varnostne dileme in prispevati k večji ozaveščenosti odgovornega managementa. Ponujamo tudi izhodiščne točke za učinkovito soočanje s kognitivnimi ovirami pri sprejemanju odločitev.

Izvirnost/pomembnost prispevka:

Prispevek je aktualen, saj analizira najnovejše raziskave o informacijski varnosti in na osnovi tega predstavlja sodobne trende. Prav tako je izviren, ker združuje spoznanja s področja psihologije tveganj in odločitev ter informacijske varnosti v organizacijski kontekst.

UDK: 004.056:005

Ključne besede: informacijska varnost, organizacija, varnostni trendi, psihologija tveganj, varnostni management, odločitveni procesi

Decision-making Factors Contributing to the Management of Information Security in Organisations

Purpose:

Information security is becoming an ever more important business process in this period characterised by uncertainty in the business environment. Its efficiency depends on various environmental, structural, and personal factors which need to be managed in order to adequately control all risks threatening organisations' survival. This paper analyses current security trends, as well as sociological and psychological obstacles in security management, with a view to clarifying different dilemmas related to the provision of information security.

Design/Methods/Approach:

The analysis of security trends was conducted on the basis of an overview of current international research on the present state of play in the field of information security. It also includes an overview of theories explaining the impact of psychological factors on decision-making processes. Assumptions regarding the reasons for irrational decisions were drawn by performing the synthesis of findings, while theoretical approaches were upgraded by placing them in the organisational and security fields.

Findings:

The authors find that organisations are not developing the function of information security in an adequate manner. The overview of current research shows that organisations are often inefficient in their response to higher security risks, since they are prevented from doing so by unfavourable business conditions, lack of expertise, traditional management mentality, changes in the field of security-related solutions and cognitive bias found in decision-makers. The authors also find that the efficiency of information security is ever more dependent on non-technical measures, whereby trained, well-developed and strategically-oriented security management plays a crucial role.

Practical Implications:

For the majority of modern organisations, security trends presented in this paper represent a great challenge in terms of achieving business success. This paper wishes to draw attention to contemporary security-related dilemmas and raise the awareness of responsible management. The paper also provides several starting points enabling an efficient confrontation with cognitive obstacles in the course of decision-making.

Originality/Value:

This paper is up-to-date, as it analyses the latest research into information security and uses such analysis to present contemporary trends. It is also original, since it combines findings from the fields of the psychology of risk and decision-making, as well as from information security, and places them in organisational context.

UDC: 004.056:005

Keywords: information security, organisation, security trends, psychology of risk, security management, decision-making processes

1 UVOD

Trenutno stanje v poslovnem okolju, ki zajema npr. velika poslovna tveganja, finančno negotovost in bolj pogoste ter nevarne grožnje, je varnostno funkcijo povzdignilo med pomembnejše skrbi organizacij. Negotovost glede ogroženosti in preživetja poslovnih entitet je vse večja, saj so razmere v medorganizacijskih odnosih in zunanjem okolju zelo nepredvidljive. Celovita varnost organizacijskega okolja je zato nujen pogoj, ki prispeva k njihovi stabilnosti, pri tem pa takšnega cilja ni mogoče doseči brez učinkovite informacijske varnosti, ki je pomemben del varnostne funkcije. Agresivna implementacija tehnoloških novosti v poslovne entitete, ki se kaže kot vse pogostejši organizacijski trend, z namenom izboljševanja in poenostavljanja poslovnih funkcij, sicer poveča produktivnost podjetij in optimizacijo njihovih procesov, obenem pa povzroči situacijo, v kateri se grožnje in ranljivosti povečajo. Zaradi stalnih sprememb na področju kibernetskih groženj in tehnoloških tveganj klasični varnostni mehanizmi postajajo neuporabni, varnost pa ob stagnaciji ostane neuresničen organizacijski cilj. Pri zagotavljanju učinkovitost informacijske varnosti so zato organizacije vse pogosteje primorane uporabljati nekonvencionalne pristope povezane z netehničnimi aspekti in strateškimi/upravljavskimi kompetencami.

1.1 Varnostna funkcija v organizaciji

Varnostna funkcija je specifična organizacijska veja in področje, ki je ni mogoče obravnavati in ocenjevati na enak način kot ostale poslovne ukrepe in aktivnosti. O tem, kdaj je organizacija v celoti ali njeno določeno področje varno, je zelo težko govoriti, saj je varnost abstraktno stanje, ki ga je težko izraziti s konkretnimi in točnimi podatki. Trček (2006) navaja, da je varnost stanje minimalnih tveganj in da stanje absolutne varnosti ne obstaja, saj bodo vedno prisotna določena tveganja, ki jih ne moremo obvladati ali predvideti. Varnostna funkcija je v organizaciji podporne narave, saj omogoča nemoteno izvajanje vsakodnevnih poslovnih aktivnosti. Vsaka organizacija, še posebej v času gospodarske nestabilnosti, pa zahteva racionalnost pri razporejanju razpoložljivih virov za podporna področja, ki morajo prispevati k izpolnjevanju organizacijskih ciljev. Kadar je varnost učinkovita, izpolnjuje zastavljene cilje na gospodaren način in s tem prispeva

k razvoju organizacije. Tako kot varnostna funkcija nasploh je tudi informacijska varnost zelo obsežno in abstraktno področje, ki za zagotovitev učinkovitosti zahteva interdisciplinaren in timski pristop ter različne sposobnosti varnostnih strokovnjakov (Ivanc, 2013; Whitman in Mattord, 2008; Thomson in Solms, 2006). Gre za večnivojski sistem, kamor vključujemo postopke managerske, tehnične/operativne in procesno politične narave, ki se nanašajo na področje preprečevanja in odkrivanja groženj ter okrevanja po morebitnih incidentih (Allen in Westby, 2007; Sethuraman in Adaikkappan, 2009). Celovita varnost je v največji meri odvisna od razvitega varnostnega managementa, ki je pristojen za sprejemanje odločitev o varnosti. Uspeh oz. izpolnjevanje zastavljenih organizacijskih ciljev se v relativno veliki meri povezuje z managersko upravljavskimi funkcijami (Peters in Waterman, 1982; Vila, 1994; Vršec, 2013), kot so razvoj organizacije, načrtovanje in definiranje organizacijskih ciljev, odzivanje na nepričakovane situacije, način in sposobnost vodenja, upravljanje s kadrovskimi viri, njihov razvoj in nadzor ter organizacijske vrednote. Pri tem je zelo pomembno, da organizacija določi in izbere pravo strategijo, kajti ukrepi so lahko učinkoviti, vendar še vedno neracionalni in neuspešni, kadar jih organizacija ne potrebuje in pri tem zasleduje napačne cilje (Afonso, Schuknecht in Tanzi, 2006). Tudi Stewart (2012) navaja, da je upravljanje organizacije uspešno, kadar ima natančno določeno strategijo razvoja, načrt zagotavljanja varnosti pa je skladen z organizacijskimi cilji. Učinkovitost managementa se močno povezuje z ustrezno klimo in kulturo v organizaciji ter splošnim vedenjem zaposlenih. Iz tega je razvidno, da so pogoji oz. kriteriji ocenjevanja uspešnosti in učinkovitosti informacijske varnosti relativno nedoločeni in povezani z zelo abstraktnimi stanji, kar ustvarja veliko nejasnosti.

