UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

MIHA VICOZI

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VLOGA POSAMEZNIKA PRI ZAGOTAVLJANJU INFORMACIJSKE VARNOSTI

Ljubljana, marec 2018 MIHA VICOZI

IZJAVA O AVTORSTVU

Podpisani Miha Vicozi, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Vloga posameznika pri zagotavljanju informacijske varnosti, pripravljenega v sodelovanju s svetovalcem prof. dr. Tomažem Turkom,

IZJAVLJAM

- da sem predloženo delo pripravil/-a samostojno;
- da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
- da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel/-a, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
- da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
- da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
- da sem pridobil/-a vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil/-a;
- da sem pri pripravi predloženega dela ravnal/-a v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil/-a soglasje etične komisije;
- da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
- da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
- da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____ Podpis študenta:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Dandanes so podjetja čedalje bolj odvisna od svojih informacijskih sistemov in ta so izpostavljena različnim grožnjam tako notranjega kot zunanjega izvora. Da se podjetja zavarujejo pred različnimi grožnjami, je treba vzpostaviti varen informacijski sistem. Tega pa lahko zagotovimo le s celovitim pristopom k informacijski varnosti. Za dosego tega podjetja uporabljajo različne tehnično zapletene rešitve, ob tem pa je treba poudariti, da je izredno pomemben tudi del, ki je povezan s človeškim faktorjem.

Številne raziskave kažejo in potrjujejo, da sta človeška nepazljivost in neinformiranost posameznika na najvišjih mestih med razlogi za vdore v informacijski sistem podjetja, zaradi okužb z zlonamerno programsko opremo in uhajanja občutljivih informacij. Zato je tudi največji izziv pri oblikovanju informacijske varnosti v podjetju prepoznati varnostne ranljivosti posameznikov in jih preoblikovati v tako imenovane prve obrambne linije vsakega podjetja (Moore, 2003).

Ljudje smo spontani, čustveni in nepredvidljivi. Večina zaposlenih, razen varnostnih strokovnjakov, ki v podjetju skrbijo za informacijsko varnost, je pretežno osredotočena zgolj na svoje področje dela in izvajanje nalog, zaradi česa niti ne opazijo morebitnih varnostnih tveganj in se tudi ne zavedajo svojih ravnanj, ki lahko utegnejo, če so nepravilne oziroma niso v skladu z varnostno politiko podjetja, vplivati na izgubo informacijske varnosti podjetja. Varnost in svoboda posameznika sta tudi na informacijskem področju obratno-sorazmerni, seveda ni namen različnih strokovnjakov, ki skrbijo za informacijsko varnost v podjetju, ustvariti toge in militantne klime, ampak vseeno se moramo vsi zavedati, da nevarnost neprestano preti, zato je bistveno, da smo ozaveščeni glede pomembnosti varovanja informacij, to pa zagotavljamo s primernimi izobraževanji in napotki ter smernicami za delo.

Pomembna je vloga varnostne ozaveščenosti v procesu vzpostavljanja informacijske varnosti in vidik psihosocialnih dejavnikov posameznikov v celotnem procesu. Ozaveščenost uporabnikov informacijske tehnologije je ključnega pomena pri zagotavljanju učinkovitosti varnostnih procesov v okolju podjetja. Lobnikar, Prislan, Markelj in Banutai (2014, str. 345) so v svoji empirični raziskavi o informacijsko-varnostni ozaveščenosti v javnem in zasebnem sektorju v Sloveniji ugotovili, da se kljub dokazanemu pomenu preventivnih aktivnosti programi informacijsko-varnostnega izobraževanja in usposabljanja zaposlenih še vedno v veliki meri nanašajo zgolj na usmerjene skupine znotraj organizacijske strukture, medtem ko je sodobna tehnologija vpletena v delo skoraj vsakega posameznika.

Tukaj pa se kaže problem, saj te skupine pogosto zaključujejo višji predstavniki podjetja, kot so direktorji, managerji, vodje oddelkov. Posamezniki ali zaposleni, kot jih v nadaljevanju magistrskega dela tudi pojmujem, imajo na višjih ravneh organizacijske strukture podjetja pridobljeno vsaj osnovno znanje o informacijski varnosti in že v osnovi predstavljajo manjše

varnostno tveganje kot zaposleni na nižjih ravneh organizacijske strukture podjetja, ki so tudi po navadi najštevilčnejši predstavniki podjetja.

Ti posamezniki se premalokrat zavedajo, da je že eden napačen oziroma nepremišljen klik ogrozi informacijsko varnost podjetja. Zato je bistveno neprestano varnostno ozaveščanje zaposlenih. Neugodna razkritja občutljivih informacij in morebitna izguba podatkov pa podjetju prineseta velike stroške in posledično tudi izgubo ugleda in morebitno izgubo tržnega deleža. Bistven je način, na katerega se bo posameznik v podjetju odzval, igral glavno vlogo pri varovanju podjetja, varovanju občutljivih podatkov in navsezadnje tudi pri varovanju osebnih podatkov svojih sodelavcev in sodelavk. Zato so ustrezno ozaveščeni posamezniki v podjetju ključ do informacijske varnosti, to »ozaveščenost« med posamezniki pa je zaradi različnih človeških faktorjev vse prej kot lahko doseči.

Namen magistrskega dela je s pomočjo domače in predvsem tuje strokovne literature proučiti in jasno opredeliti vlogo posameznika pri zagotavljanju informacijske varnosti. Raziskati želim, zakaj imamo posamezniki tako različne poglede na informacijsko varnost, kakšna je prava mera med varnostjo in svobodo zaposlenih in kateri so tisti človeški faktorji, ki so najbolj pomembni pri oblikovanju in zagotavljanju informacijske varnosti. Predvsem pa želim jasno opredeliti, kakšno vlogo naj posameznik igra pri zagotavljanju informacijske varnosti v podjetju. Na podlagi lastnih izkušenj osveščanja posameznikov o informacijski varnosti in z različnimi raziskavami ter pogledi avtorjev želim vsaj malo pomagati k boljšemu razumevanju pomembnosti osveščanja posameznikov o sami informacijski varnosti ter opredeliti, kakšno vlogo naj posameznik igra pri zagotavljanju informacijske varnosti.

Cilj magistrskega dela je skozi posamezne sklope poglobiti obstoječa znanja glede same vloge posameznika pri zagotavljanju informacijske varnosti in spodbuditi uporabo različnih ugotovitev v praksi.

Magistrsko delo v prvem delu vsebuje poglobljen teoretično-analitičen pregled strokovne literature, raziskav in člankov domačih in tujih strokovnjakov s področja informacijske varnosti. Za lažje razumevanje obravnavane tematike bo v tem delu predstavljena tudi raziskava o informacijski varnosti v slovenskem prostoru. Ta del je nastal s pomočjo opisne metode in metode komplikacije, s katero bom združil spoznanja različnih avtorjev s področja informacijske varnosti.

Drugi del magistrskega dela pa temelji na kvalitativni raziskavi na področju vloge posameznika v informacijski varnosti, v kateri bom skušal strokovno literaturo obravnavane tematike povezati s trenutnimi razmerami v podjetjih v slovenskem prostoru. V zadnjem delu magistrskega dela pa bo izvedena kvalitativna raziskava s pomočjo globinskih polstrukturiranih intervjujev, s katerimi bom skušal raziskati in ugotoviti, ali obstajajo kakšne razlike v vlogi posameznikov pri zagotavljanju informacijske varnosti med podjetji v različnih panogah različnih velikostih.

Pri izdelavi magistrskega dela bom uporabil tako teoretična znanja, ki sem jih pridobil v okviru podiplomskega študija na Ekonomski fakulteti, smer poslovna informatika, kot tudi vsa praktična znanja, ki sem jih pridobil na področju usposabljanja in osveščanja uporabnikov o sami pomembnosti informacijske varnosti.

Magistrsko delo je sestavljeno iz treh glavnih poglavji, sama tematika pa je razdelana v njegovih podpoglavjih. V uvodnem poglavju predstavljam obravnavano problematiko in opredeljujem, kaj resnično pomeni informacijska varnost, predstavljam različne definicije avtorjev in opisujem, od kod segajo njeni začetki in zakaj je dandanes v podjetjih tako zelo pomembna. V tem poglavju nadaljujem tudi z opredelitvijo same informacijske varnostne kulture, ki je sestavni del informacijske varnosti v vsakem podjetju. Za lažje razumevanje obravnavane tematike se prvo poglavje zaključuje z raziskavo o informacijsko varnostni ozaveščenosti v Sloveniji. Drugo poglavje je sestavljeno iz več podpoglavji in ta v celoti opredeljujejo vlogo posameznika v informacijski varnosti. V pripadajočih podpoglavjih predstavljam, zakaj je posameznik temeljni dejavnik informacijske varnosti in zakaj je ob enem tudi glavni vir ogrožanja varnosti informacij, nadaljujem z opredelitvijo varnostnega vedenja posameznikov ter izpostavljam in pojasnjujem ključne elemente, ki vplivajo na izboljševanje posameznikovega varnostnega vedenja. V tem poglavju je opisano, zakaj je človeški dejavnik v obravnavani tematiki tako zelo pomemben, kateri so tisti ključni, ki vplivajo na varnostno vedenje posameznika, posebna pozornost bo tudi namenjena faktorju starosti in ravni faktorja vključenosti posameznikov v varnostno politiko podjetja. Poglavje se zaključuje z večno problematiko – razkorakom med managerji in uporabniki glede zaznavanja informacijske varnosti.

V zadnjem poglavju magistrskega dela je izvedena kvalitativna raziskava s pomočjo globinskih polstrukturiranih intervjujev, za katere je značilno, da so vprašanja že vnaprej oblikovana, intervjuvancu pa pri odgovorih pušča nestrukturiran oziroma prost odgovor. Najprej opredeljujem, zakaj je kvalitativna analiza v mojem magistrskem delu pomembna. Nadaljujem z opredelitvijo globinskih polstrukturiranih intervjujev ter utemeljujem, zakaj je ta oblika intervjuja tudi najprimernejša. V podpoglavju Potek raziskave opredeljujem velikost vzorca, opomnike ter podajam končno analizo podatkov. Rezultati raziskave so podani po posameznih tematskih sklopih. V zadnjem podpoglavju opredeljujem ugotovitve ter morebitne domneve, ki so se vseskozi oblikovale skozi celotno kvalitativno analizo.

1 OPREDELITEV INFORMACIJSKE VARNOSTI

1.1 Uvod v informacijsko varnost

Informacijska tehnologija je dandanes prisotna skoraj vsepovsod in z njenim razmahom ter prodorom v različne dejavnosti, predvsem tiste, ki so upravnega in poslovnega značaja, se vedno znova in znova odpirajo številna varnostna vprašanja, katera ogrožajo tudi informacije, ki so zaupnega značaja. Dejstvo je, da informacije, ki so natisnjene v različnih papirnih

oblikah, izpodrivajo podatke v elektronski obliki. Ti prinašajo številne prednosti, a hkrati povečujejo potencialno nevarnost manipulacije, če pravočasno ne poskrbimo za ukrepe, ki bi le te informacije zaščitile (Jerman & Blažič, 2004).

De Leeuw (2007) v svojem članku navaja, da informacijska družba temelji na civilni uporabi varnostnih orodij in tehnologij, ki v danem času prispevajo k razvoju novih tehnologij. Pojav interneta je navdihnil različne interese oz. vizije posameznikov in družbe. Internet prinaša neomejen pretok informacij, a vendar prinaša tudi številna varnostna vprašanja, ki se neprestano spreminjajo.

Spodnja tabela prikazuje rabo interneta po svetu in populacijsko statistiko na dan 31. marec 2017. Skoraj polovica ljudi na svetu uporablja internet, prebivalci Azije s 50,1 % predstavljajo največji delež uporabnikov interneta, nato ji s 17,0 % sledimo prebivalci Evrope.

Tabela 1: Svetovna internetna uporaba in populacijska statistika na dan 31. marec 2017

World Regions	**Population (2017 Est.)**	**Population % of World**	**Internet Users (f/m) on 31.mar. 2017**	**Penetration Rate (% Pop.)**	**Growth % 2000-2017**	**Internet Users %**
Africa	1.246.504.865	16,6	353.121.578	28,3	7.722,1	9,4
Asia	4.148.177.672	55,2	1.874.136.654	45,2	1.539,6	50,1
Europe	822.710.362	10,9	636.971.824	77,4	506,1	17,0
Latin America / Caribbean	647.604.645	8,6	385.919.382	59,6	2.035,8	10,3
Middle East	250.327.574	3,3	141.931.765	56,7	4.220,9	3,8
North America	363.224.006	4,8	320.068.243	88,1	196,1	8,6
Oceania / Australia	40.479.846	0,5	27.549.054	68,1	261,5	0,7
World total	7.519.028.970	100,0	3.739.698.500	49,7	936,0	100,0

Vir: Internet world stats, world internet usage and statistics, 2017

De Leeuw (2007) navaja, da trend širjenja škodljivih programskih oprem preko interneta dokazuje, da trenutne varnostne prakse tako na ravni posameznikov kot tudi na ravni organizacij niso zadostne. In ko enkrat govorimo o informacijski tehnologiji, ki jo povezujemo s trendom širjenja škodljivih programskih oprem in z odpiranjem varnostnih vprašanj, govorimo o informacijski varnosti. Von Solms (2009) informacijsko varnost opredeljuje kot vedno spreminjajočo in razvijajočo se aktivnost, ki pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. Avtorji Albrechtsen, (2007), Ashenden, (2008) & Goh, (2003) v svojih delih navajajo, da je informacijska varnost sposobnost varovanja podatkov tako na ravni posameznika kot tudi organizacije pred nepooblaščenim dostopom ali njenim

spreminjanjem, ob tem pa se morajo zagotoviti razpoložljivost, zaupnost in celovitost informacij.

Mednarodna organizaciji za standardizacijo (*ang: International Organization for Standardization, ISO)* izdaja tudi standard ISO 27001 (2016) v katerem so zapisani glavni cilji informacijske varnosti, to so zaščita zaupnosti informacij, zaščita celovitosti informacij ter zagotavljanje pravočasne razpoložljivosti informacij avtoriziranim uporabnikom. Za navedbo osnovnih treh ciljev v informacijski varnosti pogosto uporabimo naziv triada CIA, ki ga združujejo kratice v angleščini (C – *confidentiality*, I – *integrity*, A – *availability*). Pri ključnih poslovnih procesih lahko organizacije osnovne tri cilje informacijske varnosti dopolnijo še z določitvijo različnih stopenj ostalih tudi pomembnih ciljev, ki so zagotavljanje overjanja in neovrgljivosti postopkov ter nadzor dostopa. Pri implementaciji osnovnih treh ciljev (triade CIA) v organizacije običajno določijo želeno stopnjo varnosti. To pomeni, da za vsak poslovni proces, ki se na ravni organizacije izvaja, se določi stopnjo zahteve po zaupnosti, celovitosti in razpoložljivosti informacije in samega sistema.

V praksi pa se moramo zavedati, da je določitev stopnje osnovnih treh ciljev informacijske varnosti precej kompleksna, saj si cilji v nekaterih primerih nasprotujejo. Lep primer je, če je naša organizacija odvisna od razpoložljivosti do spletnega dostopa, ki organizaciji omogoča neprestano in neprekinjeno poslovanje. To je možno zagotoviti s porazdeljeno vzpostavitvijo geografskih lokacijskih strežnikov, ki v prvi vrsti odpravljajo morebitne motnje, a se s tem tudi poveča možnost za morebitne napade, s čimer še bolj ogrozimo druga dva osnovna cilja informacijske varnosti, zaupnost in celovitost informacij.

1.1.1 Zgodovina informacijske varnosti

Ob prvih vdorih v računalniške sisteme se je začelo govoriti in razmišljati, kako te vdore preprečiti oziroma jih onemogočiti, začelo se je govoriti o informacijski varnosti, ki bi delovala kot neko vodilo preventivnih ukrepov za zmanjševanje tveganja morebitnih vdorov. Lynett (2015) informacije primerja z ribami, ki »tečejo« skozi morje, morje pa primerja z računalniškimi sistemi, ob tem pa pozablja na smiselnost primerjave, saj je rib zaradi različnih naravnih katastrof in pojavov, kot je globalno segrevanje, v morjih vse manj, informacij pa je v računalniških sistemih čedalje več.

Že v letu 1960 so organizacije začele posvečati večjo pozornost informacijski varnosti. Največji varnostni pomisleki so bili na dostopnih točkah, saj je lahko vsak, ki je imel splošno računalniško znanje, vdrl v sistem oz. v organizacijo in začel začasno dostopati do informacij občutljive narave. V ta namen so se oblikovale varnostne zaščite in gesla. V letu 1970 ni bilo nobenega ogromnega globalnega omrežja, ki povezuje vsako napravo v omrežje. Takrat so se velike organizacije in predvsem vlade, začele povezovati preko telefonskih linij. Ljudje so začeli vdirati v telefonske linije, ki so bile povezane z računalniki, da bi se dokopali do podatkov. V teh letih so se pojavile tudi prve skupine hekerje.

V osemdesetih letih prejšnjega stoletja je pojem »heker« že prešel v mednarodno kriminalno problematiko, saj omenjenim sistemom informacijske varnosti ni uspelo slediti stalnemu razvoju pametnih pristopov, ki so jih skupine hekerjev uporabile za vdor v računalniške sisteme. Posledica je, da je to desetletje kasneje ušlo v dobo zlonamerne programske opreme. Leta 1986 je bil tudi zaznan prvi računalniški virus imenovan »Brain«. V devetdesetih letih prejšnjega stoletja se je začela oblikovati sodobna industrija informacijske varnosti. Ljudje so začeli svoje osebne identitete prenašati na splet, vedno več je bilo virusov in groženj, v tem obdobju pa so se tudi pojavili dandanes nam dobro znani »sledilni piškotki« ki oglaševalskim omrežjem omogočajo sledenje in nadzorovanje spletnih uporabnikov (Lynett, 2015).

Vlade so že desetletja sledile in spremljale spletne kriminalce, vendar je bila večina kazni nizka, predvsem v smislu zaplembe računalniške opreme in prepovedi uporabe tehnoloških naprav za določeno časovno obdobje. To se je spremenilo z letom 2000, ko so vlade resnično začele prepoznavati nevarnosti vdiranja. Za preprečevanje oz. zmanjševanje vdorov v računalniške sisteme so se oblikovale resnejše kazni, saj so bili hekerji, ki so bili kaznovani za kibernetsko kriminaliteto priprti tudi več let. Od leta 2010 pa informacijska varnost postane resen globalni problem. Čeprav so strožji kazenski pregoni, požarni zidovi in protivirusna programska oprema služili kot odvračilo za kibernetsko kriminaliteto, še vedno niso preprečili hekerjev, da bi to početje opustili. Prav nasprotno, hekerji v tem iščejo nove izzive in so tudi drznejši in inovativnejši pri vdorih v računalniška omrežja.

Na tej točki v zgodovini informacijske varnosti so se strokovnjaki s področja varnosti začeli zavedati, da je najboljši način za zaščito podatkov, da hekerjem ti podatki na kakršen koli način niso dostopni. V ta namen so se pojavile izboljšave na področju šifriranja podatkov, katero je sestavljeno iz več ravni, tudi na digitalnih datotekah, omrežjih in prenosih podatkov. Organizacije se sedaj zavedajo pomembnosti celovite politike varovanja informacij, a ob tem se sprašujem, ali se tudi vsi mi zavedamo, kakšne posledice lahko pustijo nepremišljena dejanja, ki se odražajo kot posledice vdora v našo organizacijo, v kateri smo zaposleni ali pa tudi vdora v našo zasebnost?

1.1.2 Pomembnost informacijske varnosti

Z razvojem tehnologije je v zadnjih nekaj letih mogoče čutiti različne spremembe v našem vsakdanjem življenju. Razvoj tehnologije ukinja in ustvarja nove priložnosti, delovna mesta, zabavo, nove informacije, ki so organizacijam na dosegu roke. Z vsemi temi informacijami, ki se nenehno spreminjajo in izmenjujejo, moramo tako organizacije kot posamezniki pospešiti svojo igro, pri tem pa ob pospeševanju te »igre« ne smemo pozabiti na varnost informacij. Ko ljudje razmišljajo o varovanju informacij oz. o varnostnih sistemih za računalniška omrežja pogosto mislijo, da je dovolj dobra zaščita z geslom in protivirusno programsko zaščito. A resnica o tej varnosti je veliko večja kot tisto, kar ljudje oz. uporabniki vidijo na svojih zaslonih (Bojanc, Jerman-Blažič & Tekavčič, 2015).

Dejstvo je, da mora imeti načrt za zagotovitev varnosti informacijskega premoženja vsaka organizacija. Ko govorimo o informacijskem premoženju, mislimo predvsem na informacije, ki so zabeležene v naših računalniških sistemih. Ne glede na to, ali je načrt za zagotovitev informacijske varnosti napisan na petih ali dvestotih straneh, je proces oblikovanja načrta v obeh primerih podoben. S pisanjem načrta ljudje v organizaciji začnejo razmišljati, katere informacije in procesi so najbolj zaupni in kakšne so lahko posledice ob morebitni njihovi izgubi. Z načrtom se zagotovi informacijsko varnostni okvir z ohranjanjem organizacije na želeni ravni varnosti z ocenjevanjem tveganj, s katerimi se srečuje, njihovim odločanjem ter načrtovanjem in ublaževanjem morebitnih realiziranih varnostnih tveganj. Ob tem pa organizacije ne smejo zanemariti ohranjanje oz. posodabljanje samega načrta.

Mnogo organizacij se prepozno zaveda, da je ključno sredstvo, ki ga varnostni program pomaga zaščititi posamezni podatek. In vrednost organizacije se odraža v podatkih. Na podlagi izkušenj varovanja podatkov lahko trdim, da je dobro podatke razdeliti v različne skupine. Najraje uporabljam razdelitev podatkov v tri skupine:

1. **Podatki o izdelku oz. storitvi** ti podatki vključujejo vse informacije o izdelku oz. storitvi, vključno z načrti, oblikovanjem, patentnimi prijavami, izvornimi kodami in postopkom izvedbe.
2. **Finančni podatki** ti podatki vključujejo vse informacije, povezane s finančnimi evidencami organizacije, tudi finančne načrte in načrte za dodeljevanje sredstev za porabo na posameznih oddelkih.
3. **Podatki o strankah** ti podatki vključujejo vse informacije, povezane s strankami, kot so imena in priimki strank, njihovi stiki, statusi ter ugodnosti.

Zavedati se je treba, da vse te podatke potrebujemo za obstoj organizacije, lahko jih še nekoliko razčlenimo oz. razdelimo še na več skupin, a ob enem se moramo zavedati, da je treba določiti stopnjo varnostne zahteve za vsako skupino podatkov. Stopnja varnostne zahteve posamezne skupine se razlikuje od dejavnosti in trga, na katerem je organizacija prisotna. Zaščita podatkov v resnici pomeni zaščito njihove zaupnosti, celovitost in razpoložljivosti.

Posledica nepravilne oz. neuspešne zaščite vseh treh vidikov se lahko odraža v poslovno-finančni izgubi ali izgubi dobrega imena. Spodaj so podani primeri, ki sem jih spoznal v praksi zaradi posamezne neuspešne zaščite podatkov:

- Spoznal sem, da je neuspešnost pri zaščiti zaupnosti podatkov vodila do razkrijta strank in njihovih osebnih podatkov in s tem povezanih ukradenih številk kreditnih kartic ter osebnih stikov strank.
- Spoznal sem, da je neuspešnost pri zaščiti celovitosti podatkov povzročila posledic vdora zlonamerne programske opreme in vsiljivec je lahko prenesel poslovne skrivnosti k njihovim konkurentom.

- Spoznal sem, da je neuspešnost pri zaščiti razpoložljivosti podatkov vodila do slabe posodobitev podatkov in nezmožnosti ponovne implantacije varnostnih kopij v delovno okolje.

Informacije so vedno ukradene, zamenjane ali posnete v korist osebne koristi ali pohlepa. Na svetu obstaja mnogo različnih izmenjav digitalnih informacij, ki se izvajajo vsako sekundo in vse te informacije je treba z nekega vidika zaščititi. Za zaščito informacij imajo številne organizacije IT oddelke, ki skrbijo za varnost informacij in nadzirajo njihove omrežne sisteme. Vendar se je tukaj treba zavedati, da IT oddelki ne morejo zagotoviti popolne informacijske varnosti. Pri poudarku o pomembnosti informacijske varnosti predvsem igrajo vlogo zaposleni oz. posamezniki v organizaciji, ki z različno stopnjo ozaveščenost o informacijski varnosti tvorijo informacijsko varnostno kulturo in obenem tudi prvo obrambno linijo pred morebitnimi napadi.

Dejstvo je, da organizacije čedalje bolj poudarjajo pomembnost informacijske varnosti v njihovem delovnem okolju. Zato se v podjetjih izvajajo različna informacijska varnostna uvajanja oz. programi, ki povečujejo znanje o varnosti sistemov in podatkov med vsemi zaposlenimi. Njihova pripravljenost oz. zavzetost do učenja o informacijski varnosti v organizaciji pa je odvisna od vzpostavljene medsebojne organizacijske klime.

1.1.3 Upravljanje informacijske varnosti

Informacijska varnost v zadnjih nekaj letih postaja vedno bolj pomembna zaradi njene vsesplošne izpostavljenosti tako v medijih kot v organizacijah. Velikokrat se varnost informacij obravnava le kot tehnični del, malo ljudi pa se zaveda, da ta del predstavlja le polovico varovanja informacij. Najbolj razširjen netehnični del varovanja informacije je upravljanje informacijske varnosti, katera vključuje obvladovanja tveganj, upravljanje morebitnih incidentov, poročanje, spremljanje rezultatov in nadzor ukrepov in odgovornosti. Za zagotavljanje primerne informacijske varnosti je treba opredeliti nivoje in naloge pri upravljanju informacijske varnosti v organizaciji. Naloge je treba razdeliti na različnih nivojih organizacije, iz česar izhajajo pristojnosti in odgovornosti za uspešno zagotavljanje zaupnosti, celovitosti in razpoložljivost informacij v organizaciji (Selan & Bernik, 2008).

Upravljanje informacijske varnosti določa varnostni program, ki služi kot poslovni načrt za zaščito digitalnih sredstev in predvideva skrb za vpeljavo, vzdrževanje in nenehno izboljševanje področja upravljanja informacijske varnosti. Najbolj učinkoviti varnostni programi so tisti, ki so po naravi enostavni, razumevajoči in učinkoviti; v program pa je treba vključiti vse zaposlene na vseh nivojih organizacije. Selan in Bernik (2008) navajata, da vsak program upravljanja informacijske varnosti mora, z namenom ugotovitve doseganja posameznega cilja, imeti definirane meje sprejetja, zavrnitve in odločnosti, ki jih razumejo tudi tisti, ki se z informacijsko varnostjo neposredno ne ukvarjajo. Rezultat učinkovitega upravljanja informacijske varnosti mora vključevati (Selan & Bernik, 2008):

- strateško usklajevanje informacijske varnosti z institucionalnimi cilji,
- tvegani management – ugotavljanje, upravljanje in ublažitev nevarnosti,
- upravljanje virov,
- merjenje uspešnosti – opredelitev, poročanje in uporaba podatkov meritev upravljanja informacijske varnosti.

Eden izmed ključnih elementov upravljanja informacijske tehnologije pa je tudi informacijska varnostna politika, ki tvori združenje praks in pravil, ki določajo, kako naj organizacija upravlja, prenaša in ščiti svoje informacijske vire. Ključnega pomena je predvsem to, da mora biti varnostna politika, ki se izvaja na ravni organizacije, skladna z veljavno zakonodajo na področju varovanja informacij. Z varnostno politiko so v organizaciji določeni minimalni obvezujoči predpisi in pravila tako za celotno organizacijo kot tudi za posamezno delovno mesto in zunanje partnerje oz. sodelavce, ki imajo kakršen koli stik z informacijskimi viri organizacije.

Upravljanje informacijske varnosti lahko razdelimo na dva dela. Prvi je management izvajanja oz. operativni management, ki je temelj informacijske varnosti in zajema bistvene elemente: obvladovanje tveganj, informacijsko varnostno politiko, postopke, standarde, projektno načrtovanje, izhodišča, klasifikacije, izobraževanja in organizacijo. Drugi del pa je management odgovornosti oz. strateški management, kateri vključuje sredstva, financiranje, nadzor ter strateško zastopanje in načrtovanje, ki sta potrebni za sodelovanje v programu informacijske varnosti. Prvi del se predvsem navezuje na vse zaposlene, drugi del bolj na zaposlene na vodilnih funkcijah v organizaciji (Bernik & Selan, 2008).

Človeški viri so še eden izmed pomembnih elementov pri upravljanju informacijske varnosti. Prav vsaka organizacija mora zagotovi, da imajo vsi zaposleni, poslovni partnerji, zunanji izvajalci in tudi kupci omogočen dostop do informacijskih virov organizacije, seveda z različnimi pravili, določili in nivoji dostopa. Zavedati se morajo svojih odgovornosti in dolžnosti, ki so povezane z dostopom do informacijskih virov organizacije. Še predno se zavedajo o svojih odgovornostih in dolžnostih pa mora biti s strani organizacije poskrbljeno oz. zagotovljeno, da so ustrezno izobraženi, usposobljeni in ozaveščeni glede pravilne uporabe informacijskih virov.

Bernik in Selan (2008) v svojem prispevku ugotavljata, da je treba varnost informacijskih tehnologij in rabe informacij umestiti v strateške načrte vsake organizacije. Pripraviti je treba program informacijske varnosti in skladno s predvideno organizacijsko strukturo upravljanja informacijske varnosti opredeliti delovna mesta, ki so kakor koli povezana z odgovornostjo zagotavljanja informacijske varnosti. Le tako bi organizacije s pravilno porazdelitvijo dejavnosti na strateškem in operativnem nivoju poskrbele za zaupnost, celovitost in razpoložljivost informacij.

1.1.4 Varovanje poslovnih informacij

Shapiroin in Varian (1998) informacijo opredeljujeta kot znanje ali podatek, ki ima za podjetje določeno vrednost. Informacije je pravzaprav vse, kar se lahko digitalizira oz. kodira v zaporedje bitov. Dandanes skoraj večina podjetji uporablja elektronsko obliko informacij, saj je le ta predpogoj za prehod v elektronsko poslovanje v sodobnem omrežnem gospodarstvu. Elektronsko poslovanje organizacijam omogoča hitrejše izvajanje poslovnih procesov in hitrejši pretok poslovnih informacij. Slaba stran informacij pa je ta, da se njihova vrednost običajno težko določi.

Crum (2001) navaja, da je prvo pravilo pri zagotavljanju informacijske varnosti to, da organizacija za varovanje ne porabi več od vednosti tistega, kar dejansko varuje. Kar pomeni, da organizacije za varovanje svojih poslovnih podatkov naj ne porabijo več od njihove dejanske vrednosti. Postopek ugotovitve dejanske vrednosti poslovnih informacij pa je odvisen od načina delovanja organizacije na trgu.

Bojanc, Jerman-Blažič in Tekavčič (2015) v svojem delu navajajo, da se vrednost informacije meri s tem, da pomaga podjetju do večje inovativnosti, produktivnosti, kar pomeni, da določa načrt novih produktov oz. procesov, pomaga do učinkovitejšega trženja svojih produktov, boljših finančnih odločitev, boljšega nadzora aktivnosti in procesov; ali pa po drugi strani lahko pomaga pri ravnanju tako s kupci kot zaposlenimi. Nekatere informacije so za organizacije strateškega pomena in jih morajo skrbno zaščititi, saj morebitno njihovo razkritje organizaciji v trenutku pusti posledice, v smislu pridobitve novih konkurentov oz. ponudnikov, zasičenosti trga, zmanjšanje tržnega deleža, prodaje… Zaradi neprestanega razvoja sodobne tehnologije organizacije poslujejo čedalje hitreje, učinkoviteje in ceneje. Zato potrebujejo zmogljivejše, zanesljivejše in stabilnejše informacijske sisteme, ki tudi ščitijo poslovne informacije, ki se med samimi procesi obdelujejo.

Dejstvo je, da imajo informacije v organizacijah določene vrednosti in jih je treba varovati. Na podlagi izkušenj pri varovanju informacij menim, da je najbolj učinkovit sistem varovanja informacij ta, da informacije, na podlagi njihove vrednosti, razdelimo v skupine. Za tiste najbolj ključne oz. najbolj zaupne imamo izoblikovane posebne varnostne protokole, ki določajo kakršno koli transakcijo oziroma vpogled do poslovne informacije. Ti varnostni protokoli so podprti z informacijskimi sistemi in pogosto jih varujejo in vzdržujejo strokovnjaki na področju varovanja podatkov.

Ključnega pomena pri varovanju poslovnih informacij, je tudi to, da znamo novo pridobljene informacije razvrstiti po že izoblikovanih skupinah, saj se po le teh potem določajo varnostni protokoli, ki so odvisni od pomembnosti in zaupnosti poslovnih informacij. Treba pa se je tudi zavedati, da za poslovne informacije, ki so zaupne narave za njihov vpogled ali morebitno transakcijo po navadi potrebujemo bistveno več časa, saj je treba upoštevati in preiti vse varnostne protokole. Zaupnejše kot so informacije, večji so varnostni protokoli in zato za njihov dostop posledično potrebujemo tudi vse več časa. S strani organizacije ni smiselno

vseh informacij zaščititi z dolgimi varnostnimi protokoli, saj jim ni v interesu, da bodo njihovi zaposleni potrebovali veliko časa pri upoštevanju vseh varnostnih protokolov, ki omogočajo dostop oz. vpogled do informacij.

1.2 Informacijska varnostna kultura

Varnostna kultura dandanes postaja čedalje bolj pomembno področje, s katerim se vse pogosteje ukvarjajo tudi vodstveni delavci v različnih podjetjih. Bistvo varnostne kulture je zagotoviti in vzpostaviti na podlagi različnih vedenjskih vzorcev, odnosov, prepričanj in komunikacije nekakšno organizacijsko kulturo. Cooper (2000) varnostno kulturo opredeljuje kot odraz usklajenih organizacijskih prizadevanj, kjer se elementi organizacijske kulture usmerijo k doseganju varnostnih ciljev tako na ravni organizacije, sistematike in delovne aktivnosti. Ko varnostno kulturo organizacije podpremo z informacijskimi varnostnimi ukrepi, začnemo govoriti o informacijski varnostni kulturi. Informacijska varnostna kultura se je razvila na podlagi vedenja, ki je povezano s skrbnim varovanjem poslovnih informacij oz. podatkov.

