UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Špela Orehek

Merjenje informacijske varnostne kulture: metaanaliza anketnih merskih inštrumentov

Magistrsko delo

Ljubljana, 2017

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Špela Orehek

Mentor: izr. prof. dr. Gregor Petrič

Merjenje informacijske varnostne kulture: metaanaliza anketnih merskih inštrumentov

Magistrsko delo

Ljubljana, 2017

"*Beseda je obleka duše*." – Lucius Annaeus Seneca

Iskreno se zahvaljujem mentorju izr. prof. dr. Gregorju Petriču za strokovnost, natančno usmerjanje, hitro odzivnost in spodbudne besede pri izdelavi magistrskega dela.

Posebna zahvala je namenjena mami in fantu – hvala, ker sta s svojo nesebično podporo vedno ob meni, ko vaju najbolj potrebujem.

POVZETEK

Merjenje informacijske varnostne kulture: metaanaliza anketnih merskih inštrumentov

Ob sodobni tehnologiji, ki omogoča visoko zaščito tehničnih sistemov, je dandanes človeški dejavnik najpomembnejši vidik informacijske varnosti v organizaciji. Malomarnost ali nevednost zaposlenih privede do varnostnih tveganj, kjer so ogroženi občutljivi podatki, posledice njihovih dejanj pa občuti celotna organizacija. Zaradi tega je pomembno, da le-ta oblikuje informacijsko varnostno kulturo, preko katere zaposleni ponotranjijo norme, stališča in vedenje za doseganje višje stopnje informacijske varnosti. Cilj magistrskega dela je ugotoviti prisotnost in kvaliteto anketnih merskih inštrumentov za merjenje informacijske varnostne kulture. To smo dosegli s pomočjo metode metaanalize, ki daje sistematičen pregled nad obstoječimi vprašalniki. Vsebuje metodološko oceno z vidika kvalitete, ki se nanaša predvsem na njihovo veljavnost in zanesljivost. Analiza je pokazala, da kvalitetnih anketnih merskih inštrumentov na tem področju ni. Visoko oceno z vidika kvalitete je dosegel le en merski inštrument. Obstaja pa več veljavnih in zanesljivih merskih inštrumentov, ki merijo sorodne koncepte, zato bi indikatorje ustreznih delov vprašalnikov lahko združili v nov modificiran merski inštrument, ki bi imel pričakovano visoko kakovostno oceno. Magistrsko delo s tem predstavlja osnovo za nadaljnje raziskovanje na področju metodologije informacijske varnostne kulture.

Ključne besede: informacijska varnostna kultura, merjenje, kvaliteta, informacijska varnost, človeški dejavnik.

Measuring an information security culture: meta-analysis of survey instruments

With the modern technology that enables high security of technical systems, currently the human factor is the most important aspect of information security in an organization. Negligence or ignorance of employees leads to security risks, when sensitive data is at stake and the consequences of their actions are felt by the entire organization. For this reason, it is important to create an information security culture through which employees internalize norms, attitudes and behaviour to achieve a higher level of information security. The aim of this master's thesis is to determine the prevalence of survey instruments for measuring the information security culture. This was achieved by using the meta-analysis method that provides a systematic overview of existing questionnaires. It contains a methodological assessment from the aspect of quality, which relates primarily to their validity and reliability. The analysis showed that there are no established survey instruments in this field – only one measuring instrument has reached high evaluation from the view of quality. There are several valid and reliable measuring instruments that measure similar concepts in other fields, however relevant parts of those questionnaires could be combined into a new modified measuring instrument with the expected high quality of assessment. This master's thesis thus forms the basis for further research in the field of methodology of information security culture.

Key words: information security culture, measurement, quality, information security, human factor.

KAZALO

Kazalo slik

Kazalo tabel

1 UVOD

Informacijska varnost je v času nenehnega razvoja informacijsko-komunikacijske tehnologije (IKT) in družbe znanja eden izmed ključnih vidikov varovanja zasebnosti v smislu zaščite osebnih podatkov in informacijskih sistemov na ravni posameznika, organizacije ali države. Pomemben poudarek daje na varnostno politiko, standarde in protokole, s čimer se je možno zaščititi pred kibernetskim kriminalom (nezakoniti vdori, zlorabe in uničenje podatkov itd.).

V današnjem času visoko razvite tehnologije in človeškega znanja je vsaka organizacija izpostavljena varnostnim tveganjem in grožnjam informacijske varnosti, čemur priča vrsta kibernetskih napadov v zadnjem času. Raziskovalci in varnostni strokovnjaki vedno bolj poudarjajo, da tveganja in grožnje ne moremo učinkovito zmanjšati oziroma preprečiti le s tehnično zaščito, ampak je pri tem ključen človeški kapital zaposlenih, s katerim lahko vplivamo na ustrezno varnostno vedenje (Rančigaj in Lobnikar 2012). Organizacije se namreč še vedno premalo zavedajo, da so zaposleni z nizko stopnjo zavedanja informacijske varnosti njihova najšibkejša točka (Shaw in drugi 2009, 93).

Človeški dejavnik informacijske varnosti zajema več konceptov, v zadnjem času pa je v ospredju pojem informacijske varnostne kulture, ki kot del širše organizacijske kulture celostno obravnava miselne, vedenjske in druge vidike zaposlenih za zagotavljanje informacijske varnosti. Proces razvoja informacijske varnosti, pri katerem je sploh nastala informacijska varnostna kultura, je potekal v več valovih. Prvi val, t.i. tehnični val, je trajal do začetka 80. let prejšnjega stoletja in je zajemal tehnični vidik informacijske varnosti, nato pa se je z razmahom interneta začel drugi – menedžerski val, kjer so se vodstva organizacij začela zavedati pomena varnosti in se osredotočati na oblikovanje varnostnih politik, usmeritev in postopkov. V tretjem, t.i. institucionalizacijskem valu, ki se je pojavil v začetku 90. let, se je začela razvijati informacijska varnostna kultura, saj je pomen varnosti zaobjel širši del organizacijske kulture, zato je zanj značilna standardizacija postopkov informacijske varnosti. Sledi še upravljavski val, ki se je začel v začetku tega tisočletja, poudarek je predvsem na upravljanju informacijske varnosti, ki naj bi bil del prakse celotnega upravljanja podjetja ter današnji t.i. kibernetski val, ki se osredotoča na zaščito računalnikov in računalniške opreme pred nepooblaščenim dostopom (vdorom) (Von Solms 2000; Von Solms 2006; Kuusisto in Kuusisto 2013). Vendar samo zaščita računalnikov kljub dobri varnostni programski opremi v današnji družbi znanja ni dovolj, ampak je močna informacijska varnostna kultura tista, ki pripomore k učinkovitejšemu soočanju z varnostnimi tveganji.

Gre za relativno mlado področje raziskovanja v družboslovju, kjer prihaja do neskladij med teoretskimi zasnovami pojma informacijske varnostne kulture in dejansko uporabo koncepta v organizacijah. Med drugim je razlog za to v pomanjkanju merskih inštrumentov, ki bi na hiter, enostaven in učinkovit način organizacijam omogočili določiti stopnjo varnostne kulture in na osnovi tega načrtovati spremembe na ravni vedenja zaposlenih. V literaturi sicer obstajajo načini anketnega merjenja informacijske varnostne kulture, vendar so ti inštrumenti oblikovani na podlagi različnih modelov, zato enotnega in uveljavljenega orodja trenutno ni.

Namen magistrskega dela je sistematičen pregled, analiza kvalitete in ocena anketnih merskih inštrumentov za merjenje informacijske varnostne kulture s pomočjo metode metaanalize. Pri tem je moje glavno raziskovalno vprašanje, kateri anketni merski inštrumenti informacijske varnostne kulture se sploh uporabljajo in nadalje kateri izmed njih so kvalitetni z vidika veljavnosti in zanesljivosti. Naloga je usmerjena v raziskovanje obstoječe literature s sekundarno analizo podatkov. S tem je bil oblikovan sistematičen pregled obstoječih anketnih merskih inštrumentov, zato naloga hkrati predstavlja osnovo za nadaljnje raziskovanje na področju metodologije in merjenja informacijske varnostne kulture.

V prvem (teoretičnem) delu se magistrsko delo osredotoča na obravnavo relevantnih pojmov in modelov informacijske varnostne kulture ter njenih sorodnih konceptov, nadalje na tveganje in grožnje informacijske varnosti ter ravnanju zaposlenih, nazadnje pa še na načine merjenja informacijske kulture. Drugi (empirični) del se nanaša na izvedbo metaanalize, kamor spada predstavitev metode, izbor relevantnih raziskav (merskih inštrumentov), njihova predstavitev in evalvacija ter povzetek ugotovitev.

2 KONCEPTI ČLOVEŠKEGA DEJAVNIKA INFORMACIJSKE VARNOSTI

Raziskovalci ugotavljajo, da je človeški faktor temeljni vzrok za večino varnostnih tveganj oziroma kršitev v organizacijah (Dhillon 2001; Da Veiga in drugi 2007; Ahlan in drugi 2015, Thosou in drugi 2015). Informacijska varnostna kultura in posameznikovo zavedanje o varni uporabi tehnologije sta v obdobju razvite IKT dva ključna dejavnika, ki lahko preprečita raznovrstne grožnje in zlorabe občutljivejših podatkov. Poleg omenjenih pojmov pa obstajajo tudi drugi podobni koncepti s poudarkom na doseganju čim višje stopnje informacijske varnosti, ki jih prav tako predstavljamo v nadaljevanju.