Zaradi heterogenosti in vpliva različnih dejavnikov informacijske varnosti ni mogoče učinkovito urediti na preprost in nenačrtovan način. V praksi se organizacije pri optimizaciji varnosti informacij in odpravljanju groženj srečujejo z različnimi dilemami. K temu poleg razmer v organizaciji in zunanjem poslovnem okolju močno pripomorejo sodobni varnostni trendi, ki ustvarjajo paradoksalne varnostne situacije, ter kognitivni miselni procesi, ki vplivajo na njihov proces odločanja in načrtovanja.

2 VARNOSTNI TRENDI

V praksi na informacijsko varnost vplivajo številne situacije, ki proces ovirajo ali onemogočajo. Med takšne situacije štejemo npr. pomanjkanje finančnih virov in strokovnega znanja ali njihovo neracionalno razporejanje; paradoksalne situacije med varnostjo in funkcionalnostjo informacijskih sistemov (oz. zahteva po sprejemanju kompromisov med poslovnimi in varnostnimi potrebami); stalne spremembe na področju varnostnih storitev in tehničnih rešitev; in kognitivne pristranosti oz. miselne ovire, ki se pojavljajo pri odločevalcih. Teoretično sicer obstaja idealna situacija, v kateri so izvedeni vsi ustrezni postopki za zagotovitev optimalne informacijske varnosti: varnostni management je razvit in zavesten, tehnični oddelek je ozaveščen in na voljo, tehnologija je posodobljena, izvajajo se ustrezne meritve učinkovitosti, postopki so dokumentirani, predpisani in nadzo-

rovani, ukrepi pa upoštevajo zahteve in potrebe uporabnikov ter poslovnih procesov. Praktično pa je takšna situacija v realnem poslovnem okolju težko dosegljiva, saj se poslovne situacije nenehno spreminjajo, naklonjenost vodstva varnostnemu področju stalno niha, spreminja pa se tudi struktura tehničnih oddelkov in njihove pristojnosti/odgovornosti. Odločitve pri načrtovanju informacijske varnosti so torej pogojene z različnimi organizacijskimi dejavniki, ki variirajo ter so odvisni od vsake organizacije in managementa posebej. Se pa vsa podjetja soočajo z eksponentnimi spremembami, ki jim je težko slediti in jih razumeti. To za tehnično in strokovno nepodkovane odločevalce ustvarja dileme pri izpolnjevanju zahtev po učinkoviti in uspešni informacijski varnosti hkrati.

Vprašanje o učinkovitosti informacijske varnosti je tesno povezano s sodobnimi (varnostnimi in tehnološkimi) trendi, ki med strokovnjaki sprožajo polemike glede njihovih prednosti in slabosti. Varnostni management se zaradi potrebe po optimizaciji stroškov vse pogosteje odloča za prenos odgovornosti za informacijsko varnost k tretjim specializiranim subjektom (ali t. i. izkoriščanje zunanjih virov (ang. outsourcing) varnostnih funkcij), prenašanje podatkov v oblak in eksponentno integracijo mobilne tehnologije in z njimi povezanih aplikacij v delovne procese. Omenjenih ukrepov se organizacije poslužujejo predvsem zaradi potrebe po optimizaciji stroškov (Järveläinen, 2012; Markelj in Bernik, 2011).

Outsourcing se v času naraščajočih groženj in zahtev po učinkovitosti varnosti kaže kot najpogostejša praksa. S tem se sicer določena tveganja prenesejo na zunanje organizacije, vendar se posledično s tem povečujejo druga tveganja in grožnje. Prenos varnostnih funkcij iz organizacijskega v zunanje okolje zelo pogosto vodi tudi v zmanjševanje delovne sile za zagotavljanje informacijske varnosti znotraj organizacij, kar še posebej ogroža varnost zaupnega informacijskega kapitala – manj zaposlenih pomeni manj znanja in manj nadzora. Posledice tega se kažejo v povečani ranljivosti podjetij in večjih možnostih za napake (Fullbrook, 2009). Zato se organizacije pri sprejemanju odločitev o vzpostavljanju varnostnega sistema ne smejo držati samo načela zniževanja stroškov in izogibanja odgovornosti, temveč morajo upoštevati prednosti investicij v lastne varnostne zmogljivosti, ki so neotipljive in nefinančne narave (Hriberšek in Ribič, 2013).

Poleg outsourcinga se organizacije vse pogosteje poslužujejo storitev računalništva v oblaku, kjer gre za prenos podatkov v oblak, s tem pa se zmanjšajo stroški informacijske tehnologije in vzdrževanja. Poleg prednosti takšnega ukrepa pa se vzporedno pojavlja vprašanje informacijske varnosti, saj ni natančno določeno, kdo vse lahko dostopa do informacij in kje natanko se podatki oz. del oblaka s podatki nahaja (Markelj in Bernik, 2011). Takšne storitve zmanjšujejo nadzor nad upravljanjem informacijskega kapitala. V oblaku shranjene informacije so lahko brez vednosti lastnika dostopne različnim subjektom, zaradi česar je težko zagotoviti njihovo zaupnost in celovitost (Thomson, 2011). Ker pa je poslovanje neke organizacije odvisno tudi od dobaviteljev, poslovnih partnerjev pogodbenih izvajalcev in navsezadnje tudi od konkurence, so sestavni del poslovnega informacijskega sistema tudi podatki teh zunanjih dejavnikov (Vršec, 2013). Zaradi tega je stopnja varnosti v zunanjih, povezanih oz. partnerskih okoljih prav tako izjemno pomembna. In kadar se organizacija odloči za prenos podatkov ali storitev, organizacijska varnost postane odvisna od stanja varnosti v okoljih, na katera organizacija sama nima vpliva.

Organizacije skušajo poenostaviti delovne procese tudi s pomočjo mobilne tehnologije, ki postaja organizacijski trend, od katerega so podjetja vse bolj odvisna. Kot napovedujejo raziskave, bodo v prihodnosti najnevarnejše kibernetske grožnje usmerjene ravno v ranljivosti mobilne tehnologije (Internet security threat report,[1] 2012; TMT global security study: Raising the bar,[2] 2011), saj je v trenutnem kontekstu najmanj zaščitena in najbolj ranljiva. Razlog je v tem, da se zelo hitro razvija, medtem ko se njeni zaščiti, zaradi razširjenosti in enostavne uporabe, ki zmanjšujeta občutek tveganja, namenja izjemno malo pozornosti, tako z vidika politične ureditve kot tehnične zaščite. Vse pogosteje je mogoče zaznati tudi trend vnašanja osebnih mobilnih naprav, ki jih zaposleni koristijo v zasebnem življenju, v organizacijo in delovno okolje za izpolnjevanje službenih obveznosti (BYOD[3]). To ustvarja situacijo, v kateri se združujejo zasebne in poslovne aktivnosti uporabnika, kar povečuje možnosti za zlorabe in ranljivosti v organizacijski strukturi (Sjouwerman, 2012).

Težnja organizacij slediti spremembam in tehnološkemu razvoju je zelo velika, vendar pa nepremišljena implementacija tehnoloških novosti v organizacijsko strukturo ni primeren odziv na povečana varnostna tveganja. Dobre varnostne odločitve morajo biti podprte s trdnimi argumenti – analizami prednosti in slabosti. Ker pa je učinkovitost varnosti težko merljivo področje in velikokrat tudi neustrezno definirano, v praksi pogosto prihaja do izbire neutemeljenih varnostnih ukrepov, odločitve pa temeljijo na občutkih in netočnih informacijah.