Rančigaj in Lobnikar (2014) informacijsko varnostno kulturo opredeljujeta kot skupek odnosov, predpostavk, prepričanj, vrednosti in znanja, ki ga imajo zaposleni v odnosu do organizacijskega sistema in postopkov v vsakdanjem delu, odnos pa se predvsem kaže v spremenljivem ali nespremenljivem vedenju v obliki vedenjskih vzorcev ali načinov ravnanja in postopanju, ki kasneje postane način za pravilno urejanje stvari v organizaciji z namenom zaščite informacijske vrednosti.

V ta namen so se oblikovali tudi vsebinski sklopi, ki tvorijo načela informacijske varnostne kulture, le ti pa usmerjajo tako vedenje kot mišljenje ljudi (Organization for Economic Co-operation and Development (OECD), 2002, 9 – 12):

- **Zvestoba** uporabniki se zavedajo potrebe po varovanju informacijskih sistemov in omrežij ter se sprašujejo, kaj lahko storijo za povečanje varnosti.
- **Odgovornost** za varnost informacijskih sistemov in omrežij sloni na vseh uporabnikih, neglede na njihov položaj v podjetju.
- **Dovzetnost** uporabniki pravočasno in primerno odreagirajo, da preprečijo in odkrijejo varnostne incidente.
- **Etika** uporabniki spoštujejo medsebojne interese.
- **Demokracija** varnost informacijskih sistemov in omrežij je v skladu s ključnimi vrednotami demokratične družbe.
- **Ocena tveganj** uporabniki sodelujejo pri ocenjevanju varnostnih tveganj, na podlagi katerih se ugotavljajo morebitne grožnje in slabosti. Določijo tudi spremenljivo raven tveganj.

- **Varnostni načrt in implementacija** element varnosti je ključen element informacijskih sistemov in omrežij – tako uporabniki v svoje varnostne načrte vključujejo tehnične in netehnične ukrepe in rešitve.
- **Varnostni management** uporabniki spoštujejo in so vključeni v celovit pristop zagotavljanja varnosti, vključno z varnostnimi politikami, praksami, ukrepi in postopki, ki so usklajeni in strjeni z namenom, da se ustvari skladen varnostni sistem.
- **Ponovna ocena** uporabniki se zavedajo pomembnosti konstantnega izobraževanja na področju varnosti informacijskih sistemov. Z ocenitvijo in pregledom varnostnih sistemov in omrežij poskrbijo za ustrezne varnostne spremembe varnostne politike, praks, ukrepov in postopkov.

Vloga zaposlenega pri oblikovanju informacijske varnostne kulture pa postaja vse bolj prepoznavna in pomembna, saj je ob neprestanem razvoju informacijsko-komunikacijske tehnologije nujno, da si zaradi visoke stopnje odgovornosti in čedalje večjega zaupanja, zaposleni delijo enake poglede glede na varnost in razumejo svojo vlogo pri izvajanju informacijske varnostne kulture. V nasprotnem primeru se posledice lahko kažejo v nezainteresiranosti zaposlenih pri varovanju poslovnih informacij.

Tudi same organizacije morajo pri oblikovanju informacijske varnostne kulture odigrati pomembno vlogo, saj je ključno na kakšen način zaposlenim ob njihovi zaposlitvi opredelijo njihove vloge. Pri tem pa morajo tudi upoštevati njihovo predhodno znanje in preveriti, ali so njihova lastna prepričanja v skladu z varnostno politiko in informacijsko varnostno kulturo organizacije.

1.2.1 Stopnje informacijske varnostne kulture

V organizacijah obstajajo različne stopnje povezanosti med organizacijo kulturo in informacijsko varnostno kulturo. Lim, Shanton, Maynard in Ahmad (2009) so v svoji raziskavi ločili med tremi stopnjami informacijske varnostne strukture:

1. Informacijska varnostna kultura je v organizaciji ločena od organizacijske kulture in posledično večina zaposlenih ni seznanjena ali sploh ni vključena pri izvajanju različnih varnostni pravil. To je posledično povezano tudi z njihovim slabim znanjem in odrazom do pomanjkanja odgovornosti za razvijanje same informacijske varnostne kulture v organizaciji. Zaradi nizke ravni motiviranosti zaposleni tudi ne znajo pravilno odreagirati, ko pride do varnostnega incidenta. Celotna skrb in odgovornost se prelaga in prepušča IT-oddelku. Na ravni organizacije se na informacijsko varnostno kulturo gleda kot na dodatni strošek, in celotno finančno skrb zanj prepušča IT-oddelku, ki naj bi v okviru finančnega načrta, ki je prvotno namenjen za podporo uporabnikom, tudi poskrbelo za informacijsko varnostno kulturo.

2. Informacijska varnostna kultura predstavlja v organizaciji subkulturo organizacijske kulture, katera se kaže pri večji stopnji ozaveščenosti posameznikov o pomembnosti poznavanja področja informacijske varnosti. Občasno se izvajajo različna usposabljanja za različna področja, ki temeljijo predvsem kot upoštevanje navodil vodstva. Pogosto se usposabljanja izvajajo le na nekaterih ključnih oddelkih v organizaciji in posledica tega se lahko kaže kot oteženo sodelovanje in usklajevanje med oddelki, saj so vrednote informacijske varnosti pretežno vezane na majhno skupino posameznikov, ki v ključnih oddelkih igrajo pomembno vlogo. Nasprotno so zaposleni pri organizacijah, ki so vključeni v stopnjo 2. tipa običajno seznanjeni z varovanjem poslovnih informacij samo na njihovem delovnem mestu. Tudi na ravni organizacije se letno nameni nekaj izdatkov za izboljševanje organizacijske varnostne kulture v organizaciji.

3. Informacijska varnostna kultura je v organizaciji vključena v organizacijsko kulturo, gre za v organizacijah najbolj zaželeno stopnjo, saj je varnostna praksa odgovornost vseh zaposlenih. Organizacije redno posodabljajo in prilagajajo varnostno politiko ter neprestano zagovarjajo visoko stopnjo vključenosti zaposlenih v proces oblikovanja informacijske varnostne kulture. To se kaže kot posledica oblikovanja občutka, da si poslovne informacije ne lasti organizacija, temveč zaposleni, to pa povečuje motivacijo za spoštovanje predpisanih varnostnih pravil. Na stopnji 3. tipa imajo IT-oddelki bistveno več finančnih sredstev za celovitejšo podporo pri oblikovanju informacijske varnostne kulture. V organizacijah se organizirajo različni sestanki tudi na najnižjih ravneh, ki govorijo o pomembnosti vzdrževanja in odpravljanja morebitnih varnostnih problemov in incidentov (Lim *et al*., 2009).

1.2.2 Pomen upravljanja informacijske varnostne kulture

Informacijska varnostna struktura se zaradi številnih dejavnikov nenehno spreminja, zato je treba temu tudi prilagoditi upravljanje. Bistvo je, da organizacije, ko vpeljejo neko spremembo, ki vpliva tako na zaposlene kot same procese, to spremembo konstantno spremljajo in jo posledično nadgrajujejo. Rančigaj in Lobnikar (2014) v prispevku navajata, da je za uspešno upravljanje informacijske varnostne kulture treba upravljati procese na treh nivojih: na ravni organizacije, skupine in posameznika. Na ravni organizacije je pomembno vzpostaviti politike, postopke ter primerjavo natančnih analiz tveganja ter zagotavljanja primernih izdatkov za samo upravljanje informacijske varnostne kulture. Opredeliti in določiti je treba posameznike, ki bodo pri upravljanju informacijske varnostne kulture imeli največjo vlogo in bodo zgled drugim. Na skupinski ravni je ključno vedenje vodstva podjetja ter vzpostavitev medsebojnega zaupanja. Na ravni posameznika pa sta ključna dva dejavnika zagotavljanja informacijske varnostne kulture. Prvi dejavnik predstavlja zavedanje posameznika, kaj in na kakšen način lahko pripomore k boljši informacijsko varnostni kulturi. Drugi dejavnik pa je etičnost posameznika oziroma pripravljenost vedenja posameznika v skladu s pravili organizacije.

Informacijsko varnostno kulturo je mogoče upravljati v skladu s PDCA modelom (ang. *plan, do, check, act*), katerega značilnost je, da najprej analiziramo obstoječe stanje, planiramo naslednje ukrepe, nato sledi implementacija teh ukrepov ter posledično ocenjevanje izvedenih ukrepov. Pri PDCA modelu je ključen proces neprestanega izboljševanja oziroma trajnostnega razvoja tako kot na področju informacijske varnostne kulture v sami organizaciji. Pri samem procesu upravljanju pa ne smemo zanemariti tudi dejavnike, ki vplivajo na posameznikovo vedenje, ki se odražajo v osebnih vrednotah, občutku odgovornosti do sodelavcev in organizacije ter zaznavanju težav, s katerimi se srečuje pri upoštevanju varnostnih določil in pravil v sami organizaciji (Rančigaj Lobnikar, 2014).

Po drugi strani pa Workman, Bommer in Straub (2008) ugotavljajo, da so na voljo številni ukrepi, kako izboljšati varnostno vedenje ljudi ter na kakšen način, se naj v organizaciji oblikuje proces upravljanja informacijske varnostne kulture, a ti v praksi niso prinesli želenih pričakovanj. Ugotovili so, da se kljub obstoju različnih ukrepov, kako izboljšati varnostno vedenje ljudi, ti v praksi premalokrat implementirajo oziroma je njihovo prehajanje v prakso zaradi različnih dejavnikov oteženo in zato posledično lahko tudi pomanjkljivo. Zaradi tega se strokovnjakom na področja varovanja podatkov vse pogosteje postavlja vprašanje, kako zmanjšati razliko oziroma velik razkorak med ozaveščenostjo o informacijski varnostni in dejanskim ukrepanjem ali spremembo vedenja. Strokovnjaki na tem področju poudarjajo, da se znanje posameznikov o varnostni kulturi izboljšuje, a obenem se pojavlja nova problematika, saj posamezniki vedo, kaj in kako morajo ravnati, ko pride do določnih varnostnih vprašanj, ampak tega preprosto ne naredijo v smislu »znam in vem, kako, ampak ne delam tako« to pa je še vedno eden izmed temeljnih raziskovalnih vprašanj, ki še do danes niso bili v celoti obravnavani in raziskovani (Workman, Bommer in Straub, 2008).

1.3 Informacijsko varnostna ozaveščenost v Sloveniji

Informacijsko varnostna ozaveščenost zaposlenih v organizaciji predstavlja eden izmed ključnih členov pri vzpostavljanju celovite informacijske varnosti. Za zagotavljanje ustrezne stopnje varnosti informacij v organizaciji je treba tudi poskrbeti za ustrezen nivo uporabniške ozaveščenosti na področju informacijske varnosti. Dandanes se informacijska varnost iz tehničnih rešitev vse bolj nagiba k osredotočenosti na socialno tehnične vidike, ki tudi podarjajo pomembnost vedenja zaposlenih pri zagotavljanju informacijske varnosti. Iz tega lahko sklepamo, da je uspeh organizacije v veliki meri odvisen od tega, kako zaposleni opravljajo svoje delo in pri tem upoštevajo varnostna pravila in ukrepe organizacije. Če želimo, da zaposleni svoje delo opravljajo varno in uspešno, je v organizaciji ključen proces izobraževanja in širjenja ozaveščenosti o določenih problematikah in rešitvah. Tako sta tudi pri vzpostavljanju informacijske varnosti proces izobraževanja in širjenje ozaveščenosti ključna varnostna dejavnika, ki skupaj z varnostno politiko podjetja, katera mora biti prilagojena potrebam in sposobnosti organizacije ter zaposlenim, tvori celotno informacijsko varnost.

Za oblikovanje visoke stopnje ozaveščenosti o informacijski varnosti med zaposlenimi pa so potrebni programi, za katere na podlagi izkušenj lahko rečem, da morajo v prvi meri spodbuditi interes pri vseh udeležencih, saj ne glede na to, kako jasen, razumljiv in dosleden je program, se brez interesa udeležencev vsa znanja, novosti in prakse, pridobljene v programu, le stežka implementirajo v delovno okolje udeležencev.

Na podlagi večkratnih usposabljanj udeležencev o pomembnosti informacijske varnosti v organizaciji lahko trdim, da znanje o ukrepih, posledicah in verjetnosti incidentov res povečuje pripravljenost zaposlenih k upoštevanju pravil, a po drugi strani to znanje samo po sebi še ne povzroči spremembe v posameznikovem obnašanju in vedenju, saj je le to še vedno odvisno od stopnje motivacije in namena posameznika. Izvajalci različnih programov ozaveščanja zaposlenih pa se morajo zavedati, da gre pri oblikovanju informacijske varnosti v organizaciji za dinamične procese in te je treba zaradi nenehnih sprememb spreminjati, obnavljati in posodabljati.

Lobnikar, Prislan, Markelj in Banutai (2012) v svoji raziskavi o informacijski ozaveščenosti v slovenskem prostoru, v kateri je sodelovalo 498 udeležencev tako iz javnega kot zasebnega sektorja, ugotavljajo, da je ozaveščenost uporabnikov o informacijski tehnologiji ključnega pomena pri zagotavljanju učinkovitosti varnostnih procesov v organizacijskem okolju, vendar se kljub dokazanemu pomenu preventivnih aktivnosti, različni programi informacijsko varnostnega izobraževanja in usposabljanja zaposlenih še vedno v veliki meri nanašajo zgolj na usmerjene skupine znotraj organizacijske strukture, medtem ko je sodobna tehnologija vpletena v delo skoraj vsakega posameznika. Ugotavljajo tudi, da zaposleni stremijo k dodatnim izobraževalnim procesom na področju informacijske varnosti, posledično se tudi dviguje stopnja ozaveščenosti med zaposlenim, vendar podarjajo, da so ti izobraževalni programi v največji meri odvisni od odločitev managerjev na odločilnih pozicijah v organizacijski strukturi podjetja.

Njihova raziskava ugotavlja povezavo korelacij med znanjem, vedenjem in odnosom zaposlenih. Za najpomembnejši dejavnik ozaveščenosti se je izkazalo znanje, ki pogojuje tako vedenju uporabnikov kot odnosu do varne uporabe informacije tehnologije. Rezultati raziskave so pokazali, da se s povečevanjem znanja povečujeta pozitivno varnostno vedenje in pozitiven odnos uporabnikov. Občutek odgovornosti je v veliki meri pogojen z osebno pripadnostjo organizaciji, poznavanjem varnostnih pravil in postopkov ter doslednostjo pri nadziranju in sankcioniranju kršitev (Lobnikar, Prislan, Markelj & Banutai, 2012).

Lobnikar s sodelavci (2012) v svoji raziskavi tudi ugotavlja šibke točke v znanju o varnem vedenju v delovnem okolju. Prva šibka točka je, da uporabniki slabo poznajo pravila s področja informacijske varnosti v svoji organizaciji. Druga šibka točka je, da uporabniki ne poznajo vseh pravil in postopkov varnostnega kopiranja podatkov in o tem priča neizkušenost uporabnikov in miselnost, da je to odgovornost IT oddelka. Tretja šibka točka je, da uporabniki ne vedo, na kakšen način naj odreagirajo, ko so udeleženi v varnostnem incidentu. Posledično so avtorji tudi mnenja, da še vedno obstaja potreba po krepitvi znanja o

informacijskem varnostnem vedenju, saj je kar 29 % anketirancev v raziskavi zbralo manj kot 6 točk od možnih 10-ih. To pa v podjetjih predstavlja relativno visoko stopnjo varnostnega tveganja. Avtorji tudi ugotavljajo, da je vedenje anketirancev ob uporabi tehnologije sicer v povprečju doseglo boljše rezultate kot njihovo znanje, največje pomanjkljivosti pa se kažejo ravno v odsotnosti upoštevanja osnovnih informacijsko varnostnih pravil. Odnos zaposlenih do informacijske varnosti ocenjujejo kot dober.

Lobnikar s sodelavci (2012) v svoji raziskavi ugotavlja, da je trenutno znanje zaposlenih o varnostni politiki pomanjkljivo in bi bilo temu področju v prihodnosti treba nameniti več časa in vključevati prav vse zaposlene v organizaciji, a hkrati poudarjajo, da samo to področje ni zadostno vodilo za oblikovanje informacijske varnosti v organizaciji.

2 INFORMACIJSKA VARNOST IN VLOGA POSAMEZNIKA

2.1 Posameznik kot temeljni dejavnik informacijske varnosti

Pri izvajanju svojih rešitev za varnost informacij se organizacije običajno najprej osredotočajo na tehnične in postopkovne varnostne ukrepa, toda za učinkovito vzpostavitev informacijske varnosti, se je treba predvsem osredotočiti na uporabnike in ti se morajo zavedati in uporabljati razpoložljive varnostne ukrepe, ki so določeni v varnostni politiki in navodilih za varovanje informacij v svoji organizaciji. V nasprotnem primeru, če se organizacije ne osredotočijo tudi na same uporabnike, so predpisani varnostni ukrepi tako rekoč brezpredmetni oz. brez prave osnove za zaščito organizacije (Puhakainen, 2006).

Ob različnih aferah, ki so priča varnostnim incidentom na področju varovanja podatkov in ob nedavnih množičnih vdorih v informacijske sisteme organizacij, smo ponovno spoznali, da je človek najkritičnejši element informacijske varnosti, ki zaradi svojega neznanja in z nepremišljenim dejanjem izniči večino ali celo vse organizacijske, tehnološke, tehnične in fizične ukrepe varovanja podatkov organizacije. Puhakainen (2006) v svoji raziskavi poudarja, da želene ravni informacijske varnosti ni mogoče doseči le z uporabo tehničnih in postopkovnih varnostnih ukrepov, zato se je treba osredotočiti na uporabnike, in jih neprestano motivirati, izobraževati ter vključevati v različne varnostno-izobraževalne programe. Organizacije preprosto podcenjujejo pomembno vlogo uporabnika pri zagotavljanju želene ravni informacijske varnosti. Sedaj se postavlja vprašanje, kako opredeljujemo uporabnika oziroma posameznika.

Uporabnika oziroma posameznika predstavljajo vsi zaposleni, pogodbeni partnerji, zunanji sodelavci, svetovalci skratka vsi, ki so tako ali drugače v stiku z informacijskim sistemom organizacije. Ti lahko ogrozijo integriteto in zaupnost podatkov ali s svojim nenamernim in malomarnim delovanjem prekršijo pravila informacijske varnosti in v ta namen oblikujejo kakršni koli varnostni incident, ki bi pustil škodljive posledice organizaciji. Čedalje bolj pa se pojavlja tudi trend, da organizacije, ki imajo visok nivo varovanja informacij, med

uporabnike oziroma posameznike vključujejo tudi svoje stranke. Lep primer so banke, katere svoje stranke neprestano opozarjajo k varovanju svojih podatkov ter pravilno rabo spletnih bančnih storitev zaradi izvirnih bančnih goljufij.

Antončič (2015) v svojem delu navaja, da je v praksi velik del kršitev varne uporabe podatkov prav rezultat malomarnosti ali pomanjkljivega znanja uporabnikov. Ob tem pa tudi dodaja, da se v organizacijah tudi pojavljajo naklepne kršitve varovanja podatkov s strani posameznikov, ki se s svojim namernim posredovanjem določenih podatkov nepooblaščenim osebam ali interesnim skupinam skušajo na takšen ali drugačen način okoristiti. Zaposleni, ki posredujejo te informacije, se morajo zavedati, da lahko postanejo objekt napada zainteresiranega napadalca tudi iz vrste organizacije ali morebitnega zunanjega sodelavca. Ti napadi so po navadi premišljeno izoblikovani, tako da jih sama žrtev napada v prvi vrsti sploh ne zazna. Iz tega lahko sklepamo, da morajo organizacije pri načrtovanju različnih varnostnih ukrepov oziroma protiukrepov upoštevati tudi to, da morajo vse zaposlene, ki imajo dostop do najbolj občutljivih oziroma ključnih informacij, obravnavati kot varnostno zelo izpostavljene osebe, te osebe pa morajo v prvi vrsti izražati visoko organizacijo pripadnost in motiviranost za varovanje samega delovnega mesta. Naloga organizacije je, da za ta »delovna mesta« najprej natančno opredeli naloge in jih nato z ustrezno načrtovanimi in izvajanimi ukrepi tudi zaščiti (Antončič, 2015).

Za učinkovit varnostni sistem organizacije je treba skozi oblikovanje informacijsko varnostne kulture vključevati čisto vse posameznike oziroma uporabnike, ki so tako ali drugače povezani z organizacijo. Zavedati se je treba, da se vloge posameznikov v organizaciji razlikujejo, in tudi osebnosti med posamezniki znotraj organizacije so različne, zato je pomembno pri oblikovanju varovanja podatkov posameznike obravnavati kar se da individualno. To prinese obilico stroškov in s časovnega vidika je izredno potratno, ampak z individualnim pristopom se posamezniku resnično da vedeti, da mora biti za varnost organizacije tudi z njegove strani poskrbljeno in da je tudi vsak posameznik pomemben člen pri oblikovanju celotne informacijske varnosti. To lahko potrdim tudi iz izkušenj. Posameznik začuti večjo pripadnost organizaciji, kadar se ga obravnava na individualni ravni, saj mu s tem pokažemo, da predstavlja pomemben člen v delovanju organizacije.

Velikokrat organizacije najamejo zunanje izvajalce, ki pridejo v podjetja z namenom izvajanja varnostno-izobraževalnih programov, ampak ti programi v praksi niso najcenejši in so v prvi vrsti namenjeni posameznikom na odločilnih položajih v organizaciji. Najranljivejši člen pri zagotavljanju informacijske varnosti, pa so neinformirani zaposleni oziroma zaposleni, ki nimajo pridobljenega znanja na področju varovanju podatkov na njihovih delovnih mesti.

Vzemimo primer, da organizacija zaposluje 50 ljudi, od tega je 10 ljudi zaposlenih na vodilnih položajih organizacije. Za te zaposlene tudi organizirajo odlične varnostno-izobraževalne programe, ki so v prvi vrsti namenjeni varovanju podatkov in oblikovanju varnostne kulture. En ali dva predstavnika od 10 ljudi, ki so se udeležili izobraževalnega programa, na sestanku

posredujejo te informacije ostalim zaposlenim, ki ne zasedajo vodilnih položajev v organizaciji. Problem takšnega načina oblikovanja informacijske varnosti v organizaciji je, da posamezniki dobijo splošne informacije o varovanju podatkov, katere mogoče v prvi vrsti sploh niso relevantne za njihovo delovno mesto, seveda je posameznik na tej stopnji potem tudi nezainteresiran za iskanje in odkrivanje morebitnih varnostnih vprašanj, ki se specifično nanašajo na njegovo delovno mesto. Vodstvo podjetja je le malokrat pripravljeno po izobraževalnih sestankih na temo varovanja informacij še individualno preveriti in izobraziti posameznika za njegovo delovno mesto. Zaradi takšnega načina dela so se oblikovali standardi oziroma družina standardov ISO/IEC 27000, katerih glavna naloga je zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij ter obseganje najboljših praks in priporočil, vezanih na upravljanje varovanja informacij, ter tveganja in kontrole v kontekstu celovitega sistema upravljanja informacijske varnosti. Družina standardov ISO/IEC 27000 pa v prvi vrsti opredeljuje tudi varnostne vidike človeških faktorjev in njihovih vlog.

Primer opredelitve v standardu ISO/IEC 27002 za določila glede obnašanja in načina določevanja izvedbe kontrole informacijske varnosti ter priporočil za izvedbo varnostnega ozaveščanja najdemo v poglavju »Varnost človeških virov« v točki 7.1 z naslovom »Varnost človeških virov pred zaposlitvijo«: Organizacija mora pri zaposlovanju tako stalnega kot tudi začasnega osebja vzeti v obzir tudi varnostno odgovornost osebe, katera se bo s podpisom pogodbe o zaposlitvi in drugih morebitnih sporazumih ter z opredelitvijo varnostne vloge, zavezala k skrbni in vestni uporabi razpoložljivih informacij ter k upoštevanju varnostnih ukrepov in pravil organizacije (ISO/IEC 27002, 2013).

2.1.1 Posameznikov pogled na informacijsko varnost

Vloga uporabnikov postaja vse pomembnejša pri oblikovanju informacijske varnosti v organizaciji. Zato morajo uporabniki v tej zgodbi odigrati tudi pomembno vlogo pri oblikovanju tovrstne varnosti, s katero bi preprečili nezaželene incidente. Uporabniki lahko že s preprostimi varnostnimi ukrepi, kot so odjava iz sistema ob njihovi odsotnosti, pravilna izbira in menjava gesel, povečana pozornost pri odpiranju spletne pošte, izogibanje uporabi brez licenčne programske opreme in pazljiva uporaba sredstev v organizaciji in zunaj nje, zmanjšajo stopnjo tveganja pojavitve morebitnih varnostnih incidentov. Zato je potrebno kakršne koli morebitne pomanjkljivosti v zvezi z varnostjo informacij, ki se nanašajo na vedenje uporabnikov, ne le pojasniti posameznikom z njihovimi napakami in kršitvami, temveč z ustreznimi mehanizmi vzpostaviti v posameznikovem kontekstu določen nivo varnostnega vedenja. Za pravilno upravljanje informacijske varnosti je treba razumeti funkcijo uporabnikov znotraj njihovega delovnega konteksta in to funkcijo tudi posamezno obravnavati z vidika varovanja informacij. Dejstvo je, da so človeške ovire bolj nezanesljive kot tehnološke, kar predstavlja izziv za upravljanje varnosti uporabnikov. Vedno se pojavljajo vprašanja, kakšne ukrepe je treba uporabiti in izvajati tako na ravni organizacije kot na ravni posameznika, da bi uspešno vplivali na vedenje in zavedanje samih uporabnikov? Za odgovor na zastavljeno vprašanje je najboljše najprej analizirati posameznikove poglede na informacijsko varnost v podjetju.

Albrechtsen (str. 277, 2007) v svojem delu navaja, da je uporabniška vloga pri oblikovanju informacijske varnosti v organizacijah izrednega pomena, saj zaradi pomanjkanja znanja in posledično nepremišljenih dejanj predstavlja najšibkejši člen v informacijski varnostni verigi, ob tem pa poudarja, da igra pri odzivanju na varnostne incidente pomembno vlogo tudi človeški faktor. Avtor navaja, da je bilo področje informacijske varnosti do sedaj bolj pokrito s tradicionalno usmeritvijo v tehnološke probleme in rešitve, to področje pa do sedaj ni namenilo večje pozornosti socialno-organizacijskim vidikom in človeškim faktorjem. Z vidika posameznika je informacijska varnost samo ena izmed številnih zahtev delovnega dne, zato bo večina uporabnikov verjetno spregledalo varnostne ukrepe, če je to mogoče, in s tem olajšajo svoje delo, saj ob enem čutijo, da naloge in ukrepi, povezani z varovanjem informacij, zavirajo njihovo dnevno produktivnost. O tem govori homeostazna teorija, katera pojasnjuje individualne varnostne kompromise s percepcijo tveganja osebe in njenimi merili spremenljivosti tveganja. Posamezniki prilagodijo svoje vedenje, da bi uravnotežili posamezno in zaznano spremenljivo tveganje. Ti dve vrsti tveganj pa vplivata na različne psihološke in kontekstualne dejavnike. Posamezniki se dnevno srečujejo v ciljnih konfliktih med spremenljivim tveganjem in funkcionalnostjo in se v veliki meri nagibajo k poudarjanju učinkovitosti in zmanjšanju truda namesto k preprečitvi varnostnih incidentov oziroma morebitne izgube. V delovnem okolju posameznika, polnem različnih interesov in zahtev, bodo nosilci odločanja verjetno vedno izbrali zadovoljivo strategijo, katera išče ukrepe, ki so dovolj dobri, namesto da izbere tisto pravo strategijo, ki temelji na varnostnih vidikih organizacije (Albrechtsen, 2007).

Albrechtsen (2007) je v svoji kvalitativni študiji uporabnikov, v kateri je s pomočjo kvalitativnih intervjujev uporabnikov v servisnem centru pri IT podjetju in bančnem oddelku za svetovanje, analiziral posameznikove poglede na informacijsko varnost in pri tem ugotovil:

- Uporabniki se zavedajo, da je njihova vloga pri varovanju informacij pomembna, a ob enem obstaja razlika med njihovim namenom oziroma zavedanjem in dejanskim obnašanjem uporabnikov, saj ne izvajajo številnih varnostnih ukrepov in v večini sploh niso seznanjeni s tem, kakšne praktične ukrepe bi morali na svojih delovnih mestih za varovanje informacij sploh izvajati in sprejemati.
- Če bodo uporabniki morali povečati svojo dosedanjo nizko stopnjo varovanja informaciji, se bo posledično ustvaril konflikt prednostne naloge med uporabnostjo, učinkovitostjo in funkcionalnostjo na eni strani ter informacijsko varnostjo na drugi strani.
- Uporabniki so zaznali uporabniško-vključujoče se pristope kot učinkovito orodje za vplivanje na posameznikovo varnostno zavedanje in vedenje, z varnostnimi delavnicami ter medijsko kampanjo za ozaveščanje o varovanju informacij, ki je imela nižjo stopnjo vpliva na uporabnike, medtem ko dokumentirani predpisi, ukrepi in smernice za pričakovano vedenje na uporabnike niso imeli vpliva.

Uporabnost, učinkovitost in funkcionalnost so prednostne naloge, ki so pred informacijsko varnostjo, ki »konkurira« na drugi strani. A ob enem avtor navaja, da je treba v vsaki

organizaciji najti oziroma oblikovati ustrezen nivo uporabnosti, učinkovitosti in funkcionalnosti na eni strani in doseči zadovoljiv nivo varovanj informacij na drugi strani, kajti brez informacijske varnosti so organizacije preprosto prelahek plen za ljudi, ki stremijo k zadovoljevanju oziroma maksimiranju svojih interesov (Albrechtsen, 2007).

2.1.2 Individualni faktorji posameznikove različnosti pri zaznavanju informacijske ozaveščenosti

Posamezniki se med seboj razlikujemo po številnih faktorji. Ena izmed razdelitev posameznikov je tudi razdelitev po spremenljivkah, in sicer starosti, spolu, osebnosti in nagnjenosti k tveganju. Vse te spremenljivke tvorijo posameznikove faktorje, ki jih lahko merimo pri zaznavanju informacijsko varnostne ozaveščenosti. McCormac, Zwaans, Parsons, Calic, Butavicius, Pattinson (2017) so v svoji študiji proučili odnos med informacijsko varnostno ozaveščenostjo in posameznikovimi različnimi spremenljivkami. Informacijska varnostna ozaveščenost posameznikov se osredotoča do obsega, do katerega zaposleni razume pomembnost upoštevanja varnostnih politik, pravil in smernic ter njihovega obnašanja oziroma ravnanja, ki mora biti v skladu z varnostnimi politikami, pravili in smernicami. V študiji so informacijsko varnostno ozaveščenost merili z uporabo vprašalnikov za človeške vidike informacijske varnosti (ang. *Human Aspects of Information Security Questionnaire*), ki temelji na KAB modelu (ang. *Knowledge Attitude Behavior model)* oziroma modelu znanja, odnosa in vedenja. Vprašalnik človeških vidikov informacijske varnosti je bil sestavljen iz sedmih sklopov:

1. internetna uporaba
2. uporaba spletne pošte
3. socialna omrežja
4. management gesel
5. poročanja o incidentih
6. ravnanje z informacijami
7. mobilna uporaba.

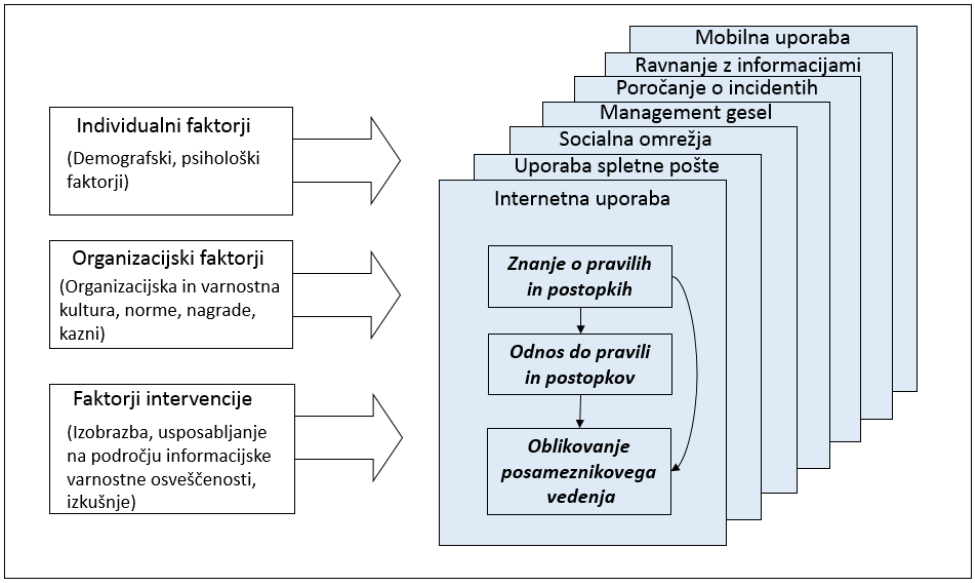
Spodaj je podani primer managementa gesel enega od sedmih sklopov vprašalnikov za človeške vidike informacijske varnosti, ki temelji na KAB modelu oziroma modelu znanja, odnosa in vedenja (McCormac *et. al.*, 2017, str. 152):

- **Znanje** »Dovoljeno mi je deliti svoja gesla na delovnem mestu s svojim sodelavcem.«
- **Odnos** »Slaba ideja je deliti svoja gesla na delovnem mestu s svojim sodelavcem, pa čeprav to sodelavec od mene zahteva.«
- **Vedenje** »Svoja gesla na delovnem mestu delim s svojim sodelavcem.«

Spodnja slika prikazuje grafični prikaz človeških vidikov informacijskega varnostnega modela, ki so ga v študiji o informacijski varnostni ozaveščenosti tudi uporabili. Iz slike je

mogoče razbrati povezanost med vsemi sedmimi sklopi s KAB modelom oziroma modelom znanja, odnosa in vedenja za posamezni sklop.