2.1 ZAVEDANJE INFORMACIJSKE VARNOSTI

Zavedanje informacijske varnosti (angl. *information security awareness*) je širši koncept, ki se nanaša na določeno stopnjo znanja računalniške pismenosti vsakega posameznika. Splošno definicijo zavedanja informacijske varnosti so oblikovali Ahlan in drugi (2015, 361), ki pravijo, da se ta nanaša na stanje ali stopnjo posameznikove zavesti, da je potrebno upoštevati pravila (varnostnega) vedenja, prepoznati potencialne nevarnosti in ustrezno ukrepati ter razumeti pomen odgovornosti za informacijsko varnost celotne organizacije.

Raziskovalci pojem pogosto obravnavajo preko dveh vidikov, in sicer prvič kot obseg, v kolikšni meri posamezniki razumejo pomen varnega informacijskega vedenja (Parsons in drugi 2017, 41). V tem kontekstu Kruger in Kearney (2006, 289) zavedanje informacijske varnosti opredeljujeta kot stopnjo posameznikovega razumevanja pomembnosti informacijske varnosti in njegove individualne odgovornosti v organizaciji. Drugi vidik pa se nanaša na posameznikovo dejansko vedenje ter zavezanost k odgovornemu obnašanju v skladu s pravili in varnostno politiko organizacije (angl. *information security policy*) (Siponen 2001).

Na podlagi tega so raziskovalci razvili t.i. KAB model (angl. *Knowledge – Attitude – Behaviour*), ki temelji na znanju, stališčih in vedenju zaposlenih. Argument v ozadju modela se nanaša na predpostavko, da v kolikor imajo zaposleni ustrezno znanje o zavedanju informacijske varnosti, bi to za posledico moralo vzpostaviti pozitivno stališče, kar pa naj bi privedlo do izboljšanega varnostnega vedenja zaposlenih (Parsons in drugi 2014, 335).

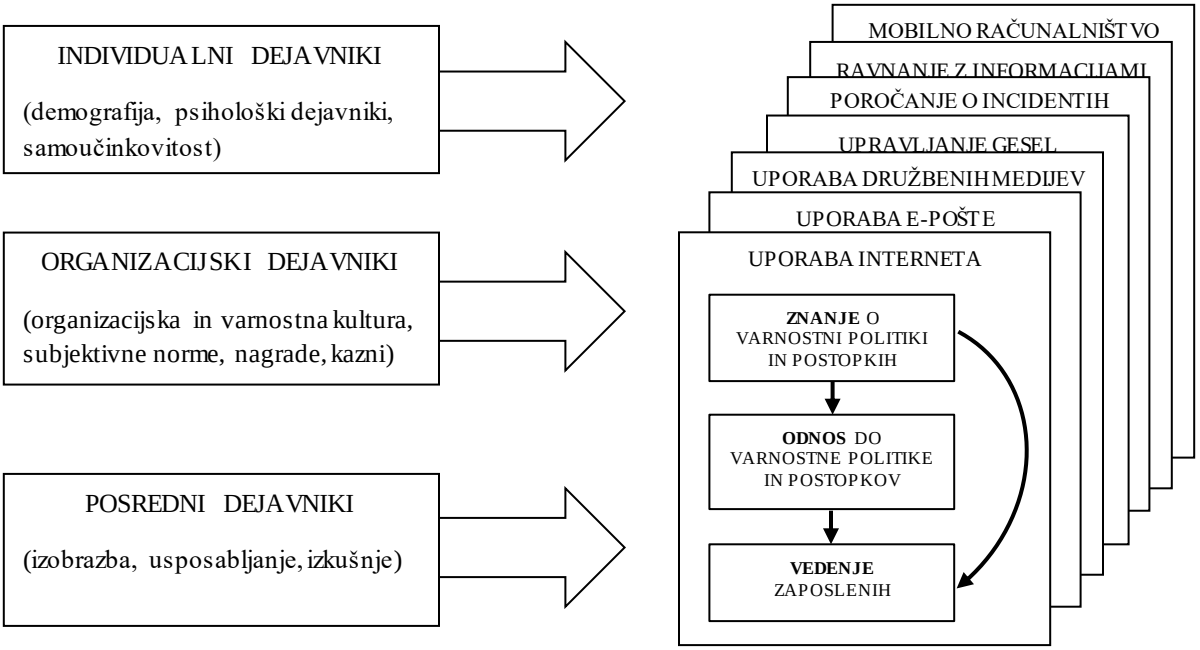
Slika 2.1: KAB model zavedanja informacijske varnosti

Vir: Parsons in drugi (2017, 48).

Izpeljan splošen model zavedanja informacijske varnosti temelji na individualnih dejavnikih, ki oblikujejo osebnost, na organizacijskih dejavnikih, ki oblikujejo varnostno kulturo ter posrednih dejavnikih, ki se nanašajo na usposabljanje. Omenjeni dejavniki vplivajo na znanje, stališče in vedenje zaposlenih, ki skupaj tvorijo zavedanje informacijske varnosti (Parsons in drugi 2017).

Na podlagi splošnega modela so avtorji oblikovali razširjen model, ki upošteva tudi sedem komponent zavedanja informacijske varnosti, in sicer uporabo interneta, elektronske pošte in družbenih medijev, upravljanje gesel, poročanje o incidentih, ravnanje z informacijami in mobilno računalništvo (McCormac in drugi 2017). Poimenovali so ga HAIS model (angl. *Human Aspects of Information Security Model*), kar v prevodu pomeni model človeškega vidika informacijske varnosti.

Slika 2.2: HAIS model – človeški vidik zavedanja informacijske varnosti



Vir: Parsons in drugi (2014, 169).

Koncept zavedanja informacijske varnosti v organizaciji temelji predvsem na človeškem faktorju ter njegovemu socialnemu in kulturnemu kapitalu, saj je zavedanje z ustreznim in doslednim usposabljanjem možno nadgraditi (Safa in drugi 2015, 68). Model HAIS zajema sedem komponent uporabe IKT, ki so prepoznane kot relevantne veščine za doseganje ustrezne stopnje zavedanja informacijske varnosti. Znanje o varnostni politiki in postopkih, ki se tiče

vsake izmed teh ravnanj, pripelje k izboljšanemu odnosu do informacijske varnosti, kar pa vpliva na bolj zavedno vedenje zaposlenih (Parsons in drugi 2014; McCormac in drugi 2017).

Kritika modela se nanaša predvsem na povezanost znanja, odnosa in vedenja zaposlenih. Nekateri raziskovalci so prišli do ugotovitev, da je med vsemi tremi dimenzijami majhna, vendar pozitivna povezanost, medtem ko drugi veljavnost modela izpodbijajo z dejstvom, da med dimenzijami obstaja (pre)velika korelacija. Teoretično gledano je pomembno, da se jasno opredeli vrsto znanja, ki ga preučuje posamezna študija oziroma na kaj se ta nanaša (McCormac in drugi 2017, 152).

Raziskovalci človeškega dejavnika informacijske varnosti so se sprva osredotočali predvsem na pojem zavedanja, v zadnjem času pa se vse bolj izpostavlja tudi pojem varnostne kulture kot bolj relevanten za raziskovanje vloge človeškega faktorja, saj temelji na širših vidikih zagotavljanja informacijske varnosti.

2.2 INFORMACIJSKA VARNOSTNA KULTURA

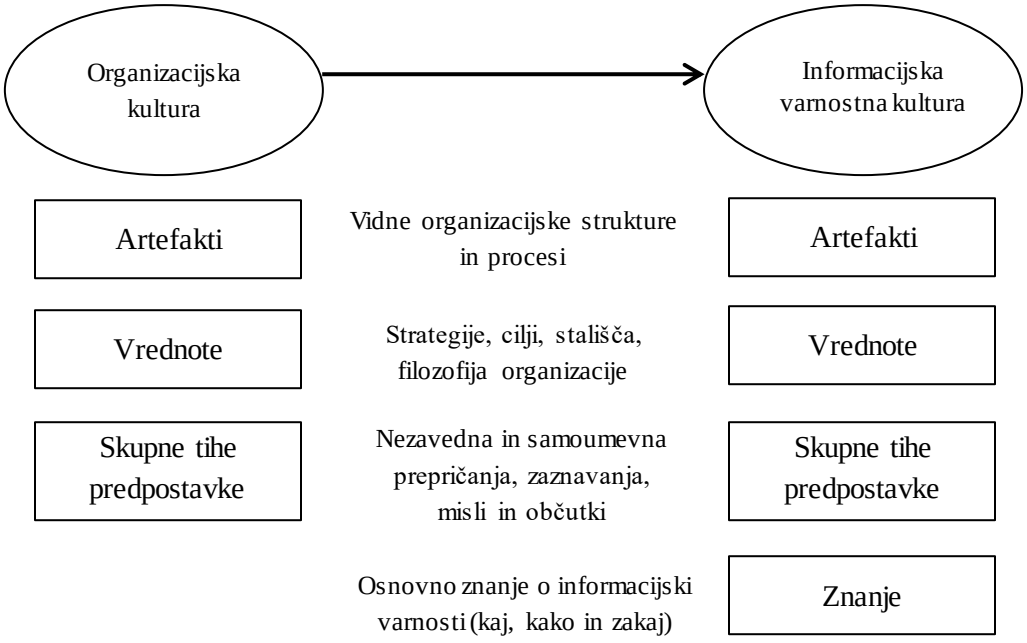
V vsaki organizaciji, ki se posveča informacijski varnosti, se bo sčasoma pojavila določena stopnja informacijske varnostne kulture kot del širše organizacijske kulture. Učinki le-te bodo vidni v vedenju, aktivnostih in znanju zaposlenih na tem področju. Močna informacijska varnostna kultura pripomore k učinkovitejšemu soočanju z varnostnimi tveganji, ki jim je v današnjem času izpostavljena praktično vsaka organizacija (Da Veiga in drugi 2007, 148).