Z informacijsko varnostjo povezane nepravilne odločitve so pogosto posledica tega, da organizacije ne izvajajo ustreznih postopkov ugotavljanja dejanskega stanja (Centre for Internet Security, 2010). Slagell (2010) ugotavlja, da je analiziranje tveganj zelo redka organizacijska praksa, na podlagi katere bi organizacije sprejemale odločitve. Če pa tovrstne analize že izvajajo, so pri tem prepuščene same sebi in lastnemu (pogosto omejenemu) znanju, analize pa so medsebojno neenotne, nedosledne in neprimerljive. Glede na dejstvo, da organizacije pogosto trpijo za pomanjkanjem strokovnega znanja, volje in finančnih virov, medtem ko so storitve varnostnih svetovalcev za veliko organizacij finančno prezahtevne, je omejeno poznavanje stanja logična posledica. To potrjujejo tudi študije, ki poročajo o stagnaciji poizkusov ocenjevanja informacijske varnosti v praksi (Mimoso, 2009). Raziskave ugotavljajo, da podjetja sicer aktivno razvijajo informacijsko varnost, vendar varnostne zmogljivosti podjetij nazadujejo od leta 2008, saj 65 odstotkov organizacij ne analizira stanja informacijske varnosti (Global state of information security survey: Eye of the storm,[4] 2012) oz. je to ocenjevanje neučinkovito in neustrezno razvito (Info Security, 2011). Odsotnost točnih in aktualnih informacij

1 *Podjetje Symantec je analiziralo informacijskovarnostne incidente v 200 državah in pri tem zabeležilo skupno 5,5 milijonov zlonamernih napadov na informacijske sisteme. Dnevno so obravnavali 4.595 primerov, pri čemer je bilo vsak dan zaznanih povprečno 82 primerov napadov na organizacije. Takšni napadi so se kazali v obliki t. i. »ciljanih napadov« z namenom vohunjenja za zaupnimi podatki (ang. ATP – advanced persistent threat), kjer gre za kombinacijo različnih groženj (npr. kombinacija socialnega inženiringa in zlonamerne programske opreme, vstavljene v informacijski sistem organizacije) (Internet security threat report, 2012).*

2 *Mednarodna raziskava opravljena v 138 organizacijah.*

3 *BYOD – Bring Your Own Device*

4 *Raziskava izvedena med 1.836 pripadniki informacijskovarnostnega managementa v 64 državah.*

o trenutnem stanju varnosti in ogroženosti ali napačne informacije, ki so posledica neustreznih postopkov ugotavljanja dejanskega stanja, vodijo v nepravilne odločitve, ki temeljijo na predvidevanjih (Pironti, 2007). Zaradi pomanjkanja informacij o dejanskem stanju varnosti se podjetja na viktimizacijo v praksi najpogosteje odzivajo z odpravo posledic prvotne viktimizacije; s povečanjem fizične varnosti, zmanjšanjem privlačnosti tarče in nadzorom dostopa (Lamm Weisel, 2005; Global state of information security survey: Changing the game,[5] 2013), ki so klasični in nezadostni ukrepi pri zagotavljanju celovite in strateško usmerjene varnosti. Najpogosteje torej uporabljajo situacijsko prevencijo, najmanj pa se v praksi uporablja socialna strategija, s katero bi ugotavljali dejanske vzroke viktimizacije in poskušali uvajati dolgoročne spremembe, saj to zahteva veliko časa in truda.

Odločitve o investiranju v razvoj varnosti so v domeni vodstvenega kadra, ki (tudi) informacijsko varnost zelo pogosto povezuje s finančno koristjo varnostnih ukrepov in z idejo, da je varnost strošek. Zaradi vse večjih finančnih omejitev morajo odgovorni za upravičevanje investicij v področje varnosti njeno učinkovitost prikazati s hitrimi in točnimi rezultati (Ashraf, 2005; Pironti, 2007). Ker pa informacijska varnost v primeru učinkovitosti daje rezultate v obliki neuresničenih groženj, jo je težko dokazati s konkretnimi (finančnimi) podatki. Kadar so implementirani ukrepi učinkoviti, je zelo zahtevno izmeriti njihov vpliv na varnostne incidente oz. oceniti, koliko je organizacija pridobila s tem, da se nepoznane grožnje niso uresničile. Neuresničitev neke grožnje lahko vodi v prepričanje, da grožnja sploh ne obstaja (Burton in Stewart, 2009), kar privede do dodatnih, neupravičenih varčevalnih ukrepov. Iz tega razloga je informacijska varnost tisto področje v organizacijah, kjer se v kriznih časih zelo pogosto agresivno zmanjšujejo investicije. To pa je še eden izmed mnogih dejavnikov, ki povečuje varnostna tveganja (Knopik in Zhan, 2010). S tem informacijska varnost postaja najbolj ogroženo varnostno področje v organizacijskih strukturah. Nasprotno pa mora biti urejanje tovrstnega področja naloga vsake organizacije, saj uporaba IKT[6] v prihodnosti ne bo upadla (trendi kažejo ravno nasprotno), prav tako pa lahko upravičeno pričakujemo nadaljnji razvoj groženj in tveganj. Za učinkovito upravljanje se morajo organizacije zavedati, da je varnost dolgoročna investicija, ki ne prinaša dobička, temveč preprečuje izgubo (ENISA, 2012).

Tako ugotavljamo, da lahko poizkusi (hitrega) prilagajanja sodobnim varnostnim trendom in tehničnim novostim brez trdne argumentacije vodijo v povečane ranljivosti. To se navadno zgodi takrat, kadar organizacije tega ne počno premišljeno in analitično ter novosti uvajajo na podlagi priporočil prodajalcev, ki imajo lahko dvomljive namene. Pri zagotavljanju učinkovitosti informacijske varnosti je zato v primeru načrtovanja in vzpostavljanja varnostnih načrtov potrebno upoštevati prednosti in slabosti sodobnih trendov informacijske varnosti ter razumeti tveganja, ki jih povzroča implementacija takšnih ukrepov (kot npr. prenos odgovornosti na zunanje subjekte). Predvsem pa mora vsaka organizacija poiskati in tako poznati odgovor na dve temeljni vprašanji:

5 *Analiza 9.300 podjetij v 128 državah je pokazala, da ima zgolj 42 odstotkov organizacij proaktivno informacijskovarnostno strategijo, medtem ko imajo preostale pomanjkljive varnostne načrte (ali pa jih sploh nimajo) in se na grožnje odzivajo pretežno reaktivno.*

6 *Informacijsko-komunikacijska tehnologija.*

- kakšno je trenutno varnostno stanje in
- kakšen je načrt za prihodnost?

Kadar se informacijska varnost načrtuje strateško in dolgoročno (kar je tudi pogoj njene učinkovitosti) mora odgovorni varnostni management jasno in natančno določiti operativne, taktične in strateške varnostne cilje. Ti morajo biti osnovani na točnih informacijah o aktualnih varnostnih ukrepih in njihovih vplivih na upravljanje ogroženosti. Na takšen način se lahko identificirajo stopnja njihove združljivosti s poslovnimi zahtevami, učinkovitosti ter varnostne vrzeli, ki jih je treba urediti v prihodnosti. Organizacija mora vedeti, kaj si želi in iz kakšne situacije bo pri doseganju ciljev tudi izhajala. Želena varnostna situacija v prihodnosti pa mora biti zastavljena racionalno in predvsem izvedljivo, saj lahko pretiran idealizem in optimizem, tako kot ravnodušnost in ignoranca, povečata obstoječa tveganja. Poznavanje trenutnega varnostnega stanja, varnostnih potreb in zmogljivosti so torej nujni pogoj učinkovitosti informacijske varnosti. Brez razumevanja omenjenih področij so neracionalne odločitve s prekomernimi in nepotrebnimi ukrepi neizogibna posledica!