Slika 1: Človeški vidiki informacijskega varnostnega modela



Vir: McCormac, Zwaans, Parsons, Calic, Butavicius & Pattinson, 2017, str. 153

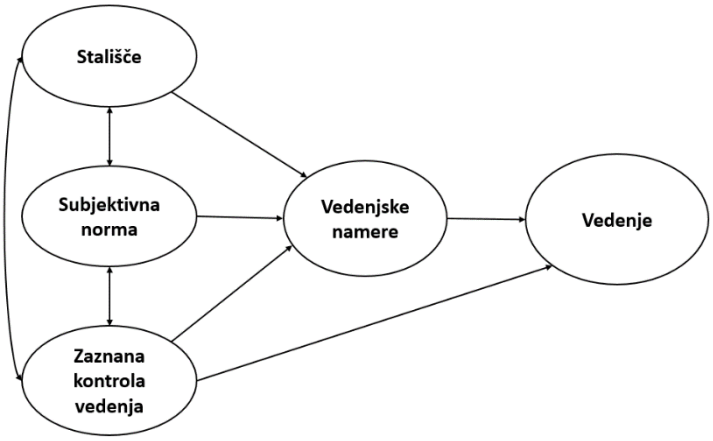
McCormac in ostali (2017) so v študiji, katera je bila izvedena na podlagi 505-ih anketirancev, ugotovili, da posameznikova zavest, odgovornost, čustvena stabilnost in nagnjenost k tveganju lepo razloži variance v informacijsko varnostni ozaveščenosti posameznikov, medem ko pri spolu in starosti tega ni mogoče razložiti. V sklopu študije je bila izvedena tudi psihična študija namerne škodljivosti izključno za analiziranje posameznikov, pri kateri so zaznali, da je ženski spol pri odpiranju tovrstnih namernih škodljivih spletnih pošt bolj pazljiv in skeptičen, prav tako so se odlično, v primerjavi s starejšimi skupinami, odrezali mladi med 18 in 25 letom. Starejše skupine so zabeležile višje rezultate pri informacijski varnostni ozaveščenosti (McCormac, *et.al.*, 2017).

2.1.3 Teorija načrtovanega vedenja (TPB) in varstveno motivacijska teorija (PMT)

Vedenje posameznika igra izredno pomembno vlogo pri oblikovanju informacijske varnosti v organizaciji. Veliko organizacij prav v ta namen oblikuje informacijska varnostna pravila in postopke, ki v prvi vrsti nudijo temelj in oporo pri zagotavljanju informacijske varnosti. Pravila in postopki tipično v organizacijah določajo stopnjo spremenljive varnostne uporabe računalniških virov, informacijsko varnostno odgovornost, stopnjo potrebnega znanja za posamezno delovno mesto in posledice, do katerih pride zaradi kršitve informacijsko varnostnih pravil in postopkov. Vse to pa lahko v organizaciji zagotovimo s primernim varnostnim vedenjem posameznikov na posameznih delovnih mestih. Ajzen (1991) v svojem delu vedenje opredeljuje kot vpliv človekovih namer in zaznane vedenjske kontrole posameznika, kjer zaznana vedenjska kontrola vpliva na učinek človekovih namer. S tega sledi, da model teorije načrtovanega vedenja (ang. *Theory of planned behavior)* vključuje

zaznano kontrolo vedenja, ki obravnava situacije, kjer ljudje nimajo popolnega namernega nadzora nad vedenjem. Obravnavajo se posameznikove ugodne in neugodne ocene vedenja. S teorijo načrtovanega vedenja je skušal pokazati koristen konceptualni okvir za obravnavanje zapletenosti človekovega socialnega vedenja. Odnos do vedenja oziroma stališča, subjektivne norme v zvezi z vedenjem in zaznan nadzor nad vedenjem običajno z visoko stopnjo natančnosti napovejo vedenjske namere posameznika. Na spodnji sliki je grafični prikaz teorije načrtovanega vedenja.

Slika 2: Teorija načrtovanega vedenja (ang. TPB)

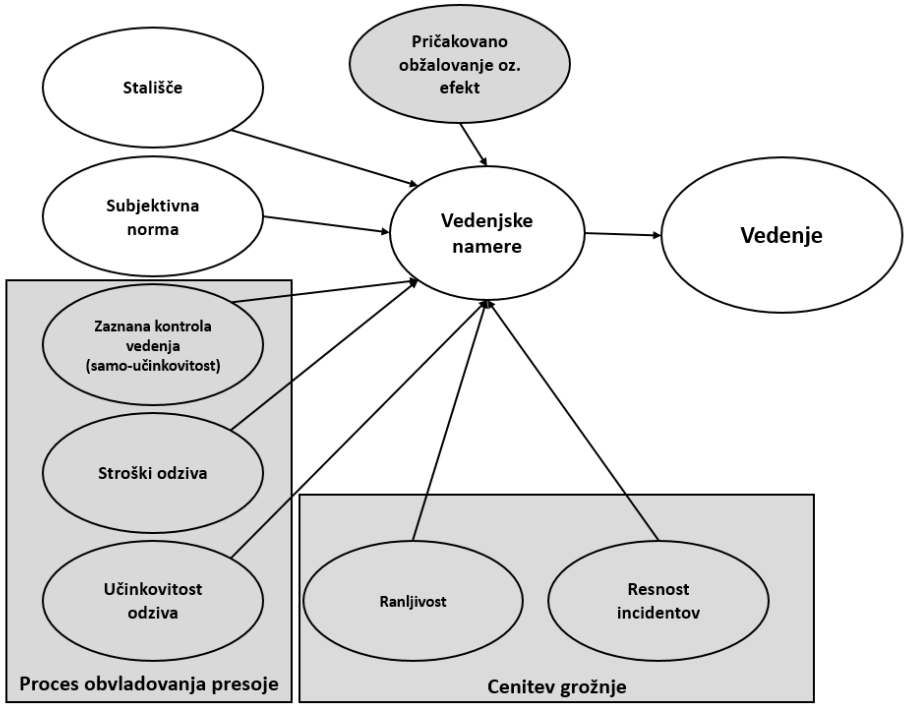


Vir: Ajzen, 1991, str. 182

To teorijo pa je mogoče uporabiti tudi pri obravnavi informacijske varnosti. Sommestad, Karlzen, Hallberg (2015) so v svojem delu »Učinkovitost teorije načrtovanega vedenja za pojasnjevanje skladnosti s politiko varovanja informacij« ugotovili, da je treba osnovnemu modelu priključiti varstveno motivacijsko teorijo (ang. *Protection motivation theory*), ki je sestavljena iz dveh skupin: procesa obvladovanja presoje in cenitve groženj. Skupina cenitev groženj ugotavlja, kako ranljiv in občutljiv je posameznik pri visoki stopnji pojava neželenih slabih stvari ter z resnostjo potencialnih incidentov in stroškov, ki so povezani s pojavom neželenih slabih stvari. Višja stopnja ranljivosti oziroma občutljivosti posameznikov in višja stopnja resnosti pojavitve potencialnih incidentov pri posameznikih sproža večjo zavednost pri upoštevanju in implementaciji varnostnih ukrepov v njihovo delovno okolje, medtem ko nižja stopnja ranljivosti/občutljivosti posameznikov in nižja stopnja resnosti pojavitve potencialnih incidentov pri posameznikih pušča manjšo zavednost, kar se tiče upoštevanja in implementacije varnostnih ukrepov v njihovo delovno okolje. Druga skupina pa je proces obvladovanja presoje in vsebuje tri dele: učinkovitost odziva, stroški odziva in samoučinkovitost.

Sommestad in ostali (2015) pa v študiji k obema modeloma dodajajo tudi pričakovano obžalovanje oziroma pričakovani efekt, ki je posledica negativnega vedenje posameznika ob določenem incidentu, ko dojame, da bi se lahko v tem položaju tudi drugače odzval in reagiral pravilneje ter v skladu z varnostno politiko organizacije. Razširitveni model teorije načrtovanega vedenja prikazuje spodnja slika.

Slika 3: Teorija načrtovanega vedenja z razširitvenima modeloma



Vir: Sommestad, Karlzen & Hallberg, 2015, str. 205

Lebek, Uffen, Neumann, Hohler in Breitner (2014) so v svoji raziskavi, ki je temeljila na teoretičnem literarnem pregledu obstoječe varnostne ozaveščenosti uporabnikov, ugotovili, da sestavni dejavniki štirih primarnih teorij: teorija načrtovanega vedenja (*TPB*), varstveno motivacijska teorija (*PMT*), teorija splošnega odvračanja oz. zastraševanja (ang. *General Deterrence Theory*) in teorija oziroma model za sprejem tehnologije (ang. *Technology Acceptance Model*), pomembno vplivajo na varnostno vedenje zaposlenih.

S sintetiziranjem rezultatov empirično testiranih modelov raziskav je predstavljena razprava o dejavnikih omenjenih teorij z dokazanimi pomembnimi vplivi na varnostno vedenje zaposlenih. Ker trdne dokaze o razmerjih med glavnimi konstrukti omenjenih teorij zagotavlja akademska literatura, se morajo prihodnje empirične študije bolj osredotočiti na dodatne dejavnike, ki vplivajo na informacijsko varnostno ozaveščenost zaposlenih in na posameznikovo vedenje namesto merjenja osnovnih odnosov. Avtorji podarjajo, da je treba v prihodnje dodatno pozornost nameniti tudi zanesljivosti poslovne inteligence, ki deluje v vlogi napovedovalca dejanskega varnostnega vedenja posameznikov.

Lebek in ostali (2014) poudarjajo, da je treba za preprečevanje nastajajočih vrzeli med teorijo in prakso, razviti dodatne ukrepe in modele procesov, ki bodo vplivali na varnostno ozaveščenost in na vedenje zaposlenih, vsi dodatni ukrepi in modeli procesov pa morajo izhajati iz že obstoječega teoretičnega znanja.

2.2 Posameznik kot vir ogrožanja varnosti informacije

Netehnični ukrepi varovanja informacij so poleg vseh tehničnih eden izmed ključnih dejavnikov uspešnosti varovanja informacij. Posamezniki lahko s svojim nepravilnim vedenjem ogrozijo celotno organizacijo ne glede na to, če so tehnični ukrepi za varovanje organizacije še tako visoko zasnovani. Bistven je celovit pristop k informacijski varnosti, ki poleg tehničnih ukrepov obsega tudi organizacijske, kadrovske in psihosocialne vidike varnega poslovanja in obravnavanja podatkov. Pri tem pa je tudi treba poudariti varnostno kulturo in ozaveščanje uporabnikov, ki skupaj tvorita pomembna gradnika v informacijski varnosti. Prav ta gradnika pa v praksi organizacijam pogosto povzročata preglavice zaradi zanemarjanja in pomanjkljive obravnave oziroma obravnave na le vnaprej določenih pozicijah in ne na celotni organizaciji. Ko govorimo o posameznikih, ki so vpeti v delovanje organizacije, ne govorimo samo o zaposlenih, ampak tudi o pogodbenih in zunanjih sodelavcih, ki imajo dostop do podatkov organizacije, saj lahko tudi ti ogrozijo integriteto, celovitost in zaupnost podatkov in ob enem lahko vključujemo tudi kupce oz. stranke, katerim moramo zagotoviti npr.: varno spletno brskanje, nakupovanje in uporabo naše spletne strani.

Antončič (2015) v svojem delu navaja, da se v praksi pojavljajo različni motivi in načini ogrožanja integritete, celovitosti in zaupnosti podatkov. Statistike kažejo, da je velik del kršitev varne obdelave oz. uporabe podatkov prav rezultat posameznikove malomarnosti ali pomanjkljivega znanja o varovanju informacij. Posledice posameznikovih malomarnih ravnanj in njihovega neznanja se lahko odražajo v delni ali popolni izgubi podatkov oziroma njihove uporabnosti, posredovanju podatkov ali omogočanju dostopa nepooblaščenim osebam. Izkušnje kažejo, da je poleg uporabe varnostnih sredstev in naprav ter izvajanja organizacijskega varovanja med preventivnimi ukrepi in postopki, ki jih za informacijsko zaščito v zvezi z zaposlenimi izvajajo organizacije, v pogojih hitrih tehnoloških sprememb najbolj učinkovita visoka varnostna kultura zaposlenih, ki je sistematično grajena in vzdrževana z ustreznim varnostnim ozaveščanjem (Antončič, 2015). Za gradnjo visoke varnostne kulture, ki je sistematično grajena in vzdrževana z ustreznim varnostnim ozaveščanjem pa se je treba najprej osredotočiti na uporabnike in njihovo delo oziroma na procese, ki jih izvajajo med delovnim časom. Zato bo v nadaljevanju na kratko predstavljeno osnovno pravilo oblikovanja gesel in njihovega pomena, kakšno vlogo naj odigra posameznik pri varovanju podatkov, kako naj prepozna socialni inženiring in psihing ter kako se lahko z enostavnimi koraki zagotovi varna uporaba mobilnih telefonov.

2.2.1 Oblikovanje in varovanje gesel

Gesla so se skozi zgodovino človeštva uporabljala v različne namene, a namen gesel ostaja ves čas enak, saj z njimi preverjamo identiteto določene osebe. To pomeni, da z vnosom gesla dokažemo, da smo dejansko tista oseba, za katero se izdajamo. Z gesli se dandanes srečujemo praktično na vsakem koraku, v službi, na domačem računalniku, imamo PIN kode na mobilnih telefonih in kode uporabljamo, da dostopamo do elektronskega bančništva ter elektronskih

napotnic. Prav zaradi neprestanega razvoja internetne tehnologije ter z bliskovitim razvojem storitev preko omrežij se pojavlja potreba po čim boljši varnosti in poznavanju uporabe gesel. Tu se postavlja vprašanje, ali je smiselno imeti za vsa zgoraj našteta prijavna okna samo eno izredno močno geslo, ali pa imamo za vsako prijavno okno drugačno. Iz osebnih izkušenj najbolj priporočam izbiro tri nivojske arhitekture gesel, katero sestavlja:

1. **Nivo –** za najbolj varovane dostope, kot so prijave v informacijske sisteme na delovnem mestu, elektronsko bančništvo itd. se uporabljajo gesla dolžine med 12 in 16 znaki z vključevanjem malih in velikih črk, številk ter posebnih znakov (npr. [DoWyL&yN$1DiyL]).
2. **Nivo** – za dostop do osebne e-pošte in različnih spletnih trgovin se uporabljajo gesla dolžine med 8 in 10 znaki, ki prav tako vključujejo male in velike črke, številke ter posebne znake (npr. K2jk,svp!).
3. **Nivo** – za dostop do raznih forumov oziroma informacijskih portalov, kot sta Morjeplovec.net, Avtomobilizem.com, se uporabljajo gesla različne dolžine, ki po navadi vsebujejo le en številčni ali posebni znak (npr. @rtičoka).

Dejstvo je, da vsi želimo ohraniti svoje podatke in informacije skrite pred nepovabljenimi gosti, še posebej, če nas nepazljivost lahko veliko stane. Ker je geslo dandanes eno izmed osnovnih elementov preverjanja istovetnosti, je pomembno, da so naša gesla kvalitetno oblikovana. Sam se iz izkušenj pri oblikovanju kvalitetnih gesel držim osnovnih 6. načel:

1. Kvalitetno geslo naj bo sestavljeno najmanj iz 8 znakov.
2. V geslu naj bodo uporabljene tako velike kot male črke.
3. Geslo naj vsebuje numerične in alfanumerične znake.
4. Gesla je dobro »začiniti« s posebnimi znaki na tipkovnici (npr. @, § ,&,=).
5. Dobro je izbirati tuje ali izmišljene besede.
6. Uporabimo izraze, ki si jih bomo lahko zapomnili.

Spodaj so zapisani primeri kvalitetnih gesel, katere je smiselno oblikovati za najbolj varovane dostope:

»Kdor drugemu jamo koplje, sam vanjo pade!«	Geslo: K2jk,svp!
»*Pastirica žgance kuha, notri pade ena muha!«.*	Geslo: pŽk,no3P1m!
»*Do what you love and you never work one day in your life«*	Geslo: [DoWyL&yN$1DiyL]

Kvalitetnejše kot je geslo, težje ga je uganiti, zato so nepridipravom prve tarče tisti, ki nimajo ustrezno oblikovanih gesel za varovanje svojih informacij in podatkov. Nepridipravi za pridobivanje gesel v veliki meri uporabljajo dve metodi:

- Prva metoda je socialni inženiring in temelji na pridobivanju gesel s pomočjo telefonskih klicev in elektronskih pošt. Tukaj se predvsem računa na naivnost in neinformiranost uporabnikov o varovanju podatkov. Dobro poznan je primer, ko so z metodo ribarjenja

gesel (phishing) nepridipravi razposlali na tisoče elektronskih obvestil, s katerimi so stranke banke prosili, da vpišejo številko bančnega računa in geslo na prirejeni strani za krajo podatkov zaradi izboljšave elektronskega bančnega sistema.

- Druga metoda pa je bolj tehnično usmerjenja, saj nepridipravi uporabljajo za pridobitev gesel različne programe, ki s pomočjo slovarjev in številčnice išče in preizkuša besede in besedne zveze iz slovarja. Dobro znana je tudi tehnična metoda s pomočjo iskanja kombinacij znakov (*ang. Brute forcing method*) na tipkovnici. V tem primeru programi iščejo gesla najprej s 3 znaki (aaa, aab, aac), nato s štirimi in petimi znaki. Ti programi so učinkoviti samo do dolžine šestih znakov, v katerih ni številk oz. se lahko z razširitvijo programa doda tudi iskanje številk najprej z 2 znakoma (a1, a2, a3).

Ozaveščenost o pomembnosti oblikovanja kakovostnih gesel se izboljšuje, toda še vedno so in bodo žrtve, saj v osnovi niso vsi posamezniki vpeti v osnovna varnostna izobraževanja o varovanju informacij oziroma so posledično zaradi pomanjkanja znanja in svoje malomarnosti prva tarča hekerjev.

Zaradi povečane ozaveščenosti v javnosti o pomembnosti oblikovanja kakovostnih gesel so Shen, Yu, Xu, Yang in Guan (2015) v svoji raziskavi skušali ugotoviti, kako se gesla s časom spreminjajo in kako jih uporabniki razumemo v danem kontekstu. Raziskava je bila izvedena na Kitajskem, na več kot šestih milijonih obravnavanih gesel. Ugotovili so, da je povprečna dolžina gesel vsaj 12 % daljša od prejšnjih rezultatov, gesla 75 % uporabnikov so sestavljena iz 8 do 10 znakov, kar je razvidno tudi iz spodnje tabele.

Tabela 2: Pogostost ponavljanja različnih dolžin gesel, izraženih v odstotkih

Število znakov	**Frekvenca (pon.)**	**Odstotek (%)**
1-3 znaki	739	0.01
4 znaki	6,675	0.10
5 znakov	33,039	0.51
6 znakov	82,998	1.29
7 znakov	16,923	0.26
8 znakov	2,338,639	36.38
9 znakov	1,552,182	24.14
10 znakov	930,881	14.48
11 znakov	628,832	9.78
12 znakov	369,537	5.75
13 znakov	167,861	2.61
14 znakov	154,979	2.41
15 znakov	75,347	1.17
16 znakov	49,648	0.77
17-34 znakov	20,352	0.32
1-34 znakov	6,428,632	100.00

Vir: Shen, Yu, Xu, Yang & Guan, 2015 str. 134

Tudi sama uporaba številk v geslih se je drastično povečala, saj izbira gesel več uporabnikov temelji na številčnem zaporedju 123456789. Tudi uporaba posebnih znakov, predvsem znaka

. s 34,57 % in **@** s 25,43 %, ki v tabeli 3 predstavljata najvišji delež uporabe simboliziranih znakov.

Tabela 3: Pogostost uporabe posebnih simbolov pri oblikovanju gesel

Simboli	Odstotek%	Simboli	Odstotek (%)
.	34.57	(	1.29
@	25.43	^	1.23
!	10.92	;	1.10
*	9.19	_	0.96
-	7.81	,	0.86
#	6.62	]	0.55
+	5.47	[	0.55
/	3.36	>	0.42
$	3.32	‘	0.42
?	2.69	<	0.36
&	2.52	\	0.32
=	2.09	:	0.30
%	2.00	{	0.09
Space	1.46	}	0.08
)	1.41	“	0.07
~	1.34	|	0.05

Vir: Shen, Yu, Xu, Yang & Guan, 2015 str. 135

A vseeno avtorji poudarjajo, da ne glede na to, kako kvalitetno je geslo, če se uporabnik na delovnem mestu, npr. med malico ali svojo kakršno koli odsotnostjo, pozabi odjaviti iz sistema, lahko prav tako nosi hude posledice.

Iz osebnih izkušenj lahko dodam, da uporabnika pri oblikovanju in varovanju gesel najbolj motivira, da se ga enostavno obvesti o tem, da informacijski sistemi samodejno zapisujejo vsako aktivnost posameznega uporabnika v dnevnike imenovane *ang. Log files.* Tako je mogoče ugotoviti, kdo je kaj in kdaj počel s podatki v sistemu.

Če nekdo pridobi ali ukrade uporabniško ime in geslo, bo ob svojem početju prikril svojo pravo identiteto, odgovornost pa bom nosil uporabnik, kateremu je bila identitet vzeta. Pri tem pa je tudi treba poudariti, da pretiravanje pri dolžini in znakih za gesla ni ravno dobrodošlo, saj se potem uporabniki konstanto srečujejo s tehniki v oddelku za informatiko in ti morajo ponastaviti njihova gesla, ki se jih zaradi pretiravanja pri dolžini in zaporedju znakov težko zapomnimo. Veliko problematiko, pa predstavljajo tudi raznorazni lističi, na katerih uporabniki shranjujejo svoja gesla. La ta so velikokrat prilepljena na različne računalnike, robove monitorjev, drsne ploskve računalniških mišk, pisarniške mize …

Najboljše je, da je v varnostni politiki organizacije zapisano, da je tovrstna shramba gesel prepovedana ter bo zoper osebo, ki ne upošteva omenjenega ukrepa izveden postopek, ki bo v nadaljevanju preprečeval tovrstne kršitve.

2.2.2 Vloga posameznika pri varovanju podatkov

Vloga posameznika pri varovanju podatkov ni samo upoštevanje vseh pravil in ukrepov, ki so predpisani v varnostni politiki organizacije. Treba je osvojiti neko doslednost pri varnostnem bontonu in vsa ta pravila in ukrepe dopolniti z neko človeško smiselnostjo, da se v podjetju poskrbi za varno rabo vsega, kar utegne povzročiti zlorabo ali odtekanje zaupnih podatkov.

V nadaljevanj so predstavljeni osnovni pristopi varnostnega bontona, ki se je oblikoval v praksi oz. so to nekakšna nezapisana pravila, ki bi jih morali poznati prav vsi zaposleni in jih implementirati na svoja delovna mesta:

- USB-ključkov ali CD-jev s podatki ne puščamo na delovnih mestih oz. se njihovi uporabi pri bolj pomembnih podatkih izogibamo.
- Ko zapustimo delovno okolje oz. računalnik, četudi le za kratek čas, ga moramo vedno zakleniti. To je pogosta napaka posameznikov, ki delovno okolje zapustijo z mislijo »saj bom takoj nazaj, skočim samo do sodelavca« in ne zaklenejo računalnika.
- Ko imamo opravka z različnimi premiki računalniških in pametnih komponent organizacije, na katerih so shranjeni poslovni podatki, le teh ne smemo puščati na nenadzorovanih mestih. Saj se kar redno dogaja, da se ob posebnih priložnostih, kot so selitve pisarn, preurejanje delovnega okolje, sejemski ali marketinški dogodki, rado zgodi, da vsa ta oprema leži na hodniku pred pisarnami ali celo na stopniščih ter pred dvigali, kjer je pretok ljudi največji. Pri kraji računalniške opreme ne smemo pozabiti, da je škoda dvojna, saj smo poleg izgube informacij priča tudi odtujitvi fizične opreme (npr. prenosnega računalnika).
- V organizacijah je čedalje manj informacij v papirnati obliki, zato tudi posamezniki pozabljajo, da se zaupne informacije ne natisnejo na list papirja in ne mečejo v smetnjake. Če moramo list papirja s takimi informacijami zavreči, bodimo pozorni, da papir trajno uničimo, npr. z rezalnikom papirja. Dandanes so papirnate oblike najbolj pogoste pri poročilih in pogodbah, ki v prvi vrsti služijo kot kopije, shranjene v različnih registratorjih organizacij.
- Dobra praksa je, da ob odhodu iz delovnega mesta posamezniki ugašajo računalniško opremo, seveda razen tiste, ki mora zaradi funkcionalnosti delovati neprekinjeno. Obstaja sicer majhna verjetnost, da v določeni napravi pride do samovžiga in posledično do požara in nepopisne škode.

Dejstvo je, da sta varnost in svoboda posameznika tudi na informacijskem področju obratno-sorazmerni, ker v prvi vrsti ni namen, da se z visoko stopnjo zaščite varovanja podatkov ustvari militantna klima na delovnih mestih organizacije. Po drugi strani pa se je treba zavedati, da nevarnost priti neprestano, zato je bistveno, da so posamezniki osveščeni glede pomembnosti informacij, to pa zagotavljamo s primernimi izobraževanji in napotki za delo.

2.2.3 Socialni inženiring in psihing

Posamezniki se prepogosto preveč zanašamo na informacijsko varnostno opremo, ki sama po sebi še ni zadosten vir varovanja informacij. Tudi najboljša tehnologija prav nič ne pomaga, če ne uporabljamo zdrave pameti. Človeška narava je zaupljiva in kriminalci jo s pridom izkoriščajo. Dejstvo je, da iznajdljivi hekerji nenehno iščejo točke, ki jim omogočajo vdor v sistem in dostop do pomembnih podatkov. Ena izmed metod vdora je tudi socialni inženiring, ki v prvi vrsti pomeni uporabo različnih tehnik manipuliranja posameznikov oziroma skupine ljudi z namenom, da le ti izvedejo določene poteze in te kasneje izdajo zaupne informacije. Neprestan razvoj tehnologije nam na eni strani olajšuje delo, na drugi strni pa prinaša nove varnostne izzive. Na podlagi izkušenj lahko z za gotovostjo trdim, da s sodobno tehnologijo hekerji iz javnih virov in socialnih omrežij, kot so Google, Facebook, Instagram, Twitter, pridobijo podatke, ki so na različne načine povezani s točno določenim posameznikom in njegovo okolico. Te podatke nato uporabijo za posebno pripravljena sporočila, ki zaradi personaliziranega konteksta, hitro pritegnejo našo pozornost in se v prvi vrsti sploh ne zdijo varnostno vprašljiva. Sporočila vsebujejo povezave do škodljivih spletnih strani ali programov, zato lahko kaj hitro okužimo svoje naprave in s tem posledično tudi razkrijemo zaupne podatke. Pri masovnih prevarah hekerji v prvi vrsti uporabljajo metodo z znamkami priznanih podjetij, izdelkov ali storitev ter metodo varnostnih opozoril, s katero skušajo uporabnika prepričati, da uporablja zastarelo različico programa, katero jo je zaradi vnaprej nemotenega delovanja potrebno nemudoma posodobiti.

Psihing oziroma ribarjenje gesel je še ena izmed metod pridobivanja podatkov, za katero je značilno, da heker razpošlje na tisoče uporabniških naslovov lažno sporočilo, v katerem nas neka organizacija (po navadi finančna institucija) poziva k vnosu zaupnik podatkov (npr. prijave v spletno banko). Ta sporočila so videti pristna, in če je uporabnik dejansko stranka te finančne institucije, obstaja velika verjetnost, da bo sledil navodilom in oddati svoje podatke. Pogosto se dogajajo tudi telefonske prevare, ki so še ena izmed oblik ribarjenja gesel, v kateri nas skuša izredno spreten sogovornik prepričati k temu, da mu zaupamo raznorazne osebne in zaupne podatke, pogosto se prestavljajo kot osebe v višjem managementu njihovih pogodbenih partnerjev. Posameznik se mora v trenutku pogovora zavedati, da so ti sogovorniki izredno dobro podkovani za tovrstno komuniciranje in je možnost, da jim izdamo zaupen podatek velika.

Phishing pa je trenutno zelo razširjen tudi na družbenih omrežjih, ki omogočajo takojšne sporočanje Twitter, Facebook, Skype … V teh primerih običajno je videti tako, da uporabnik prejme sporočilo, ki je spet »persolizirane« narave in pošiljatelj sporočila je po navadi naš prijatelj, ki nam pošlje spletno povezavo. Seveda klikanje na take povezave ni priporočeno, saj nas povezave pripeljejo do zlonamernih spletnih strani. Zaradi zlorab s pomočjo socialnega inženiringa je izjemno pomembno, da vsi zaposleni strogo upoštevajo pravila interne informacijske varnostne politike. Informacijska varnostna politika vsebuje formalni zapis varnostnih mehanizmov in drugih pravil, ki jih morajo upoštevati vsi posamezniki z dostopom do opreme, prostorov in informacij.

2.2.4 Mobilna izpostavljenost

Mobilne naprave so postale del našega vsakdanjika, tako v zasebnem kot tudi v poslovnem življenju. Prenosni računalniki, predvsem pa pametni telefoni in tablice, nam zaradi svoje priročne prenosljivosti in zmogljivosti omogočajo, da veliko stvari lahko opravimo kjer koli. A ob enem se morajo uporabniki zavedati, da je na teh napravah tudi ogromno zaupnih osebnih in velikokrat tudi poslovnih podatkov. Prav zaradi ogromne količine podatkov so te naprave postale privlačna tarča raznih kriminalcev, ki izkoriščajo posameznikove slabe navade ter njihovo neinformiranost. Med največje grožnje, ki zadevajo varnost mobilnih naprav, lahko vključujemo:

- Izgubo podatkov zaradi izgube ali kraje mobilne naprave. V tem primeru ponudniki oziroma proizvajalci mobilnih telefonov omogočajo sledljivost preko GPS-a, ki ga lahko ob izgubi ali kraji mobilnega telefona enostavno uporabimo, da poiščemo njihovo lokacijo oziroma z oddaljeno prijavo izbrišemo vse podatke, ki so shranjeni v mobilnem telefonu.
- Zlonamerne aplikacije, ki kradejo uporabniške podatke. Nameščanje aplikacij naj poteka preko uradnih trgovin (Windows Phone Store, App Store, Google Play ...). Pred prenosom aplikaciji se je vedno dobro pozanimati, kakšne podatke aplikacija potrebuje. Bolj odprte mobilne platforme, kot je npr. Android, omogočajo nalaganje nepreverjenih aplikacij, tudi takšnih, ki z naše naprave prekrito kradejo uporabniške podatke.
- Uporaba nezavarovanih in lažnih brezžičnih (Wi-Fi) omrežji. Uporabniki pogosto uporabljajo javna brezplačna nezavarovana omrežja, z namenom, da prihranijo pri stroških uporabe mobilnega omrežja, a vendar obstajajo tudi možnost prisluškovanja oziroma posnemanja podatkovnega prometa, na napravi, ki je povezana v brezplačno nezavarovano omrežje. Za brskanje po spletnih vsebinah je varnejše uporabiti povezo do spleta preko mobilnega operaterja, ki ponuja 3G ali LTE (*ang. Long term evolution),* pri tem načinu dostopa pa je priporočljivo poznati količino zakupljenega podatkovnega prometa, s katero uporabnik razpolaga v naročniškem razmerju.

2.3 Vpliv varnostnih opozoril pri spodbujanju informacijske ozaveščenosti posameznika

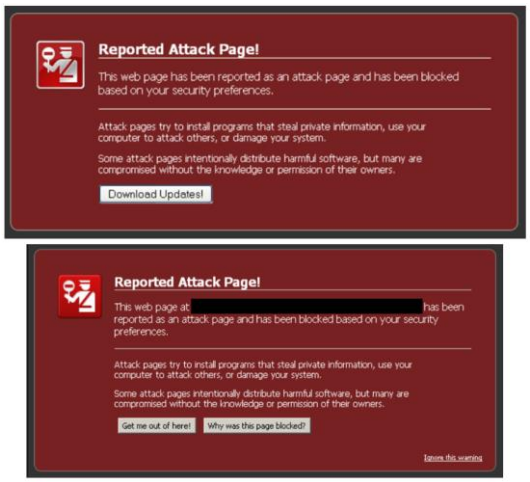
Varnostna opozorila igrajo pomembno vlogo pri opozarjanju uporabnikov na grožnje, ki jim neprestano pretijo. Zato se morajo zavedati njihovega pomena in pomembnosti pravilnega odreagiranja. Varnostna opozorila se pogosto pojavljajo kot opozorilna okna, ki uporabnika obveščajo o določeni grožnji oziroma nevarnosti. Delujejo kot prvi pokazatelj grožnje in so vsekakor povezana z osveščanjem in izboljševanjem informacijski varnosti v organizaciji (Fajdiga, 2015).

Na mobilnih telefonih se srečamo z varnostnim opozorilom že takoj pred namestitvijo željene aplikacije. V tem primeru nas varnostno opozorilo obvešča o tem, da željena aplikacija za

njeno nemoteno delovaje potrebuje dostop do npr. naše lokacije, internetne povezave in naših podatkov. Včasih nekatere aplikacije npr. potrebujejo tudi dostop do naših kontaktov ali podobnih zasebnih podatkov. Zato je treba vedno dobro prebrati mobilna varnostna opozorila, do česa aplikacija dejansko potrebuje dostop za njeno nemoteno delovanje. Poznamo tudi varnostna opozorila v brskalnikih, večinoma mislimo na SSL *(ang. Secure Socket Layer)* in TLS *(ang. Transport Layer Security)* opozorila oziroma protokola, ki skrbita za varno medmrežno povezavo. Ta opozorila se nam prikažejo, ko hočemo obiskati spletno stran, s katero je nekaj narobe, bodisi zaradi njene pomanjkljive varnostne zaščite ali okuženosti z različnimi programi, ki ogrožajo naše naprave.

Temna stran varnostnih opozoril pa se kaže v lažnih pojavnih oknih, ki se pojavijo med brskanjem po spletnih vsebinah. Ta lažna pojavna okna oziroma lažna varnostna opozorila so pogosto videti kot prava in uporabnika prepričujejo, da prenesejo najprej posodobitev, katera bo omogočila nadaljnje brezskrbno brskanje po željeni spletni strani. Primer lažnega in pravega varnostnega opozorila lahko vidimo na spodnji sliki. Ob kliku na »prenesi posodobitve« se dejansko prenese zlonamerni skener, ki računalnik okuži z zlonamerno kodo, ki bodisi zakodira naše podatke ali prepreči dostop do željenih programov, datotek, internetnega dostopa ... (Fajdiga, 2015).

Slika 4: Primer lažnega in pravega varnostnega opozorila



Uporabniki se morajo zavedati, da namen pravega varnostnega opozorila ni prenašanje različnih posodobitev, ampak obveščanje o varnostno vprašljivih straneh in nam prepušča odločitev, ali bomo z ogledom strani nadaljevali ali se pa se bomo zaradi varnostnega opozorila odločili, da željene spletne strani ne obiščemo.