Pojem informacijska varnostna kultura (angl. *information security culture*) se je prvič pojavil konec 20. stoletja, ko so raziskovalci ugotovili, da pomembnost informacijske varnosti v organizaciji močno narašča. Zato so informacijsko varnost začeli obravnavati v okviru holističnega pristopa kot celovit koncept, ki pripada delu organizacijske kulture (Martins in Eloff 2002, 204–205). Schein je konec 20. stoletja organizacijsko kulturo opredelil kot vzorec osnovnih prepričanj, ki ga je razvila določena skupina ljudi, in ga je mogoče prilagajati zunanjim spremembam in notranji integraciji ter se ga priučiti (Schein 1987, 6–9). Pojem kulture v tem kontekstu dobro ponazarja tudi naslednja misel: »Kultura je duša organizacije – prepričanja, vrednote in način, kako se le-te kažejo. Pri tem mislim na strukturo kot okostje ter meso in kri. In kultura je duša, ki stvar drži skupaj in ji daje življenje.« – Henry Mintzberg.

Informacijska varnostna kultura torej temelji na osnovnih načelih organizacijske kulture, usmerjena pa je v področje informacijske varnosti organizacije.

Sprva so informacijsko varnostno kulturo opisovali zelo ohlapno, in sicer kot človeške atribute, ki prispevajo k zaščiti vseh vrst informacij v določeni organizaciji (Dhillon 2001, 166). Sistematično pa sta pojem med prvimi poskušala opredeliti Martins in Eloff, ki pravita, da informacijsko varnostno kulturo označujejo določene značilnosti, kot so dojemanje, stališča in odnos zaposlenih, ki so sprejete in ponotranjene na ravni organizacije. Prav tako se informacijska kultura nanaša na predpostavko o tem, kaj je in kaj ni sprejemljivo glede informacijske varnosti v organizaciji (Martins in Eloff, 2002, 205). Bolj natančno definicijo sta oblikovala Da Veiga in Eloff (2010, 198), ki informacijsko kulturo definirata kot »stališča, predpostavke, prepričanja, vrednote in znanje, ki jih zaposleni nenehno uporabljajo v interakciji z organizacijskimi sistemi«. Vsaka taka organizacija ima določene prakse varovanja informacij, ki jih vključujejo v delovno okolje (Martins in Eloff 2002). Interakcija in dejanja pa imajo za posledico sprejemljivo ali nesprejemljivo ravnanje, ki se kaže v artefaktih (vedenjskih vzorci in načini ravnanja), ki tako postanejo način dela v organizaciji za zaščito svojih informacijskih sredstev (Da Veiga in Eloff 2010; Van Niekerk in Von Solms 2010).

Slika 2.3: Opredelitev informacijske varnostne kulture



Vir: Van Niekerk in Von Solms (2010, 479).

Ta definicija temelji na Scheinovem modelu tristopenjske organizacijske kulture, ki jo sestavljajo artefakti (vidne organizacijske strukture in procesi), vrednote (stališča organizacije, strategija, cilji) in skupne tihe predpostavke (nezavedna in samoumevna prepričanja, zaznavanja, misli in občutki, ki navzven niso vidni). Van Niekerk in Von Solms (2010) sta tej opredelitvi za oblikovanje informacijske varnostne kulture dodala še četrto stopnjo, in sicer nujno potrebno osnovno znanje informacijske varnosti.

Informacijsko varnostno kulturo pa lahko razumemo tudi kot oblikovanje ustreznih prepričanj in vrednot s področja varnosti, na katerih temelji vodenje zaposlenih, da bi s svojim vedenjem dosegli varno informacijsko okolje v organizaciji (AlHogail in Mirza 2015, 286).

V najnovejših raziskavah se omenja tudi pojem informacijske varnostne subkulture, ki temelji na predpostavki, da imajo zaposleni iz različnih geografskih, etničnih ali starostnih skupin različne vrednote in prepričanja glede varovanja informacij in interakcije z informacijski sistemi. Organizacija ima lahko prevladujočo informacijsko varnostno kulturo in eno ali več subkultur. V dominantno skupino spada večina zaposlenih, ki posedujejo temeljne vrednote informacijske varnosti v organizaciji, medtem ko subkultura označuje manjšo skupino zaposlenih, ki delijo skupne vrednote informacijske varnosti, ki so povezane z njihovim delovnim okoljem, oddelkom, geografskim območjem, državljanstvom ali drugimi značilnostmi določene skupine (Da Veiga in Martins 2017, 72).

Skupno vsem omenjenim definicijam informacijske varnostne kulture je človeški vidik delovanja v organizacijah, ki se kaže v posameznikovem vedenju in njegovem kapitalu. Vedenje se nanaša na upoštevanje načel informacijske varnosti, kapital pa se nanaša na posameznikovo znanje in spretnosti glede informacijske varnosti, ki jih vsakodnevno uporablja pri delu (Rančigaj in Lobnikar 2012).

2.2.1 STOPNJE INFORMACIJSKE VARNOSTNE KULTURE

Informacijska varnostna kultura v organizaciji je odraz usklajenega delovanja sistemov in ravnanja zaposlenih za doseganje varnostnih ciljev (Rančigaj in Lobnikar 2012, 3). Razvija in oblikuje se skozi čas, ko zaposleni sčasoma preko usposabljanj in izkušenj pridobivajo notranjo osveščenost glede pomembnosti informacijske varnosti. V organizacijah, kjer ne vlagajo v razvoj informacijske varnosti, pa ta ni razvita oziroma zelo slabo razvita. Informacijska

varnostna kultura temelji na dejavnikih organizacijske kulture, zato lahko primerjamo njuno povezanost na različnih stopnjah. Lim in drugi (2009, 91–92) so opredelili tri povezave med organizacijsko in varnostno kulturo ter na podlagi tega sklepali na stopnjo varnostne kulture, in sicer:

- informacijska varnostna kultura je ločena od organizacijske kulture – nizka stopnja varnostne kulture;
- informacijska varnostna kultura je subkultura organizacijske kulture – srednja stopnja varnostne kulture;
- informacijska varnostna kultura je integrirana v organizacijsko kulturo – visoka stopnja varnostne kulture.

Kadar je informacijska kultura ločena od organizacijske, gre za nizko stopnjo varnostne kulture, saj le-ta ni del načrtovanja in upravljanja s kadri. Posledično je nizka stopnja zavedanja informacijske varnosti zaposlenih, prav tako pa ti nimajo zadostnega znanja in občutka odgovornosti, saj niso ustrezno vključeni v proces informacijske varnosti. Organizacijska varnostna politika je sicer lahko oblikovana, vendar vodstvo ni dovolj dosledno pri njenem izvajanju v praksi. Na varnost organizacija gleda kot strošek, zato se s tem bežno ukvarjajo le v informacijsko-tehnoloških (IT) oddelkih.

O srednji stopnji informacijske varnostne kulture govorimo takrat, ko je varnostna kultura subkultura organizacijske kulture. To pomeni, da v organizaciji obstajajo manjše skupine ljudi oziroma oddelki, kjer so ljudje zaradi narave dela bolj ozaveščeni o informacijski varnosti (poleg IT oddelka še npr. računovodski in kadrovski oddelek). Kljub temu pa sta komunikacija in sodelovanje med ostalimi oddelki oslabljena. Pogostokrat se usposabljanje za večjo ozaveščenost in znanje informacijske varnosti izvaja samo za določene zaposlene.

Visoka stopnja varnostne kulture pa pomeni, da je le-ta del organizacijske kulture. S tem so vsi zaposleni vključeni v proces informacijske varnosti in se zavedajo svoje odgovornosti. Organizacijska varnostna politika in ostale varnostne prakse se dosledno izvajajo in zaposleni poznajo postopke ravnanja v primeru varnostnih incidentov (groženj). Informacijska varnostna kultura je tako globoko integrirana v organizacijsko kulturo, da zavedanje o informacijski varnosti zaposlenim nezavedno postane način dela pri vsakodnevnih opravilih.