3 DEJAVNIKI SPREJEMANJA ODLOČITEV

Na varnostno situacijo v organizacijskem okolju vplivajo zunanji, organizacijski in osebnostni dejavniki. Finančna kriza, varnostni in tehnološki trendi so situacije, ki jih uvrščamo v področje zunanjih in organizacijskih dejavnikov. Te lahko upravljamo zgolj do določene mere oz. se nanje lahko zgolj odzivamo s pravilnimi in racionalnimi odločitvami. Na racionalnost teh odločitev vplivajo tudi osebnostni in psihološki dejavniki, ki se pojavljajo pri tistih, ki so pristojni za njihovo sprejemanje. Informacijska varnost je tako kot tehnična tudi kriminološka in psihološka tema in jo je kot takšno potrebno obravnavati, če se želi zagotoviti celovit pristop pri njenem pojasnjevanju. Zajema različne psihološke vidike, od delovanja in osebnostnih značilnosti storilcev, vedenja in odnosa zaposlenih pri uporabi tehnologije, odnosa vodstva do varnostne funkcije, do percepcije tveganj in ogroženosti ter psiholoških procesov, ki se odvijajo pri odločevalcih.

3.1 Strah, negotovost in dvom

Pri analiziranju in pojasnjevanju odločitev o informacijski varnosti v organizacijskem okolju je potrebno upoštevati tri glavne psihološke ovire, ki pogosto vodijo v neustrezna varnostna stanja; to so strah, negotovost in dvom, ki jih je težko ustrezno obvladovati brez trdnih in veljavnih analiz tveganj. Omenjeni psihološki dejavniki predstavljajo problem, kadar se pojavijo pri varnostnem managementu, ki lahko zaradi tega sprejema neracionalne odločitve, tveganja precenjuje ali podcenjuje in implementira nepotrebne varnostne kontrole.

Strah, negotovost in dvom se najpogosteje pojavijo pri tistih posameznikih, ki nimajo na voljo ustreznega znanja in razumevanja o informacijski varnosti ter kadar pri njenem urejanju ne izhajajo iz dejanskega stanja. V kombinaciji z nasi-

čenostjo trga s tehnološkimi in varnostnimi rešitvami pa se negotovost in dvom pri odločevalcih še povečujeta. Takšno situacijo zelo pogosto izkoristijo neetični varnostni strokovnjaki, ki lahko na ta način pospešijo svoj posel (Baddeley, 2011). Gre za poznano marketinško taktiko, ki se jo pogosto poslužujejo vodilna ali monopolna podjetja za ohranjanje konkurenčne prednosti. Kot ugotavlja že Pfaffenberger (2000), je na področju IKT taktika povečevanja strahu med uporabniki informacijskih sistemov zelo pogosta in že uveljavljena praksa. Z eksponentnim povečevanjem kibernetske kriminalitete v zadnjih letih pa je še toliko bolj učinkovita. Države uporabljajo podobno taktiko pri upravičevanju, povečevanju ali izkazovanju vojaške in gospodarske moči, še posebej pa v kriznih časih.

Pri ustvarjanju prepričanja o ogroženosti veliko vlogo odigrajo tudi informacije, ki jih pridobimo iz zunanjega okolja. K ustvarjanju strahu na področju zaznave tveganj v povezavi s tehnologijo močno pripomorejo mediji, ki s svojim poročanjem vplivajo na splošno mnenje v družbi. Zelo pogosto, zaradi potrebe po senzacionalnem poročanju, mediji izpostavljajo bolj dramatične in manj pogoste oblike (tudi kibernetske) kriminalitete, kar pri ljudeh ustvarja neupravičen strah (Levi, 2008). In glede na to, da negativne izkušnje s kriminaliteto in grožnjami praviloma (ne pa nujno) vplivajo na zaznano verjetnost viktimizacije (Meško, Šifrer in Vošnjak, 2012), lahko upravičeno domnevamo, da odmevne informacije o varnostnih incidentih, ki jih ljudje pridobijo od medijev, poosebijo in pretvorijo v osebno izkušnjo, njihova percepcija tveganja pa je zaradi tega večja, kot je v resnici. Informacijska tehnologija že sama po sebi pri neveščih oz. neusposobljenih ljudeh izziva občutke negotovosti in kadar mediji prekoračijo svojo vlogo informatorja in nalogo ozaveščanja (kar je zelo pogosta praksa), se posledica lahko kaže ne samo v strahu pred kriminaliteto, temveč tudi v strahu pred tehnološkimi novostmi. Takšno obliko strahu imenujemo tehnofobija (Gilbert, Lee-Kelley in Barton, 2003). In kadar je družba izpostavljena pretiranemu zastraševanju, lahko pride do neupravičenega zavračanja tehnoloških novosti in nevarnega vedenja ali pa ravno nasprotno, do uporabe pretiranih in nepotrebnih varnostnih kontrol za tveganja, ki sploh ne obstajajo.

Takšna zavajanja in pretiravanja se pojavljajo tudi na področjih zagotavljanja varnosti v organizacijskem okolju, pri čemer ponudniki in izvajalci varnostnih storitev vplivajo na prepričanost ljudi o ogroženosti z lažnimi in popačenimi statistikami (Slagell, 2010). Podjetja, ki se ukvarjajo s proizvodnjo in prodajo tehnoloških rešitev pa poleg zastraševanja, s katerim pospešujejo prodajo lastnih storitev in produktov, uporabljajo tudi različne načine, s katerimi preprečujejo nakup in uporabo konkurenčnih proizvodov, kot npr. svarila in opozorila uporabnikov pred novimi, tveganimi sistemi; izgradnja takšnih sistemov, ki so nezdružljivi s konkurenčnimi proizvodi ali pa otežijo kasnejšo zamenjavo sistemov; višje cene popravil sistemov v primeru njihove kombinacije z drugimi proizvodi ipd. Najbolj problematična metoda, ki lahko ogrozi preživetje ponudnikov tehnoloških rešitev in storitev, pa so naznanila novih produktov s strani vodilnih podjetij, ki sploh še niso v izdelavi, niti jih nimajo namena razvijati. Na takšen način se preusmeri pozornost od tehnoloških novosti tekmecev in prepreči njihova prodaja (Prentice, 1996). Monopolna podjetja z omenjenimi metodami zlorabljajo svojo moč, zavirajo razvoj konkurence in produktov, potrošnike/organizacije pa silijo v

nakup slabših proizvodov, ki so precenjeni (Pfaffenberger, 2000). Vse to ima lahko še hujše posledice kot samo precenjevanje produktov in tveganj; zaradi tega lahko uporabniki postanejo ravnodušni ali neobčutljivi na realna in nevarna tveganja, hitri in učinkoviti odzivi pa niso izvedljivi, ker se pozornost preusmeri na manj pomembna področja. Takšna situacija predstavlja etično dilemo, ko se varnostni management odloča o outsourcingu informacijske varnosti in postopkih certifikacije po varnostnih standardih s pomočjo varnostnih svetovalcev.