Fajdiga (2015) je v svoji raziskavi o vplivu varnostnih opozoril na varnost uporabnika, v kateri je sodelovalo 143 anketirancev, skušal potrditi oziroma ovreči tri hipoteze. Prve postavljene hipoteze ne moremo ovreči, saj je ugotovil, da varnostna opozorila pozitivno vplivajo na način rabe informacijske varnosti, saj je kar 85 % anketirancev po pojavitvi varnostnega opozorila zavrnilo dostop oziroma prenos aplikacije. Anketiranci so bili tudi

mnenja, da varnostna opozorila uspešno pomagajo pri ohranjanju informacijske varnosti. Le redki niso razumeli pomena varnostnih opozoril. Druga postavljena hipoteza je bila v raziskavi le delno potrjena, saj je raziskava pokazala, da varnostna opozorila v celoti ne delujejo kot sredstvo izobraževanja uporabnikov informacijsko komunikacijske tehnologije. Le redki so se pozanimali o določenem varnostnem opozorilu in posledično o njegovi grožnji.

Avtor poudarja, da je večina anketirancev namen varnostnih opozoril razumela, kar je v prvi vrsti tudi smisel varnostnih opozoril, a težave je, da ta opozorila med anketiranci niso sprožila velikega zanimanja za poizvedovanje o sami grožnji. Tudi tretja hipoteza je bila delno potrjena, saj uporabniki informacijsko-komunikacijske tehnologije premalo posvečajo pozornost varnostnim opozorilom, saj večina anketirancev še nikoli ni obiskala spletnih strani, kot so varninainternetu.si, safe.si ali cert.si, ki uporabnike ozaveščajo o pomembnosti informacijske varnosti tako v poslovnem življenju kot zasebnem. Problem se kaže predvsem v pomanjkanju motivacije oziroma v nezainteresiranosti uporabnikov do izobraževanja na področju varnostnih opozoril.

Fajdiga (2015) poudarja, da je za motiviranost posameznikov tudi pri zainteresiranosti nad varnostnimi opozorili, ključna sprememba v informacijski kulturi ter vpeljava posameznikov v raznorazne informacijsko varnostne izobraževalne programe. Pri tem pa poudarja, da bi lahko tudi mediji v njihovem prostoru, večjo pozornost posvetili osveščanju posameznikov o pomembnosti informacijske varnosti.

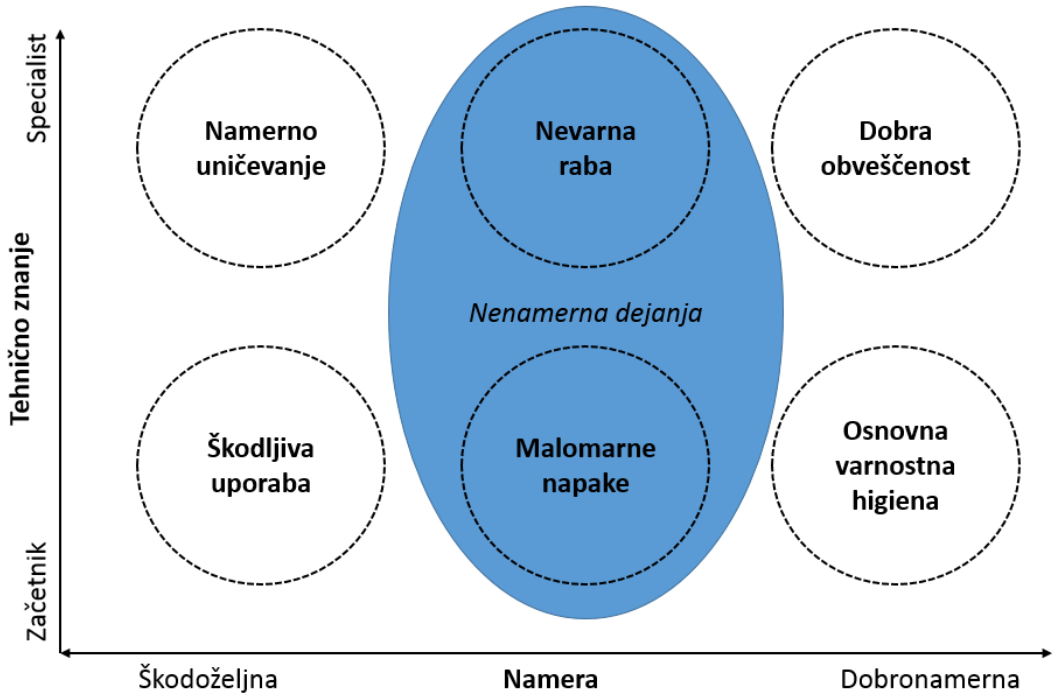
2.4 Varnostno vedenje posameznikov

Veliko strokovnjakov na področju varovanja informacij verjamejo, da je spodbujanje k boljšemu varnostnemu vedenju, in s tem povezano omejitvijo slabega vedenja končnega uporabnika, eden izmed ključnih načinov zagotavljanja učinkovite varnosti informacij znotraj organizacij. Neprestano spreminjajoča se tehnologija tudi v organizacijah na področju posameznikovega vedenja pušča posledice, ki jih ne smemo zanemariti. Prav zato vsak članek oziroma raziskava o varnostnem vedenju posameznikom, upravljavcem informacijske tehnologije razširjuje celoten koncept razumevanja posameznikovega varnostnega vedenja.

Prav zato so Stanton, Stam, Mastrangelo in Jolton (2004) v raziskavi skušali analizirati posameznikovo varnostno vedenje ter stroki ponuditi še drugačno razumevanje obravnavane tematike. Za lažjo obravnavo so najprej razvili dvodimenzionalno taksonomijo posameznikovega varnostnega vedenja, ki vključuje šest kategorij: namerno uničevanje, škodljiva uporaba, nevarna raba, malomarne napake, dobra obveščenost in osnovna varnostna higiena. Rezultati analize so pokazali, da se zgoraj omenjenih šestih kategorij varnostnega vedenja posameznika dobro prilega na novo razvijajoči se dvodimenzionalni shemi, kjer prva dimenzija zajema tehnična znanja, potrebna za uresničitev varnostnega vedenja, druga dimenzija pa zajema posameznikovo vedenje oziroma namero (vključno zlonamernimi,

nevtralnimi in dobronamernimi nameni). Dvodimenzionalno taksonomijo posameznikovega varnostnega vedenja, z vključujočimi šestimi kategorijami prikazuje spodnja slika.

Slika 5: Dvodimenzionalna taksonomija posameznikovega varnostnega vedenja



Vir: Stanton, Stam, Mastrangelo & Jolton, 2004 str. 127

Z dvodimenzionalno taksonomijo posameznikovega varnostnega vedenja so skušali preoblikovati do takrat nedodelan seznam varnostnih vedenj v bolj obvladljive, lažje razumljive in prepoznavne dimenzije. Stanton in drugi (2004) v svoji raziskavi ugotavljajo, da imajo končni uporabniki oziroma posamezniki precej mračen pogled na ukrepe in pravila, ki so potrebna za sprejetje osnovne varnostne higiene, katero uporabijo in predpisujejo varnostni strokovnjaki. Eden izmed teh ukrepov je npr. tudi mesečno spreminjanje gesel. Med drugi tudi ugotavljajo, da je razlog za učinkovito ali neučinkovito varnostno vedenje odvisno od same organizacije. Pri posameznikih, ki v organizacijah opravljajo precej od varnosti odvisne naloge, beležimo učinkovitejše varnostno vedenje kot pri posameznikih, katere naloge niso varnostno vprašljive oziroma je njihova varnost na nizkem nivoju.

Z dvodimenzionalno taksonomijo varnostnega vedenja posameznikov je bilo mogoče reproducirati mehanizme, ki se lahko končnemu uporabniku pomagajo premakniti iz kategorije malomarnih napak v kategorijo osnovne varnostne higiene, za katero je značilno, da posamezniki poznajo vsaj osnovna varnostna pravila in ukrepe, ki jih predpisuje varnostna politika organizacije. Ti mehanizmi, ki omogočajo tovrstne premike posameznikov, se predvsem nanašajo na učinkovitejše varnostno usposabljanje, osveščanje in poznavanje sprememb ter dodeljevanje nagrad za širitev razumevanja varnostnih pravil in ukrepov med sodelavci skozi varnostno kulturo organizacije.

Dejstvo je, da se različni mehanizmi varnosti strojne in programske opreme, pogosto uporabljajo za krepitev informacijskih sistemov. Ob tem pa se moramo zavedati, da ti »sistemi« sami po sebi niso zadostno merilo za učinkovito varovanje informacij, saj so ranljivi prav zaradi nepričakovanih in nezaželenih vedenj uporabnikov, ki so neprestano tesno povezani z informacijami v informacijskem sistemu organizacije. Prav zaradi tega se je treba osredotočiti tudi na varnostno vedenje uporabnikov.

Takšnega mnenja so tudi Ögütçü, Testik in Chouseinoglou (2015), ki v svoji raziskavi proučujejo stopnje tveganja, povezanega s posameznikovim varnostnim vedenjem, s katerim posledično lahko ogroža informacijsko varnost organizacije. Proučujejo tudi preventivne ukrepe, ki jih posamezniki uporabljajo pri morebitnih grožnjah, katerim so izpostavljeni ter v kakšni meri posamezniki resnično zaznavajo varnostno tveganje.

Avtorji so v raziskavi oblikovali štiri lestvice, katerih namen je določitev stopnje varnostnega tveganja, povezanega s posameznikovim varnostnim vedenjem. To so: lestvica vedenjskega tveganja, konservativna vedenjska lestvica, lestvica izpostavljenosti kaznivemu dejanju ter lestvica zaznanega obsega tveganja. Raziskava je bila izvedena na porečju skupin, in sicer: študentov, akademikov, administrativnega osebja ter osebja izobraževalnih institucij, ki so na različnih geografskih in socialno-ekonomskih območjih.

Ögütçü in drugi (2015) v svoji raziskavi ugotavljajo, da obstajajo velike razlike med skupinami znotraj lestvice vedenjskega tveganja, konservativnimi vedenjskimi lestvicami ter lestvicami izpostavljenosti kaznivemu dejanju. V lestvici zaznanega osebnega tveganja pa med posameznimi skupinami ni bilo mogoče zaznati razlik. Znotraj lestvice vedenjskega tveganja so se pojavile največje razlike, saj je skupina študentov prepričljivo zasegla najvišje mesto, kar pomeni, da je ta skupina z vidika vedenjskega tveganja najbolj tvegana, saj se jim uporaba različnih novodobnih rizičnih tehnologij ne zdi prav nič sporna in varnostno vprašljiva. Najmanjšo stopnjo vedenjskega tveganja je na tej lestvici mogoče pripisati skupini administrativnega osebja, saj se je ob povečanju stopnje ogroženosti, tudi njihovo vedenje spremilo v bolj zaščitniško. Tudi v konservativni vedenjski lestvici in lestvici izpostavljenosti kaznivemu dejanju so bile manjše, a omembe vredne razlike med študenti in ostalimi skupinami, saj je skupina študentov zaradi uporabe rizičnih tehnologij bolj izpostavljena in ob enem nagnjena h kaznivemu dejanju kot ostale skupine.

Avtorji tudi ugotavljajo, da ne glede na to, v kateri skupini je posameznik, je mogoče njegovo vedenje z različnimi pristopi in varnostnimi izobraževanji, saj malce spremeniti in preusmeriti v nižjo stopnjo varnostnega tveganja.

Varnostno vedenje posameznikov bo treba v organizacijah vse bolj nadzorovati, spremljati in izobraževati, le na tak način bodo lahko posamezniki dosegali nižjo stopnjo varnostnega tveganja, povezanega z njihovim vedenjem, ter posledično pripomogli k boljšemu in učinkovitejšemu sistemu varovanju informacij v organizaciji.

2.4.1 Kaj vplivna na varnostno vedenje posameznika?

Da Veiga in Eloff (2010) v svoji raziskavi ugotavljata, da bi moral biti pristop do oblikovanja informacijske varnosti v organizaciji v prvi vrsti osredotočen na vedenje zaposlenih, ki s svojimi dejanji z vidika varovanja informacij pri svojem delu uspešno ali neuspešno implementirajo pravila in ukrepe, ki morajo biti v skladu z varnostno politiko organizacije. Torej, na vedenje posameznikov vpliva veliko dejavnikov. Izhajamo lahko iz dejavnikov, ki zajemajo npr. zaznavanje groženj, kontrole, preobremenjenost, nezadovoljstva pri opravljanju vsakodnevnih nalog, nizke motivacije in pripravljenosti do dela. Vsi ti dejavniki vplivajo na posameznikovo varnostno vedenje, ki v našem primeru ustvarja in določa stopnjo posameznikove ranljivosti in možnosti kršitve informacijskih varnostnih pravil organizacije. Tudi na podlagi izkušenj, ki sem jih pridobil pri izobraževanju posameznikov o pomembnosti varovanja informacij, lahko poudarim problematiko vsakodnevnega spreminjanja razpoloženja uporabnikov, ki se posledično tudi odraža v posameznikovem varnostnem vedenju.

Posamezniki, ki so pred obiskom delovnega mesta doživeli različne negativne dogodke, ki znižujejo njihovo razpoloženje in s tem povezano vedenje, v trenutku slabega razpoloženja, z vidika varnosti, niso najbolj primerni za opravljanje najbolj zahtevnih nalog, ki so z vidika varovanja informacij izredno občutljive. Ne glede na razpoloženje pa pri posameznikih na nižjih delovnih mestih ugotavljam, da se ob večjih posodobitvah ali implementacijah različnih programskih oprem za varovaje in odpravo oziroma odkrivanje groženj, kljub neprestanemu izobraževanju in poudarjanju o pomembnosti varovanja informacij, pojavi mišljenje, da je sedaj ob prenovitvi programske opreme, njihovo varnostno vedenje nepomembno, saj sedaj nove posodobitve ali implementacija programa skrbi za njihovo varno izvajanje vsakodnevnih nalog.

To pa je tudi ena izmed problematik, saj zaradi čedalje večje priljubljenosti različnih programskih oprem za zmanjševanje morebitnih groženj pri varovanju podatkov, posamezniku povzroči in pušča predstavo o popolni učinkovitosti pri njihovem odkritju in odpravi. Ta trend, v katerem se posamezniki lahko znajdemo, pa lahko pušča posledice v obliki nepremišljenih in nenamernih vedenj, ki povečujejo ne samo ranljivost samega uporabnika, ampak tudi ranljivost celotne organizacije.

Hickmann Klein in Mezzomo Luciano (2016) sta v svoji raziskavi analizirala posameznikovo varnostno vedenje pri uporabi elektronske pošte. Avtorja sta na podlagi vedenjskih teorij razvila teoretični model in z njim povezane hipoteze z namenom razumevanja, do kakšne mere zaznavanja groženj, nadzora in nezadovoljstva uporabnikov lahko pri posamezniku povzročimo odgovorno varnostno vedenje. V raziskavi je sodelovalo 171 anketirancev obeh spolov na različnih delovnih mestih v Braziliji. Oblikovala sta 6 hipotez, ki vplivajo na razvoj teoretičnega modela vedenjske varnosti posameznika.

Prva hipoteza je bila oblikovana glede na zaznavanje uporabnikov pri dovzetnosti za grožnjo in resnosti same grožnje, saj če pri posamezniku zaznamo večjo dovzetnost za preprečevanje varnostnih incidentov, bo verjetno tudi sam pokazal večje zanimanje za višjo stopnjo varnostnega vedenja. Liang in Xue (2009) zaznano resnost opredeljujeta kot stopnjo, do katere posameznik dokaže, da se bodo negativne posledice različnih groženj uresničile.

H1*: Zaznana dovzetnost za grožnje informacijski varnosti pozitivno vpliva na posameznikovo varno vedenje v zvezi z informacijsko varnostjo.*

Druga hipoteza je bila oblikovana na podlagi posameznikovih sprejetih odločitvah, povezanih z ustreznim varnostnim vedenjem, ko se zavedajo občutljivosti in resnosti pojavitve groženj.

H2: *Zaznana resnost grožnje informacijski varnosti pozitivno vpliva na posameznikovo varno vedenje v zvezi z informacijsko varnostjo.*

Tretja hipoteza je bila oblikovana na podlagi ugotovitev, da zanesljivost odkrivanja groženj pozitivno vpliva na posameznikove namere, ki so povezane z upoštevanjem smernic v varnostni politiki organizacije. Saj ko posamezniki ugotovijo, da bodo s svojimi namerami kršili varnostno politiko organizacije, jih bodo prav zaradi tega spremenili in varnostno uskladili

H3: *Zaznavanje zanesljivosti odkrivanja neupoštevanja smernic za informacijsko varnost pozitivno vpliva na posameznikovo varno vedenje v zvezi z informacijsko varnostjo.*

Četrta hipoteza opredeljuje kazni oziroma sankcije glede nespoštovanja varnostnih pravil, ki vplivajo na posameznikovo varnostno vedenje.

H4: *Zaznavanje in poznavanje sankcij zaradi neupoštevanja smernic v zvezi z informacijsko varnostjo pozitivno vpliva na posameznikovo varno vedenje v smislu informacijske varnosti*.

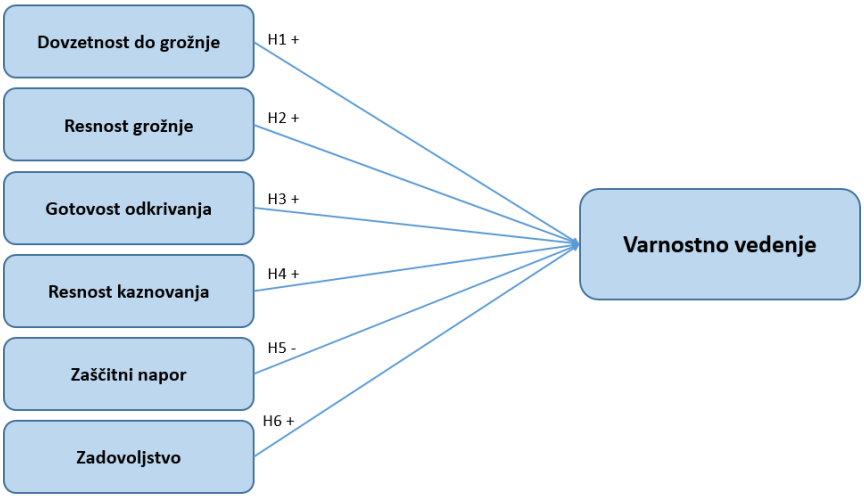
Peta hipoteza opredeljuje posameznikova spoznavna prizadevanja, kot so denar, čas, neprijetnost in razumevanje. Ta prizadevanja po besedah Liang in Xue (2009) ustvarijo vedenjske ovire in zmanjšajo motivacijo za varno vedenje oziroma ravnanje v zvezi z informacijsko varnostjo zaradi analize stroškov in koristi. Če so stroški višji od koristi, posamezniki verjetno ne bodo sprejemali vedenja, ki so ga priporočili strokovnjaki na različnih področjih.

H5: *Zaznavanje prizadevanj za varovanje, ki sledi smernicam za varnost informacij, negativno vplivajo na posameznikovo varno vedenje v zvezi z informacijsko varnostjo.*

Zadnja hipoteza opredeljuje obstoj možnosti kršitve posameznika zaradi pomanjkanja motivacije, ki je posledica medsebojnih odnosov med sodelavci in nadrejenimi za upoštevanje in implementacijo varnostnih ukrepov in pravil v njihovo delovno okolje.

H6: *Zadovoljstvo med sodelavci in nadrejenimi pozitivno vpliva na posameznikovo varno vedenje v zvezi z informacijsko varnostjo.*

Slika 6: Teoretični model posameznikovega varnostnega vedenja



Vir: Hickmann Klein & Mezzomo Luciano, 2016, str. 483

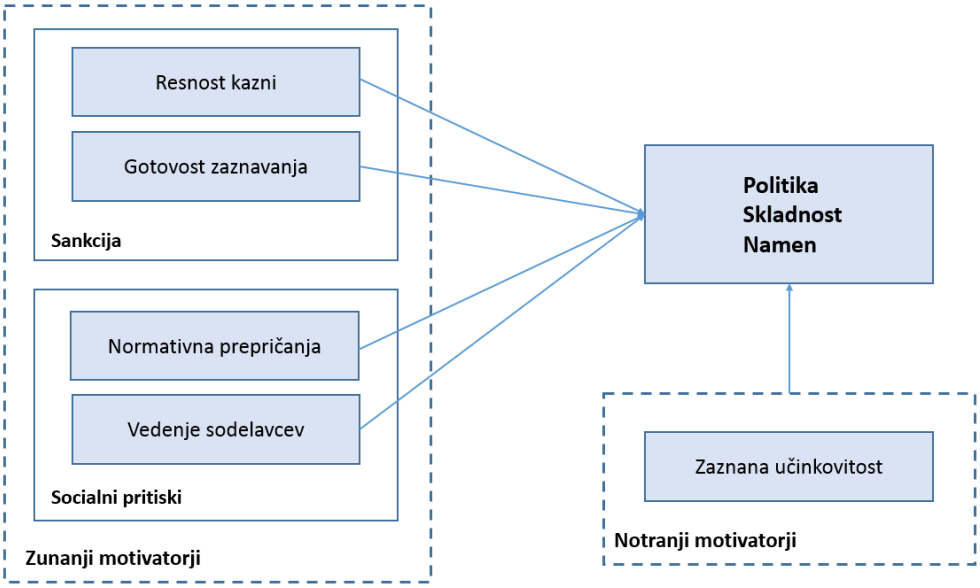
Slika 6 prikazuje teoretični model posameznikovega varnostnega vedenja z vključitvijo omenjenih hipotez. Hickmann Klein in Mezzomo Luciano (2016) v svoji raziskavi ugotavljata, da so zaznavanje dovzetnosti do groženj, resnosti grožnje in zadovoljstvo odločilni dejavniki za varno vedenje pri uporabi oziroma skrbi za zlonamerno programsko opremo v elektronskih sporočilih s podporo hipotez H1, H2, H6 in delno s hipotezo H3.

Rezultati tudi kažejo, da učinek zaznavanje resnosti kaznovanja ni najbolj pomemben dejavnik, pa čeprav je bila tudi ta hipoteza H4 podprta. Hipoteza H5 ni bila potrjena, saj v raziskavi ni bilo mogoče zaznati posameznikovega prizadevanja k dodatnemu zaščitniškemu naporu. Avtorja poudarjata, da zaščitniški napor s seboj prinaša tudi dodatno število postopkov, ukrepov in nalog, ki jih lahko posamezniki napačno dojamejo kot nenamerno oviro, katera lahko oteži ali celo ogrozi uporabnikovo delovanje pri varnostnem vedenju. Programi ozaveščanja bi morali posameznike usposabljati in izobraževati v smislu, da vsak posameznik razume prednost kontrole in zmanjševanja tveganja za morebitne grožnje.

Avtorja poudarjata, da se varnostne odločitve sprejemajo šele, ko se uporabniki zavedajo resnosti groženj in da so zanje dovzetni. Zato je izredno pomembno neprestano razvijanje smernic za ozaveščanje posameznikov, ki poudarjajo dovzetnost do grožnje in resnost grožnje. In prav poudarjanje dovzetnosti in resnosti grožnje, pri uporabniku sproži razumevanje po varnostni potrebi, opredelitvi njihovih vlog in odgovornosti pri varovanju informacij v organizaciji (Hickmann Klein & Mezzomo Luciano 2016).

Tudi Herath in Rao (2009) sta v svoji študiji analizirala posameznikovo varnostno vedenje, povezano z vlogo kaznovanja, izvajalnega pritiska in zaznane učinkovitosti s strani ukrepov zaposlenih. Pri tovrstnih raziskavah se je treba zavedati, da na posameznikovo vedenje vpliva veliko dejavnikov, ki prav zaradi različnih profilov osebnosti ljudi tudi različno vplivajo. Spodnja slika prikazuje grafični prikaz zunanjih in notranjih motivatorjev.

Slika 7: Zunanji in notranji motivatorji informacijsko varnostnega vedenja



Vir: Herath & Rao, 2009, str. 156

Pri opredeljevanju dejavnikov posameznika lahko ločimo notranje in zunanje motivatorje, ki bodisi pozitivno ali negativno vplivajo na posameznikovo varnostno vedenje. Notranji motivatorji so predvsem odraz zaznane učinkovitosti s strani posameznikov, medtem ko zunanje motivatorje ločimo v dve skupini. Prva skupina je skupina kazni in opredeljuje motivatorja resnosti kazni in gotovost zaznavanja groženj.

Drugo skupino pa sestavljata motivatorja, normativna prepričanja in vedenje sodelavcev, ki se povezujeta v skupini pod imenom socialni pritiski. Ti konstantni pritiski, ki se odražajo v normativnih prepričanjih, subjektivnih normah in medsebojnem vedenju med zaposlenimi in nadrejenimi tudi že v prejšnji raziskavi dokazano vplivajo na varnostno vedenje posameznikov pri varovanju informacij. Avtorja v svoji raziskavi ugotavljata, da ima raziskava več ključnih ugotovitev (Herath in Rao, 2009).

- Prvič, da tako notranji kot zunanji motivatorji resno vplivajo na namere posameznika pri spoštovanju varnostne politike v organizacije. To se predvsem odraža v posameznikovi pripravljenosti za udejstvovanje na različnih izobraževalnih treningih, ki se izvajajo na ravni neobveznega pristopa. Posamezniki z močnimi notranjimi in zunanjimi motivatorji pristopajo na izobraževalne treninge ne glede na njihovo obveznost ali izvajalno-udejstvovalnega pritiska nadrejenega.

- Drugič, da ima tudi družbeni vpliv pomembno vlogo pri varnostnem vedenju, saj normativna prepričanja v zvezi s pričakovanji nadrejenih, IT vodstva in sodelavcev igrajo pomembno vlogo pri varnostnem vedenju zaposlenih. V raziskavi ni ugotovljeno samo, da pričakovanja sodelavcev, temveč tudi njihova ravnanja, pomembno vplivajo na skladnost zaposlenih z varnostno politiko organizacije. To kaže, da lahko snovalci in upravljavci varovanja informacij izboljšajo skladnost z varnostjo, tako da izboljšajo varnostno klimo, ki tvori varnostno kulturo organizacije.
- Tretjič, da zanesljivost odkrivanja pozitivno vpliva na varnostni namen. V smislu dojemanja, da njihovi vsakdanji ukrepi, ki so povezani z varovanjem informacij, predstavljajo razliko pri doseganju splošne varnosti organizacije. Če se zaposleni zavedajo, da obstaja večja verjetnost, da bodo v okviru svojih dnevnih nalog naleteli na kakršne koli grožnje, bodo bolj sledili in upoštevali varnostna pravila in ukrepe, ki jih predpisuje varnostna politika organizacije.
- Ugotovljeno je bilo tudi to, da ima resnost kaznovanja tako v prejšnji raziskavi kot tudi v tej negativni vpliv na namere varnostnega vedenja. Pri proučevanju vloge sankcij in njihovega negativnega vpliva avtorja predlagata, da so negativne spodbude v smislu kazni učinkovite samo pri spodbujanju soglasnega sodelovanja in udejstvovanja na celotni ravni organizacije, vendar je njihova uporaba preprosto pogost neenakomerna in lahko povzroči neskladje med zaposlenimi (Herath in Rao, 2009).

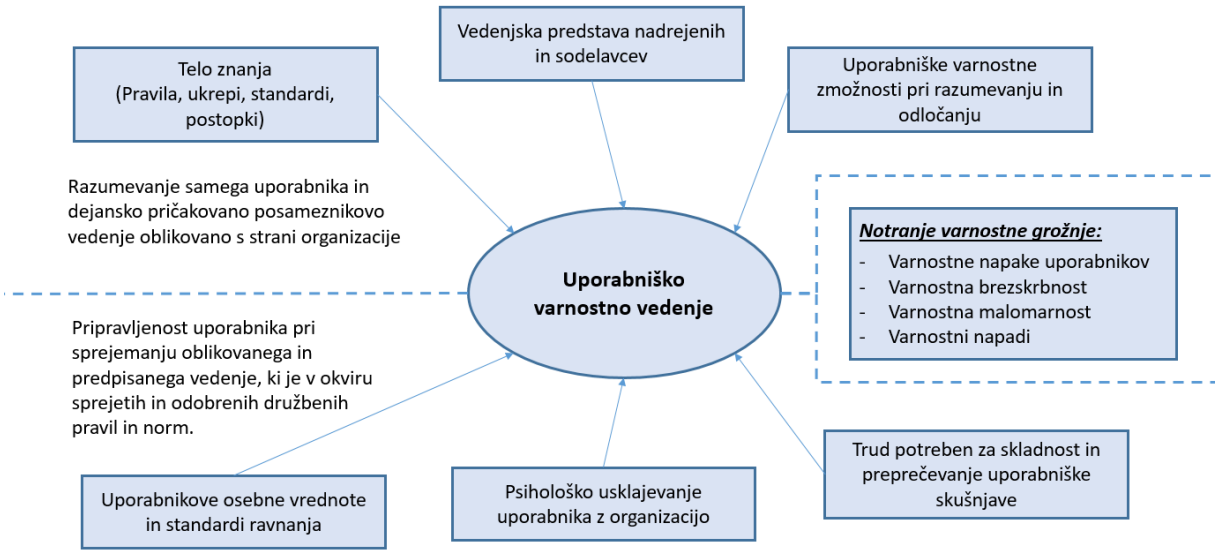
2.4.2 Ključni elementi izboljševanja varnostnega vedenja

Organizacije čedalje bolj posvečajo svojo pozornost obravnavi notranjih varnostnih groženj, saj smo prav posamezniki oziroma uporabniki znotraj organizacij najšibkejši členi v informacijski varnostni verigi. Prav zaradi tega se oblikujejo številni tečaji, ki so usmerjeni v samo izobraževanje posameznikov o pomembnosti varovanja informacij v organizacijah. A kljub temu ti tečaji sami po sebi z vidika posameznikov ne pritegnejo veliko pozornosti, zato je prva naloga pri tovrstnih tečajih posameznike dejansko motivirati in jim pojasniti, zakaj prav oni predstavljajo ključen del pri varovanju informacij v organizaciji.

Ko posamezniki razumejo pomembnost svoje vloge pri varovanju informacij, lahko začnemo z različnimi izobraževalnimi tečaji. Na omenjenih tečajih pa se je ključno osredotočiti na dejavnike, ki jih lahko pri posameznikih s pomočjo izobraževalnih tečajev tudi izboljšamo in nadgradimo.

Leach (2003) je v svoji študiji ključne dejavnike izboljševanja varnostnega vedenja najprej ločil v dve skupini. Prvo skupino predstavljajo dejavniki, ki zajemajo razumevanje samega uporabnika in dejansko pričakovano posameznikovo vedenje, oblikovano s strani organizacije. Druga skupina pa zajema dejavnike, ki vplivajo na osebno pripravljenost uporabnika pri sprejemanju oblikovanega in predpisanega vedenja, ki je v okviru sprejetih in odobrenih družbenih pravil in norm.

Slika 8: Ključni elementi izboljševanja varnostnega vedenja



Vir: Leach, 2003, str. 692

Zgornja slika prikazuje šest vplivnih dejavnikov, ki vplivajo na vedenje in ravnanje uporabnikov. Jasno je, da lahko organizacije pri izboljševanju omenjenih dejavnikov pričakujejo izboljšavo samo na nekaterih dejavnikih, ki jim posledično posvečajo večjo pozornost. Skoraj nemogoče pa je na ravni organizacije hkrati izboljševati vseh šest dejavnikov, saj je najprej treba skozi vedenjsko predstavo nadrejenih in sodelavce izobraževati, pri čemer je izredno pomembno usklajevanje posameznikovih vrednot in prepričanj z vrednotami organizacije.

Leach (2003) v svoji študiji ugotavlja, da organizacije lahko najbolj ogrozijo svojo notranjo varnost tako, da se osredotočijo predvsem na tiste dejavnike, ki jih realno že nadzirajo. To je najlažje, vendar visoko izobraževanje skoraj nič ne pomaga, če v organizaciji ne znajo uskladiti uporabnikovih osebnih vrednot z vrednotami organizacije. Organizacije morajo pridobiti čim širšo širino pokrivanja omenjenih dejavnikov izboljševanja posameznikovega varnostnega vedenja, a ob enem ne morejo pričakovati, da bo celotno njihovo osebje na svoja delovna mesta implementiralo visoke osebne standarde in norme, povezane z varovanjem informacij. Poleg tega ne morejo pričakovati, da bo celotno osebje spoštovalo in igralo po vseh pravilih in ukrepih, ki jih določa in predpisuje varnostna politika organizacija. Tukaj je ključa komunikacija in usklajevanje posameznikovih pričakovanj in zahtev z zahtevami organizacije (Leach, 2003).

Ker organizacije ne morejo izboljševati vseh dejavnikov posameznikovega varnostnega vedenja na enkrat, je smiselno se osredotoči najprej na ključne tri dejavnike, pomembne pri zmanjševanju groženj notranjega izvora (Leach, 2003):

- **Vedenjska predstava nadrejenih in sodelavcev** – Če organizacija želi, da se njihovi posamezniki držijo varnostnih pravil, mora le te podpreti s sistemi, ki bi zagotovili

upoštevanje njenih načel in politik. Le nekaj slabih varnostnih praks v realnosti lahko v organizaciji vzpostavi, da so vse varnostne prakse v očeh osebja oslabljene in nepotrebne, zato je pomembno, kdo in na kakšen način varnostne prakse izvaja. Treba je neprestano spremljanje na področjih, kjer so znanja s strani varovanja podatkov oslabljena bodisi zaradi nasprotujočih se sporočil posameznikov ali nasprotnih praks v sistemih. V tem primeru je treba konkretno posredovanje višjih vodstvenih sodelavcev, ki natančno raziščejo in razjasnijo problematiko osebja. Pri dobrem varnostnem vedenju pa je izrednega pomena tudi nagrajevanje osebja, ki se lahko kaj hitro spremenijo v osebje, ki jih je treba z dodatno motivacijo prepričati o usposabljanju in sprejemanju ustreznih ukrepov in pravil.