2.2.2 KOMPONENTE INFORMACIJSKE VARNOSTNE KULTURE

Informacijsko varnostno kulturo v organizaciji sestavlja več komponent. Raziskovalci na znanstvenem področju so v svojih raziskavah prišli do različnih ugotovitev, katere komponente se pojavljajo pri merjenju informacijske kulture. Pri tem se osredotočajo predvsem na človeški vidik oblikovanja informacijske varnostne kulture. Komponente, ki so se pojavljale v dosedanjih analizah, lahko povzamemo v spodnji tabeli, ki prikazuje še razlago pomena komponente in seznam avtorjev oziroma raziskav, kjer je bila prepoznana posamezna komponenta.

Tabela 2.1: Komponente informacijske varnostne kulture

Komponente	**Opis**	**Raziskovalci/literatura**
Upravljanje	Vloga upravljanja oziroma vodenja je ključna za oblikovanje kulture, saj temelji na oblikovanju strategije informacijske varnosti organizacije	ISF (2000) Van Niekerk in Von Solms (2005) Dojkovski in drugi (2007) Da Veiga in Eloff (2010) Faily in Fléchais (2010) Greene in D'Arcy (2010) AlHogail (2015) Flores in Ekstedt (2016)
Varnostna politika	Znanje in zaznavanje pravil in postopkov varnostne politike je temelj za ustvarjanje skupnih vrednot in prepričanj in pozitivno vpliva na informacijsko varnostno kulturo	ISF (2000) Vroom and Von Solms (2004) Thomson in drugi (2006) Knapp in drugi (2009) Da Veiga and Eloff (2010) Alnatheer in drugi (2012) Box in Pottas (2013) Da Veiga (2015) Sherif in drugi (2015)
Varnostno vedenje	Varnostno vedenje se nanaša na zaščito informacijskih sredstev na podlagi upoštevanja varnostne politike organizacije	Vroom in Von Solms (2004) Ngo in drugi (2005) Albrechtsen (2010) Herath in Rao (2009) Furnell in Thomson (2009) Alfawaz in drugi (2010) Da Veiga in Eloff (2010) Hassan in Ismail (2012) Sherif in drugi (2015)
Skladnost z informacijsko varnostjo	Skladnost se nanaša na poznavanje varnostne politike in ravnanje v skladu z njenimi pravili in naj bi bila vidna lastnost varnostne kulture	Furnell in Thomson (2009) Greene in D'Arcy (2010) Parsons in drugi (2014) Tsohou in drugi (2015) Sherif in drugi (2015)
Znanje	Znanje, ki ga zaposleni posedujejo o razumevanju informacijske varnosti, in vpliva na to, kako ravnajo z informacijami in organizacijskimi sredstvi	Zakaria (2006) Van Niekerk in Von Solms (2006) Thomson in drugi (2006) Hassan in Ismail (2012)

Komponente	Opis	Raziskovalci/literatura
Zavedanje in usposabljanje	Trening zavedanja informacijske varnosti zaposlenih se izvaja zato, da bi razumeli tveganje in izvajali ustrezno kontrolo ter se ravnali po pravilih informacijske varnosti	OECD (2002) Van Niekerk in Von Solms (2005) Thomson in drugi (2006) Flores in Ekstedt (2016) Dojkovski in drugi (2007) Alnatheer in drugi (2012) Herold (2011) Kruger in drugi (2011) Hassan in Ismail (2012) Hovav in D'Arcy (2012) Parsons in drugi (2014) Sherif in drugi (2015) Da Veiga in Martins (2015) AlHogail (2015) Safa in drugi (2015)
Dejavniki tveganja / Operativno upravljanje	Način, na katerega organizacije prepoznajo, preprečujejo, odkrivajo in se odzivajo na varnostne incidente	OECD (2002) ISF (2000) Sabbagh in Kowalski (2012) Munteanu in Fotache (2015) Shameli-Sendi in drugi (2016)
Upravljanje sprememb	Prilagajanje spremembam s tehnološkega vidika je v vsaki organizaciji nujno, zato je potrebno pomagati zaposlenim z vključevanjem in sprejetjem sprememb, da postanejo del kulture	Ngo in drugi (2005) Da Veiga in Martins (2010) Hassan in Ismail (2012) AlHogail (2015)

Vir: povzeto in prilagojeno po Da Veiga in Martins (2017, 76–78).

Komponente, ki so del informacijske varnostne kulture, lahko razdelimo na notranje in zunanje. Zunanji dejavniki se nanašajo na zunanje vplive družbenega konteksta na zaposlenega, notranji dejavniki pa na vpliv, ki je povezan s posameznikom kot način ravnanja, ki izhaja iz notranjosti posameznika. Med notranje dejavnike torej uvrščamo skladnost z informacijsko varnostjo in varnostno vedenje, med zunanje pa upravljanje, varnostno politiko, zavedanje in usposabljanje, operativno upravljanje in upravljanje sprememb. Komponento znanja lahko obravnavamo kot notranji ali zunanji dejavnik, saj na eni strani regulira posameznikovo ravnanje, po drugi strani pa na stopnjo znanja vplivajo drugi dejavniki iz okolja (Da Veiga 2017, 75).

Komponenta zavedanja in usposabljanja informacijske varnosti se v raziskavah kot dejavnik informacijske varnostne kulture pojavlja največkrat. Kritzinger in Von Solms (2010, 841) verjameta, da sta usposabljanje in trening zavedanja informacijske varnosti ključna dejavnika, ki zmanjšujeta tveganje za kršitev informacijske varnosti v organizaciji. Pri zaposlenih, ki so bili deležni usposabljanj, so v določenih časovnih intervalih merjenja zaznali višjo stopnjo informacijske varnostne kulture kot pri tistih, ki se usposabljanj niso udeležili (Da Veiga in

Martins 2015a). Na drugi strani pa raziskovalci ugotavljajo, da samo pridobivanje znanja in usposabljanje za informacijsko varnost ni dovolj, ampak gre za skupek dejavnikov, ki vzajemno vplivajo na višjo stopnjo informacijske varnosti organizacije (Metalidou in drugi 2014). Poudarek na treningu veščin zavedanja informacijske varnosti ima pozitiven učinek na informacijsko varnostno kulturo, ki se s tem skozi čas izboljšuje (Da Veiga in Martins 2014, 56). Prav tako so raziskovalci potrdili, da višja stopnja zavedanja informacijske varnosti pomeni tudi boljšo informacijsko varnostno kulturo v organizaciji (Parsons in drugi 2017, 43). Prehod zavedanja informacijske varnosti v varnostno kulturo je zaznan v trenutku, ko zaposleni kot skupina začnejo varnostna tveganja in grožnje dojemati kot nesprejemljive in spremenijo svoje vedenje (Rančigaj in Lobnikar 2012, 3). Iz tega lahko sklepamo, da je zavedanje informacijske varnosti pomemben dejavnik, ki sooblikuje varnostno kulturo, in hkrati nujen predpogoj za njen nastanek.

Temu sledita komponenti varnostno vedenje in varnostna politika. Varnostno vedenje se nanaša zaščito informacijskih sredstev na podlagi upoštevanja varnostne politike organizacije, varnostna politika pa na dojemanje in upoštevanje pravil in postopkov, kar je temelj za ustvarjanje skupnih vrednot in prepričanj. Sklepamo, da so omenjene tri komponente vsekakor pomembne pri oblikovanju varnostne kulture. V nekaterih raziskavah se pojavljajo tudi druge komponente, ki se navezujejo na definicijo pojma informacijske varnostne kulture (npr. odnos, norme, komunikacija, zaupanje).

2.2.3 MODELI INFORMACIJSKE VARNOSTNE KULTURE

Kot že omenjeno, gre za relativno mlado področje raziskovanja, zato uveljavljenih modelov proučevanja informacijske varnostne kulture še ni. Raziskovalci so sicer na osnovi definicije pojma in načel organizacijske kulture na različne načine poskušali osnovati okvirje za razvoj in delovanje informacijske varnostne kulture, vendar ima vsak izmed njih določene pomanjkljivosti. V nadaljevanju so predstavljeni modeli informacijske varnostne kulture, ki so se do sedaj pojavili v znanstveni in strokovni literaturi.

Da Veiga in Martins (2010, 198–202) sta vzpostavila model ISCF (*Information Security Culture Framework*) za oblikovanje informacijske varnostne kulture, ki temelji na načelih širše organizacijske kulture. Model vključuje vedenjski vidik zaposlenih kot glavni dejavnik informacijske varnosti, kar pomeni, da je vedenje zaposlenih ključni dejavnik, ki določa

kvaliteto organizacijske in posledično tudi informacijske varnostne kulture. Posamezne komponente informacijske varnosti vplivajo na informacijsko varnostno vedenje (angl. *information security behaviour*) zaposlenih, ki ga razumemo kot interakcijo med zaposlenimi in organizacijskimi sredstvi[1]. Skladno varnostno vedenje zaposlenih z upoštevanjem navodil pravilnega ravnanja preko implementacije teh komponent pa oblikuje določeno stopnjo informacijske varnostne kulture. Informacijska varnostna kultura je opredeljena na treh stopnjah, in sicer na individualni, skupinski in organizacijski ravni, upoštevajoč Scheinov model opredelitve organizacijske kulture. Model tako predvideva oblikovanje organizacijske informacijske varnostne kulture – organizacijski artefakti, vrednote in predpostavke; skupinske informacijske varnostne kulture – skupinski artefakti, vrednote in predpostavke ter individualne informacijske varnostne kulture – individualni artefakti, vrednote in predpostavke. Podobno strukturo prav tako zagovarjata Rančigaj in Lobnikar (2012), ki sta ugotovila, da je za uspešno upravljanje informacijske varnostne kulture potrebno izvajanje procesov na vseh treh omenjenih nivojih.