3.2 Sprejemanje ustreznih odločitev za informacijsko varnost

Poleg omenjenih psiholoških dejavnikov na sprejemanje odločitev vplivajo tudi kognitivni psihološki procesi, ki se odvijajo znotraj vsakega posameznika. Gre za avtomatizirane miselne procese, na podlagi katerih posameznik presoja in ocenjuje situacije oz. informacije, ki jih ima na voljo. Omenjeni procesi so pri sprejemanju odločitev o varnosti še toliko bolj prisotni, saj varnost pri ljudeh vzbuja močna stališča in občutke. Lahko so zelo uporabni, v primeru popačenih informacij ali zunanjih pritiskov pa lahko vodijo v sprejem tveganih odločitev. Ker se odvijajo na nezavedni ravni, se jih ljudje pogosto ne zavedajo in jih posledično tudi ne upravljajo.

S sociološkega in psihološkega vidika so z občutki in načinom zagotavljanja varnosti povezani trije sklopi teorij; to so ekonomska vedenjska teorija (pojasnjuje, kako psihološki intrapersonalni procesi vplivajo na ekonomske in finančne odločitve ljudi); psihologija sprejemanja odločitev (pojasnjuje vpliv razuma, hevristik in intuicije na sprejemanje odločitev); in psihologija tveganj (pojasnjuje, kako ljudje zaznavamo tveganja, zakaj jih precenjujemo ali podcenjujemo).

Ekonomske vedenjske teorije v ospredje proučevanja postavljajo posameznika kot racionalno bitje, ki je izrazito individualistične in egoistične narave. Pojasnjujejo, da se ljudje za aktivnosti ali določeno vedenje odločamo na podlagi ocene koristi in škode, ki sledi izbranemu vedenju (Baddeley, 2011). Začetna teorija (tj. teorija racionalne izbire) predvideva, da ima posameznik pri sprejemanju odločitev na voljo zadostno količino informacij, je dobro organiziran in ima sposobnosti ter voljo proučiti vse možne alternative. Kasnejša nadgradnja omenjenih teorij pa ugotavlja, da obstaja razlika med tem, kako naj bi se ljudje vedli in kako se v določenih situacijah dejansko odzivamo, saj so v praksi redko izpolnjeni vsi pogoji racionalnega odločanja (Simon, 1955). Po omenjeni teoriji je takšno odločanje v največji meri pogojeno s situacijskimi dejavniki in znanjem, ki ga posameznik poseduje v trenutku dane situacije (Sandri, 2009).

Enako je tudi v organizacijskem okolju, pri čemer je potrebno upoštevati še nekatere druge dejavnike, ki vplivajo na ekonomsko oz. racionalno vedenje poslovnih entitet, kot so npr. težnja po konkurenčnosti, potreba po varčevanju, želja po hitrih in konkretnih rezultatih. Vse to zelo otežuje upravičevanje investicij v varnostno področje. Najpogosteje se organizacije (tiste, ki se odločijo izvajati postopke ocenjevanja) v težnji po učinkovitosti na podlagi analiz cena/zmogljivost (ang. cost/benefit) odločajo, kakšne so koristi in izdatki izbranega varnostnega ukrepa. Z varnostnega vidika pa omenjene analize niso priporočljiv način tehtanja koristi

možnih ukrepov in kontrol, saj je za podajanje točnih ocen potrebno imeti na voljo natančne podatke o ogroženosti, ki pa jih organizacije pogosto nimajo (Stewart, 2012). Ocenjevanje koristi in škode pa je na podlagi tovrstnih analiz nerealno in neučinkovito. Problem dodatno poglablja še poplava informacij v kibernetskem prostoru, kjer je na voljo sicer dovolj informacij, ki pa so neurejene in (pogosto) nezanesljive. Zato je težko identificirati informacije, ki jih potrebujemo in so točne ter zanesljive. V sklopu omenjene teorije teorija omejene racionalnosti vidiku pomanjkanja relevantnih in točnih informacij dodaja še vidik pomanjkanja časovnih virov. Zelo pogosto so organizacije pod časovnim pritiskom, od managementa pa se zahtevajo hitre odločitve. Omenjena teorija navaja, da ljudje v situaciji, ko nimamo na voljo (ustreznih) informacij in časa, poenostavimo odločitvene in miselne procese. V takšni situaciji redko sprejemamo odločitve na podlagi natančne analize možnih alternativ in navadno sprejmemo prvo zadovoljivo odločitev, ki pa ni nujno tudi najbolj optimalna ali racionalna. Po tej teoriji ljudje pod pritiskom težimo k zadovoljitvi in ne k optimizaciji (Simon, 1956). Iz tega sledi, da je sprejem racionalnih in posledično najbolj učinkovitih odločitev izjemno zahtevna naloga. Varnostno področje je kompleksno, zaradi številnih zunanjih, osebnih in organizacijskih omejitev ter konstantnih pritiskov s strani vodstva in zunanjega okolja pa so manj racionalni ukrepi povsem razumljivi. Odločitvene procese in razloge posameznika je treba razlagati in razumeti z organizacijskega vidika, ki upošteva vpliv zunanjega okolja, in skupin, ki jim posameznik pripada, trenutne okoliščine ipd.

Poleg ekonomskih vedenjskih teorij razloge neracionalnih odločitev o varnostnih ukrepih razlaga tudi teorija sprejemanja odločitev, ki pojasnjuje kognitivni proces obdelave informacij. Na splošno se ljudje pri sprejemanju odločitev zanašamo na logiko in statistiko ali hevristike (Gigerenzer in Gaissmaier, 2011). Omenjena teorija pri razlagah odločitev upošteva vpliv intuicije in hevristik, ki predstavljajo alternativo oz. nasprotje logičnim in analitičnim procesom reševanja problemov ter sprejemanja odločitev. Intuicija je najpogostejši način sprejemanja managerskih odločitev, ki temelji na nepreverjenih prepričanjih, mnenju in občutku odločevalca. S pomočjo intuicije sprejete odločitve so lahko uspešne in učinkovite, vendar je dobro razvita intuicija odvisna od preteklih izkušenj, povratnih informacij, znanja in temperamenta odločevalca (Jacobs, 2011). Z intuicijo so povezane še hevristike – avtomatizirani miselni vzorci oz. kognitivni miselni procesi, ki potekajo na zavedni ali nezavedni ravni in ignorirajo določene informacije (Tversky in Kahneman, 1974). So lahko zelo dober način sprejemanja vsakodnevnih in manj pomembnih odločitev, kadar ima odločevalec na voljo veliko količino nepreglednih informacij in dobre pretekle izkušnje, lahko pa vodijo v kognitivne pristranskosti in hude sistematične napake (Gigerenzer in Gaissmaier, 2011). Obstaja več različnih kognitivnih pristranskosti in hevristik, ki so pogost način sprejemanja odločitev v organizacijskem okolju, z varnostnega vidika pa so pomembne predvsem tri vrste:

- Hevristika razpoložljivosti
  Ljudje verjetnost nekega dogodka (lahko npr. varnostne grožnje) ocenjujemo na podlagi tega, kako hitro si lahko podoben dogodek prikličejo v spomin. Pogosto izpostavljanje redkih primerov lahko vzbudi občutek, da so ti pogostejši (Slagell, 2010) (in če so npr. v medijih določene grožnje, ki so relativno nepogoste, v določenem trenutku posebej izpostavljene, ima lah-

ko odločevalec občutek, da je tveganje večje, kot je v resnici). V kombinaciji s podcenjevanjem tveganj in prevelikim optimizmom pa lahko omenjena hevristika vodi v prepričanje, da grožnje sploh ne obstajajo, saj v preteklosti organizacija z njimi še ni imela opravka (oz. jih ni zaznala) (Baddeley, 2011).