- **Uporabniške varnostne zmogljivosti pri razumevanju in odločanju** – Ljudje smo si po naravi različni, ampak odločitve, ki jih sprejmemo, postanejo del našega življenja in oblikujejo našo osebnost. Prav tako je pri odločitvah, ki smo in jih bomo sprejeli na podlagi varovanja informacij. Organizacija mora pri tem odigrati pomembno vlogo, saj morajo svojim uporabnikom zagotoviti dobro raven izobraževanja na področju varovanja podatkov, ker lahko le na podlagi slednjega uporabniki enostavneje sprejemajo varnostne odločitve zanesljivo in pravilo. V nasprotnem primeru se je težko izogniti različnim grožnjam, ki pretijo na organizacije in njihove podatke. Zdrav občutek je nekaj, kar lahko vsakdo prepozna, saj gre za spretnost odločevanja in ne kopičenje znanja. Tudi nespametna izobraževanja lahko v organizacijah pustijo posledice, saj so lahko uporabniki po njih še šibkejši in ne močnejši, zaradi prisotne zmedenosti, ki je posledica kopice informacij in znanja, omenjenega na tovrstnih izobraževanjih. Zdrav varnostni razum je nekaj, kar se lahko poučuje. Dejstvo je, da je vsakega uporabnika posebej, treba naučiti načel in pravil, ki so potreba za usmerjanje njihovih odločitev pri vsakdanjih opravilih in nalogah, ki jih izvajajo na njihovem delovnem mestu.
- **Psihološko usklajevanje posameznika z organizacijo** – Če organizacija zagotovi, da so njene norme in vrednote usklajene s posameznikovimi prepričanji in vrednotami, lahko z razvijanjem posameznikovih razumnih odločitev zmanjša tako število kot resnost varnostnih napak posameznikov. Prav tako se bo zmanjšala nenamerna komponenta grožnje notranje varnosti malomarnih dejanj in nepremišljenih napak uporabnikov. Pri sami stopnji vzpostavitve usklajevanja med posameznikom in organizacijo pa je ključa varnostna kultura. Prav ustvarjanje močne varnostne kulture je najboljši način, kako motivirati posameznike za dosledno, natančno in zavestno odločanje, ki posledično vpliva na psihološko usklajevanje posameznika z organizacijo. Tudi o varnostnih vprašanjih se mora v organizaciji redno poročati in ne samo na najvišjih nivojih. Vse pomanjkljivosti v organizacijah se morajo obravnavati kot resna vprašanja, ki morajo vzbuditi pozornost tako pri nižjih kot najvišjih ravneh.

Leach (2003) v svoji študiji tudi ugotavlja, da se ključno vodilo pri izboljševanju posameznikovega varnostnega vedenja odraža v samem vodenju in njegovem pristopu. Če se osebje na odločilnih pozicijah v organizaciji ne zmeni za informacijsko varnost, le zakaj bi se potemtakem zanjo morali zanimati ostali zaposleni v organizaciji.

Tudi Albrechtsen in Hovedn (2010) v svoji študiji raziskujeta elemente izboljševanja posameznikovega varnostnega vedenja, ki so prisotni v manjših organizacijah, ki si z vidika finančnih sredstev ne morejo privoščiti dragih izobraževalnih tečajev na tematiko informacijske varnosti. Izvedena je bila raziskava, ki je proučevala posameznikovo vedenje pred programom in po programu o osveščanju varovanja informacij. A pri tem je treba podariti, da gre za drugačno študijo, saj se obravnavana tematika v tej študiji razlikuje od glavnih ukrepov ozaveščanja o varnosti informacij, ki običajno poskušajo vplivati na oblikovanje posameznikove vedenjsko-varnostne ravni s pomočjo strokovnih pristopov, formalnih predstavitev in masovnih izobraževanj.

Vsi ti glavni ukrepi informiranja posameznikov o varovanju podatkov v ozadju običajno potekajo od zgoraj na navzdol, se pravi od vodstva pa vse do najnižjih skupin zaposlenih. Zaradi tega je ta študija še toliko zanimivejša, saj se avtorja osredotočata na majhne skupine posameznikov, ki izboljšujejo posameznikovo varnostno vedenja s programom lokalnega sodelovanja vseh zaposlenih, s skupnimi razmisleki, procesi, idejami in ustvarjanju znanja na organizacijsko manjšinski ravni. In prav ta medsebojna udeležba lokalnih sodelavcev s skupnimi procesi in idejami povzročajo kratkoročne spremembe v ozaveščenosti in posameznikovemu vedenju o varovanju informacij.

Avtorja ugotavljata, da se je prav v vseh skupinah med udeleženci raziskave po izvedenem programu bistveno razširil razpon kazalnikov o varnostnem osveščanju in vedenju oziroma z drugimi besedami, ustvarile so se pozitivne spremembe v varnostnem zavedanju in vedenju na ravni posameznikov. Z merjenjem medsebojnih odnosov in znanja posameznikov do informacijske varnosti, pred in po implementaciji programa, študija uspešno kaže, da majhne kratkotrajne delavnice, ki temeljijo na povečevanju informacijske varnosti, zagotavljajo močne spremembe v posameznikovem varnostnem vedenju. Ugotovljeni so bili tudi ključni elementi izboljševanja posameznikovega varnostnega vedenja. To so sodelovanje zaposlenih, medsebojni dialog, razmišljanje v medsebojno razumljivem jeziku, ki temelji na posameznikovih vrednotah in prepričanjih, skupnem zaupanju v skupino in izmenjavi lokalnega do sedaj pridobljenega in utemeljenega znanja. Vsi ti elementi pa morajo za uspešno nadgrajevanje posameznikovega varnostnega vedenja temeljiti na medsebojnem sodelovanju in ustreznem vodenju (Albrechtsen & Hovedn, 2010).

Pa vendar je pri vseh teh elementih izboljševanja posameznikovega varnostnega vedenja treba upoštevati, da ti »elementi« niso normativ za izboljševanje, saj prikazujejo samo možen pristop, katerega je mogoče prilagoditi tudi drugačnemu kontekstu ali celo drugačni vrsti nevarnosti in grožnjam. Zato ni nikoli povsem dobro v organizaciji implementirati čisto enakih varnostnih shem, katere avtorji v svojih študijah tudi obravnavajo in predstavljajo.

Pri izboljševanju posameznikovega varnostnega vedenja pa so tudi pomembne različne raziskave in analize, ki opredeljujejo in sooblikujejo naslednje smernice informacijske varnosti v organizacijah. Crossler, Johnston, Lowry, Hud, Warkentin in Baskerville (2013) v svoji študiji ugotavljajo, da si morajo strokovnjaki na področju informacijske varnosti še

naprej prizadevati za vključevanje drugačnih disciplin in modelov, na primer tisti, katerih so v preteklosti izhajali samo iz teoretičnih in metodoloških temeljev. Spodnja tabela prikazuje ugotovitve avtorjev na področju prihodnjih smernic v informacijski varnosti.

Tabela 4: Prihodnje smernice informacijske varnosti

Tematika:	**Moramo**	**Moramo premagati**
Notranje odklonsko vedenja	Ločiti med notranjim odklonskim vedenjem od notranjega nepravilnega vedenja in nadzora Meriti odklonsko vedenje	Omejitve raziskovalnega pristopa Družbeno zaželeno pristranskost
Razkrivanje skrivnostnega sveta hekerjev	Jasno razlikovati med vrstami hekerjev, ki jih preiskujemo Razumeti značilnosti različnih vrst hekerjev Določiti motivacijske izvore za različne vrste hekerjev	Ovire za identifikacije in dostopnosti do hekerskih skupnosti Omejene raziskovalne metodologije
Izboljševanje skladnosti informacijske varnosti	Razumeti primerno povezavo in usklajevanje strahu na podlagi prepričljivih komunikacij z interesi občinstva Razločiti med različnimi vrstami strahu Uporabiti uveljavljene vedenjske modifikatorje, kot sta odvračanje in zaznavanje organizacijske privlačnosti Razumeti motivatorje, ki spodbujajo zaposlene k odgovornosti in skladnosti Razumeti, kako posameznike na boljše načine spremeniti v varnostne zaveznike organizacije	Neenotno komunikacijsko vplivanje Omejene metode za zajemanje in razlikovanje med različnimi čustvi
Raziskovanje medkulturnih vidikov informacijske varnosti	Uporabiti uveljavljene medkulturne koncepte vedenjskih raziskovalnih projektov Razviti teoretično razumevanje za razlikovanje med informacijsko varnostnim vedenjem in kulturnimi stališči	Posploševanje posameznih kulturnih študij v medkulturne in druge koturne kontekste
Problematika merjenja in zbiranja podatkov	Izboljšati metode zbiranja in merjenja podatkov, povezanih z varnostjo Zajeti dejansko varnostno vedenje (varnostne kršitve, vdiranje, neskladnost z ukrepi in pravili) Bolje izkoristiti podatke, ki niso neposredno povezani z varnostjo za napovedovanje varnostnih izidov	Omejen dostop do podatkov, povezanih z varnostjo Omejene metode za zajemanja posameznikovega vedenja Premajhno uporabo kvalitativnih podatkov

Vir: Crossler, Johnston, Lowry, Hud, Warkentin & Baskerville 2013, str. 97

Izzivi za doseganje pomembnih raziskovalnih prispevkov se bodo vse bolj odražali na osredotočanju pozornosti pri razvijanju različnih načinov merjenja posameznikovega vedenja, povezanega z varovanjem informacij. Pri tem pa ne smemo pozabiti, da se poudarki na informacijsko varnost spreminjajo z nastankom novih groženj, ki se pojavljajo tako na tehničnih kot netehničnih ravneh (Crossler, *et. al.,* 2013).

2.5 Vloga človeškega faktorja

Parsons, McCormac, Pattinson, Butavicius in Jerram (2014) navajajo, da sama uporaba tehnologij za varnost informacij vedno ne vodi do izboljšanja varnosti. Prav zaradi tega človeški dejavniki igrajo pomembno vlogo pri zagotavljanju varnosti. Dejavniki, kot so posamezna razlika, kognitivne sposobnosti, zaznavanje tveganja in osebne lastnosti, lahko pomembno vplivajo na varnostno vedenje posameznikov. Na vse te dejavnike vpliva tudi organizacijska kultura in varnostno okolje, v katerem se pojavljajo. Prav ti dejavniki pa lahko zaradi različnega medsebojnega prekrivanja in vplivanja povzročijo vedenje, ki pogosto ogroža varnost informacij.

Številni tehnični napredki na področju informacijskih znanosti vedno ne zagotavljajo varnejšega okolja. Zato informacijske varnosti ni mogoče razumeti ali opisati zgolj kot tehnični problem. Tehnološke naprave, kot so računalniki, pametni telefoni, tablice, upravljajo ljudje, kar pomeni, da je pri varnosti informacij treba vzeti tudi v obzir vprašanje o človeških dejavnikov. Človeški dejavniki vplivajo na to, kako posamezniki komunicirajo s tehnologijo informacijske varnosti in prav ta medsebojna komunikacijska interakcija je pogosto škodljiva za varnost informacij. Zato je treba razumeti, kakšno vlogo ima človeški faktor pri zagotavljanju informacijske varnosti (Parsons *et. al.,* 2014).

Človeški faktor pa tudi občutno vpliva na kršitve informacijske varnosti, ki jo lahko razvrstimo na več različnih načinov. Swain in Guttman (1983) opredeljujeta pet različnih napak v človeškem faktorju, ki se lahko uporabijo za razlago kršitev informacijske varnosti. Prvič, obstajajo opustitvena dejanja, v katerih ljudje pozabijo opraviti potrebno ukrepanje. Na primer, na področju informacijske varnosti bi to lahko pomenilo neuspešno spreminjanje gesel ali neuspešno odjavljanje posameznikov iz računalniških sistemov. Drugič, napake so običajno dejanja nepremišljenosti, v katerih ljudje nepravilno izvajajo postopek ali ukrepe, kot je zapisovanje gesel npr. na različnih samolepilnih listkih. Tretjič, številne napake nastanejo zaradi tujih dejanj. Četrtič, napake lahko povzročijo zaporedna dejanja, ki vključujejo ostale posameznike, posledično se le te izvajajo v napačnem vrstnem redu. Petič, časovne napake, ki jih povzročijo ljudje, ki v določenem času ne opravljajo svojih nalog.

Furenll (2005) ugotavlja, da je pravzaprav večina napak človeškega faktorja naključnega izvora. Nenamerne napake človeškega faktorja so pravzaprav povezane z načinom, kako posameznik sodeluje s sistemom, in dokazi kažejo, da lahko ljudje naletijo na težave že pri

iskanju, razumevanju in uporabi zaščitnih elementov, zato je njihova interpretacija izredno pomembna.

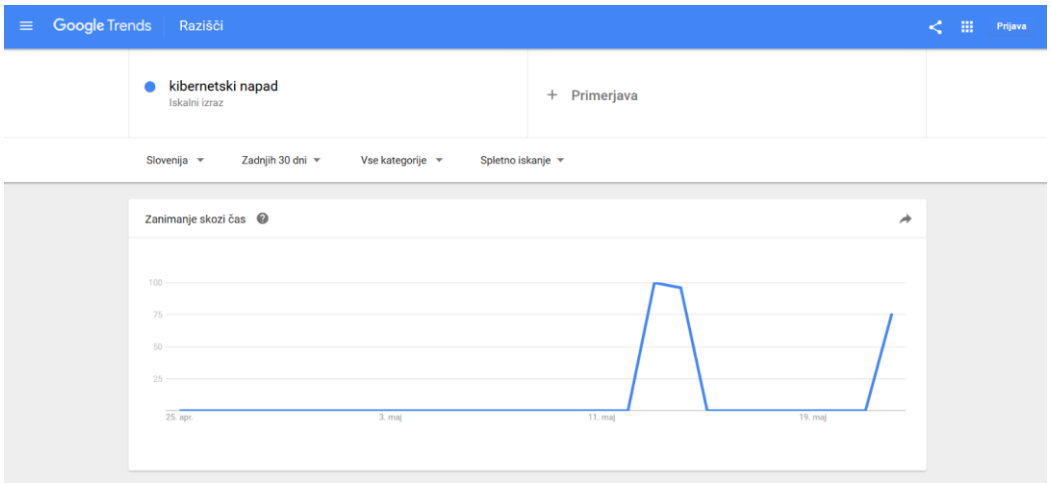
Obenem pa Schultz (2005) opozarja, da je treba poudariti tudi pomen uporabnosti interakcije med slabo uporabnostjo in človeško željo po iskanju bližnjic, ki so varnostno vprašljive. V bistvu varnostne tehnologije pogosto vključujejo zapletene kontra-intuitivne procese, ki jih večina posameznikov težko razume. Prav zaradi zapletenih postopkov se posamezniki odločajo za uporabo bližnjic oziroma se hočejo »tem postopkom« izogniti, kjer koli je to mogoče in s takšnimi dejanji povečujejo verjetnost kršitve in ogrozitve informacijske varnosti. Tudi nemotivirani uporabniki kažejo na to, da je varnost pri njih šele sekundarni ali terciarni cilj, zato ljudje pogosto nimajo motivacije za sledenje in upoštevanje zapletenih varnostnih postopkov (Schultz, 2005).

2.5.1 Človeški faktorji, ki vplivajo na varnostno vedenje posameznika

Parsons in drugi (2014) v svoji študiji opisujejo več različnih človeških faktorjev, ki vplivajo na varnostno vedenje posameznika. V svoji študiji vključujejo načine, na katere posamezniki sprejemajo odločitve ter pristranskost in hevristiko, ki vplivata na zaznavanje posameznikovega tveganja, vključno z razpoložljivostjo hevristike in pristranskosti optimizma. Pomembna pa je tudi stopnja nadzora posameznikov, saj, če ljudje občutijo prevelik pritisk oziroma preveliko stopnjo nadzora nad tem, kar počnejo, bolj tvegajo in precenjujejo njihove sposobnosti nadzora nad grožnjami. V nadaljevanju so predstavljeni človeški faktorji, ki vplivajo na varnostno vedenje posameznika oziroma na zaznavanje varnostnega tveganja (Parsons *et. al.*, 2014).

- **Hevristična razpoložljivost** – Eden najpomembnejših predsodkov posameznikov je znan kot hevristična razpoložljivost, ki temelji na ideji, da ljudje po navadi presodijo pogostost ali verjetnost dogodka na podlagi tega, kako hitro in kako dobro se je nekega dogodka mogoče spomniti. To je tudi tesno povezano z medijsko pokritostjo dogodkov, saj ko se zgodijo dogodki velike razsežnosti, so tudi veliko bolj nepozabni in opevani. Problem medijskega prostora pa je, da podcenjujejo dogodke, ki imajo večjo pogostost pojavljanja, saj z njihovega vidika niso zanimivi, ker ne ponujajo neke svežine in nove tematike. V informacijski varnosti v to tematiko sodijo vprašanja, ki vključujejo dejavnike, ki so priča slabi usposobljenosti posameznikov z neustreznimi postopki in slabo zasnovanimi sistemi. Po drugi strani pa imajo različni hekerski napadi velikih razsežnosti, veliko medijsko pozornost in pokritost. Spodnja slika prikazuje pogostost iskanja izraza »kibernetskega napada« ki se je zgodil v prvi polovici maja in je imel svetovne razsežnosti. Zaradi velike medijske pokritosti omenjene tematike, so tudi posamezniki začeli poizvedovati in iskati, kaj dejansko kibernetski napad pomeni. Na sliki vidimo, da pred napadom ni bilo zaznanega iskanja pod besedo »kibernetski napad« po napadu in medijskem poročanju pa je iskalnik zabeležil 100-kratno iskanja omenjene besede.

Slika 9: Prikaz hevristične razpoložljivosti v praksi



- **Optimistična pristranskost** – največja problematika omenjenega faktorja je, da je takšna oblika pristranskosti še posebej prisotna in razširjena na področju informacijske varnosti, saj različni dokazi kažejo, da večina uporabnikov ne verjame, da bi hekerje utegnilo zanimati prav njihove informacije in podatki, ki jih imajo shranjene na svojih računalnikih. V tem primeru se ti uporabniki ne morejo postaviti v vlogo žrtve, saj so mnenja, da do tega sploh ne bo prišlo. Prav tako je ta oblika posebej razširjena tudi, ko ljudje pričakujejo različne opozorilne napise in oznake, ki kažejo na njihovo ranljivost. Njihova prepričanost v smislu: »če ni opozorilnih znakov, so tudi v prihodnje izvzeti iz varnostnih tveganj« je napačna, saj prav zaradi prevelikega optimizma podcenjujejo resnost tveganja in tudi zato nimajo oziroma ne kažejo kakršne koli motivacije biti v stiku s posodobljenimi varnostnimi ukrepi, popravki in pravili. V praksi pogosto slišim, da imajo na računalnikih samo excelove preglednice in wordove dokumente, in da za varovanje le teh ne potrebujejo nikakršnih ukrepov, povezanih z varovanjem informacij. Ob enem pa se ravno zaradi prevelikega optimizma pristranskosti ne zavedajo, da ravno te preglednice in dokumenti posamezniku predstavljajo vir informacij in osnovo za njihovo vsakdanje delo.
- **Raven nadzora** – posamezniki imajo lahko tudi nerealno oblikovano raven nadzora oziroma z drugimi besedami nerealno oblikovan optimizem za tveganja, saj so mnenja, da ko so stvari pod njihovim osebnim nadzorom, grožnje obravnavajo kot manj tvegane. Te osebe lahko z nespoštovanjem varnostnih politik povzročijo resne posledice. V praksi opažam predvsem tako obliko vedenja pri posameznikih, ki imajo v kolektivu visoko ali kar najvišjo raven usposobljenosti za svoje delo. Prav pri teh posameznikih je velika verjetnost, da bo njihova visoka usposobljenost in spretnost razlog za precenitev ravni nadzora in zmožnosti nadzora nad grožnjo.
- **Raven znanja** – pomanjkanje znanja posameznikov lahko predstavlja veliko tveganje na področju varovanja informacij. Zavedam se, da je pogosto z vidika posameznika težko razumeti tveganje in s tem morebitne povezane grožnje brez razumevanja osnovnih pojmov, ukrepov in pravil informacijske varnosti. Primer faktorja ravni znanja se v praksi prav pogosto pojavlja npr. pri oblikovanju gesel. Posamezniki v večini ne razumejo, zakaj

morajo imeti dolga gesla, ki si jih komaj zapomnijo. Zakaj mora geslo vsebovati velike, male črke, številke in posebne znake? V tem primeru je treba posamezniku natančno opredeliti in opisati omenjeno problematiko oblikovanja gesel. Razložiti mu je treba, da lahko hekerji z različnimi programi oziroma generatorji ugotavljajo njihova gesla. Krajša in enostavnejša so gesla, lažje ga pridobijo in uporabijo za krajo podatkov. Zato je raven znanja ne samo pri oblikovanju gesla, ampak tudi pri ostalih ravneh znanja informacijske varnosti pomembna za preprečevanje morebitnih varnostnih groženj.

- **Kompenzacija tveganja** – je človeški faktor, ki pomaga razložiti, zakaj se posamezniki, ki se zavedajo varnostnih postopkov, v praksi povsem vedno ne držijo varnostnih načel, ki so v skladu z varnostno politiko organizacije. Kompenzacijo tveganja posamezniki dojemajo tako, da zaradi izboljšane ali posodobljene zaščite varnostnih ukrepov npr. požarne zaščite, zmanjšujejo morebitne grožnje in zato lahko spremenijo svoje vedenje, ki je z vidika varovanja informacij varnostno vprašljivo. V praksi se to pogosto pojavlja takrat, ko v organizacijah na različnih sestankih svojim zaposlenim delijo znanje, da so v organizaciji vzpostavili nove tehnične varnostne mehanizme za zmanjševanje groženj. Ob ne vključevanju posameznikov v proces vzpostavitve novih tehničnih mehanizmov, to pri njih vzbudi manjše zanimanje in manjšo skrb za varovanje informacij z mislijo, da bodo sedaj novi varnostno-tehnični mehanizmi poskrbeli za njihovo varnost na njihovem delovnem mestu.
- **Kumulativno tveganje** – je dejavnik, ki predstavlja verjetnost nezaželenega dogodka v smislu grožnje. Posamezniki se zavedajo, da je pojavitev nezaželenega dogodka v določenem časovnem obdobju izredno majhna, ob tem pa pozabljajo na možnost, da to tveganje s časom narašča. Praktični premer kumulativnega tveganja je, če se posameznik na določen dan med malico ne odjavi iz sistema. Verjetnost za nastanek grožnje ob neupoštevanja varnostnega protokola na tisti dan je sicer zelo majhna, a vendar, če se posameznik v času malice tedensko ali celo mesečno ne odjavlja iz sistema, je tveganje za nastanek grožnje veliko večje.
- **Opustitev predsodkov** – v tem primeru posamezniki ocenijo stopnjo neukrepanja ob določenih situacijah in sprejmejo določeno tveganje, ki je z njim povezano. Praktični primer je redno, mesečno ali tedensko, spreminjanje svojih gesel. Posameznik v tem primeru oceni stopnjo neukrepanja in sprejme določeno tveganje, ki je povezano z oblikovanjem gesla na (več)letni uporabi. Pri takem vedenju lahko posameznika dejansko z različnimi programskimi okni na mesečni ravni, ki zahtevajo najprej vnos starega in potem še vpis novega gesla, prisilimo v mesečno spreminjanje gesel. Ob tem pa uporabniku onemogočimo, da izbere isto različico gesla, kot ga je uporabljal v prejšnjem mesecu.
- **Vpliv poznavanja** – Poznavanje varnostnih tveganj je v samem procesu izobraževanja varovanja informacij ključnega pomena. Novejša in neznana tveganja so pogosto pri posameznikih manj podcenjena, saj posamezniki v celoti niso seznanjeni z omenjeno tveganostjo, a ob enem naj poudarim, da je prevzemanje novejšega in nezaželenega tveganja med posamezniki nezaželeno. Z drugimi besedami, posamezniki bodo bolj verjetno prevzemali tveganja, s katerimi so v celoti seznanjeni. V praksi to pomeni, če so

posamezniki v celoti seznanjeni s posledicami in koristmi na področju redne mesečne menjave gesel, bo tovrstna oblika veliko bolj zaželena kot različne uporabe generatorjev gesel ali drugačnih oblik preveritve istovetnosti osebe.

- **Vpliv opisovanja** – način opisa oziroma oblikovanja varnostnih ukrepov in tveganj lahko pomembno vpliva na posameznikovo zaznavanje varnosti le teh. V praksi to pomeni, da posamezniki vedno strmimo k maksimiranju naših koristi bodisi finančnih ali osebnih. Tako je tudi pri organizacijah. Posamezniki bodo z večjo verjetnostjo upoštevali ukrepe in pravila, povezana z varnostno politiko organizacije, če bo opis temeljil na možnih dobičkih namesto izgubah. Oziroma z drugimi besedami, opis mora temeljiti na poudarku posameznikovih koristi. Posameznikom je treba z opisom razložiti, kakšne koristi bodo imeli, če bodo upoštevali in implementirali varnostne protokole na njihovo delovno mesto. To pa je veliko težje kot opisovanje raznoraznih posledic, ki bodo posameznike doletele ob neupoštevanju predpisanih varnostnih ukrepov.
- **Osebnost in kognitivni slog** – Posamezne razlike v zvezi s faktorjema, kot sta osebnost in kognitivni slog, lahko vplivajo tudi na zaznavanje tveganja in nagnjenosti k sprejemanju. Z drugimi besedami osebnost in kognitivni slog močno vplivata na posameznikovo zaznavanje pomembnosti na področju varovanja informacij. Ločimo osebe, ki so nenaklonjene tveganju, osebe, ki so do tveganja nevtralne, in osebe, ki so tveganju naklonjene. V praksi to pomeni, da posamezniki, ki na splošno zavračajo tveganje, bodo na področju informacijske varnosti previdnejši in upoštevali bodo pravila in ukrepe, predpisane v varnostni politiki organizacije. Bolj bodo pozorni tudi na stroške, povezane s tveganjem in njihovim nepravilnim varnostnim vedenjem in ravnanjem.
- **Vpliv družbenih faktorjev** – tudi skupinska prepričanja in norme vplivajo na varnostno vedenje posameznikov. Ljudje na splošno upoštevamo skupinske norme in prepričanja, kar se odraža v posledici, če v skupini prevladuje mnenje, da je varnost informacij pomembna in resna težava, potem bodo vsi posamezniki v tej skupni z zavzetostjo in resnostjo upoštevali varnostne predpise in ukrepe, povezane z varnostno politiko organizacije. Po drugi strani pa imajo lahko družbeni vplivi tudi negativne posledice, ki so lahko tudi kompleksne narave. Lep primer je, ko sodelavec prosi za geslo za prijavo v neki sistem, ki ga le občasno uporablja. Če mu geslo posredujemo, lahko kršimo varnostno politiko organizacije, v nasprotnem primeru pa, če gesla svojemu sodelavcu ne zaupamo, je zavrnitev delitve gesla mogoče razumeti kot znak nezaupanja in lahko z omenjeno potezo, kaj hitro zaostrimo medsebojne odnose. Ti družbeni oziroma socialni in skupinski dejavniki so močno povezani z organizacijo kulturo podjetja. Se pravi, če je varnostna kultura v organizaciji na visokem nivoju, sodelavec v takem primeru v prvi vrsti ne bi prosil za posredovanje gesla, ampak bi prosil za posameznikovo pomoč pri omenjeni problematiki. Omenjeni pristop reševanja težav znotraj organizacije se odraža v dobri medsebojni komunikaciji in povezanosti, ki predstavljata osrednja člena vsake organizacijske kulture.

Posamezniki imajo in bodo tudi v prihodnosti imeli pomembno vlogo pri varovanju informacij. Organizacije aktivno uporabljajo varnostne tehnologije, vendar varnosti ni

mogoče doseči samo s pomočjo tehnoloških orodij, saj brez upoštevanja človeškega faktorja, organizacija kot taka ne more zagotoviti ustrezne ravni varnosti. Uporabnikova prepričanja, stališča in dojemanje varovanja informacij oblikuje njihovo varnostno vedenje, na katero lahko s pravilnimi izobraževanji in treningi tudi vplivamo. Te vrste posameznikovega vedenja, ki vključujejo človeške faktorje, pa lahko tudi v nadaljevanju opredelimo (Dourish *et al,* 2004, Leach 2003 &Parkin, *et al,* 2009):

- **Pomanjkanje informacijske varnosti** – z različnimi dejanji lahko zaradi pomanjkanja znanja kaj hitro kliknemo na nevarne povezave, delimo gesla s prijatelji, pozabimo implementirati varnostna pravila, ukrepe in postopke v naš vsakdanjik. Ob tem pa se dejansko tudi ne zavedamo, kakšna so morebitna tveganja in posledice omenjenih dejanj.
- **Nevednost** – posamezniki pogosto zaradi pomanjkanja motivacije in lastne nevednosti preprosto ignorirajo implementacijo varnostnih pravil v svoj vsakdanjik.
- **Napadi** – posamezniki pa lahko zaradi občutka medsebojnega slabega spoštovanja in občutka zanemarjanja s strani organizacije z namernimi dejanji oškodujejo in oblikujejo grožnje, ki temeljijo iz osebnih razlogov. Tovrstni načini napadov so pogosto veliko bolj kompliciran od različnih hekerskih napadov, saj le ti posamezniki delujejo z namero, da na največji možni način prizadenejo in oškodujejo organizacijo.
- **Pragmatizem** – mlajše generacije so bolj pragmatične glede varnostnih potreb organizacije, poznajo tveganja in so pripravljene, da jih tudi upoštevajo in sprejemajo, ampak samo v primeru, če tovrstno sprejemanje povezanih dejanj z informacijsko varnostno prinaša boljše plačilo, saj sedaj poleg vsakodnevnih nalog skrbijo tudi za njihovo varno in pravilno uporabo.
- **Nesmiselnost** – hekerji bodo vedno s svojimi spretnostmi našli načine, kako slediti tehnološkim izboljšavam in jih uporabiti za različna nezakonita dejanja. Zato je z vidika organizacije pomembno vsem zaposlenim pokazati, da so stvari pod nadzorom in sredstva zavarovana, samo če se vsi držijo varnostnih pravil in ukrepov na področju varovanja informacij.

2.5.2 Vpliv starostnega faktorja na varnostno osveščanje posameznika

Tudi starostni faktor pomembno vpliva na varnostno osveščanje posameznikov. Wilford in Wakunuma (2014) v svoji študiji ugotavljata, da so starejši strokovnjaki na področju informacijske tehnologije pokazali znatno višje zavedanje in zaznavanje samega razumevanja glede pomena etičnih vprašanj pri varovanju informacij od mlajši strokovnjakov. Študija je bila izvedena z intervjuji 26 strokovnjakov na področju informacijske varnosti iz celega sveta. Kar 70 % intervjuvancev v izbranem vzorcu je presegalo mejo 50-tih dopolnjenih letih.
Študija obravnava starost kot dejavnik pri zavedanju etičnih vprašanj v smislu: kako večja ozaveščenost in skrb vplivata na zrelost trenutnih strokovnjakov na področju informacijske varnosti. Trenutno nosilci odločitev in oblikovalci politik, ki pripadajo starejši skupini, še vedno težijo k temu, da so precej bolj zreli in imajo večjo ozaveščenost glede etičnega razumevanja in zaskrbljenosti kot mladi strokovnjaki.

Najnovejša in aktualna ozaveščenost se je oblikovala na podlagi dolgoletnih izkušenj, znanja in vzrokov za zaskrbljenost priznanih strokovnjakov. Študija v nadaljevanju dokazuje, da se zaradi povečevanja izkušenosti in etičnosti, posameznikom dolgoročno tudi izboljšuje produktivnost in učinkovitost, hkrati pa tudi ščitenje organizacijo in s tem povezano povečevanje ugleda. Iz zapisanega lahko sklepamo, da so zrelost, izkušnje in funkcionalno strokovno znanje kazalniki ravni etičnega vedenja oziroma zavedanja. Poleg tega avtorici v svoji študiji tudi ugotavljata, da imajo starejši strokovnjaki zaradi dolgoletnih izkušenj večje spretnosti, ki se jih da priučiti šele z leti proučevanja različnih izzivov in razmer, zato bodo tudi manj verjetno sodelovali pri različnih varstveno izobraževalnih usposabljanjih oziroma treningih. To potrjuje tudi dejstvo, da je bilo pri starejših strokovnjakih zaradi dolgoletnih izkušenj, znanja in zrelosti zaznan višji nivo znanja o razumevanju etičnih pomislekov kot pri mlajših udeležencih. Glede na to, da študija poveličuje izkušnje, in ne le »talenta«, ki vodijo k dobremu odločanju, zavedanju in razumevanju, je vseeno treba zagotoviti, da so strokovnjaki na področju informacijske varnosti ne glede na starost vedno izpostavljeni visokim standardom in pričakovanjem etičnega vedenja nadrejenih. Pomembno pa je tudi, da je sama etika predmet izobraževanja na tehničnih ravneh, saj lahko le z vključevanjem etike ublažimo problematiko pomanjkanja izkušenj, ki je bila zaznana pri mlajših strokovnjakih (Wilford &Wakunuma 2014).

2.5.3 Raven faktorja vključenosti posameznika v varnostno politiko organizacije

Faktor vključenosti posameznikov v varnostno politiko organizacije igra pomembno vlogo pri oblikovanju varnostnega vedenja posameznikov. Varnostna politika se v organizaciji izvaja s kombinacijo posameznikovih dejanj, procesov in tehnoloških kontrol. Z vidika posameznikov varnostna politika usmerja zaposlene, ki obdelujejo informacije in določajo izhodišča, na podlagi katerih se sprejemajo etične odločitve pri obravnavi organizacijskih informacij. Politika vpliva na način, kako zaposleni sodelujejo z informacijskimi sredstvi organizacije in posledično na njihovo usmerjanje varnostnega vedenja, ki mora biti v skladu s pravili in ukrepi ter raznoraznimi pogodbenimi zahtevami. Za upoštevanje varnostne politike organizacije pa sta pomembna predvsem dva dejavnika: to sta zavedanje in neprestano usposabljanje posameznikov (De Veiga, 2016).

Poleg zavedanja in usposabljanja posameznikov, pa obstajajo tudi drug številni dejavniki, ki z različnimi raziskavami dokazano vplivajo na zaznavanje skladnosti posameznikov z varnostno politiko organizacije. Ena izmed tovrstnih raziskav je tudi raziskava Herath in Rao (2009), ki ugotavljata in opredeljujeta poleg zavedanja in usposabljanja posameznikov še tri dodatne dejavnike, ki vplivajo na skladnost posameznikov z varnosti politiko. In sicer dojemanje groženj glede resnosti kršitve, organizacijske zavezanosti in socialni vplivi ter razpoložljivost virov. Vsi ti dejavniki tudi dokazano vplivajo na skladnost posameznikov z varnostno politiko organizacije.

De Veiga (2016) v svoji raziskavi ugotavlja, da je kultura informacijske varnosti posameznikov, pri tistih, ki so bili seznanjeni in so prebrali varnostno politiko organizacije, precej bolj pozitivna v primerjavi z zaposlenimi, ki z varnostno politiko niso bili seznanjeni in je tudi niso prebrali. Ugotavlja tudi, da samo branje varnostne politike uspešno prispeva k pozitivnemu vplivanju na varnostno kulturo organizacije. Tudi sama varnostna kultura v organizacije, ki predstavlja splošno dojemanje o varovanju informacij večine zaposlenih, se s časoma razvija in postaja vse močnejša. Tudi pri posameznikih, ki niso bili seznanjeni in niso prebrali varnostne politike, se je v organizaciji oblikovala nekakšna subkultura, v kateri je bilo mogoče zaznati povečano zanimanje za seznanjenost in branje varnostne politike organizacije. Zavedanje o varnostni politiki informacij pomembno prispeva k spodbujanju in izoblikovanju močnejše varnostne kulture. V takem okolju lahko pričakujemo tudi manj morebitnih incidentov oziroma groženj človeškega izvora (De Viega, 2016). Torej, večji kot je faktor vključenosti posameznika v varnostno politiko organizacije večje bo posameznikovo zavedanje o pomembnosti varovanja informacij in posledično manjša bo verjetnost pojavitve različnih varnostnih incidentov oziroma groženj.