Individualna raven se nanaša na zaposlene v organizaciji, katerih lastnosti (npr. starost, zakonski stan, osebnostne in psihološke značilnosti) vplivajo na njihovo varnostno vedenje. Kot hipotetičen primer, ki pa v realnosti nujno ne drži, bi lahko navedli ravnanje oseb različnih starosti; mlajša oseba bi z večjo verjetnostjo izbrala močno geslo (naključno sestavljeno geslo iz malih in velikih črk ter številk oziroma simbolov) kot starejša oseba, ki ni tako vešča tehnoloških orodij, prav tako pa si težje zapomni kompleksnejša gesla. Komponenti informacijske varnosti, ki zajemata individualno raven, sta torej upravljanje zaposlenih (kamor spadajo zavedanje zaposlenih, etično obnašanje in zasebnost) in upravljanje sprememb na področju informacijske varnosti organizacije.

Skupinska raven se nanaša na skupinsko delovanje zaposlenih (oddelek, projektni tim itd.), kjer sta za visoko stopnjo ustreznega varnostnega vedenja potrebna vodenje in nadzor. Primer skladnega varnostnega vedenja na skupinski ravni je upoštevanje pravila o prepovedanem nameščanju nelicenčne programske opreme na vseh programskih sredstvih, ki so v lasti organizacije ali ki jih zaposleni uporabljajo na delovnem mestu. Komponente informacijske varnostne kulture, ki učinkujejo skupinsko raven po tem modelu, so upravljanje varnosti in njeni postopki (z vidika prava in nadzora), program upravljanja varnosti, upravljanje zaposlenih

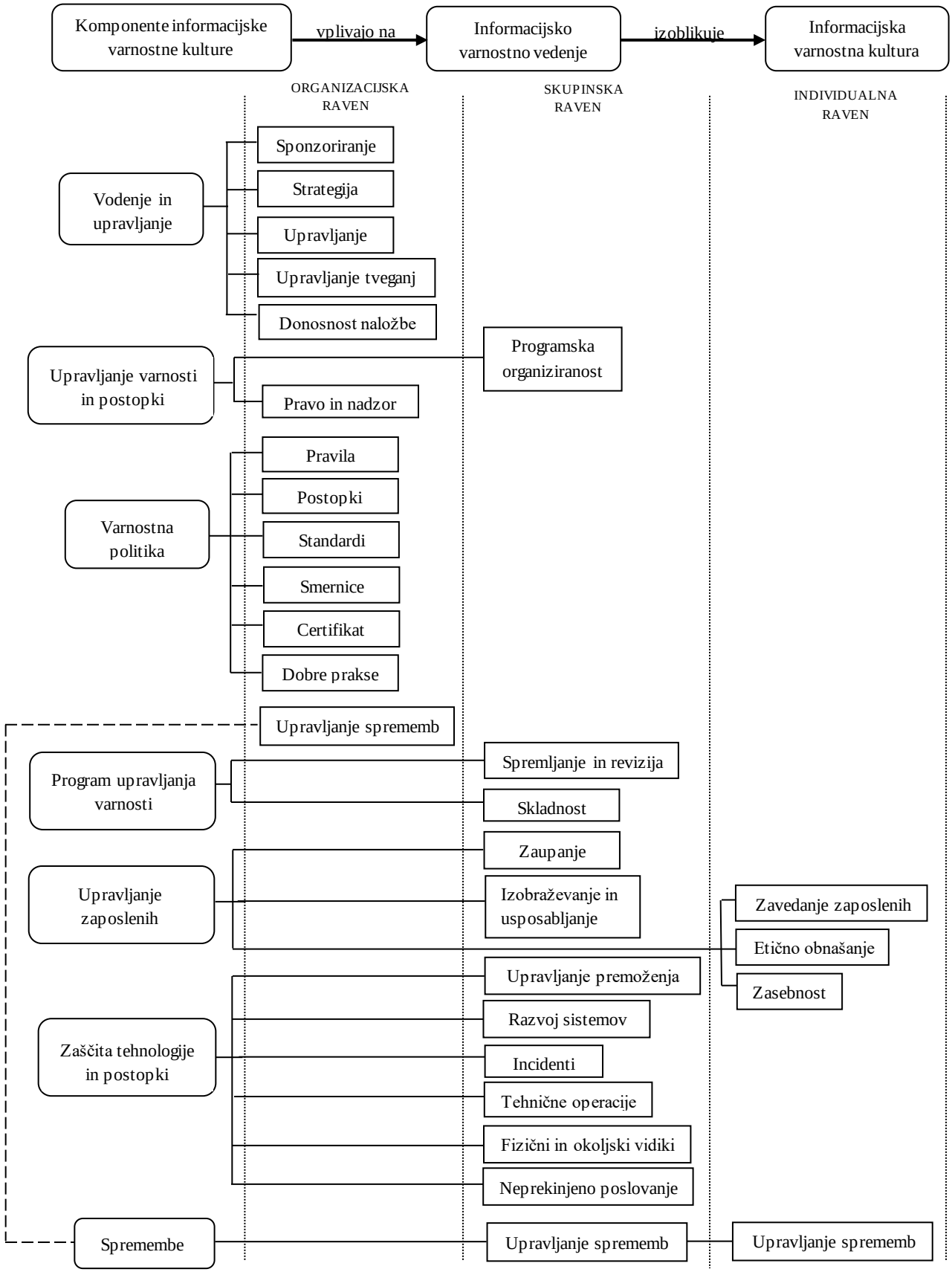
[1] Organizacijska sredstva se nanašajo na *fizična sredstva* (računalniška strojna oprema), *programska sredstva* (operacijski sistemi, aplikacije) in *informacijska sredstva* (znanje ali podatek, ki ima določeno vrednost) (Bojanc in drugi 2014).

(predvsem izobraževanje in usposabljanje), zaščita tehnologije (kamor med drugim spadata poročanje o incidentih in tehnične operacije v zvezi z njimi) ter upravljanje sprememb na področju informacijske varnosti organizacije.

Organizacijska raven pa vključuje tiste dejavnike, ki kažejo, ali organizacija deluje usklajeno in v skladu s temeljnimi akti, kot so vizija, strategija in politika delovanja organizacije. Za njihovo implementacijo na področju varnosti je običajno odgovorno vodstvo ali pa vodilni v informacijskih oddelkih. Primer varnostnega vedenja na organizacijski ravni je zagotavljanje nenehnega dostopa do interneta in notranjega omrežja z namenom ustreznega delovanja informacijske varnostne opreme (virusna in požarna zaščita, elektronska orodja za upravljanje varnosti). Informacijska varnostna kultura na organizacijski ravni se kaže v vodenju in upravljanju, upravljanju varnosti vključno s postopki ter varnostni politiki.

Gre za kompleksen model, ki informacijsko varnostno kulturo obravnava na treh ravneh, glede na vsako komponento informacijske varnostne kulture. Konceptualno je model dobro zasnovan, saj je prilagodljiv in omogoča tudi implementacijo drugih komponent, ki se med raziskavami razlikujejo. Poimenovanje komponent v tem modelu pa se zdi nekoliko nekonsistentno, saj so si med seboj precej podobne. Denimo, med komponentama upravljanje varnosti in postopki ter program upravljanja varnosti ni bistvenih razlik v vsebinskem smislu, kar bralca lahko zmede. Po nepotrebnem sta ti dve komponenti ločeni, saj bi jih bilo bolje združiti. Komponente modela vsebujejo še posamezne podkomponente, kjer bi bili lahko zajeti vsi vidiki obeh podobnih glavnih komponent. Drugo pomanjkljivost vidimo v dejstvu, da komponente glede na definicijo pojma ne zajemajo vseh vidikov informacijske varnostne kulture. Model se ne navezuje na merjenje stališč, vrednot, znanja ali drugih atributov, ki se nanašajo predvsem na človeški faktor, kar v osnovi zagovarja koncept informacijske varnostne kulture.

Slika 2.4: Model ISCF – Da Veiga in Martins



Vir: Da Veiga in Martins (2010, 200).

Manj modificiran in bolj splošen model oblikovanja informacijske varnostne kulture je predlagal AlHogail (2015a, 568–571), ki ga je prav tako poimenoval model ISCF. Ta je sestavljen iz petih komponent: strategije, tehnologije, organizacije, ljudi in okolja. Tudi ta model temelji na vedenjskemu vidiku zaposlenih, ki se kaže skozi pripravljenost, odgovornost, upravljanje ter družbeno regulacijo. Cilj modela je vzpodbuditi skladno informacijsko varnostno vedenje zaposlenih z namenom varovanja informacijskih sredstev.