- Hevristika sidranja
  Ljudje vrednost dogodka ali pojava ocenjujemo na podlagi neke srednje izhodiščne vrednosti, ki jim je ponujena, ni pa nujno tudi pravilna (z varnostnega vidika se to pogosto dogaja pri ocenjevanju škode uresničene kibernetske grožnje, ki je zelo pogosto subjektivna in ni podprta z natančnimi analizami) (Epley in Gilovich, 2006).
- Hevristika reprezentativnosti
  Povzroča, da lastnosti določenega dogodka ocenjujemo na podlagi stereotipov in lastnosti celotne skupine, v katero ta dogodek, ukrep ali pojav spada (npr. odločevalci zaradi neutemeljenih prepričanj stalno uporabljajo ali se izogibajo storitvam enega ponudnika) (Tversky in Kahneman, 1974).

Vpliv posameznikove percepcije, občutkov in stališč na odločitvene in miselne procese spada v sklop teorij psihologije tveganj, ki so:

- KAB teorija
  KAB teorija, ki se ukvarja s proučevanjem vpliva ozaveščenosti ljudi na njihovo vedenje in spodbujanjem oz. motiviranjem zaposlenih za varnostno pozitivno vedenje. Glede na KAB teorijo se s povečevanjem znanja spreminja odnos do obravnavane tematike, posledično pa ima sprememba v odnosu vpliv na vedenje posameznika. Vendar pa spremembe v vedenju niso tako enostavne, saj nanje vpliva več spremenljivk, pri čemer znanje odigra največjo vlogo.
- TRA teorija
  Da bi razumeli proces spreminjanja odnosa in vedenja je potrebno razumeti tudi TRA (theory of reasonable action), ki je predhodnica TPB (theory of planned behaviour) teorije. Slednja je ena izmed najbolj uveljavljenih teorij pojasnjevanja povezave med odnosom in vedenjem posameznika ter opisuje posredne in neposredne vplive na omenjeno razmerje (Ajzen, 1991).
- TPB teorija
  Glede na TPB teorijo so spremembe v vedenju posameznika odvisne od njegovih namenov oz. motivacije. Ta je pogojena z dvema faktorjema: odnosom in subjektivnimi normami. Iz tega sledi, da je namen izvršiti neko aktivnost večji, kadar ima do le-tega pozitiven odnos (kaj je posamezniku všeč in kaj ne) in izoblikovane močne subjektivne norme (kaj posameznik meni, da se od njega pričakuje) (Khan, Alghathbar, Nabi in Khurram, 2011). Prepričanjem, odnosu in normam je Bandura (1977) pri pojasnjevanju posameznikovega vedenja in odločitev dodal še spremenljivko »občutek samonadzora«. Z njo pojasnjuje, da se posameznik lažje odloči za neko aktivnost, kadar ima večji občutek nadzora oz. kontrole nad določeno situacijo. In ker so zaposleni kot uporabniki v organizacijskem okolju pogosto neustrezno informirani o pravilih, razlogih sprememb in tehnologiji sami, se počutijo nemočne, zaradi tega pa lahko izoblikujejo

negativne norme in odnose do omenjenega področja. Varnostno negativno vedenje, ignoranca in neupoštevanje varnostnih pravil so v takšnem primeru pogosta praksa zaposlenih.

S spodbujanjem proaktivnega varnostnega vedenja se ukvarjata:

- Varnostnomotivacijska teorija (Protection motivation theory)
  Ukvarja se s proučevanjem vedenja potrošnikov in se uporablja na področju marketinga, managementa in varnostnih storitev (Cismaru in Lavack, 2006). Omenjena teorija (Rogers, 1975) ugotavlja, da se posameznik za neko aktivnost odloči na podlagi subjektivne ocene ranljivosti (občutek ogroženosti), nevarnosti (zaskrbljenost), samoučinkovitosti (prepričanje, da lahko sam izvede določeno dejanje, aktivnost), uspešnosti odziva oz. ukrepa (prepričanje, da bo ukrep odpravil grožnjo) in izdatkov/stroškov (neugodje, ki ga bo ob izvedbi aktivnosti ali ukrepa doživel).
- Teorija tveganj
  Na splošno ugotavlja, da smo ljudje pri ocenjevanju lastne ogroženosti nagnjeni k podcenjevanju, kadar se primerjamo z drugimi subjekti; menimo, da smo manj ogroženi kot drugi (West, 2008). Največje napake pa se pojavljajo pri ocenjevanju nevarnosti in verjetnosti tveganj; posledic groženj; uspešnosti varnostnih ukrepov in primerjanju tveganj s finančnimi izdatki za njihovo upravljanje. Razlog je v tem, da ljudje večino odločitev sprejemamo ob nepopolni informiranosti; v takšnem primeru relevantne informacije iščemo v okolju, z opazovanjem, razlaga situacije pa je odvisna od intrapersonalnih dejavnikov in osebnih izkušenj (Floyd, Prentice-Dunn in Rogers, 2000).

Iz povzetih psiholoških in sociološkiih teorij je razvidno, da so z vidika uporabnikov tehnologije subjektivne norme in odnos zelo pomemben dejavnik, ki vpliva na njihovo varnostno pozitivno vedenje. V organizacijskem okolju je zato na splošno neozaveščenost in neinformiranost uporabnikov glavni razlog njihovega odpora do sprememb in tehnologij. Posledično je med takšnimi uporabniki odnos do varnosti negativne narave, njihova pripravljenost zaobiti varnostne kontrole in pravila pa zato večja. Z vidika managementa in odločevalcev pa omenjene kognitivne pristranskosti in hevristike predstavljajo pomemben dejavnik, ki vpliva na ne/racionalnost odločitev in zelo pogosto vodi v napačne ocene vrednosti in verjetnosti dogodkov ter pojavov. Kadar posameznikovi občutki in osebna stališča ne temeljijo na točnih informacijah so pogosto neutemeljena in neupravičena. Takšna situacija je posebej pogosta na področju varnosti in ocenjevanja tveganj, kjer subjektivnost vodi v precenjevanje manj pomembnih groženj in zapostavljanje kritičnih ranljivosti. V kombinaciji s slabo razvito intuicijo oz. neizkušenostjo, strahom, negotovostjo in priporočili neetičnih svetovalcev je neučinkovita informacijska varnost popolnoma logičen končni rezultat.