2.6 Informacijski varnostni razkorak med managerji in uporabniki

Številne raziskave kažejo, da obstaja informacijski varnostni razkorak med managerji in uporabniki glede njihovih različnih pogledov in izkušenj o praksah na področju varovanja informacij. Partridge (2005) v svoji raziskavi proučuje tradicionalni digitalni razkorak, katerega lahko razumemo kot socialno-ekonomsko perspektivo, ki se ukvarja z dostopom do informacijsko-komunikacijske tehnologije, zlasti interneta in z možnostjo uporabe te tehnologije za polno sodelovanje v poslovnem, političnem in družbenem življenju. Prav ta digitalni razkorak pušča posledice tudi v informacijsko varnostnem razkoraku med managerji in uporabniki. Warschauer (2002) v svoji raziskavi trdi, da je treba digitalni razkorak razumeti širše tudi v psihološkem, kulturnem in sociološkem smislu. Saj v tem primeru ne gre le za fizični dostop do računalnikov in povezljivosti, ampak tudi za zmožnost posameznikov, da v celoti tudi izkoristi informacijski sistem organizacije, ki mu je trenutno na voljo.

Strokovnjaki za informacijsko varnost večinoma obravnavajo uporabnike kot grožnje varnosti informacij, uporabniki pa menijo, da so prav zaradi nerazumnih odločitev in pravil strokovnjakov, neizkoriščen vir pri varovanju informacij (Albrechtsen, Hovden, 2009). Omejena interakcija med uporabniki in upravljavci informacijske varnosti povzroča pomanjkanje medsebojnega razumevanja pri obravnavi različnih stališč. In prav ti različni pogledi na interpretacije informacijske varnosti so razlog, da upravljavci informacijske varnosti s svojimi praktičnimi metodami strmijo k implementaciji nerealnih ukrepov, pravil in predpostavk, zaradi katerih so prav pristopi upravljanja slabo usklajeni z dinamiko delovnega dne posameznikov.

Albrechtsen in Hoved (2009) v svoji raziskavi ugotavljata, da imajo uporabniki in upravljavci informacijske varnosti zaradi različnih pristojnosti, oblik pooblastil ter racionalnosti tudi

različne poglede glede stališč informacijske varnosti. Dejstvo je, da sta ohranjanje in neprestano izboljševanje na področju informacijske varnosti v organizaciji glavni dve nalogi upravljavcev oziroma managerjev za informacijsko varnost. A ob tem ne smemo pozabiti, da imajo posamezniki na drug strani prav tako pomembne naloge, ki so predvsem usmerjene v doseganje organizacijskih ciljev glede produktivnosti, uspešnosti, dobička itd. Ob tem pa se morajo zavedati, da so prav ti uporabniki odgovorni za vzdrževanje informacijske varnosti v organizaciji, saj upravljavci informacijske varnosti sami po sebi brez vključitve uporabnikov ne morejo zagotoviti željene stopnje ravni varovanja informacij.

Avtorja v raziskavi tudi ugotavljata, da digitalni razkorak, sam po sebi ni grožnja za funkcionalnost upravljanja informacijske varnosti. Vendar pa razlike pri pristopu, izkušnjah, razumevanju in prednostnih nalogah med managerji in uporabnikih na omenjenem področju vodijo k strategijam upravljanja s strani managerjev, ki temeljijo na nekoliko pristranskem mnenju, da posamezniki predstavljajo bolj grožnjo varnosti kot vir za ohranjanje in povečevanje informacijske varnosti (Albrechtsen & Hoved, 2009). Ne glede na razkorake pa v praksi opažam, da tako upravljavci informacijske varnosti kot uporabniki čedalje bolj zahtevajo večjo interakcijo in medsebojni dialog na področju varovanja informacij. Prav takšen pristop pa bo v prihodnosti izboljševal razumevanje med različnimi nalogami tako managerjev informacijske varnosti kot uporabnikov. Prav z večjo interakcijo in medsebojnim dialogom bi bili ukrepi na področju varovanja informacij učinkovitejši, ob tem pa se bi med omenjenima skupinama zmanjševal tudi informacijsko varnostni razkorak.

3 KVALITATIVNA RAZISKAVA NA PODROČJU VLOGE POSAMEZNIKA V INFORMACIJSKI VARNOSTI

Empirični del magistrskega dela se osredotoča na kvalitativno raziskovanje v obliki polstrukturiranih globinskih intervjujev, pri katerih se prav glavna vrednost odraža v prilagodljivosti in odprtosti na eni strani, ter možnosti oblikovanja podrobnejših odgovorov, miselnostih in zaključkov intervjuvancev na drugi strani. V ta namen je bila v nadaljevanju tudi izvedena kvalitativna raziskava na področju vloge posameznika pri zagotavljanju informacijske varnosti v organizacijah. Vsi intervjuji pa so zasnovani in usmerjeni v proučevanje vloge posameznika pri zagotavljanju informacijske varnosti v organizaciji. Pri oblikovanju vprašanj za intervjuje mi je bila v oporo celotna teoretična podlaga, ki sem jo vseskozi pridobival s temeljitim pregledom strokovnih člankov in knjig na področju informacijske varnosti v organizacijah.

Namen kvalitativne raziskave je na podlagi polstrukturiranih globinskih intervjujev ugotoviti, kakšna je vloga posameznika pri oblikovanju in zagotavljanju informacijske varnosti ter kateri so tisti človeški faktorji, ki so najbolj pomembni pri oblikovanju in zagotavljanju informacijske varnosti v organizaciji. Z raziskavo pa tudi skušam ugotoviti, ali se vloga posameznika pri zagotavljanju informacijske varnosti v organizacijah razlikuje glede na

panogo in velikost podjetja. V ta namen sem v raziskavo tudi skušal vključiti podjetja različnih panog in različnih velikostih.

3.1 Kvalitativna raziskava

Kvalitativna raziskava je primerna predvsem za preiskovalno delo, saj zaradi svoje prilagodljivosti in odprtosti omogoča natančnejšo opredelitev obravnavane tematike, pridobivanje novih idej in smernic, dopolnjevanje, potrjevanje ter natančnejšo razlago same kvalitativne analize. Malhotra (2002) navaja, da se glavna značilnost kvantitativnih raziskav predvsem odraža v njihovem namenu pridobivanja kvalitativnega razumevanja osnovnih razlogov in motivov. Ob tem pa poudarja, da mora biti vzorec utemeljen na majhnem številu nereprezentativnih enot, da je zbiranje podatkov nestrukturirano, saj analiza podatkov ne temelji na uporabi različnih statističnih metod, ampak na podlagi pridobljenega rezultata analize, ki pa se odraža prav v osnovnem razumevanju proučenega problema. Tudi Denzin in

Lincoln (2005) opredeljujeta kvalitativno raziskavo, kot raziskavo, ki v prvi vrsti vključuje naravnistične pristope, povezane s trenutnim svetovnim stanjem v obravnavani tematiki. To pomeni, da kvalitativni raziskovalci na splošno proučujejo stvari v njihovih naravnih okoljih, poskušajo občutiti in razložiti različne pojave v smislu razumevanja pomenov v obravnavani tematiki. Prav zaradi proučevanja stvari v njihovih nravnih okoljih je kvalitativna raziskava koristen vir informacij za opredeljevanje ozadja obravnavanega vprašanja. S tovrstnim raziskovalnim pristopom pa povečujemo tudi možnost natančnejše opredelitve določenih mnenj in izkustev intervjuvancev.

Avtorja poudarjata, da se kvalitativne raziskave z uporabo intenzivnejših metod raziskovanja, kot so npr. globinski polstrukturirani intervjuji, omogoča bogatejši in širši pogled na obravnavano tematiko. Tudi medsebojni odnos med tako imenovanim respondentom (intervjuvancem) in izpraševalcem je v tej obliki raziskovanja precej daljši, golobji in prožnejši (Denzin & Lincoln, 2005).

Glavne metode kvalitativnega raziskovanja so: individualni globinski intervjuji, fokusne skupine in različne projektivne tehnike. Intervjuje delimo na nestrukturirane, polstrukturirane in strukturirane. V svoji kvalitativni analizi sem izbral globinske individualne polstrukturirane intervjuje, s katerimi skušam na najboljši možni način pridobiti nekaj pomembnih odgovorov in mnenj respondentov na obravnavano tematiko magistrskega dela. Pri tem moram podariti, da je obravnavana tematika z vidika respondenta izredno občutljiva, zato sem moral biti še toliko bolj pazljiv pri izbiri raziskovalne metode. Z izbrano metodo kvalitativnega raziskovanja bom na najboljši možni način opredeliti vlogo posameznika pri oblikovanju in zagotavljanju informacijske varnosti ter najpomembnejše človeške faktorje in raziskal, če se vloga posameznika razlikuje glede na velikost organizacije in prisotnosti v različnih panogah.

3.2 Globinski polstrukturirani intervjuji

Malhotra in Briks (2003) navajata, da je globinski intervju že v svoji osnovi zasnovan oziroma usmerjen v nestrukturirani direktno-osebni intervju, s katerim intervjuvar odkriva poglede, odnos, prepričanja, motivacijo in občutke subjekta do določene tematike. Globinski intervjuji trajajo različno: od pol ure pa tudi do več kot ene ure. Intervjuvar ima možnost, da celoten intervju opravi v enem obisku ali pa se odloči za serijo medsebojnih srečanj med intervjuvancem in izpraševalcem. V sami raziskavi sem se odločil, da izberem enkratni obisk na posameznega intervjuvanca, saj je z vidika obravnavane tematike ta oblika tudi najbolj smiselna, saj sem se s sogovorniki za polstrukturirani globinski intervju zaradi njihove delovne obremenjenosti in zasedenosti, dogovarjal tudi po več tednov.

Malhotra in Briks (2003) v svoji študiji pojasnjujeta, da naj se izpraševalec skozi celoten intervju drži osnovne tematike oziroma osnovnega področja obravnave. Avtorja poudarjata, da se bistvo polstrukturiranih globinskih intervjujev skriva v nepredvidljivih in nepričakovanih podvprašanj, ki se razvijajo skozi celotno medsebojno komunikacijo. Izpraševalec mora v intervjujih zagotoviti primerna ter smiselna podvprašanja in hkrati sogovorniku tudi zagotoviti pogovorno sproščujoče okolje. Prav vodenje in usmerjanje poteka intervjuja predstavlja glavna gradnika za oblikovanja pogovorno sproščujočega okolja, ki je še toliko bolj pomemben, ko obravnavamo tematike, ki so v določenih pogledih izjemno občutljive.

Tudi Churchill in Brown (2004) v svoji študiji pojasnjujeta, da se glavna značilnost v polstrukturiranih globinskih intervjujih kaže v možnosti oblikovanja različnih podvprašanj v posameznih sklopih intervjuja. Prav ta podvprašanja pa pri kasnejšem preiskovanju in analiziranju posameznikovih odgovorov, predstavljajo glavni odraz kakovosti polstrukturiranih globinskih intervjujev.

Z globinskimi individualnimi polstrukturiranimi intervjuji skušam na najboljši možni način pridobiti nekaj pomembnih odgovorov in mnenj izpraševalcev na obravnavano tematiko. Z izbrano metodo kvalitativnega raziskovanja bom na najboljši možni način opredelil vlogo posameznika pri oblikovanju in zagotavljanju informacijske varnosti, opredelil najpomembnejše človeške faktorje in raziskal, če se vloga posameznika razlikuje glede velikosti organizacije in njenega delovanja v različni panogi. V ta namen sem tudi skušal pridobiti sogovornike, ki so v svojih organizacijah odgovorni za informacijsko varnost ter izobraževanje posameznikov ob dodeljevanju varnostnih vlog, pravil in ukrepov v njihovem vsakdanjem delavniku.

Pri samem oblikovanju vprašanj sem veliko pozornost, prav zaradi precej občutljive tematike, namenim dejstvu, ki poudarjajo avtorji, da je treba že pred samim začetkom intervjuja zagotoviti pogovorno sproščeno okolje. Sogovornik se mora počutiti sproščeno in lagodno, saj bo le na ta način imel možnost posredovanja iskrenih in zanesljivih odgovorov.

Prvi pristop pri samem oblikovanju in zagotavljanju pogovornega sproščujočega okolje je izbira lokacije intervjuja. Intervjuji so potekali v sogovornikovih pisarnah, saj se v njih sogovorniki počutijo domače in tudi prostor je po navadi dovolj zvočno izoliran za snemanje intervjuja. Če sem intervju snemal, sem se moral s sogovorniki že vnaprej dogovoriti in v večni primerov tudi podpisati izjavo o zagotavljanju anonimnosti in molčečnosti.

Glavne prednosti globinskih intervjujev v primerjavi s fokusnimi skupinami se predvsem kažejo v (Malhotra, 2003):

- **Heterogenosti** – globinski intervjuji v primerjavi s fokusnimi skupinami na nek način ne omejuje posameznikovih mišljenj, saj so le ta po navadi v fokusnih skupinah vodena s strani celotne skupine. Tudi drugače razmišljujoči posamezniki se v tovrstnih skupinah ne počutijo najbolj sproščene.
- **Delovni obremenjenosti** – najboljši udeleženci globinskih intervjujev so pogosto posamezniki z izredno natrpanimi urniki, zato pogosto nimajo časa se udeleževati različnih fokusnih skupin. Prav zaradi natrpanih urnikov je v tem primeru najboljša oblika globinskega intervjuja, kar na njegovi lokaciji. S tem korakom tudi pokažemo, da cenimo njihov čas in se ob enem potrudimo, da ta čas tudi najbolje izkoristimo.
- **Vplivu izpraševalca** – izpraševalec je pri skupinskih diskusijah vedno omejen in nima veliko možnosti eksperimentiranja. Medtem ko pri globinskih intervjujih, izpraševalci lahko eksperimentirajo in dodajajo nova vprašanja, ki so povezana z obravnavano temo. Za izboljševanje samega vzdušja lahko tudi pred vprašanji podajo kakšen kompliment.
- **Zapisovanju odgovorov** – v primerjavi s fokusnimi skupinami je globinski intervju pogosto bolj primeren, ko želimo intervjuvati točno določeno osebo, saj potemtakem nimamo težav z analiziranjem oziroma pripisovanjem določenih odgovorov določenemu udeležencu fokusne skupine.
- **Globljem pogledu** – z globinskimi intervjuji imamo na splošno večji vpogled v obravnavano problematiko.
- **Sproščujočem vzdušju** – čeprav mora izpraševalec zagotoviti sproščujoče vzdušje med intervjujem, je to pogosto veliko lažje doseči kot pri fokusnih skupinah.
- **Lažji organizaciji** – z razliko od fokusne skupine imamo pri globinskem intervjuju samo enega sogovornika oziroma udeleženca, zaradi katerega je potem tudi veliko laže vse skupaj organizirati.
- **Izvedbi** – izpraševalec dobi veliko informacij, že s tem, ko sogovornika spozna in ga vidi na njegovem vsakdanjem delovnem mestu oziroma v njegovem naravnem okolju. Pogosto prihaja do tega, da je izpraševalec v globinskih intervjujih udeležen v delovno atmosfero sogovornika, ta pa pomaga pri oblikovanju celotne slike o sodelujočem.

Churchill in Brown (2004) navajata tudi nekaj slabosti globinskih intervjujev v primerjavi s fokusnimi skupinami:

- **Stroški** – globinski intervjuji so za izpraševalca po navadi veliko dražji kot oblikovanje fokusnih skupin, saj se zaradi individualne obravnave vsakega sogovornika stroški močno povečajo.
- **Vpletenost udeleženca** – pogosta slabost globinskih intervjujev je, da je treba udeleženca izjemno motivirati za obravnavano temo, ob tem pa ne smemo pozabiti, da po navadi imamo na voljo le slabo uro, to pa je za nekatere vrste raziskav občutno premalo.
- **Čas in velikost vzorca** – s fokusnimi skupinami hitro narašča število udeležencev, medtem ko se pri globinskih intervjujih to število giblje po navadi prav zaradi stroškov obravnave med štirimi in petimi udeleženci oziroma sogovorniki. Tudi z vidika obravnave so globinski intervjuji izjemno časovno potratni.
- **Skupinska dinamika** – pri globinskih intervjujih ni skupinske dinamike, ker sta v celoten proces intervjuja vpeta samo dva: izpraševalec in intervjuvanec.

3.3 Potek raziskave

3.3.1 Določitev vzorca in potek raziskave

Polstrukturirane globinske intervjuje uvrščamo med kvalitativne raziskave, ki navadno temeljijo na namenskih vzorcih. To pomeni, da gre pri tej obliki intervjuja za neverjetnostjo vzorčenje, katerega glavna značilnost je, da raziskovalec oziroma izpraševalec namensko izbere vzorčne enote. Raziskovalec v prvi vrsti izbira tiste enote, ki so po njegovi presoji oziroma mnenju najbolj reprezentativne za proučevano populacijo. Poenostavljeno v svojo raziskavo vključuje tiste enote, za katere je mnenja, da prav oni predstavljajo najboljše predstavnike določene skupine. V svoji raziskavi sem v vzorec vzel tiste enote, ki so po moji presoji oziroma mnenju najbolj reprezentativne za proučevano populacijo.

V prvi vrsti so bili v vzorec vzete osebe, ki so neposredno odgovorne za informacijsko varnost v svoji organizaciji. V večjih organizacijah so to pogosto osebe na delovnem področju imenovanemu CISO (*ang. Chief Information Security Officer)* oziroma danes se tudi uporablja izraz CSO (*ang. Chief Security Officer*) za osebe, katerih dnevne naloge so izključno vezane za zagotavljanje informacijske varnosti v organizaciji. Ker sem skušal v svojo analizo vključiti tudi manjša podjetja, ki so v slovenskem prostoru številčno najmočnejša, so bile v analizo tudi vključene osebe, ki so poleg ostalih delovnih nalog odgovorne tudi za informacijsko varnost.

Naj poudarim, da je namensko vzorčenje v prvi vrsti z vidika oblikovanja analize dokaj ugodno, hitro ter ustrezno, vendar pa na drugi strani ne omogoča posploševanja podatkov za določeno populacijo, saj populacija zaradi namenskega vzorčenja ni jasno definirana. Raziskovalec oziroma izpraševalec se mora zavedati, da je taka oblika vzorčenja subjektivna in njen izid oziroma vrednost je popolnoma odvisna od raziskovalčevega mnenja, presoje in strokovnosti. Prav zaradi tega je izjemno pomembno, da izpraševalec na obravnavanem

področju s temeljitim strokovnim pregledom literature pridobi določeno širino, katera mu kasneje nudi in omogoča analiziranje obravnavanega področja.

3.3.2 Izvedba in potek intervjujev

Po pregledu različnih korakov, stopenj in okvirjev za izvajanje intervjujev sem določil, da tiste ključne posamezne okvirje združim in oblikujem šest posameznih korakov, na podlagi katerih so bili intervjuji tudi izvedeni:

1. **Določitev obravnavanega področja** – obravnavno področje sem določil že v teoretičnem delu magistrskega dela in se nanaša na ugotavljanje vloge posameznika pri zagotavljanju informacijske varnosti. Kakšno vlogo ima dejansko posameznik v celotnem procesu zagotavljanja informacijske varnosti.
2. **Načrtovanje in oblikovanje intervjujev** – ta korak zajema velikost, obsežnost in izbiro sogovornikov v intervjujih. Treba je bilo izdelati tudi opomnik, ki mi je v prvi vrsti nudil oporo med izvedbo intervjujev ter nekakšno zagotovilo za njihovo lažjo obravnavo in primerjavo.
3. **Izvedba intervjujev** – predstavlja osrednji del raziskave, zato je ključnega pomena, da vsi intervjuji potekajo na primerni lokaciji v sproščujočem ozračju. Da bo temu res tako, so bili intervjuji izvedeni v sogovornikovih pisarnah. Pred izvedbo intervjuva pa je izredno pomembno izkazovanje hvaležnosti in zainteresiranosti v obravnavani tematiki.
4. **Analiza intervjujev** – v koraku analize je predhodno treba opraviti tudi transkripcijo, ki predstavlja nekakšno osnovo za dobro analizo. Pred analizo je treba dodobra proučiti vse oblike shranjevanja intervjujev - tako raznoraznih zapisanih mislih in idej, ki nastanejo med samim intervjujem kot tudi obliko zvočnega snemanja intervjuja, če je tovrstna oblika bila s strani sogovornika dovoljena. Uporabljal sem analize po posameznih tematskih sklopih.
5. **Verifikacija** – predstavlja zadnji korak pri obdelavi posameznih intervjujev. Namen tega koraka je določitev zanesljivosti, veljavnosti in splošne uporabnosti rezultatov v raziskovanem področju. Treba je natančno opredeliti, ali je celotna raziskava bila uspešna s strani obravnavanega področja. Saj se velikokrat zgodi, da je raziskava raziskovala področje, katerega zaradi nestrukturirane oblike analiziranja v prvi vrsti sploh ni imela namen raziskati.
6. **Podajanje rezultatov** – predstavlja zadnji korak, v katerem moramo bralcu na berljiv, razumljivi in primaren način pojasniti ugotovitve, ki so se oblikovale med kvalitativno raziskavo. Pri predstavitvi svojih rezultatov bom uporabil tekstovno poročanje, ki bo v prvi vrsti vključevalo vse glavne pojme, podajal bom glavne ugotovitve, katere bodo tudi v nadaljevanju združene v zaključku oziroma v sklopu oblikovanja morebitnih domnev.

Prav vsi intervjuji so potekali v sogovornikovih pisarnah, saj so si le tako lahko vzeli nekaj dragocenega časa in sodelovali v intervjujih. Spodnja tabela prikazuje vzorec sogovornikov in nekaj osnovnih podatkov o organizacijah, v katerih so zaposleni. Vzorec sestavljajo peti

predstavniki, ki so v organizacijah odgovorni za izvajanje različnih procesov, nalog in delujejo na področju informacijske varnosti.

Tabela 5: Značilnosti intervjuvancev

Oseba	Spol (m/ž)	Izkušnje na obravnavanem področju (leta)	Delovno mesto
A	M	4	Manager informacijske varnosti (CISM)
B	Ž	3	Vodja oddelka za sistem in inf. varnost
C	M	6	CSO (Chief Security Officer)
D	M	8	CISO (Chief information security officer)
E	M	1	IT oddelek - Poslovni analitik

Tabela 6 prikazuje podrobne podatke o izvedenih polstrukturiranih globinskih intervjujih in informacijo o velikosti podjetja. Zaradi zagotavljanja anonimnosti tako intervjuvancev kot organizacije tabela ne vključuje opisa dejavnosti organizacije, saj bi z njim lahko nehote razkril identifikacijo tako intervjuvancev kot tudi organizacije.

Tabela 6: Podatki o izvedenih polstrukturiranih globinskih intervjujih

Oseba	Datum intervjuja	Čas intervjuja (min)	Lokacija intervjuja	Velikost podjetja
A	19.10.2017	62	Ljubljana	Veliko
B	23.10.2017	58	Kranj	Majhno
C	25.10.2017	64	Maribor	Srednje
D	26.10.2017	70	Ljubljana	Veliko
E	2.11.2017	54	Ljubljana	Malo

Pri razvrščanju organizacije glede na velikost podjetja sem uporabil Zakon o gospodarskih družbah (ZGD-1NPB14), v katerem 55. člen opredeljuje velikost in pogoje za uvrstitev organizacije v mikro, majhno, srednje ali veliko družbo.

3.3.3 Opomnik za izvedbo polstrukturiranih globinskih intervjujev

Pri polstrukturiranih globinskih intervjujih je izrednega pomena tudi oblikovanje opomnika, ki na eni strani nudi oporo med izvedbo intervjuja in na drugi strani deluje kot nekakšno zagotovilo za lažjo obravnavo in primerjavo medsebojnih intervjujev. Opomnik je sestavljen iz štirinajstih vprašanj in podvprašanj. Vsa vprašanja in podvprašanja so usmerjenja v opredeljevanje vloge posameznika pri zagotavljanju informacijske varnosti v organizaciji. Vprašanja so zasnovana na način, ki omogoča razkritje dodatnih pogledov ter ozadji posameznih pojmov in mislih intervjuvancev. Vsa vprašanja pa so tudi oblikovana na podlagi tematskih sklopov, ki sem jih kasneje uporabil pri sami navzkrižni metodi analiziranja intervjujev.

Opomnik za izvedbo polstrukturiranih globinskih intervjujev je sestavljen in osmih tematskih sklopov in ti združujejo štirinajst vprašanj in podvprašanj:

- Prvi tematski sklop predstavlja nekakšen uvod v intervju in je bolj splošen, saj raziskujem, kako intervjuvanci pravzaprav razumejo pojme, kot so informacijska varnost, informacijska varnostna kultura in upravljanje informacijske varnosti.
- Drugi sklop predstavlja razumevanje informacijske strukture in samooceno stopnje zadovoljstva z informacijsko varnostjo v njihovih organizacijah.
- V tretjem sklopu raziskujem njihov pogled na najpogostejšo šibkost ureditve informacijske varnosti znotraj njihove organizacije.
- V četrtem sklopu raziskujem njihove poglede na opredeljevanje same vloge posameznika pri varovanju podatkov.
- V petem sklopu raziskujem pomembnost varnostne politike v organizaciji in udejstvovanje posameznikov na različnih delavnicah in tečajih o informacijski varnosti.
- V šestem sklopu raziskujem njihov pogled na dejavnike, ki močno vplivajo na varnostno vedenje posameznikov.
- V predzadnjem sedmem sklopu združujem raziskovanje ključnih elementov izboljševanja varnostnega vedenja posameznika z opredelitvijo vloge človeškega faktorja v organizaciji pri varovanju podatkov.
- V zadnjem sklopu pa raziskujem njihove poglede na trenutno najbolj zahtevne dejavnike varovanja podatkov in njihove poglede pri prihodnjih izzivih in smernicah na področju informacije varnost v njihovi organizaciji.

V prilogah sledijo vprašanja, ki so bila oblikovana v opomniku kot pomoč pri izvedbi polstrukturiranih globinskih intervjujev.

3.3.4 Analiza podatkov

V primerih, ko se je potek intervjuja lahko snemal, sem uporabil metodo zgoščevanja različnih pomenov in zaključkov intervjuvancev po posameznih sklopih. Te pomene oziroma zaključke sem dobesedno prepisal na bolj zgoščen in za analiziranje intervjujev obvladljiv način. Pri intervjujih, pri katerih je bila izražena želja, da se ne snemajo, sem si sproti po posameznih sklopih zapisoval odgovore, mnenja, presoje in zaključke intervjuvancev. Zaradi različnega načina shranjevanja intervjujev, sem moral tudi intervjuje, v katerih so intervjuvanci izrazili željo, da se jih ne snema, še enkrat dobesedno prepisati na bolj zgoščen in za analiziranje obvladljiv način. Iz prepisa obeh oblik shranjevanja intervjujev sem dobil sistematizirano obliko, v kateri so bili podani ključni odgovori in mnenja intervjuvancev. Le z načinom dobesednega prepisa vseh posameznih intervjujev sem ohranil glavna dejstva in misli posameznih intervjuvancev.

Za analizo polstrukturiranega globinskega intervjuja sta primerna dva pristopa. S prvim pristopom lahko analiziramo in se osredotočimo na posamezne intervjuje in tako oblikujemo

posamezne sklope podajanja odgovorov. Drugi pristop pa je, da s pomočjo navzkrižne analize povezujemo odgovore in misli vseh intervjuvancev. Pri prvem načinu iščemo predvsem razlikovanje med intervjuji in njihovimi odgovori, medtem ko pri drugem načinu s povezovanjem različnih odgovorov iščemo širino oziroma globino pri posameznem sklopu oziroma vprašanju. Analiza intervjujev je izvedena z navzkrižno analizo, s katero povezujem odgovore intervjuvancev po posameznih tematski skopih, kateri so oblikovani na podlagi opomnika za intervjuje.

3.4 Rezultat raziskave

Rezultat raziskave podajam po tematskih sklopih, ki so bili oblikovani v opomniku za izvedbo polstrukturiranih globinskih intervjujev. Vsi sklopi si sledijo po zaporedju, po katerem sem tudi izvedel posamezni intervju. Na začetku so tematski sklopi bolj splošnih tem, nato se pomikajo do bolj specifične tematike in tematike opredeljevanja vloge posameznika pri zagotavljanju informacije varnosti. Na koncu pa so tudi podane domneve, ki so se oblikovane na podlagi povezovanja teoretičnega dela z rezultati analize polstrukturiranih globinskih intervjujev.

3.4.1 Analiza raziskave po tematskih sklopih

3.4.1.1 Razumevanje pojmov: informacijska varnost, varnostna kultura, upravljanje informacijske varnosti

Vsi intervjuvanci so se v tem uvodnem sklopu dobro odrezali in mi tudi na kratek in jasen način razložili razliko med omenjenimi pojmi. Najbolj natančno opredelitev pri razumevanju pojma informacijska varnost je podala oseba C, ki informacijsko varnost opredeljuje kot nekakšen skupek njihovih strategij, s katerimi upravljajo procese, orodja in politike, potrebne za preprečevanje in odkrivanje tako notranjih kot zunanjih groženj, ki bi morebitno negativno vplivale na delovanje njihove organizacije. Nadaljuje »*Bistvo informacijske varnosti je v varovanju podatkov in pravilne razporeditve med njihovo razpoložljivostjo, zaupnostjo in celovitostjo«*. Oseba B čisto na kratko razloži, da informacijsko varnost razume kot pojem, ki v organizacijah na splošno opredeljuje neko stanje splošne zaščite pred nepooblaščeno uporabo njihovih informacij oziroma ukrepov, sprejetih za dosego zlonamernega cilja.

Medtem ko oseba A informacijsko varnost opredeljuje kot neprestano upravljanje s tveganji, povezanimi z morebitnimi napadi oziroma grožnjami. Osebi B in E razumeta informacijsko varnost kot neko osnovo za nemoteno in predvsem varno delovanje svoje organizacije. Ob tem poudarjata, da si zaradi majhnosti organizacije in omejenih sredstev ne morejo privoščiti visoke stopnjo zaščite na področju informacijske varnosti, ampak vseeno to ni izgovor, da na tem področju njuni podjetji ne bi bili dejavni. Oseba D pri tem poudarja ključni dve besedi, ki sta po njegovem mnenju osnovna gradnika informacijske varnosti, to sta varnost (*ang. Security*) in zasebnost (*ang. Privacy*), kateri je med seboj treba tudi ločiti. Nadaljuje z razlago:

»*Varnost je tehnološka funkcija, ki ščiti dostop do podatkov, ščiti pred nepooblaščenimi dostopi do informacij, medtem ko je zasebnost pravna funkcija, ki določa, kdaj in komu je dostop do določenih informacij dovoljen. Zasebnost v naši organizaciji predstavlja temelj ščitenja podatkov pred nepooblaščenimi razkritji«.*

Pri opredeljevanju informacijske varnostne kulture sta osebi A in C razložili, da je opredeljevanje omenjenega pojma resnično težko natančno razložiti in definirati, saj na eni strani povezuje informacijsko varnost z organizacijsko kulturo organizacije in na drugi strani v to povezuje tudi vse zaposlene tako znotraj kot zunaj organizacije. Oseba D varnostno kulturo razume kot: »*Medsebojni odnos, ki je odraz povezanosti zaposlenih v smislu varnostnega zavedanja in vedenja pri varovanju vseh informacijskih sredstev podjetja*«. Oseba B opredeljuje, da je temeljni gradnik varnostne kulture organizacijska kultura s pridihom informacijske varnosti. Oseba E informacijsko varnostno kulturo opredeljuje kot nekaj, kar povezuje njihove zaposlene v celotno kulturo podjetja, ki je podprta z neko splošno informacijsko varnostjo.

Pri opredeljevanju upravljanja informacijske varnosti v njihovih organizacijah se je večina intervjuvancev osredotočala na opredeljevanje varnostne politike podjetja ter na vključevanje obvladovanja tveganj, upravljanje morebitnih incidentov, poročanja, neprestanega spremljanja rezultatov, ukrepov in odgovornosti. Oseba D je pri tem poudarila, da gre pri opredeljevanju upravljanja informacijske varnosti za bistveno večji obseg kot samo oblikovanje varnostne politike podjetja ter spremljanje morebitnih tveganj in incidentov. Nadaljuje »*Upravljanje informacijske varnosti v našem podjetju razdelimo na dva dela. V prvi del zajemamo celotno obvladovanje tveganj, vse standarde, postopke, procese, izobraževanja, varnostno politiko itd., v drugi del upravljanja informacijske varnosti pa vključujemo vsa sredstva za financiranje prvega dela.* Ob tem pa je tudi poudaril, da je treba s strani organizacije vse procese in naloge, ki se izvajajo za zagotavljanje informacijske varnosti, tudi razdeliti in prilagoditi različnim nivojem oziroma oddelkom znotraj organizacije. Tudi Bernik in Selan (2008) podobno opredeljujeta upravljanje informacijske varnosti, saj prav tako razdeljujeta upravljanje informacijske varnosti na dva dela, in sicer: management izvajanja oziroma operativni management in strateški management oziroma management odgovornosti.

3.4.1.2 Informacijska struktura in samoocena stopnje zadovoljstva informacijske varnosti

S tem sklopom sem imel kar precej težav, saj so se sogovorniki precej izogibali sami opredelitev njihove informacijske strukture in medsebojnih povezav. V veliki večini so se prav oni opredelili kot odgovorne osebe ali kot posrednik za njeno neprestano izboljševanje. Dobil sem odgovore, da je njihova informacijska struktura nekaj posebnega in ne bi želeli prikazovati celotne slike podjetja. A dejali so tudi, da njihova informacijska struktura ne predstavlja nobenih omembe vrednih posebnosti, ki bi jih lahko izpostavili. Vsebinsko so nekaj povedali o samih programih, ki jih zaposleni uporabljajo pri vsakodnevnih nalogah. Oseba C je pri tej tematiki govorila, da v njihovi organizaciji uporabljajo SCADA (ang.