Slika 2.5: Model ISCF – AlHogail

<table>
<tr><th></th><th>Strategija</th><th>Tehnologija</th><th>Organizacija</th><th>Ljudje</th><th>Okolje</th><th><u>Razvojno orodje:</u>
Upravljanje
s spremembami</th></tr>
<tr><td rowspan="3">Pripravljenost</td><td colspan="5" rowspan="3">Pripraviti zaposlene k varnostnemu vedenju z usposabljanjem, ozaveščanjem in pridobivanjem znanja ter spremeniti njihovo percepcijo</td><td>Usposabljanje</td></tr>
<tr><td>Fokusne skupine</td></tr>
<tr><td>Agenti za spremembe</td></tr>
<tr><td rowspan="3">Odgovornost</td><td colspan="5" rowspan="3">Zagotoviti varnostno vedenje zaposlenih s spremljanjem in nadzorom, nagrajevanjem in sankcioniranjem</td><td>Motivacija</td></tr>
<tr><td>Merjenje</td></tr>
<tr><td>Vključevanje</td></tr>
<tr><td rowspan="3">Upravljanje</td><td colspan="5" rowspan="3">Zagotoviti podporo vodstva z vključevanjem zaposlenih v postopke upravljanja, učinkovito komunikacijo in medsebojni odnos</td><td>Podpora</td></tr>
<tr><td>Sredstva</td></tr>
<tr><td>Komunikacija</td></tr>
<tr><td>Družbena regulacija</td><td colspan="5">Upoštevati zunanje dejavnike (nacionalna kultura, etično vedenje, vladne pobude ter pravni sistem)</td><td>Analiza kulture</td></tr>
<tr><td colspan="7"><u>Rezultat:</u>
Vedenje (artefakti), vrednote, predpostavke in znanje za krepitev informacijske varnosti</td></tr>
<tr><td colspan="7">Prejšnje stanje ČAS Novo stanje</td></tr>
</table>

Vir: AlHogail (2015a, 570).

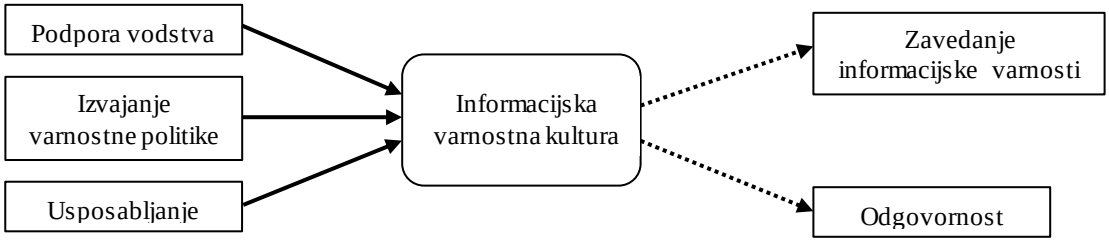
Dimenzija strategije se nanaša na izvajanje različnih postopkov varovanja informacij, kot so varnostna politika, ukrepi, standardi in smernice, ki so namenjeni varovanju informacijskih sredstev. Tehnološka dimenzija v tem kontekstu opredeljuje tehnologije (strojna in programska oprema, naprave, aplikacije), ki se v organizaciji uporabljajo za tehnično zaščito informacijskih sredstev. Nadalje se dimenzija organizacije nanaša na prepričanje, vrednote, predpostavke, norme in znanje, kar predstavlja značilnosti zaposlenih v organizaciji. Četrta dimenzija ljudi se nanaša na ravnanje in vedenje vseh zaposlenih, ki so v stiku z informacijskimi sredstvi. Dimenzija okolja pa se nanaša na določene zunanje elemente, ki vplivajo na organizacijsko strukturo in delovanje (pravni in regulativni sistemi s strani države, vladne usmeritve itd.) oziroma okolje, v katerem organizacija deluje. Vseh pet dimenzij je obravnavanih skozi

omenjene štiri vedenjske vidike zaposlenih. Pripravljenost se kaže v posameznikovi motivaciji za pridobivanje znanja, usposabljanju in spremenjenem zavedanju informacijske varnosti. S tem je povezano tudi področje odgovornosti, ki se nanaša na uspešno izvajanje ukrepov in načel za večjo informacijsko varnost, ki jo organizacija lahko spodbuja preko spremljanja in nadzora ter nagrajevanja. Upravljanje se navezuje na varnostno politiko, načela in usmeritve, ki posredno preko zapisanih pravil vplivajo na vedenje zaposlenih. Družbena regulacija pa je povezana z okoljem in upošteva nacionalno kulturo, zakone in pravni red ter spodbuja etično vedenje zaposlenih v smislu informacijske varnosti.

Model je precej ohlapen kar se tiče dimenzij informacijske varnostne kulture, saj zajema veliko področij, od tehnološkega pa do okoljskega vidika in se ne osredotoča samo na človeški faktor. Sicer izpostavlja vedenjski vidik zaposlenih kot temeljno vodilo, vendar ga obravnava v širšem smislu, ne samo preko notranjih, ampak tudi zunanjih dejavnikov (npr. okolja). Definicija pojma informacijske varnostne kulture pa se osredotoča predvsem na notranje organizacijske dejavnike, ki se nanašajo na zaposlene in organizacijsko kulturo.

Na podlagi temeljitega pregleda literature so Altanheer in drugi (2012) razvili celosten model za razumevanje informacijske kulture. Dejavnike so razmejili na tiste dejavnike, ki vplivajo na oblikovanje informacijske varnostne kulture ter tiste, ki predstavljajo ali odražajo informacijsko varnostno kulturo. Ugotovili so, da na informacijsko varnostno kulturo vplivajo informacijska politika, usposabljanje in podpora vodstva (angl. *top management support*), medtem ko se informacijska kultura odraža v odgovornosti in zavedanju informacijske varnosti.

Slika 2.6: Model informacijske varnostne kulture – Altanheer



Vir: Altanheer in drugi (2012, 5).

Model ima pet komponent, ki sestavljajo informacijsko varnostno kulturo. Podpora vodstva se nanaša na zavzetost oblikovanja in posodabljanja varnostne politike ter drugih ukrepov za

vzdrževanje visoke stopnje informacijske varnosti, kamor spadajo npr. spremljanje in nadzor ravnanja zaposlenih, dodeljevanje odgovornosti za informacijsko varnost ključnim kadrom, zagotavljanje finančnih virov za napredek informacijske varnosti ipd. K temu vidiku sovpada izvajanje varnostne politike, ki je primarno v domeni vseh zaposlenih v organizaciji, po drugi strani pa so za nadzor nad doslednim izvajanjem in upoštevanjem pravil organizacijske varnostne politike običajno zadolženi ljudje v IT oddelkih. Na informacijsko varnostno kulturo po tem modelu vpliva tudi usposabljanje, s katerim naj bi se zmanjšala varnostna tveganja, hkrati pa izboljšalo varnostno vedenje zaposlenih. Preko vpliva omenjenih treh dejavnikov se stopnja varnostne kulture odraža v zavedanju informacijske varnosti in odgovornosti [2] zaposlenih. Zavedanje informacijske varnosti zaposlenih se v tem kontekstu nanaša na zavest zaposlenih, da je njihovo ravnanje povezano z varnostnimi tveganji, odgovornost pa na sposobnost razumevanja pomena vedenja v skladu z informacijsko varnostjo (Altanheer in drugi 2012, 2–5).

Ta model je pomemben z vidika razumevanja oblikovanja informacijske varnostne kulture v smislu njenih dejavnikov in komponent. Namreč ni nujno, da imajo vsi sestavni deli varnostne kulture tudi vpliv nanjo, temveč so lahko samo komponente, ki sooblikujejo varnostno kulturo.

Relevanten model informacijske varnostne kulture je bil nedavno predstavljen v poročilu o organizacijski varnostni kulturi, vendar pa še ni bil objavljen v znanstvenih publikacijah. Razvila sta ga Roer in Petrič (2017), ki informacijsko varnostno kulturo v skladu z zgodovino razumevanja tega pojma obravnavata preko sedmih vidikov, in sicer komunikacije, stališč, norm, znanja in ozaveščenosti (zavedanja), vedenja, skladnosti z varnostno politiko ter zavedanja odgovornosti zaposlenih. Model temelji na predpostavki, da organizacija lahko doseže informacijsko varnost le s sinergijo tehničnih in sociokulturnih sistemov, kar pomeni usklajeno delovanje tehnologije in zaposlenih v organizaciji. Komponente informacijske varnostne kulture po tem modelu zajemajo vse širše vidike, ki so pomembni za organizacijsko kulturo nasploh. Na vedenje zaposlenih vplivajo stališča do informacijske varnostne kulture, ki se kažejo v previdnosti pri ravnanju z občutljivimi podatki; norme, ki se nanašajo na zaznavanje ravnanja sodelavcev; znanje zaposlenih, ki ima eksplicitno moč pri odzivanju na težave glede informacijske varnosti ter skladnost, ki se nanaša na upoštevanje organizacijske varnostne politike. Poleg omenjenih petih komponent pa na stopnjo informacijske varnostne kulture vplivata še komunikacija, ki se nanaša na komunikacijske kanale in odzivnost pri poročanju o

[2] angl. *security ownership*, kar v kontekstu varnostne kulture najbolj ustrezno prevajamo kot odgovornost.

težavah ter zavedanje odgovornosti v smislu, kako zaposleni dojemajo njihovo vlogo za varnost celotne organizacije (Roer in Petrič 2017, 32–35).