4 SKLEP

Če zgoraj omenjene in opisane pogoje učinkovitosti informacijske varnosti na kratko povzamemo, lahko ugotovimo, da je informacijska varnost učinkovita,

kadar je vnaprej načrtovana in dodeljena v pristojnost sposobnemu upravljavskemu kadru. Ob upoštevanju ugotovitev analize varnostnih trendov v kombinaciji s splošno neugodnim stanjem v poslovnem okolju in vse večjimi varnostnimi tveganji pa lahko upravičeno sklepamo, da se ustvarja velik pritisk ravno na glavni element učinkovitosti informacijske varnosti – varnostni management, kar povzroča omejitve pri doseganju zastavljenih varnostnih ciljev. Potrebe organizacij po hitrih in cenovno sprejemljivih rešitvah so velike, zaradi česar organizacije pogosto nimajo časa, volje in/ali finančnih zmogljivosti, da bi odločitve snovale na podlagi kakovostnih analiz ogroženosti in splošne učinkovitosti. Ker je informacijska varnost, kljub svojemu pomenu, v organizaciji podporne narave, pa se ji z vidika sprejemanja odločitev za reševanje problemov ne namenja poglobljena pozornost, kar je posledica tradicionalne, tehnično usmerjene mentalitete informacijske varnosti. Zaradi omenjenih pritiskov je tudi vpliv psiholoških dejavnikov in kognitivnih miselnih procesov oz. kognitivnih pristranskosti večji, kar ustvarja situacijo, v kateri so logični in primerni varnostni ukrepi prilagojeni organizacijskim potrebam redka organizacijska praksa. To pa ogroža končno uspešnost in posledično konkurenčnost organizacij.

Opisani problemi in predstavljene varnostne dileme dokazujejo, da je učinkovitost informacijske varnosti najpogosteje ogrožena zato, ker organizacije v poizkusih sledenja hitremu razvoju IKT in tehničnim ukrepom pozabljajo na prispevek človeškega faktorja k varnostnem stanju v organizaciji (Ashraf, 2005). Tveganja, ki so povezana z omenjenimi trendi, se sicer lahko uravnotežijo z različnimi ukrepi, vendar je potreben celovit in ne samo parcialen ter površinski pristop. Veliko je odvisno od varnostnega managementa, ki mora tveganja uravnotežiti z natančnimi pogodbami z zunanjimi izvajalci in partnerji, postopki certificiranja po mednarodnih informacijskovarnostnih standardih in dosledno zunanjo revizijo sistemov (Järveläinen, 2012). Tiste gospodarske družbe, ki se resno lotevajo varovanja poslovnega informacijskega sistema, morajo izdelati politiko varovanja informacij, uvajati standarde varovanja in neprekinjenega poslovanja (Vršec, 2013). Predvsem se je potrebno zavedati, da tehnični ukrepi ne morejo biti učinkoviti, kadar jih uporabniki ne upoštevajo in ne razumejo varnostnih pravil (Herath in Rao, 2009), zaradi česar je potrebno varnostno ozaveščanje in vpletenost uporabnikov v varnostne procese organizacije. Že zgodnje psihološke teorije ugotavljajo, da je znanje najpomembnejši element pozitivnega varnostnega vedenja. Tudi Spears in Barkhi (2010) sta ugotovila, da aktivna udeležba zaposlenih pri vzpostavljanju varnostnih ukrepov skupaj s programi ozaveščanja pomembno vpliva na dvig dejanske stopnje informacijske varnosti v organizaciji. Enakega stališča je tudi NIST (Wilson in Hash, 2003), ki v svojih priporočilih navaja, da stanje ozaveščenosti zaposlenih vpliva na manjšo stopnjo informacijskih incidentov. Medtem so Talib, Clarke in Furnell (2010) s pomočjo raziskave prišli do ugotovitve, da ljudje večino z varno uporabo IKT povezanega znanja pridobimo ravno v delovnem okolju. Programi izobraževanja in usposabljanja so torej še toliko bolj pomembni, saj v delovnem okolju pridobljeno znanje prenašamo na druga okolja izven organizacije. Raziskave ugotavljajo tudi, da je človek najpogostejši vzrok informacijskovarnostnih incidentov, še posebej v težkih ekonomskih časih, saj povečan stres in občutek strahu pred izgubo službe povzroči, da se zaposleni pogosteje obnašajo

deviantno (TMT global security study …, 2011). Bernik in Meško (2011) pa sta ob analizi zavedanja in dojemanja kibernetskih groženj med uporabniki interneta v Sloveniji ugotovila, da na splošno obstaja pomanjkanje ozaveščenosti o kibernetskih grožnjah in zakonodaji na tem področju. Iz tega sledi, da je nujno, da se poleg fizičnega in tehničnega varovanja v varnostni sistem uvedejo tudi sodobna managerska orodja varovanja poslovnih procesov, če se želi zagotoviti ustrezno vodenje v kriznih situacijah (Vršec, 2013).

Da bi omenjene dileme in varnostne izzive čim bolje upravljali, je treba poznati tudi možna kognitivna izkrivljanja, ki se lahko pojavijo pri pojasnjevanju groženj in ocenjevanju varnostnih tveganj. Refleksivni in analitični pristopi so najboljši način minimaliziranja subjektivnosti in napak pri odločanju. In kot ugotavlja Jacobs (2011), se morajo odgovorni pri sprejemanju odločitev vprašati, kakšni so razlogi določene odločitve in kakšne so možnosti preverjanja njihove pravilnosti. Za zagotovitev učinkovitosti informacijske varnosti je treba upravljati tudi čustvene komponente, ki lahko vplivajo na neželeno vedenje ali neracionalne odločitve. Predvsem pa se je potrebno zavedati, da informacijska varnost ni zgolj tehnično področje, temveč je proces, ki zahteva obravnavo različnih psiholoških in sociološkihvidikov (Baddeley, 2011). Takšen proces sicer zahteva sistematični pristop, voljo in čas, vendar so dolgoročni učinki na stanje informacijske varnosti v tem primeru največji.

Ob vseh omenjenih pogojih je izjemno pomembno predvsem to, da se varnostni management, ki je pristojen za določanje odgovornosti, pristojnosti in načrtovanje informacijske varnosti nasploh, zaveda morebitnih napak, ki se lahko pojavijo pri sprejemanju odločitev. V primeru dvoma in negotovosti je treba zagotoviti predvsem dovolj časovnih in strokovnih virov, ki bodo prispevali k logičnim sklepom in izbiri racionalnih ukrepov. Pri sprejemanju odločitev morajo biti vzpostavljeni odprti komunikacijski kanali in konstruktiven konflikt med zaposlenimi, saj se s tem zmanjšuje prostor za enostranske in nepreverjene odločitve. Predvsem pa mora imeti managemet posluh za ideje in pripombe zaposlenih, vodstvo pa mora varnost in kredibilnost vključiti med temeljne vrednote in vizijo organizacije.

LITERATURA

Afonso, A., Schuknecht, L. in Tanzi, V. (2006). *Public sector efficiency: Evidence for new EU member states and emerging markets.* Frankfurt: European Central Bank.

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, *50*, 179–211.

Allen, J. H. in Westby, J. R. (2007). *Governing for enterprise security: Implementation guide US-CERT: Article 1 – Characteristics of effective security governance*. Pittsburg: Carneige Mellon University.

Ashraf, S. (2005). *Organization need and everyone's responsibility: Information security awareness – Global Information Assurance Certification Paper*. Bethesda: SANS Institute. Pridobljeno na http://www.giac.org/paper/gsec/4340/organization--everyones-responsibility-information-security-awareness/107113

Baddeley, M. (2011). *Information security: Lessons from behavioural economics*. Cambridge: Gonville and Caius College.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215.

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

Burton, S. in Stewart, S. (2009). *Security implications of the global financial crisis*. Austin: Stratfor Global Intelligence. Pridobljeno na http://www.stratfor.com/weekly/20090304_security_implications_global_financial_crisis

Centre for Internet Security. (2010). *The CIS consensus security metrcis*. Pridobljeno na http://benchmarks.cisecurity.org/en-us/?route=downloads.metrics

Cismaru, M. in Lavack, A. M. (2006). Marketing communications and protection motivation theory: Examining consumer decision-making. *International Review on Public and Non Profit Marketing, 3*(2), 9–24.