Supervisory Control And Data Acquisition) z DoS (ang. *Denial Of Service*) in DDoS (ang. *Distributed Denial Of Service*) zaščito, ki je v prvi vrsti namenjena zmanjševanju tveganja za izgube podatkov, strank, ugleda in gospodarske škode, ki bi lahko nastali zaradi vdora v njihov sistem. Medtem ko oseba D pri tej tematiki razlaga o strukturirani postavitvi strežnikov, saj so imeli do sedaj že veliko težav predvsem s prekomerno vlago in nepooblaščenimi vdori. Nato podaja, da so v zadnjih letih te težave odpravili, saj imajo postavljene strežnike na različnih lokacijah, za katere v njihovi organizaciji ve le malo ljudi in tudi možnost dostopa ima zelo malo ljudi.

Oseba A odgovarja, da informacijske strukture organizacije v celoti ne bi izpostavljal. Poudarja, da je izredno težko oceniti, katera strojna in programska oprema, bo imela v svoji življenjski dobi odkritih največ ranljivosti in v kakšnih obsežnostih. Poudarjajo, da napadalci izkoriščajo kakršne koli informacije o ranljivosti informacijske strukture podjetja in napadajo tako omrežja, omrežne rešitve, strežnike, aplikacije kot tudi medsebojne povezave. Oseba E je edina oseba, katera se v tem sklopu ni opredelila kot odgovorna za izboljševanje informacijske strukture in je pri odgovoru na to vprašanje začela razlagati o organizacijski strukturi podjetja. Četrto vprašanje ocenjujem kot neuspešno, saj tudi z dodatnimi vprašanji in nekoliko drugačno zasnovo oziroma interpretacijo samega vprašanja med intervjuji nisem uspel pridobiti informacij, ki sem jih želel.

Sogovorniki so bili bolj zgovorni, ko so podajali samooceno, povezano s stopnjo zadovoljstva z informacijsko varnostjo v njihovih podjetjih.

Oseba A je podala oceno 7. Zaposlena je na delovnem mestu managerja informacijske varnosti s certifikatom (CISM) in dobro pozna ozadje celotne informacijske varnosti organizacije. Njegove delovne obveznosti obsegajo tudi pisanje tedenskih in mesečnih poročil o izboljšavah na področju informacijske varnosti in odkrivanju morebitnih groženj v njihovi organizaciji. Ob tem poudarja, da je trenutno v njihovi organizaciji zaposlenih kar nekaj strokovnjakov s področja informacijske varnosti in ob enem poudarja, da je to področje, katerega na splošno velika podjetja čedalje bolj cenijo in kadrovsko tudi neprestano razvijajo. Podano oceno pojasnjuje: »*V podjetju imamo kar nekaj vzpostavljenih mehanizmov za povečevanje informacijske varnosti: od digitalnih podpisov pa vse do različnih ravni avtorizacije, katera je potrebna na določenih ravneh organizacije, zato stopnjo informacijske varnosti ocenjujem s 7.*«

Oseba B je vodja oddelka za sisteme in informacijsko varnost. Podala je oceno 7 in jo pojasnjuje z argumenti, da čeprav gre za majhno podjetje, v katerem se nikakor ne splača šolati posebnih varnostnih oziroma sistemskih inženirjev, ki bi bili dejavni samo na področju informacijske varnosti, je vseeno mnenja, da je to področje nujno ne glede na velikost podjetja. Nadaljuje *»V podjetju bi lahko še veliko naredili za samo izboljšavo informacijske varnosti, ampak smo trenutno zadovoljni in samo stopnjo informacijske varnosti ocenjujemo s 7, ob tem pa vseeno poudarjam, da z razpoložljivimi sredstvi, ki so resnično minimalni, skušamo maksimalno zagotoviti varno poslovanje našega podjetja.«*

Oseba C je podala oceno 8 in je trenutno v svojem podjetju na poziciji CSO (Chief Security Officer). Oceno pojasnjuje, da so v njihovem podjetju vedno v koraku z razvojem informacijske varnosti. Trenutno imajo kar nekaj mehanizmov varovanja podatkov od dvofaktorske avtorizacije z EMV-CAP-om, kateri je trenutno na udaru zaradi oteževalnih dostopov, vse do različnih identifikacijah mehanizmov uporabnikov. Zaradi specifične dejavnosti imajo kar nekaj varnostnih protokolov, kateri niso podprti samo z različnimi varnostmi sistemi, ampak tudi z neprestano fizično prisotnostjo varnostnikov.

Oseba D je v svojem podjetju trenutno na poziciji CISO. To je oseba, ki ima dolgoletne izkušnje na področju varovanja informacij in pri ocenjevanju stopnje zadovoljstva z informacijsko varnostjo v podjetju. Pravi: *»V času mojega kadrovanja na poziciji CISO do sedaj nismo zaznali oz. beležili večjih groženj, ki bi neposredno vplivale na sam ugled oziroma poslovanje našega podjetja. To je priča temu, da je trenutni varnostni sistem v našem podjetju zadovoljiv. Seveda se vedno znova in znova odkrivajo pomanjkljivosti oziroma tako imenovane varnostne luknje, katere je potrebno neprestano odkrivati, kontrolirati in odpravljati. Z neprestanim odkrivanjem in kontroliranjem celotnega informacijskega sistema znižujemo možnost pojavitve groženj, zato stopnjo zadovoljstva z informacijsko varnostjo v našem podjetju ocenjujem z 8. Vedno pa je prostor, kjer bi bilo potrebno določene procese z vidika varovanja informacij bolje zaščititi oziroma prenoviti!«*

Oseba E je podala oceno 6. Trenutno opravlja delo podatkovnega analitika in je zaradi preteklih odmevnih množičnih napadov dobil s strani direktorice dodatno zadolžitev za vpeljavo osnovnih informacijsko varnostnih pristopov v organizacijo. V pogovoru prizna, da je to področje, v katerega je pred letom dni vstopil relativno na novo in zaradi majhnosti podjetja z vidika finančnih sredstev precej oteženo. Pove, da se nikakor ne morajo primerjati z varnostnimi pristopi, ki jih uporabljajo večja podjetja, a vendar poudarja, da se lahko z nekaj truda in voljo tudi z minimalnimi sredstvi zagotovi neko splošno informacijsko varnost majhnega podjetja. Pred tem v podjetju tudi niso imeli opredeljene oziroma spisane varnostne politike in si proces pisanja varnostne politike štejejo kot pomemben korak k zagotavljanju splošne informacijske varnosti.

3.4.1.3 Šibkost ureditve informacijske varnosti

Oseba A kot najpogostejšo šibkost ureditve informacijske varnosti znotraj organizacije opredeljuje samega uporabnika, saj je mnenja, da so uporabniki kljub številnim delavnicam in varnostno izobraževalnim treningom še vedno premalo informirani o sami pomembnosti varovanja informacij. Nadaljuje: »*Sam se velikokrat zavzemam za izobraževanje uporabnikov na različnih seminarjih in delavnicah, potrebno je izobraževati ne samo ljudi na vodilnih pozicijah, ampak vsakega posameznika, ki je vpet v samo poslovanje podjetja.«* Ob tem tudi dodajam primer bank, ki poleg notranjega izobraževanja uporabljajo tudi zunanjega, in sicer z različnimi izobraževalnimi tehnikami pozivajo uporabnike k varnejši uporabi njihovih e-bančnih storitev.

Tudi osebi C in D sta mnenja, da je uporabnik tisti, ki še vedno predstavlja največjo šibkost ureditve informacijske varnosti. Poleg tega osebi tukaj dodajata, da se je treba vprašati tudi o oddelčnih procesih, ki pogosto z vidika varovanja podatkov niso najbolje oblikovani. Problem pa se kaže tudi pri zasledovanju ciljev, ki so si po navadi med različnimi oddelki nasprotno sorazmerni. Oseba C podaja primer, kako njihovi procesni managerji oziroma operativni management v velik meri zasleduje cilje, ki so zgolj usmerjeni v neprestano izboljševanje kakovosti in produktivnosti, na drugi strani pa se le malokrat zavedajo, da je treba zagotoviti tudi določeno stopnjo informacijske varnosti, za katero ti managerji v prvi vrsti nimajo prav velikega posluha. Oseba C zaključuje: »*Tako kot v ostalih podjetjih tudi v našem seveda prihaja do nasprotnih ciljev managerjev na različnih pozicijah. Zato je še toliko bolj pomembno cilje najprej oceniti in jih rangirati po pomembnosti, vse to pa je mogoče doseči le z neprestanim usklajevanjem in medsebojno komunikacijo. Bolj, ko managerji zasledujejo samo svoje cilje, vezane na njihove oddelke, posledično se čez čas oblikuje večja šibkost ureditve informacijske varnosti v organizaciji.«*

Oseba D v samem intervjuju dodaja, da se je o šibkosti ureditve informacijske varnosti treba vprašati širše, v smislu, zakaj je posameznik vedno znova na udaru, ko govorimo o šibkih točkah pri varovanju posameznikov. Res je, da so prav posamezniki z različnimi nepremišljenimi potezami glavna grožnja informacijski varnosti, vendar če s primernimi izobraževalnimi pristopi zmanjšujemo stopnjo nepremišljenih potez uporabnikov, potem si lahko namesto vse šibkejše ureditve zagotovimo čedalje močnejšo ureditev informacijske varnosti. Ob tem pa tudi poudarja, da se vse bolj zavzameva tudi za obveščanje vseh njihovih strank za varnejše medsebojno poslovanje in varnejše transakcije informacij.

Prav tako tudi osebi B in E opredeljujeta v samem intervjuju posameznika kot najpogostejšo šibkost ureditve informacijske varnosti znotraj organizacije. Oseba B k temu tudi dodaja, da je treba vsakega posameznika posebej izobraziti, kakšne ukrepe za varovanje informacij naj uporablja pri vsakodnevnem izvajanju nalog.

3.4.1.4 Vloga posameznika pri varovanju podatkov

Oseba A odgovarja, da je vloga posameznika v njihovem podjetju pri varovanju informacij zelo pomembna. Zaposleni poleg vseh dnevnih aktivnosti tudi sodelujejo pri odkrivanju in poročanju o morebitnih grožnjah, ki bi lahko ogrozile poslovanje podjetja. Dodaja, da so organizacije lahko uspešne le, če so prizadevanja zaposlenih združena s tehnologijo. To tehnologijo pa je treba neprestano varovati, saj v vsakem podjetju predstavlja enega izmed ključnih stebrov poslovanja. Na zastavljeno podvprašanje, ali posameznika v njihovem podjetju opredeljujejo kot grožnjo ali kot osnovi vir oziroma steber za gradnjo obrambnih mehanizmov pred morebitno grožnjo, po premisleku odgovarja: *»posameznika v našem podjetju še vedno v veliki meri obravnavamo kot grožnjo, saj je nadrejenim na različnih pozicijah izredno težko razložiti in jih podučiti, da je potrebno posameznika obravnavati kot osnovni steber za obrambo pred morebitnimi napadi«.* Dodaja, da se je treba vprašati, kaj

lahko posameznik resnično na svojem delovnem mestu naredi, da z minimalnimi dnevnimi aktivnostmi povečuje informacijsko varnost podjetja. Ob tem pa tudi dodaja, da mora biti vsak posameznik odgovoren za svoja dejanja, in če slučajno njihova nepremišljena dejanja vodijo do oblikovanja različnih groženj, mora odgovornost zanje sprejeti in s pomočjo strokovnjakov na področju varovanja informacij tudi sooblikovati rešitev.

Oseba B pravi, da je vloga posameznika v veliki meri odvisna od prizadevanja oziroma motivacije, na kakšen način želi posameznik svoje delovno okolje in posledično okolje podjetja tudi zaščiti. Podaja, da je v organizaciji trenutno edina oseba, ki je poleg rednih dnevnih nalog aktivna na področju izobraževanja sodelavcev in sodelavk o pomembnosti varovanju podatkov. Med zaposlenimi neprestano poudarja, da se osnovno vodilo do oblikovanja varnega podjetja odraža v upoštevanju posameznikov pri izvajanju praktičnih ukrepov, kot sta kakovostna izbira gesel, pazljivost pri spletni pošti in odjavljanju iz računalniških sistemov v času njihove odsotnosti. Poudarja, da za tovrstno vlogo posameznika pri varovanju podatkov ne potrebujejo velikih finančnih izdatkov za njihovo izobraževanje, temveč je potrebno samo spodbujanje posameznikove volje, da ta postane soudeleženec pri varovanju podatkov podjetja.

Oseba C v celotnem sklopu poudarja, da je izredno pomembna vloga zaposlenih, da se naučijo medsebojne komunikacije z oddelki, ki skrbijo za informacijsko varnost podjetja. Tako na ravni celotnega podjetja kot na ravni posameznika je treba razpravljati o različnih varnostnih incidentih, poleg tega je treba tudi oblikovati »klimo«, ki spodbuja posameznika k razmišljanju, kako z nekim minimalnim obremenitvenim korakom zagotovi večjo varnost v svojem delovnem okolju. Posameznika, v podjetju ne opredeljujejo kot grožnjo, ampak kot osnovni vir obrambnega mehanizma pred morebitnimi grožnjami. V ta namen imajo tudi oblikovane polletne seminarje oziroma delavnice, na katerih spodbujajo uporabo različnih komunikacijskih kanalov za sprotno dopolnjevanje o sami tehnologiji, zagotavljanju njene varnosti in razpravljanju o medsebojnih odnosih pravilnega varnostnega vedenja. Enkrat mesečno pa izvajajo tudi sestanke, na katerih je v ospredju prav tematika varovanja podatkov ter obravnava različnih predlogov in misli za njeno izboljševanje.

Oseba D pri opredeljevanju vloge posameznika v ospredje poudarja miselnost, da je v njihovi organizaciji predvsem treba spremeniti pogled vodilnih ljudi pri izvajanju različnih dnevnih zadolžitev zaposlenih. Poudarja, da je posameznikova naloga ni zagotavljanje varnosti, ampak opravljanje različnih aktivnosti, katere posledično podjetju prinašajo dodano vrednost na različne načine. Treba je najti določeno sorazmerje, med varnostjo in delovno aktivnostjo, ki pa mora biti za vsako delovno mesto individualno oblikovana. »*Posameznik mora spoštovati ukrepe in pravila, ki jih predpisuje varnostna politika in ob tem tudi sodelovati pri odkrivanju in poročanju nadrejenim o morebitnih varnostnih incidentih oziroma grožnjah.«* Poudarja, da si trenutno zelo prizadeva k oblikovanju neformalnih srečanj s posamezniki na različnih odmorih, kosilih, športnih aktivnostih, pri katerih posledično pogovor pripelje tudi do tematike varovanja podatkov. Poudarja, da je tovrstna oblika časovno zelo potratna, ampak na drug strani tudi zaradi neformalne oblike dosti bolj učinkovita, kot različni seminarji in

delavnice, na katerih posameznika dejansko prisilimo, da začne razmišljati o informacijski varnosti na delovnem mestu.

Na podvprašanje, ali posameznika v njihovi organizaciji obravnavajo kot osnovi vir oziroma steber za gradnjo obrambnih mehanizmov pred morebitnimi grožnjami odgovarja: *»Sam posameznika obravnavanem kot osnovi steber za gradnjo varnostnega mehanizma, katerega je potrebno neprestano izboljševati in izpopolnjevati, ob tem pa je potrebno paziti, da z različnimi varnostnimi ukrepi ne otežujemo izvajanje dnevnih nalog posameznikov«*. Ob koncu pogovora na vlogo posameznika pri varovanju podatkov doda misel: *»Potrebno je tudi nekoliko spremeniti same izobraževalne procese na različnih seminarjih in delavnicah, pri katerih posameznika velikokrat neposredno obravnavajo kot glavni vir grožnje in ne kot osnovi gradnik informacijske varnosti«.*

Oseba E je odgovarja, da je v njihovem podjetju trenutno vsak posameznik zadolžen za osnovno varovanje podatkov. Poudarja, da se zaveda problematike pri opredeljevanju vloge posameznika, na kakšne načine naj varuje podatke. Poudarja, da je v zadnjem letu izvedel kar nekaj aktivnosti, ki pripomorejo k boljšemu varovanju podatkov. V podjetju so prepovedali hrambo gesel na različnih lističih ter trenutni v podjetju uporabljani programi uporabnika prisilijo, da na mesečni ravni oblikujejo nova gesla. Ob tem pa opaža, da tovrstni pristop ni najbolj učinkovit, saj imajo sedaj uporabniki oblikovani le dve gesli, ki ju potem mesečno izmenjujejo med različnimi programi. Oseba E posameznika opredeljuje kot grožnjo, saj v njihovem podjetju nimajo zadostnih finančnih sredstev, ki bi jih lahko porabili za oblikovanje posameznikovih stebrov za gradnjo obrambnih mehanizmov pred morebitnimi grožnjami. Vseeno pa poudarja, da se tudi z minimalnimi sredstvi lahko zagotovi neko splošno informacijsko varnost podjetja.

3.4.1.5 Varnostna politika in vključenost zaposlenih

Oseba A odgovarja, da se večina zaposlenih v organizaciji zaveda pomembnosti varnostne politike in obenem pravi, da misli, da jo v veliki večini upoštevajo. Seveda, obstajajo posamezniki, ki mislijo, da varnostna politika na njihovem delovnem mestu ne pride v poštev. Pri tovrstnih posameznikih se je treba vprašati, s katerimi ukrepi lahko njihovo mišljenje. Pri neupoštevanju predpisane varnostne imamo na voljo različna opozorila in ob njihovem neupoštevanju lahko izvedemo ukrepe, kot je ukinitve različnih bonusov. V skrajni sili, če ugotovimo, da posameznik namerno ne upošteva varnostne politike in želi z njenim neupoštevanjem škodovati organizacij sledi prekinitve oziroma odpoved delovnega razmerja. V njihovi organizaciji se posamezniki udeležujejo raznoraznih delavnic in tečajev o informacijski varnosti. Ob tem poudarja, da trenutno poteka oblikovanje delavnic na področju informacijske varnosti za posamezne oddelke v organizaciji. Ob tem opaža težavo, da je treba zaradi različnih spretnosti in razumevanja ljudi v posameznih oddelkih strukturo in vsebino tovrstnih delavnic spremeniti in nekoliko drugače oblikovati.

Oseba B priznava, da v njihovi organizaciji sicer imajo varnostno politiko, ampak se zaradi majhnosti podjetja kaj dosti čez leta ne spreminja. Zaveda se, da zastarela varnostna politika ne prinaša željene ravni informacijske varnosti, ob tem pa tudi dodaja, da jo imajo namen v naslednjem letu posodobiti. Priznava tudi, da se sama na letni ravni udeleži delavnice ali seminarja o informacijski varnosti in potem vse pridobljene informacije prenese na zaposlene. Ob tem se tudi zaveda, da bi bilo treba v prihodnosti bolj vključevati vse zaposlene v tovrstne delavnice. V ospredje pa tudi postavlja težavo, saj so tovrstna izobraževanja za majhna podjetja preprosto predrage in ta sredstva raje porabijo za pospeševanje prodaje ali vložijo v razvoj novega produkta.

Tudi osebi C in D sta mnenja, da je varnostna politika nekaj, kar bi morala imeti vsaka organizacija ne glede na panogo in njeno velikost. V obeh podjetjih se posamezniki v veliki večini zavedajo pomembnosti varnostne politike. Pravzaprav so tudi skozi vrsto let delovanja na trgu skupaj z zaposlenimi sooblikovali varnostno politiko. Oba sogovornika poudarjata, da je treba varnostno politiko konstantno spreminjati in usklajevati z novodobnimi zahtevami in smernicami, ki se oblikujejo na področju informacijske varnosti. Tudi zaposleni v obeh organizacijah se redno udeležujejo različnih seminarjev in delavnic na temo informacijske varnosti. Ob tem pa oseba D dodaja, da so pri njih tovrstne delavnice nekoliko drugače oblikovane, saj je v ospredju predvsem individualni pristop k zagotavljanju informacijske varnosti na posameznih delovnih mestih.

Oseba E odgovarja, da so varnostno politiko podjetja spisali v zadnjem letu in ugotavlja, da je prav proces odkrivanja varnostnih lukenj tisti, ki varnostni politiki dodaja poseben čar. Njihovi zaposleni se trenutno ne udeležujejo raznoraznih delavnic s področja varovanja informacij, se pa zaveda, da je to treba v organizaciji v prihodnosti spremeniti. Ob enem pa tudi dodaja, da je organizacija v tem trenutki zaradi majhnega obsega poslovanja nekoliko nezanimiva za različne vdore in grožnje morebitnih hekerjev.

3.4.1.6 Dejavniki varnostnega vedenja posameznikov

Oseba A v ospredje postavlja dva dejavnika, ki močno vplivata na varnostno vedenje posameznika, to sta predvsem kontrola in preobremenjenost posameznikov. Prvi dejavnik je zelo odvisen od stopnje kontrole, ki se izvaja na določenih delovnih mestih. Poudarja, da smo si posamezniki med seboj izjemno različni in nekateri enostavno želijo biti kontrolirani, saj s tem v primeru kakršnih koli težav in nepravilnosti porazdelijo oziroma preložijo del odgovornosti na kontrolorja. Drugi pa kakršno koli kontrolo zaznavajo kot nekaj, kar sporoča, da dela ne opravljajo dovolj kakovostno oziroma v skladu s pravili, ukrepi in politiko podjetja, zato se nad njimi tudi izvršuje kontrola. Tukaj sogovornik poudarja, da je treba posameznikom v tovrstnih primerih razložiti, da se posledično kontrola ne izvaja zaradi posameznikove stopnje kakovosti opravljenega dela, ampak zaradi njegove pozicije opravljanja dnevnih nalog, ki so za organizacijo izjemno pomembne, zato je treba uvesti dodatno kontrolo na področju varovanj informacij. S takšno opredelitvijo sogovornik dodaja, da lahko pri večini posameznikov spremenimo mišljenje, da kontrola na njihovih delovnih

mesti ni tako napačna. Pri dejavniku preobremenjenosti pa dodaja, da je treba najprej posameznika razbremeniti, šele potem z določenimi dnevnimi izvajalnimi ukrepi in pravili povečevati varnostno vedenje posameznika, saj bo skoraj vsak posameznik zaradi prekomerne preobremenitve nezadovoljen še z dodatnimi zadolžitvami in zahtevami ne glede nato, s katerega področja prihaja.

Oseba B v ospredje predvsem postavlja dejavnik nizke motivacije za pripravljenost pri širjenju informacijske varnosti v podjetju. Poudarja, da so sodelavci in sodelavke v veliki večini mnenja, da za tako majhno podjetje ni treba upoštevati niti osnovnih informacijsko varnostnih pristopov, saj so zaradi majhnosti nezanimivi za kakršne koli grožnje. Ob tem tudi poudarja, da zaposleni v njihovem podjetju opravljajo v povprečju tri ali več funkcij zato jih je tudi izredno težko motivirati za upoštevanje osnovnih varnostnih ukrepov, ki bi jim še dodatno oteževalo vsakdanje delo.

Oseba C v ospredje postavlja kar nekaj dejavnikov od kontrole, zaznavanje groženj, pripravljenosti do sodelovanja oziroma učenja, nezadovoljstvo na delovnih mestih, preobremenjenosti, družinskih vplivov in podobno. V pogovoru razlaga, da je izredno težko v ospredje postaviti in določiti nekaj dejavnikov, ki močno vplivajo na varnostno vedenje. Nekateri od naštetih dejavnikov lahko na neko osebo močno vplivajo in puščajo posledice, ki se lahko kažejo tudi v nepremišljenih potezah in oblikovanju novih varnostnih tveganj med tem, ko pri drugih na njihovo delo in varnostno vedenje preprosto nimajo vpliva.

Oseba D v pogovoru o dejavnikih, ki močno vplivajo na varnostno vedenje, v ospredje postavlja tri dejavnike: kontrola, zaupanje in nezadovoljstvo posameznikov na njihovih delovnih mestih. Sogovornik dodaja, da je prvi dejavnik izredno občutljive narave. Nadaljuje: »*Ljudje na splošno ne želimo biti kontrolirani, saj ljudje ob besedi kontrola takoj pomislijo na nekaj slabega. Potrebno je vzpostaviti sistem, s katerim posamezniku zaupamo, da opravlja samokontrolo nad njegovimi delovnimi aktivnostmi, za katere je tudi neposredno odgovoren«*. Ob tem pa poudarja, da se mora posameznik pri samokontroli zavedati, da morebitne njegove posledice ob nepravilnih dejanjih, ki so varnostno občutljive, lahko občutijo vsi zaposleni oziroma celotna organizacija. Tudi nezadovoljstvo posameznikov na njihovih delovnih mestih lahko vodi do vzpostavitve problematike pri varnostnem vedenju. Sogovornik dodaja, da pri posameznikih, ki na njihovih delovnih mestih niso zadovoljni, zaznavajo tudi izjemno nizko stopnjo varnostnega vedenja. »*Tovrstni posamezniki posledično izražajo nizko stopnjo pripadnosti sami organizaciji, zaradi katere tudi ne kažejo kakršnega koli zanimanja za njeno varovanje«*. Ob tem oddaja, da gre za dolgotrajni proces, v katerem pri posamezniku najprej skušajo odkriti razloge za njegovo nezadovoljstvo na delovnem mestu.

Oseba E v tem sklopu v ospredje postavlja predvsem motivacijo oziroma nezainteresiranost posameznikov, saj so zaposleni v njihovem podjetju preprosto preveč fokusirani samo na njihova področja, ki jih opravljajo v vsakdanjem delavniku. Poudarja: »*Čeprav imamo v našem podjetju odlične medsebojne odnose, vseeno vsak posameznik rad opravlja naloge, za*

katere je v prvi vrsti tudi plačan«. Ob tem tudi dodaja, da že tako ali tako nekateri zaposleni izvajajo delovne procese izven delovnega časa, saj jim preprosto med delovnim časom ne uspe vse narediti. V ospredje še enkrat postavlja problematiko, da se pri majhnih podjetjih preprosto ne splača veliko vlagati v informacijsko varnost, ki je s stroškovnega vidika za majhna podjetja izjemno velika.

3.4.1.7 Elementi izboljševanja varnostnega vedenja posameznikov

Oseba A kot ključen element izboljševanja varnostnega vedenja posameznika v njihovem podjetju vidi v zavzetosti zaposlenih pri sprejemanju novih smernic, ukrepov in pravil v informacijski varnosti. Poudarja, da je treba zaposlenim na vseh ravneh pred implementacijo različnih novih smernic, ukrepov in pravil na področju informacijske varnosti tematiko tudi predstaviti in razložiti, zakaj jo je treba spoštovati in implementirati v njihovo delovno okolje. Ob enem tudi poudarja, da človeški faktor igra odločilno vlogo pri sami zavzetosti zaposlenih pri sprejemanju novi smernic, ukrepov in pravil na področju informacijske varnosti. Predvsem v smislu medsebojne povezanosti oziroma vpliva sodelavcev. Razložil mi je tudi primer, ko so na različnih oddelkih implementirali nove varnostne ukrepe glede možnosti dostopa do arhiviranih podatkov. Prepričati je bilo treba samo vodilne zaposlene, da z novimi minimalnimi varnostnimi ukrepi zmanjšujejo možnost izginotja arhiviranih podatkov. Treba je vedeti, kdo je tisti, ki je na posameznem oddelku deležen spoštovanja med zaposlenimi. Oseba A poudarja, da imajo ti posamezniki izjemno velik družbeni oziroma delovni vpliv na ostale zaposlene v njegovem oddelku.

Oseba B pojasnjuje, da je v njihovem podjetju veliko elementov, ki bi jih bilo treba pri varnostnem vedenju posameznikov izboljšati. Najbolj izpostavlja element znanja in pripravljenosti učenja, saj ostali zaposleni v njihovem podjetju nimajo znanja o informacijski varnosti, sama pa poudarja, da zaradi ostalih delovnih nalog, ki jih vsakodnevno opravlja, preprosto nima časa se posvetiti izobraževanju sodelavcev in sodelavk. Poleg tega tudi poudarja, da bi morala biti tovrstna izobraževanja organizirana izven delovnega časa, za kar pa večina posameznikov ni zainteresirana.

Tudi oseba C je bila v intervjuju podobnega mnenja kot oseba A, saj se tudi v njihovi organizaciji neprestano trudijo pri povečavanju same zavzetosti uporabnika pri sprejemanju različnih oblik varnostnega vedenja. Sogovornik razmišlja predvsem o samemu ozadju, ki vpliva na zavzetost uporabnika, saj pri ugotavljanju, zakaj so nekateri uporabniki bolj zavzeti od drugih pri implementaciji novih varnostnih mehanizmov, v ospredje postavlja prav pripadnost k podjetju. Ugotavlja, da se to predvsem kaže v zaposlenih, ki se udeležujejo različnih neformalnih srečanj, zabav, prireditev in so bistveno bolj zavzeti pri izvajanju in ohranjanju varnostnih mehanizmov na njihovih delovnih mestih, kot zaposlenih, ki se zaradi različnih razlogov ne udeležujejo tovrstnih neformalnih srečanj. Tudi na vprašanje o človeškem faktorju odgovarja, da je vsak posameznik drugačen in vsakodnevno prihaja na delo iz drugačnega ozadja z drugačnimi družbenimi vplivi in znanjem, ki ga pridobiva tudi

izven delovnega časa. Vse to pa vpliva tudi na sprejemanje kakršni koli sprememb in tudi na same spremembe na področju varovanja podatkov na njihovih delovnih mestih.

Oseba D se je osredotočila na elemente, ki se v prvi vrsti nanašajo na razumevanje posameznika, v smislu, zakaj bi posameznik z nekatero spremembo varovanja podatkov dobesedno spreminjal svojo vsakodnevno rutino. Pri tem poudarja, da ključen element posameznikovega izboljševanja varnostnega vedenja predstavlja prav individualni pristop do posameznikovega razmišljanja. Nadaljuje: *»Vsakemu posamezniku je potrebno na individualni ravni dejansko razložiti, zakaj prav on/ona predstavlja ključen del pri varovanju informacij v naši organizaciji*.«

Dodaja tudi, da je treba večkrat z različnimi sestanki s posamezniki vzpostaviti medsebojni stik, da tudi oni povedo svoja mnenja in misli o izvajanju in implementaciji različnih varnostnih sprememb na njihovih delovnih mestih. Z omenjenim pristopom se tudi spodbudi nekakšno medsebojno zaupanje, ki povečuje motivacijo in zavzetost za upoštevanje različnih varnostnih pravil in ukrepov znotraj organizacije. Poudaril pa je tudi še en element izboljševanja varnostnega vedenja: posameznikovo pripravljenost oziroma element posameznikove nagnjenosti k spremembam – tu je mislil predvsem starejše posameznike v organizaciji. Pri vprašanju o pomembnosti človeškega faktorja odgovarja podobno kot oseba C, saj ima vsak posameznik v svojem življenju oblikovane različne cilje, ki so že na začetku njihovih poti oblikovani s človeškimi faktorji, ki neposredno vplivajo na njihovo delovanje in življenje v njihovem vsakdanjem okolju. Tu je govoril o dejavniku družbe in njenem vpliva, saj je mnenja, da te družba, v kateri se skozi celotno življenje giblješ, tudi sooblikuje.

Oseba E je pri ključnih elementih izboljševanja varnostnega vedenja posameznika v njihovem podjetju poudarila element prizadevanja do sprememb. Na kratko razloži, če posameznik že v osnovi ni zainteresiran do sprememb, potem se takega človeka izredno težko motivira za odkrivanje in sodelovanje na novih področjih. V ospredje predstavlja tudi osebnost človeka in njegovo nagnjenost do sprememb. Ugotavlja tudi, da mladi neprestano hrepenijo po spremembah, medtem ko se starejši veliko raje držijo ustaljenih smernic.

3.4.1.8 Vidiki ter bodoči izzivi in smernice v informacijski varnosti

Prav vsi intervjuvanci so se v tem sklopu dotaknili sedaj najbolj aktualne teme GDPR (*ang. General Data Protection Regulation),* o kateri lahko že od oktobra beremo v časopisih, kot so Finance, Manager, IKT Informator. GDPR je splošna uredba o varstvu podatkov, ki bo veljala za vsa podjetja, ki poslujejo v Evropski uniji in obdelujejo kakršne koli osebne podatke. Gre za novo EU uredbo o varstvu podatkov, katero morajo organizacije do konca maja 2018 implementirati in njihovo poslovanje uskladiti z zahtevami uredbe. Oseba A k tem dodaja, da gre za velik korak naprej v sami zakonodaji o varovanju podatkov. In da z omenjeno regulativo na področju varovanja podatkov od sedaj prihajajo najbolj obsežne spremembe.

Osebi B in E, zaposleni v manjših podjetjih, že sedaj opozarjata, da bo ta regulativa verjetno dodobra pretresla majhna podjetja, ki s poslovanjem zbirajo osebne podatke. Pri tem tudi poudarjata, da bo treba pridobiti pooblaščeno osebo za varstvo podatkov, saj v obeh primerih sistematično spremljajo posameznike. Opozarjata pa tudi na stroške, saj se bo treba v obeh podjetjih udeležiti različnih posvetov s strokovnjaki in to ni ravno poceni.

Medtem ko osebi D in C kar z navdušenjem govorita o celotni uredbi o varstvu podatkov in sta mnenja, da bi morala podobna uredba obstajati že veliko prej. Oseba D tudi poudarja, da ima Slovenija že tako ali tako bolj restriktivno ureditev varstva osebnih podatkov kot druge države EU. Sogovornik edino težavo vidi pri skladnosti poslovanja manjših podjetij, pri katerih bo verjetno treba prenoviti tudi nekatere informacijske rešitve in delovne procese. Oseba C nadaljnje izzive informacijske varnosti vidi v globalnem mobilnem trgu, ki je trenutno še vedno v fazi razvoja z obsežno rastjo. Organizacije vse bolj uporabljajo različne komunikacijske oblike z različnimi mobilnimi mrežami. Po sogovornikovih besedah bo treba vzpostaviti dodatne varnostne mehanizme na omenjenem področju, saj vsakoletno beležimo izredno rast mobilnih zlonamernih programskih oprem, ki letno prizadene na milijone tako poslovnih kot zasebnih uporabnikov.

Oseba A izzive predvsem vidi v varnostni vzgoji in družbeni odgovornosti uporabnikov. Poudarja, da se področje informacijske varnosti prav v zadnjem letu izredno nadgrajuje, saj se čedalje več strokovnjakov z različnimi študijami išče različne načine varovanja podatkov. Nadaljuje: *»Še vedno bo ključno izobraževanje uporabnikov o trenutnih grožnjah in njihovem širjenju, le na tak način lahko v prihodnosti zmanjšamo vpliv spletnega kriminala«.* V pogovoru tudi omenja, da bo treba v prihodnosti spremeniti pristop k izobraževanju posameznikov in se pohvali, da je idejni vodja novega izobraževalnega pristopa, ki temelji na dodatku k plači za stalno varnostno pripravljenost zaposlenega. Poudarja tudi dosedanjo težavo, če so bili različni seminarji do sedaj neobvezni, je bil njihov obisk relativno zelo slab, ko so izobraževanja obvezna za vse zaposlene, se posamezniki pogosto pritožujejo. Zato sedaj s sodelavci oblikujejo program, v katerem posamezniku prepuščajo izbiro glede obiskov seminarjev.