V primerjavi z ostalimi modeli informacijske varnostne kulture gre za edini model, ki upošteva komunikacijski vidik organizacijske kulture, ki se nanaša na koherentno in kohezivno delovanje skupine. Nova je tudi komponenta zavedanja odgovornosti zaposlenih do informacijske varnosti, na katero ostali raziskovalci sicer opozarjajo, nihče pa je ni vključil v model varnostne kulture. Splošno gledano se vse zajete komponente izrazito osredotočajo na človeški faktor, ki je glavni akter organizacijske informacijske varnosti v sodobnem času. Model je dobro zasnovan, saj upošteva vse temeljne vidike varnostne kulture, ki so že bili omenjeni. Pomanjkljivost modela se nanaša na teoretsko poglobljenost in utemeljitev na znanstvenem področju, saj v ozadju ni razlage o mehanizmu delovanja modela ter teorij, s katerimi bi pojasnili povezave med komponentami. Sicer pa se odlično prilega definiciji pojma, zato bi bilo smiselno, da se konceptualno razširi in umesti v znanstveno raziskovalno področje.

2.3 SORODNI KONCEPTI

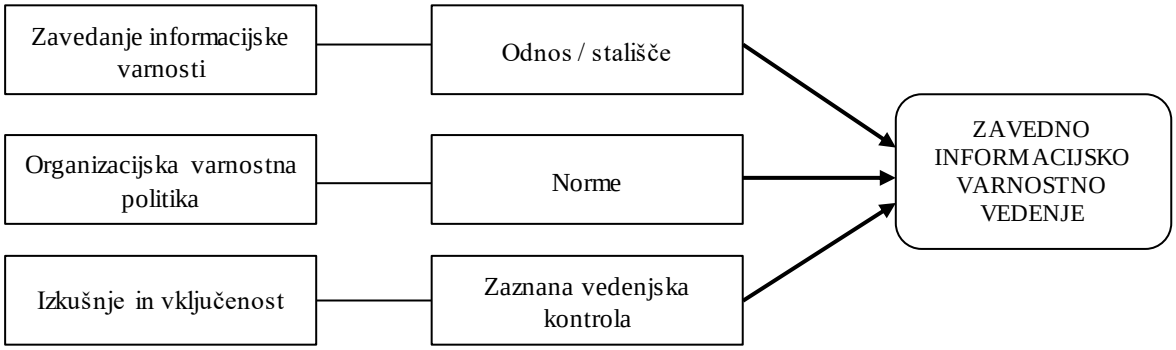
V literaturi se pojavljajo tudi drugi podobni koncepti, ki se nanašajo na človeški dejavnik za doseganje čim višje stopnje informacijske varnosti.

Eden takih je kultura varovanja informacij (angl. *information protection culture*), ki je bil izpeljan iz informacijske varnostne kulture, le da gre za ožji pojem. Velik poudarek daje na zasebnost in varovanje podatkov kot način dela v organizaciji. Kultura varovanja informacij je tako opredeljena kot skupna stališča, predpostavke, prepričanja in znanje zaposlenih, ki prispevajo k varstvu in zasebnosti informacij v kateremkoli trenutku obdelovanja in ravnanja s podatki, kar se kaže v etičnem in skladnem vedenju zaposlenih (Da Veiga in Martins 2015a, 249). Z drugimi besedami gre za spoštovanje načel zasebnosti pri obdelavi osebnih podatkov. Lahko bi rekli, da kultura varovanja informacij predstavlja dimenzijo informacijske varnostne kulture, kajti informacijska varnostna kultura je v organizaciji lahko prisotna brez kulture varovanja informacij, obratno pa ni mogoče.

Safa in drugi (2015) so oblikovali celovit koncept, ki se osredotoča na dejavnike, ki vplivajo na skrb za zavedno informacijsko varnostno vedenje (angl. *information security conscious care behaviour*). Skrb za zavedno informacijsko varnostno vedenje pomeni, da uporabnik

(zaposleni) razmišlja o posledicah svojih dejanj v smislu informacijske varnosti, kadar je v stiku z informacijskimi sistemi, še posebej kadar ima opravka z internetom. Izkazalo se je, da gre za učinkovit koncept za zmanjšanje in preprečevanje incidentov v zvezi z informacijsko varnostjo v organizaciji (Rhee in drugi 2009), zato so mu posvetili več pozornosti. Pojem se je razvil iz informacijskega varnostnega vedenja na podlagi teorije načrtovanega vedenja in varnostno-motivacijske teorije, ki zagovarjata, da se vedenje posameznika spreminja na podlagi odnosa, zato je pojem skrb za zavedno ravnanje po mnenju avtorjev bolj ustrezen (Safa in drugi 2015, 66).

Slika 2.7: Model zavednega informacijskega varnostnega vedenja



Vir: Safa in drugi (2015, 67).

Model temelji na treh glavnih dejavnikih, in sicer zavedanju informacijske varnosti, organizacijski varnostni politiki ter izkušnjah in vključenosti posameznika. Zavedanje informacijske varnosti po tem modelu spreminja odnos zaposlenih, kar posledično vpliva na njihovo vedenje (Safa in drugi 2015, 67). Stopnjo zavedanja zaposlenih je mogoče povečevati predvsem z usposabljanjem preko tečajev, delavnic, igre vlog in predstavitev, hkrati pa se (nezavedno) okrepi tudi znanje informacijske varnosti (Alberchtsen in Hovden 2010). Drug ključen vidik modela zavednega informacijskega varnostnega vedenja je organizacijska varnostna politika, preko katere se oblikujejo subjektivne norme skladnega vedenja zaposlenih (npr. izogibanje izmenjavanju/pošiljanju materiala z občutljivimi podatki). Varnostna politika opisuje pravila ravnanja z organizacijskimi sredstvi in predstavlja pritisk in nadzor nad zaposlenimi, ki ga izvajajo vodje in nadrejeni. Zato notranja in zunanja motivacija [3]

[3] Notranja motivacija je želja posameznika, da doseže svoj cilj, ki se kaže v njegovem interesu, radovednosti, pozitivnem zunanjem ugledu itd. in ni odvisna od zunanjih spodbud. Zunanja motivacija pa se kaže v zunanjih spodbudah (pohvala nagrajevanje, ocenjevanje), ki so glavni dejavniki za doseganje določenega cilja (Marentič Požarnik 2000, 188–189).

posameznika vplivata na njegovo ravnanje za doseganje čim bolj skladnega vedenja pri upoštevanju varnostne politike. Tretji dejavnik izkušnje in vključenost zaposlenih pa se nanaša njihov na trud, čas in energijo, ki so vloženi z namenom izboljšanja varnostnega vedenja. To se izraža v zaznani vedenjski kontroli posameznika, ki s samoučinkovitostjo vpliva na zavedno informacijsko vedenje (Safa in drugi 2015, 68–69).

Model zavednega informacijskega varnostnega vedenja zaposlenih je precej podoben konceptu informacijske varnostne kulture, saj zajema komponente, ki sovpadajo z definicijo varnostne kulture. Izmed šestih komponent so glede na opredelitev varnostne kulture in njenih modelov relevantne štiri, in sicer zavedanje informacijske varnosti, varnostna politika, stališča in norme. Preostali dve komponenti (izkušnje in vključenost ter zaznana vedenjska kontrola) se pri merjenju varnostne kulture načeloma ne pojavljata, čeprav bi vsebinsko prav tako lahko sodili v model. Konceptualno je model zavednega informacijskega varnostnega vedenja zelo dobro utemeljen z omenjenimi teorijami človeškega kapitala, kar omogoča poglobljeno raziskovanje. Prilagojen model bi bil lahko primeren tudi za nadaljnje raziskovanje in merjenje informacijske varnostne kulture.

3 INFORMACIJSKA VARNOST IN RAVNANJE ZAPOSLENIH

Mednarodna organizacija za standardizacijo (angl. *International Organization for Standardization* – ISO) pripravlja različne dokumente za vodenje organizacij in eden izmed njih se nanaša tudi na varnost organizacij (skupina ISO/IEC 27000). Najbolj znan in uporabljen standard, ki vsebuje zahteve in priporočila ter organizacijam omogoča doseganje določene stopnje informacijske varnosti, je dokument z naslovom Sistemi upravljanja informacijske varnosti (International Organization for Standardization 2017). Deluje kot osnova za vzpostavitev zavedanja informacijske varnosti, kar pa sčasoma oblikuje informacijsko varnostno kulturo.