ENISA. (2012). *Return on security investment.* Pridobljeno na http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

Epley, N. in Gilovich, C. (2006). The anchoring and adjustment heuristics. *Psychological Science, 17*(4), 311–318.

Floyd, D. L., Prentice-Dunn, S. in Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429.

Fullbrook, M. (2009). Tips on stamping out data leakage & industrial espionage during recession. *ICT Review: Computer Hardware and Software Review Journal,* (Mar.). Pridobljeno na http://ictreview.blogspot.com/2009/03/tips-on-stamping-out-data-leakage.html

Gigerenzer, G. in Gaissmaier, W. (2011). Heuristic decision making. *Annual Review of Psychology, 62*, 451–482.

Gilbert, D., Lee-Kelley, L. in Barton, M. (2003). Technophobia, gender influences and consumer decision-making for technology-related products. *European Journal of Innovation Management, 6*(4), 253–263.

Global state of information security survey: Changing the game. (2013). London: PWC. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

Global state of information security survey: Eye of the storm. (2012). London: PWC. http://www.pwccn.com/webmedia/doc/634653330562192188_rcs_info_security_2012.pdf

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

Hriberšek, Z. in Ribič, A. (2013). Korporativna varnost kot konkurenčna prednost podjetja. *Korporativna varnost, 2*(3), 30–33.

Info Security. (2011). *Most enterprises poor at measuring information security effectiveness.* Pridobljeno na http://www.infosecurity-magazine.com/view/16928/most-enterprises-poor-at-measuring-information-security-effectiveness/

Internet security threat report. (2012). Mountain View: Symantec. Pridobljeno na http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Apr_worldwide_ISTR17

Ivanc, B. (2013). Varovanje občutljivih podatkov v informacijskih sistemih. V I. Bernik in B. Markelj (ur.), *Sodobni aspekti informacijske varnosti* (str. 6–11). Ljubljana: Fakulteta za varnostne vede.

Jacobs, J. (2011). A call to arms: It's time to learn like experts. *ISSA Journal,* (Nov.), 31–34. Priobljeno na http://beechplane.files.wordpress.com/2011/11/a-call-to-arms_issa1111.pdf

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security, 20*(5), 332–349.

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

Knopik, C. in Zhan, J. (2010). *The effects of financial crises on american financial institutions information security.* Prispevek na 5th Conference on Future Information Technology, 21.–23. 5. 2010. Madison: Dakota state University.

Lamm Weisel, D. (2005). *Analyzing repeat victimization* (Tool Guide No. 5). Center for Problem-Oriented Policing. Pridobljeno na http://www.popcenter.org/tools/repeat_victimization/print/

Levi, M. (2008). White-collar, organised and cyber crimes in the media: Some contrasts and similarities. *Crime, Law and Social Change, 49*(5), 365–377.

Markelj, B. in Bernik, I. (2011). Mobilni dostop z vidika informacijske varnosti do podatkov v oblaku. V T. Pavšič Mrevlje in I. Areh (ur.), *Zbornik prispevkov 12. slovenski dnevi varstvoslovja.* Ljubljana: Fakulteta za varnostne vede. Pridobljeno na http://www.fvv.uni-mb.si/dv2011/zbornik/informacijska_varnost/Markelj-Bernik-Oblak.pdf

Meško, G., Šifrer, J. in Vošnjak, L. (2012). Punitivnost, viktimizacija in strah pred kriminaliteto pri študentih varstvoslovja – rezultati spletne ankete. *Varstvoslovje, 14*(1), 75–96.

Mimoso, M. S. (12. 3. 2009). Number-driven risk metrics fundamentally broken. *SearchSecurity*. Pridobljeno na http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html#

Peters, T. J. in Waterman, R. H. (1982). *In search of excellence: Lessons from America's best-run companies.* London: HarperCollins Publishers.

Pfaffenberger, B. (2000). The rhetoric of dread: Fear, uncertainty and doubt in information technology marketing. *Knowledge, Technology & Policy, 13*(3), 78–92.

Pironti, J. P. (2007). Developing metrics for effective information security governance. *ISACA Journal, 7*(2), 1–5.

Prentice, R. (1996). Vaporware: Imaginary high-tech products and real antitrust liability in a post-Chicago world. *Ohio State Law Journal, 57*(4), 1163–1262.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Consumer Psychology, 91*(1), 93–114.

Sandri, S. (2009). *Reflexivity in economics: An experimental examination on the self-referentiality of economic theories.* Berlin: Physica-Verlag.

Sethuraman, S. in Adaikkappan, A. (2009). Information security program: Establishing it the right way for continued success. *ISACA Journal, 9*(5), 1–7.

Simon, H. A. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics, 69*(1), 99–118.

Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychological Review, 63*(2), 129–138.

Sjouwerman, S. (2012). 2013 security prediction. *Cyberheist News, 2*(53). Pridobljeno na http://blog.knowbe4.com/cyberheistnews-vol2-53/

Slagell, A. (2010). Thinking critically about computer security trade-offs. *Skeptical Inquirer, 34*(4). Pridobljeno na http://www.csicop.org/si/show/thinking_critically_about_computer_security_trade-offs/

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

Stewart, A. (2012). Can spending on information security be justified? *Information Management & Computer Security, 20*(4), 312–326.

Talib, S., Clarke, N. L. in Furnell, S. M. (2010). *An analysis of information security awareness within home and work environments.* Prispevek na 5th International Conference on Availability, Reliability and Security: ARES 2010, 15.–18. 2. 2010. Cracow: IEEE Computer Soc. Pridobljeno na http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7348&context=ecuworks

Thomson, K. L. in Solms, R. (2006). Towards an information security competence maturity model. *Computer Fraud & Security, 18*(5), 11–15.

Thomson, L. L. (2011). Cybercrime and escalating risks. V L. Thomson (ur.), *Data breach and encrypton handbook* (str. 3–16). Chicago: American Bar Association Section of Science & Technology Law.

TMT global security study: Raising the bar. (2011). New York: Deloitte. Pridobljeno na http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdf

Trček, D. (2006). *Managing infomation systems security and privacy*. Berlin: Springer.

Tversky, A. in Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases science. *Science, New Series, 185*(4157), 1124–1131.

Vila, A. (1994). *Organizacija in organiziranje*. Kranj: Moderna založba.

Vršec, M. (2013). Varovanje poslovnega informacijskega sistema na osnovi politike varovanja informacij. *Korporativna varnost, 2*(3), 9–11.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34–41.

Whitman, M. E. in Mattord, H. J. (2008). *Management of information security*. Boston: Course Technology Cengage Learning.

Wilson, M. in Hash, J. (2003). *Building an information technology security awareness and training Program – NIST Special Publication 800-50.* Gaithersburg: National Institute for Standards and Technology. Pridobljeno na http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

O avtorjih:

Kaja Prislan, mag. var., asistentka za področje varnostnih sistemov in doktorska študentka na Fakulteti za varnostne vede Univerze v Mariboru.

Dr. Igor Bernik, docent, predstojnik Katedre za informacijsko varnost in prodekan za izobraževalno dejavnost na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: igor.bernik@fvv.uni-mb.si