Varnostno izobraževalni seminarji, bodo za posameznika potekali enkrat do dvakrat mesečno. Ob upoštevanju vseh varnostnih ukrepov, pravil in njihovi implementaciji v delovno okolje, bo posledično njim dodeljen dodatek k plači za stalno varnostno pripravljenost, katere višine še niso čisto določili. V primeru ugotovitve kakršne koli varnostne kršitve jim bo dodatek za stalno varnostno pripravljenost odvzet. Z drugačnim pristopom bodo posameznike skušali prepričati, da je vsak posameznik odgovoren za zagotavljanje varnosti v svojem delovnem okolju. Povedal je tudi, da trenutno rešujejo težavo glede oblikovanja pravilne matrike za izplačevanje dodatka k plači za stalno varnostno pripravljenost, saj se njihova delovna mesta z vidika varnostnega tveganja v njihovi organizaciji izjemno razlikujejo.

Ob koncu intervjuja oseba D zaključuje, da je osnovna problematika spletnega kriminala v lahkem dostopu do brezplačnega znanja in različnih škodoželjnih programov, ki jih

posamezniki lahko uporabijo za škodoželjna dejanja posameznikom ali organizacijam. Zaveda se, da je dostop do virov, ki ponujajo tovrstna znanja in škodoželjne programe, izjemo težko omejiti, zato je mnenja, da se sama problematika kaže že v vzgoji in osebnosti ljudi. Ljudi je treba seznaniti, da če se že odločijo, da bodo izvajali škodoželjne aktivnosti, naj imajo v mislih, da vedno obstaja nekdo nekje, ki ima boljše znanje in lahko njihovo identiteto z drugačnimi pristopi in razmišljanjem tudi razkrije. Opozarja tudi, da se dandanes večina hekerjev opredeljuje kot etičnega (*izraz etični heker*) in s tem prekrivajo svoje prave namene in identiteto. Nadaljuje, da obstajajo tudi certifikati etičnega hekerja, ki vso zadevo še poslabšujejo, saj je dandanes beseda »etično« čisto preveč izrabljena in čedalje bolj izgublja svoj pomen.

3.5 Ugotovitve in oblikovanje domnev

Rezultat kvalitativne raziskave je tudi oblikovanje sedmih domnev, povezanih z opredeljevanjem vloge posameznika pri zagotavljanju informacijske varnosti. Za oblikovanje domnev iz petih polstrukturiranih globinskih intervjujev navajam najpomembnejše misli in citate intervjuvancev, ki se nanašajo na izbrane tematske sklope. Vse domneve so oblikovane na podlagi citatov in mislih intervjuvancev, kateri so bili vzeti v vzorec, zato na podlagi vzorca ne moremo sklepati, da te oblikovane domneve veljajo tudi na celotni populaciji.

Prva domneva je oblikovana na podlagi povprečne stopnje zadovoljstva z informacijsko varnostjo, katera je bila v obravnavanem vzorcu izražena z vrednostjo 7.2 .

Oseba A: »*V podjetju imamo kar nekaj vzpostavljenih mehanizmov za povečevanje informacijske varnosti od digitalnih podpisov pa vse do različnih ravni avtorizacije, katera je potrebna na določenih ravneh organizacije, zato stopnjo informacijske varnosti ocenjujem s 7.*«

Oseba B: »*V podjetju bi lahko še veliko naredili za samo izboljšavo informacijske varnosti, ampak smo trenutno zadovoljni in samo stopnjo informacijske varnosti ocenjujemo s 7, ob tem pa vseeno poudarjam, da z razpoložljivimi sredstvi, ki so resnično minimalni, skušamo maksimalno zagotoviti varno poslovanje našega podjetja.*« Oseba C je podala oceno 8 in jo pojasnjuje, da vedno sledijo korakom v razvoju informacijske varnosti. Trenutno imajo v organizaciji implementiranih kar nekaj sodobnih mehanizmov varovanja podatkov.

Oseba D: *»Z neprestanim odkrivanjem in kontroliranjem celotnega informacijskega sistema znižujemo možnost pojavitve groženj, zato stopnjo zadovoljstva z informacijsko varnostjo v našem podjetju ocenjujem z 8. Vedno pa je prostor, kjer bi bilo potrebno določene procese z vidika varovanja informacij bolje zaščititi oziroma izboljšati!«* Oseba E informacijsko varnost podjetja ocenjuje s 6 in opozarja, da prej niso imeli varnostne politike, tako da si proces pisanja štejejo kot pomemben korak k zagotavljanju splošne informacijske varnosti.

Povprečna ocena je bila izračunana na podlagi seštevka vseh posameznih ocen, deljenih s številom intervjujev v obravnavanem vzorcu. Na podlagi samoocene stopnje zadovoljstva z informacijsko varnostjo na obravnavanem vzorcu lahko trdim, da je še vedno veliko prostora za njeno izboljševanje. Na obravnavnem vzorcu lahko tudi trdim, da imajo manjše organizacije pri samoocenjevanju stopnje zadovoljstva informacijske varnosti nekoliko slabšo samooceno kot velike. Glavi razlog za slabšo samooceno je predvsem v pomanjkanju finančnih sredstev, ki so neposredno povezana z vlaganji v informacijsko varnost.

Druga domneva potrjuje, da je uporabnik še vedno najpogostejša šibkost ureditve informacijske varnosti znotraj organizacije.

Prav čisto vsi intervjuvanci opredeljujejo posameznika kot najpogostejša šibkost ureditve informacijske varnosti znotraj organizacije. Razlogi se predvsem kažejo v nepremišljenih dejanih in družbenih vplivih iz zunanjega okolja ter nezainteresiranosti do spoštovanja pravil in ukrepov, ki jih predpisujejo varnostne politike organizacij. Ob tem pa osebi C in D izpostavljata, da je treba spremeniti mišljenje pri uporabnikih in jih začeti obravnavati kot osnovi vir oziroma steber za gradnjo obrambnih mehanizmov pred morebitnimi grožnjami.

Tretja domneva opredeljuje vlogo posameznika pri varovanju podatkov, ki se predvsem izraža v spoštovanju pravil in ukrepov, ki jih predpisuje varnostna politika, v medsebojni komunikaciji ter odkrivanju in poročanju o morebitnih grožnjah.

Oseba A navaja, da je glavna vloga posameznika v organizaciji prav sodelovanje pri odkrivanju in poročanju o morebitnih grožnjah ter sooblikovanju varnostne politike podjetja. Oseba B navaja, da je vloga posameznika odvisna od njegove motivacije in pripravljenosti, na kakšen način posameznik želi njegovo delovno okolje in okolje podjetja tudi zaščititi. Oseba C navaja, da je izredno pomembna vloga zaposlenih, da se naučijo medsebojne komunikacije z oddelki, ki skrbijo za informacijsko varnost podjetja. Treba je razpravljati tako na ravni celotnega podjetja kot na ravni posameznika o različnih varnostnih incidentih.

Oseba D poudarja, da posameznikova vloga v ospredju ni zagotavljanje varnosti, ampak opravljanje različnih aktivnosti, ki posledično podjetju na različne načine prinašajo dodano vrednost. Treba je najti določeno sorazmerje med varnostjo in delovno aktivnostjo, ki pa mora biti za vsako delovno mesto individualno oblikovana. »*Posameznik mora spoštovati ukrepe in pravila, ki jih predpisuje varnostna politika in ob tem tudi sodelovati pri odkrivanju in poročanju nadrejenim o morebitnih varnostnih incidentih oziroma grožnjah.«*

Četrta domneva opredeljuje položaj posameznikov, saj se v veliki večni skoraj vsi posamezniki zavedajo pomembnosti varnostne politike.

Večina intervjuvancev je opredelila, da se posamezniki v njihovih organizacijah zavedajo same pomembnosti varnostne politike. Nekoliko slabši rezultat beležim pri samem vključevanju posameznikov na seminarje oziroma delavnice za širjenje splošnega znanja o

informacijski varnosti. Na obravnavanem vzorcu predvsem opažam razliko, da se zaposleni oziroma posamezniki v večjih podjetjih bolj pogosto udeležujejo tovrstnih izobraževalnih delavnic, v manjših podjetjih pa preprosto nimajo dovolj finančnih sredstev, s katerimi bi zaposlenim lahko zagotovili udeležbo na tovrstnih izobraževanjih.

Tudi Leach (2003) v svoji študiji ugotavlja, da je posameznikovo zavedanje o pomembnosti varnostne politike eno izmed ključnih vodil pri izboljševanju varnostnega vedenja posameznika.

Peta domneva opredeljuje kontrolo, motivacijo in nezadovoljstvo na delovnem mestu, ki predstavljajo dejavnike, ki močno vplivajo na varnostno vedenje posameznika.

Tabela 7: Ključni dejavniki, ki močno vplivajo na varnostno vedenje posameznika

Oseba	**Dejavniki, ki močno vplivajo na varnostno vedenje posameznika**
A	kontrola in preobremenjenost posameznikov
B	nizka motivacija
C	kontrola, zaznavanje groženj, pripravljenost sodelovanja, nezadovoljstvo na delovnem mestu
D	kontrola, zaupanje in nezadovoljstvo posameznikov na njihovih delovnih mestih
E	motivacija oziroma nezainteresiranost posameznikov

Zgornja tabela prikazuje ključne dejavnike, ki so bili največkrat omenjeni pri opredeljevanju dejavnikov, ki močno vplivajo na varnostno vedenje posameznika s strani intervjuvancev. Največkrat omenjeni dejavnik v intervjuju je kontrola, nato sledita motivacija in nezadovoljstvo posameznikov oziroma zaposlenih na njihovih delovnih mestih.

Šesta domneva trdi, da so zavzetost posameznika, nagnjenost k spremembam in samo znanje, ključni elementi izboljševanje varnostnega vedenja posameznika.

Tabela 8: Ključni elementi izboljševanja varnostnega vedenja posameznika

Oseba	**Ključni elementi izboljševanje varnostnega vedenja posameznika**
A	zavzetost zaposlenih pri sprejemanju novih smernic, ukrepov in pravil
B	element znanja in pripravljenosti za učenje
C	zavzetost uporabnika pri sprejemanju ukrepov in pravil varnostnega vedenja
D	individualni pristop do posameznikovega razmišljanja, nagnjenost k spremembam
E	element prizadevanja do sprememb oziroma nagnjenost k spremembam

Tabela 8 prikazuje ključne elemente izboljševanja varnostnega vedenja posameznika, opredeljene s strani intervjuvance. Zavzetost posameznika in nagnjenost k spremembam na

obravnavanem vzorcu predstavljata ključa elementa izboljševanja varnostnega vedenja posameznika. Nato sledi tudi element znanja. Iz tega lahko sklepamo, da bo treba v prihodnosti v vključenih organizacijah veliko postoriti pri povečevanju same zavzetosti posameznikov pri sprejemanju novih smernic, ukrepov in pravil varnostnega vedenja z morebitnimi nagradami ali bonusnimi sistemi. Treba se je vprašati, kakšni so razlogi za posameznikovo nezavzetost in nenagnjenost k novim spremembam. Oseba D kot rešitev za izboljševanje varnostnega vedenja navaja: *»Vsakemu posamezniku je potrebno na individualni ravni dejansko razložiti, zakaj prav on/ona predstavlja ključen del pri varovanju informacij v naši organizaciji*.«

Tudi Leach (2003) v svoji študiji tudi ugotavlja, da se ključno vodilo pri izboljševanju posameznikovega varnostnega vedenja odraža v samem vodenju in njegovem pristopu oziroma razlagi, zakaj je določena sprememba njuno potrebna in kakšne prednosti ter zadolžitve prinaša v posameznikovo delovno okolje.

Sedma domneva opredeljuje človeški faktor kot eno izmed najpomembnejših vlog pri zagotavljanju informacije varnosti.

Oseba A opredeljuje človeški faktor kot odločilno vlogo pri sami zavzetosti zaposlenih pri sprejemanju novi smernic, ukrepov in pravil na področju informacijske varnosti. Predvsem v smislu medsebojne povezanosti oziroma vpliva sodelavcev. Oseba C na vprašanje o človeškem faktorju odgovarja, da je vsak posameznik drugačen, ima drugačno ozadje z drugačnimi družbenimi vplivi in znanjem, katero pridobiva tudi izven delovnega časa. Vse to vpliva tudi na sprejemanje raznih sprememb na področju varovanja podatkov na njihovih delovnih mestih.

Oseba D je mnenja, da ima vsak posameznik v svojem življenju oblikovane različne cilje, kateri so že na začetku njihovih poteh oblikovani s človeškimi faktorji, ki neposredno vplivajo na njihovo delovanje in življenje v njihovem vsakdanjem okolju. V ospredje je predvsem postavljal dejavnik družbe in njenega vpliva, saj je mnenja, da te družba, v kateri se celo življenje giblješ, tudi sooblikuje. Oseba E kot človeški faktor, ki pomembno vpliva na vlogo posameznika pri zagotavljanju informacijske varnosti, postavlja osebnost človeka in njegovo nagnjenost k spremembam.

Tudi Parsons in drugi (2014) v svoji študiji ugotavljajo, da človeški faktor pomembno vpliva na vlogo posameznika pri zagotavljanju informacijske varnosti. V študiji opisujejo več različnih, ki pomembno vplivajo na varnostno vedenje posameznika. Študija vključuje načine, na katere posamezniki pod različnimi vplivi sprejemajo odločitve, ki vplivajo na zaznavanje posameznikovega tveganja. Ob tem pa tudi poudarjajo, da je pomembna tudi sama stopnja nadzora posameznikov, saj če posamezniki, občutijo premočan pritisk izvrševalne kontrole s strani nadrejenih, bolj tvegajo in precenjujejo njihove sposobnosti nadzora nad grožnjami.

3.6 Omejitve in odprta vprašanja za nadaljnje raziskovanje

Dejstvo je, da področje informacijske varnosti ni relativno novo raziskovalno področje, vendar se premalokrat podrobno raziskuje odnos posameznika oziroma njegove vloge pri zagotavljanju informacijske varnosti. Veliko raziskav na področju informacijske varnosti temelji prav na oblikovanju različnih metod in izobraževalnih pristopov usmerjenih k samemu posamezniku. Vendar šele v zadnjih nekaj letih strokovnjaki v tovrstne raziskave vključujejo tudi opredeljevanje človeškega faktorja ter elemente in dejavnike, ki tudi dokazano v tej kvalitativni raziskavi pomembno vpijajo na izboljševanje samega varnostnega vedenja posameznika. V ta namen je bila tudi izvedena kvalitativna analiza na področju vloge posameznika pri zagotavljanju informacijske varnosti.

Pri analizi oviro predstavlja vzorec intervjuvancev, saj je zaradi časovne in stroškovne komponente izredno težko izvesti polstrukturirane globinske intervjuje na velikem vzorcu. Zavedam se, da je vzorec s petimi intervjuvanci relativno majhen, kar ob enem tudi vzbuja dvom v reprezentativnost odgovorov. Zato bi bilo smiselno oblikovane domneve potrditi s širšo raziskavo, v kateri bi lahko zajeli večje število ne samo slovenskih, ampak tudi evropskih strokovnjakov, na področju varovanja informacij pri opredeljevanju njihovega pogleda na vlogo posameznika pri zagotavljanju informacijske varnosti. Zanimiva bi bila tudi raziskava, ki bi primerjala stroškovno porabo sredstev, namenjenih za izboljševanje varnostne vloge posameznika pri zagotavljanju informacijske varnosti med organizacijami različnih velikosti s samooceno stopnje zadovoljstva informacijske varnosti. Glede na to, da so bili v raziskavi ugotovljeni tudi ključni človeški faktorji, ki pomembno vplivajo na zaznavanje in posameznikovo sprejemanje informacijske varnosti, bi bilo izredno koristno izvesti raziskavo, ki bi v ospredju raziskovala dejavnike, ki vplivajo na izpostavljene človeške faktorje.

Če izhajamo iz razumevanja, da so strokovnjaki, ki v podjetjih delujejo na področju informacijske varnosti tudi soodgovorni za izboljševanje posameznikove vloge, bi bilo smiselno tudi proučiti in opredeliti vse metode in pristope, ki pri posameznikih vzbujajo večjo nagnjenost k spremembam in zavzetost zaposlenih za varovanje podatkov v njihovih delovnih okoljih. Saj so prav ta dva elementa intervjuvanci opredeliti kot ključna pri izboljševanju varnostnega vedenja posameznika v njihovih organizacijah. Te pristope in metode bi bilo treba tudi natančno opredeliti in določiti. Na obravnavanem področju kar veliko raziskav temelji na samemu podajanju primerov dobrih praks, pri katerih pa moramo paziti, da niso nujno aplikativne na čisto vse organizacije.

4 SKLEP

Številni tehnični napredki na področju informacijskih znanosti vedno ne zagotavljajo varnejšega okolja. Zato informacijske varnosti ni mogoče razumeti ali opisati zgolj kot tehnični problem. Tehnološke naprave, kot so računalniki, mobilni telefoni, tablice, upravljajo ljudje, kar pomeni, da je pri varnosti informacij treba vzeti v obzir tudi vprašanje o človeških

dejavnikih. Človeški dejavniki posledično vplivajo na to, kako posamezniki komunicirajo s tehnologijo in prav ta medsebojna komunikacijska interakcija, katera vsebuje nepremišljena človeška dejanja, je pogosto škodljiva tako z vidika varovanja informacij kot z vidika celotne organizacije. Precej očitno je, da dandanes samo tehnične rešitve ne bodo preprečevale kršitev in groženj povezanih z informacijsko varnostjo. Zato številni strokovnjaki poudarjajo, da je neprestano izobraževanje posameznikov oziroma uporabnikov tehnologij ključnega pomena pri oblikovanju željene stopnje informacijske varnosti v organizaciji.

Organizacije morajo spodbujati in vzdrževati kulturo, v kateri se vrednotijo in oblikujejo pozitivna varnostna vedenja. Treba je razumeti in rešiti uporabne izzive, povezane z informacijsko varnostjo. To pomeni, da morajo biti varnostne funkcije smiselne, enostavne za iskanje, vidne in priročne za uporabo, tako da na eni strani ne otežujejo vsakdanjega dela posameznika in na drugi strani s posameznikovimi izvajalnimi ukrepi zagotavljajo večjo varnost informacij v organizaciji. Posameznike je treba vseskozi izobraževati o pomenu ozaveščenosti o varnosti, ki mora tudi vključevati vedenjska usposabljanja.

Problematika, ki jo ugotavljam, je, da dandanes še vedno niso vsi posamezniki vpeti v izobraževalni proces varnostnega vedenja. V večini organizacij razlog za neizobraževanje posameznikov pripisujejo pomanjkanju finančnih sredstev. Neizobraženost posameznikov na področju informacijske varnosti pa lahko vidno pušča posledice, ki se predvsem odražajo pri slabem opredeljevanju posameznikovega pomena, vedenja in zaznave informacijske varnosti.

V magistrskem delu ugotavljam, da posameznikova vloga ni zagotavljanje varnosti, ampak opravljanje različnih delovnih aktivnosti in procesov, ki posledično organizaciji tudi prinašajo neko dodano vrednost, seveda na različne načine. Varnost in svoboda na delovnem mestu sta obratno-sorazmerni, zato je pri opredeljevanju posameznikove vloge ključno določiti razmerje med varnostjo in delovno aktivnostjo posameznikov. To razmerje pa mora biti oblikovano za vsako delovno mesto posebej, saj kakršno koli posploševanje ni dobrodošlo. Na eni strani imajo organizacije delovna mesta, ki so z vidika informacijske varnosti izredno občutljiva, na drugi strani, pa tista, ki jim osnovni pristopi informacijske varnosti čisto zadoščajo. Ne glede na delovno mesto morajo posamezniki odigrati pomembno vlogo tudi pri odkrivanju in poročanju o morebitnih grožnjah ter pri spoštovanju pravil in ukrepov, predpisanih z varnostno politiko organizacije.

Ljudje smo spontani, čustveni in nepredvidljivi. Neprestano komuniciramo s tehnološkimi napravami in sprejemamo odločitve v zvezi z informacijsko varnostjo. Na način, kako v danem trenutku reagiramo in posledično sprejemamo naše odločitve je vsekakor zelo dinamično in zapleteno vprašanje. Obstaja veliko dejavnikov, ki jih je treba upoštevati. Na primer, pomembno je priznati vpliv posameznikovega medsebojnega razlikovanja, osebnih lastnosti, kognitivnih sposobnosti itd. Ob enem pa obstajata tudi pristranskost in hevristika, ki vplivata na to, kako posamezniki zaznavamo tveganje. Vsi ti dejavniki nam na nekakšen način pomagajo razložiti, zakaj posamezniki sprejemajo določene odločitve ter zakaj imamo tako različne poglede in mnenja o področju informacijske varnosti.

Na zaznavanje tveganj in medsebojnih razlikovanj pa vpliva tudi okolje, v katerem se posamezniki neprestano gibljemo. Kultura in klima organizacije lahko zagotovo pomembno vplivata na vrednote, vedenje in vizijo posameznikov. Zato je razumevanje varnostne kulture organizacije in notranjega varnostnega okolja lahko dober vpogled v to, zakaj nekateri posamezniki spoštujejo predpisano vedenje in zakaj nekateri posamezniki prav to predpisano vedenje zanemarjajo oziroma zapostavljajo.

Glavna skrb v informacijski varnosti so grožnje, ki se oblikujejo zaradi neupoštevanja posameznikov pri izvajanju različnih ukrepov in pravil, predpisanih z varnostno politiko ali skrbno načrtovanimi napadi hekerjev. Cilj skoraj vsakega napada je z različnimi metodami pridobiti občutljive podatke, ki se lahko kasneje zlorabijo v škodo posameznika ali organizacije. Dejstvo je, da se za zmanjševanje omenjenih varnostnih groženj posamezniki ne smejo samo zavedati potencialnih napadov in njenih posledic, temveč tudi naučiti ustreznih ravnanj, ki preprečujejo možnost nastanka tovrstnih groženj. Pri tem je izredno pomembna vloga posameznika, ki je tudi odvisna od posameznikove motivacije in njegove same pripravljenosti. Pri tem pa se premalokrat vprašamo, na kakšen način želimo posamezniki resnično zaščititi svoje delovno okolje in okolje podjetja.

LITERATURA IN VIRI

1. Ajzen, I. (1991). Theory of planned behaviour. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.
2. Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289.
3. Albrechtsen, E. & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476–490.
4. Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432–445.
5. Alerouda, A. & Zhoub, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160–196.
6. Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308–313.
7. Antončič, M. (2015). *Zaposleni kot temeljni dejavnik informacijske varnosti.* Ljubljana: Anigma,
8. Asanka Gamagedara Arachchilage, N. & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312.
9. Ashenden, D. (2008). Information Security management: A human challenge*? Information Security Technical Report, 13*(4), 195–201.
10. Bojanc, R., Jerman-Blažič, B. & Tekavčič, M. (2014). *Informacijska varnost v podjetniškem okolju*. Ljubljana: Ekonomska fakulteta.
11. Chen, C. C., Shaw, R. S. & Yang, S. C. (2006). Mitigating information security risk by increasing user security awareness: a case study of an information security awareness system. *Information Technology, Learning, and Performance Journal*, 24, 1–14.
12. Churchill G. A. jr., Brown J. T. (2004): Basic Marketing Research (5th ed.). Thomson South-Western.
13. Cohen, F. (2006). *Information Security Awareness Basics*. New Jersey: Kingston.
14. Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days? *Information security technical report, 14*(4), 1–11.
15. Cooper, M. D. (2000). Towards a model of safety culture. *Safety Science, 36*(2), 111–136.
16. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.
17. Crume, J. (2001). *Inside Internet Security*. Boston: Addison Wesley.
18. Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security, 24*(2), 139–151.
19. Da Veiga, A. & Eloff, J.H.P. (2009). A framework and assessment instrument for information security culture. *Computers & Secu*rity, *29*(2), 196–207.

20. De Leeuw, K. (2007). *The History of Information Security*. Amsterdam: University of Amsterdam.
21. Dezin, N.K. & Lincoln. Y. S. (2005). *Handbook of Qualitative research* (3th ed.). London: Sage.
22. Dodge, R. C. Jr., Carver, C. & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73–80.
23. Dourish, P., Grinter, R.E., Delgado de la Flor, J. & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing, 8*(6), 391–401.
24. Fajdiga, S. (2015). *Vpliv varnostnih opozoril na varnost porabnika informacijsko komunikacijske tehnologije* (diplomsko delo). Maribor: Fakulteta za varnostne vede.
25. Furnell, S. (2005). Why users cannot use security. *Computers and Security, 24*, 274–279.
26. Goh, R., (2003). *Information Security: The Importance of the Human Element* (Ph. D.) Lahore: Preston University.
27. Hagen, J.M. (2009). Human Relationships: A Never-Ending Security Education Challenge? IEEE Security & Privacy, *7*(4), 65–67.
28. Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision support systems, 47*(2), 154–165.
29. Hickmann Klein, R. & Mezzomo Luciano, E. (2016). What influences information security behavior? A study with Brazilians users. *Journal of Information Systems and Technology Management, 13*(3), 479–496.
30. Internet World Stats. World internet usage and population statistics, March 31, 2017, update (31. marec 2017). Najdeno 1. avgusta 2017 na spletnem naslovu: http://www.internetworldstats.com/stats.htm.
31. Information technology - Security techniques - Information security management systems (5. februar 2016). Najdeno 8. avgusta 2017 na spletnem naslovu: http://www.iso27001security.com/html/27000.html.
32. Information technology - Security techniques - Code of practice for information security controls (5. oktober 2016). Najdeno 18. avgusta 2017 na spletnem naslovu: http://www.iso27001security.com/html/27002.html.
33. Jerman Blažič, A. (15. januar 2006). Informacijska varnost. Najdeno 20. junija 2017 na spletnem naslovu: http://www.monitor.si/clanek/informacijska-varnost/122021/?xURL=301
34. Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685-692.
35. Lebek, B., Uffen J., Neumann, M., Hohler, B. & H. Breitner, H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review, 37*(12), 1049–1092.
36. Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly,* 71–90.

37. Lim, J. S., Shanton C., Maynard, S. & Ahmad, A. (2009). *Exploring the Relationship between Organizational Culture and Information Security Culture*. Proceedings of the 7th Australian Information Security Management Conference. Perth, Zahodna Avstralija.
38. Lobnikar, B., Prislan, K., Markelj, B. & Banutai, E. (2012). Informacijskovarnostna ozaveščenost v javnem in zasebnem sektorju v Sloveniji. *Varstvoslovje*, *14*(3), 345–363.
39. Lynett, M. (2015). A History of Information Security From Past to Present. Najdeno 19. junija 2017 na spletnem naslovu: http://blog.mesltd.ca/a-history-of-information-security-from-past-to-present.
40. Malhotra, N. K. (2002). *Basic Marketing Research: Applications to Contepuary Issue*s. New Jersey: Prentice Hall
41. McCormac A., Zwaans T., Parsons K., Calic D., Butavicius M. & Pattinson M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69,* 151–156.
42. Moore, M. (25. junij 2003). Pillars of your community, *CSO online*. Najdeno 19. junija 2017 na spletnem naslovu: www.csoonline.com/read/010903/pillars.com.
43. Nikolakopoulos, T. (2009). *Evaluating the human factor in information Security* (Master's degree). Oslo: University of Oslo.
44. Organization for economic co-operation and development (OECD). (13. avgust 2002*). Guidelines for the security of information systems and networks*. Najdeno 2. avgusta 2017 na spletnem naslovu: http://www.oecd.org/dataoecd/16/22/15582260.pdf.
45. Ögütçü, G., Testik, Ö. M. & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers & Security, 56, 83–93.
46. Parkin, S.E., Van Moorsel, A.P.A & Coles, R. (2009). An Information Security Ontology Incorporating Human-Behavioural Implications. *Proceedings of the 2nd international conference on security of information and networks*. Najdeno 8. Avgusta 2017 na spletnem naslovu: https://www.researchgate.net/publication/221506957_An_Information_Security_Ontology_Incorporating_Human-Behavioral_Implications
47. Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334–345.
48. Partridge H. (2005). Establishing the human dimension of the digital divide. *Information security and ethics: social and organizational issues*. IRM Press, Hersey, USA, 23-47
49. Peltier, T. R. (2005). Implementing an information security awareness program. *The EDP Audit, Control, and Security Newsletter*, *33*(1), 1–18.
50. Puhakainen, P. (2006). *A designed theory for information security awareness*. Linnanmaa: Faculty of Science.
51. Rančigaj, K. & Lobnikar, B. (2012). *Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture.* Maribor: Fakulteta za varnostne vede.
52. Rheea, H., Kimb, C. & Ryuc, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816–826.

53. Schultz, E (2005). The human factor in security. Computers and Security, 24, 425–426.
54. Selan, D. & Bernik, I. (2011). *Upravljanje informacijske varnosti – strateški in operativni vidik.* Maribor: Fakulteta za varnostne vede.
55. Shen, C., Yu, T., Xu, H., Yang, G. & Guan, X. (2015). User practice in password security: An empirical study of real-life passwords in the wild. *Computer & Security, 61,* 130–141.
56. Shapiro, C., & Varian H. (1998). *Information Rules*. Boston: Harvard Business School Press.
57. Sommestad, T., Karlzén, H. & Hallberg, J. (2015).The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*(2), 200–217.
58. Stantona, J.M., Stama, K. R., Mastrangelo, P. & Jolton, J. (2004). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.
59. Swain, A. D., & Guttman, H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. NUREG/CR-1278, U.S. Nuclear Regulatory Commission, (Washington D.C.).
60. Von Solms, S. H. (2009). *Information security governance*. New York, London: Springer.
61. Zakon o gospodarskih družbah. *Uradni list RS št. 42/2006, 60/2006* popr., 26/2007-ZSDU-B, 33/2007-ZSReg-B, 67/2007-ZTFI (100/2007 popr.), 10/2008, 68/2008, 23/2009; Odl. US: U-I-268/06-35.
62. Warschauer M. (2002). Reconceptualizing the digital divide. *First Monday, 7*(7).
63. Wilford, S. H. & Wakunuma, K. J. (2014).Perceptions of ethics in IS: how age can affect awareness. *Journal of Information, Communication and Ethics in Society, 12*(4), 270–283
64. Workman, M., Bommer, W. H. & 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.

PRILOGE

KAZALO PRILOG

PRILOGA 1: Slovar slovenskih prevodov tujih izrazov

International Organization for Standardization (ISO)	Mednarodna organizacija za standardizacijo
Confidentiality	Zaupnost
Integrity	Celovitost
Availability	Razpoložljivost
Plan, Do, Check, Act model	Model planiranja, izvedbe, preveritve in ukrepanja (PDCA model)
Knowledge Attitude Behavior model	Model znanja, odnosa in vedenja (KAB model)
Theory of planned behaviour	Teorija načrtovanega vedenja (TPB)
Protection motivation theory	Varstveno motivacijska teorija (PMT)
General Deterrence Theory (GDT)	Teorija splošnega odvračanja zastraševanja
Technology Acceptance Model	Model za sprejem tehnologije (TAM)
Brute forcing method	Tehnična metoda s pomočjo iskanja znakov
Log files	Dnevne datoteke
Long term evolution	Omrežje LTE
Secure Socket Layer	Opozorilni protokol SSL
Transport Layer Security	Opozorilni protokol TLS
Security	Varnost
Privacy	Zasebnost
Supervisory control and Data acquisition	Sistem za nadzor kontrolo in podatkovno pridobivanje (SCADA)
Denial Of Service	Zavrnitev storitve (DoS)
Distributed Denial Of Service	Porazdeljena zavrnitev storitve (DDoS)
General Data Protection Regulation	Splošna uredba o varstvu osebnih podatkov (GDPR)

PRILOGA 2: Opomnik za izvedbo polstrukturiranih globinskih intervjujev

1. SEGMENT INTERVJUJA: značilnosti intervjuvancev in intervjujev

Kontaktna oseba: oseba, spol, izkušnje na obravnavanem področju, delovno mesto
Intervju: datum intervjuja, čas intervjuja, lokacija intervjuja
Specifikacija organizacije: velikost organizacije

2. SEGMENT INTERVJUJA: kvalitativna odprta vprašanja

1. Pojasnite, kako v vaši organizaciji razumete informacijsko varnost in kakšno vlogo igra le ta v vašem podjetju?

2. Pojasnite, kako je v vašem podjetju razumete informacijsko varnostno kulturo?

3. Pojasnite, kako v vašem podjetju upravljate informacijsko varnost?

4. Kakšna je vaša informacijska struktura in kdo je v vašem podjetju odgovoren za njeno izboljševanje?

5. Na lestvici od 1 do 10 samoocenite stopnjo zadovoljstva z informacijsko varnostjo v vašem podjetju?
    a. Pojasnite vašo oceno

6. Kaj menite katera je najpogostejša šibkost ureditve informacijske varnosti znotraj organizacije?
    a. Kaj menite katere so še ostale šibkosti ureditve informacijske varnosti znotraj organizacije

7. Pojasnite kakšno vlogo ima posameznik pri varovanju podatkov v vašem podjetju?
    a. Opredeljujete posameznika kot grožnjo ali kot osnovni vir oz. steber za gradnjo obrambnih mehanizmov pred morebitnimi grožnjami?

8. Razložite ali se vaši zaposleni zavedajo pomembnosti varnostne politike in ali jo v celoti upoštevajo?
    a. Kakšne ukrepe izvajate, če se posamezniki ne upoštevajo varnostno politiko podjetja, oz. na kakšen način rešujete tovrstno problematiko?

9. Pojasnite, kaj za organizacijo kot celoto predstavljajo raznorazne udeležbe posameznikov na delavnicah in tečajih o informacijski varnosti?
    a. Se zaposleni udeležujejo različnih delavnic in tečajev?
        i. Če da, koliko zaposlenih obiskuje tovrstne tečaje ter kako pogosto?

10. Kaj menite, kateri so tisti dejavniki, ki močno vplivajo na varnostno vedenje posameznika?

11. Kateri so po vašem mnenju ključni elementi izboljševanja varnostnega vedenja posameznika v vašem podjetju?

12. Menite, da človeški faktor igra pomembno vlogo pri zagotavljanju informacijske varnosti? Razložite oz. pojasnite?

13. Kateri so po vašem mnenju trenutno najbolj zahtevni vidiki oziroma dejavniki varovanja podatkov v današnjih organizacijah?

14. Kakšne izzive in smernice na področju informacijske varnosti v vaši organizaciji lahko pričakujete v prihodnosti?