Poleg fizičnih in programskih sredstev so raznim tveganjem in grožnjam izpostavljeni predvsem zaposleni. Malokdo izmed njih se zaveda vseh nevarnosti, ki jim pretijo od zunaj, saj se tehnike napadov hitro spreminjajo in dopolnjujejo, prav tako pa so premalo pozorni na svoje varnostno vedenje. To povečuje možnosti za nastanek kršitev, v tem kontekstu pa ima veliko vlogo informacijska varnostna kultura, ki s širjenjem pomena informacijske varnosti preprečuje vzroke nastanka varnostnih incidentov.

3.1 TVEGANJA IN GROŽNJE INFORMACIJSKE VARNOSTI

Obstaja več vrst zlorab organizacijskih sredstev, še najbolj so na udaru informacijska sredstva in občutljivejši podatki, ki imajo za organizacijo določeno vrednost. Običajno se zlorabe nanašajo na pridobitev oziroma razkritje zaupnih podatkov z namenom izsiljevanja ali izkoriščanja.

Pod pojmom grožnje (lahko tudi kršitev, varnostni incident) razumemo nepričakovane in nezaželene dogodke, ki ogrožajo informacijsko varnost in lahko povzročijo škodo v organizaciji. To pomeni, da moramo vsak dogodek, ki negativno vpliva na procese ohranjanja zaupnosti, razpoložljivosti in celovitosti, obravnavati kot kršitev (ISO/IEC 27000 2016). V tem kontekstu Krausz (2014, 56–58) obravnava tri vrste varnostnih kršitev, in sicer:

- kršitev zaupnosti, ki se nanaša na kršenje načel in smernic varnostne politike organizacije (npr. ravnanje zaposlenega, ki je v nasprotju s pravili varnostne politike);
- kršitev razpoložljivosti, zaradi česar pride do zmanjšane zmožnosti delovanja IT sistemov v organizaciji (npr. množica nezaželenih sporočil elektronske pošte, ki blokirajo poštni strežnik ali virus, ki se razširi v omrežju);
- kršitev integritete, do katere pride zaradi napak pri shranjevanju, prenosu in ravnanju z informacijskimi sredstvi (npr. izguba podatkov).

Hkrati so zaupnost (angl. *confidentiality*), celovitost (angl. *integrity*) in razpoložljivost (angl. *availability*) trije glavni cilji informacijske varnosti, zato se v literaturi za označevanje pogosto uporablja angleška kratica CIA (Bojanc in drugi 2014, 20).

Dandanes so organizacije zaradi razvoja IKT in globalizacije močno vpete v delovanje preko internetnih tehnologij zaradi česar prihaja do večje izpostavljenosti organizacijskih sredstev. S pojavom interneta se je dostopnost do računalnikov in druge tehnološke opreme zelo povečala, kar pa omogoča lažjo zlorabo informacijskih sistemov in podatkov. Zaradi razvoja na področju tehnologije in varnostnih storitev se varnostna industrija hitro prilagaja na nove izzive. Razvijajo se novi produkti na ravni tehnične zaščite, ki omogočajo varno delovanje tehnologije pri povezovanju na različna omrežja, ali pa nove oblike strokovnih usposabljanj za zaposlene (Rusjan 2010, 81). Najpogosteje uporabljeni metodi na ravni tehnične zaščite sta protivirusna

programska oprema in požarni zid, ki ju uporablja praktično vsaka organizacija (Richardson 2008; Safa in drugi 2015).

Varnostne grožnje, ki pretijo zaposlenim v organizacijah in ne nazadnje posameznikom nasploh, predstavljajo največjo nevarnost informacijskim sistemom in informacijskim sredstvom (podatki, ki imajo neko vrednost). Razdelimo jih lahko glede na njihovo usmeritev, in sicer na uničenje, spremembo ali krajo informacijskih sredstev, razkritje zaupnih informacij ter prekinitev delovanja storitev. Povzročitelj grožnje je lahko človek, v primerih višje sile pa tudi naravni pojavi (npr. udar strele) (Bojanc in drugi 2014, 42). Britanska vladna raziskava kaže, da so napadi v večini primerov izvedeni s strani zunanjega nepooblaščenega uporabnika (BIS 2015, 6). To so vsi tisti posamezniki, ki ne delujejo znotraj organizacije (uporabljajo organizacijske storitve, vendar niso zaposleni) in tretje osebe (npr. kibernetski kriminalci, vohuni, teroristi). Nevšečnosti pa lahko povzročijo tudi notranji oziroma pooblaščeni uporabniki, to pa so zaposleni, ki namerno presežejo svoja pooblastila ali storijo nenamerno napako (Bojanc in drugi 2014, 42–47). Najbolj tipične grožnje in tehnike napadov, ki zaposlenim pretijo s strani zunanjega uporabnika, so:

- vdor (angl. *intrusion*): najbolj klasična oblika napada in pomeni nepooblaščen dostop do sistema s pomočjo uporabnikovih podatkov – najpogosteje se zgodi z zlorabo gesel. Najbolj razširjena tehnika zlorabe gesel je socialni inženiring (angl. *social engineering*), kjer napadalec na zvit in premišljen način z manipulacijo zaupanja uporabnika poskuša pridobiti čim več njegovih osebnih podatkov in tako poskuša uganiti geslo oziroma druge pomembne podatke (SI-CERT[4] 2017; Rusjan 2010, 75);
- kraja identitete oziroma osebnih podatkov (angl. *identity theft*): zloraba, ki se nanaša na krajo digitalnih identifikatorjev (predvsem digitalno potrdilo, certifikat, uporabniška imena in gesla na raznih omrežjih, podatki o bančnih računih) z zavajanjem uporabnika. V zadnjem času je najbolj razširjena tehnika napada spletno ribarjenje oziroma lažno predstavljanje (angl. *phishing*), kjer napadalec uporabnika preko lažnih e-poštnih sporočil preusmeri na ponarejeno (potvorjeno) spletno stran, kjer ta vpiše svoje podatke, ti pa se nato samodejno pošljejo napadalcu, ki s tem dobi dostop do dotičnih informacij[5]. Za organizacije so najbolj nevarni t.i. usmerjeni napadi (naprednejše oblike spletnega

[4] SI-CERT (angl. *Slovenian Computer Emergency Response Team)*: nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij, ki nudi pomoč in tehnično svetovanje uporabnikom ob varnostnih grožnjah oziroma zlorabah.

[5] V nekaterih primerih se uporabniku pri kliku na povezavo potvorjene strani samodejno naloži zlonamerna programska oprema (npr. »key-logger«), ki beleži uporabnikove aktivnosti (npr. pritiski na tipkovnico).

ribarjenja - angl. *spear phishing* in *whaling*), saj se osredotočajo na zaposlene ter osebe na višjih položajih (Bernik in Prislan 2012, 57);

- okužbe (angl. *malware*): najbolj razširjen varnostni problem, ki se nanaša na ohromitev oziroma uničenje informacijskega sistema ali računalniške opreme preko podtaknjenih zlonamernih programskih kod (npr. virusi, črvi, trojanski konj, bot v omrežju). Napad se izvede s pošiljanjem elektronskih sporočil, pojavnih oken, pogovornih programov itd., ki vsebujejo okužene spletne povezave ali datoteke, preko katerih se na računalnik samodejno naloži zlonamerna programska oprema (SI-CERT 2017);
- spletne goljufije (angl. *internet scam*) in potegavščine (angl. *hoax*): širjenje neresnične in zavajajoče vsebine (npr. verižna pisma, nigerijska prevarantska pisma s finančnimi obljubami[6], lažna sporočila s prošnjo za pomoč), ki deluje podobno kot pri okužbah in spletnem ribarjenju z namestitvijo zlonamerne programske opreme, kar napadalcu omogoča pridobitev osebnih podatkov (SI-CERT 2017);
- »naslanjanje[7]« (angl. *tailgating*): ena najpogostejših zlorab brez uporabe tehnologije, in sicer gre za nepoštene obiskovalce organizacije, ki preko lažnih situacij in navidezno vljudnostjo od zaposlenih izsilijo nepooblaščen dostop do organizacijskih prostorov ali opreme (Aurigemma in Mattson 2017, 218).

Pri vseh naštetih grožnjah so sredstvo za doseganje cilja predvsem zaposleni, preko katerih zlonamerneži pridejo do svojih tarč (najpogosteje organizacijski podatki ali denar). Obstaja sicer več varnostnih ukrepov na ravni tehnične zaščite, in sicer preventivni ukrepi, ki zmanjšujejo verjetnost za incident (protivirusna programska oprema, požarni zid, kriptografija, redno posodabljanje programske opreme, varnostna politika itd.), korektivni ukrepi, ki zmanjšujejo izgubo v primeru incidenta (redno varnostno kopiranje in arhiviranje, zavarovanje tveganja) ter detekcijski ukrepi, ki skrajšajo čas o zaznavi incidenta (sistemi za zaznavanje vdorov v omrežju, limanica). Vendar pa ti ukrepi v celoti ne morejo zaščititi in preprečiti tovrstne napade (Bojanc in drugi 2014, 55–56).

Varnostna tveganja pa s svojim ravnanjem lahko povzročijo tudi zaposleni brez vpliva tretje osebe. Tako ravnanje štejemo pod incidente notranjih uporabnikov, ki so pogosto posledica

[6] Elektronska sporočila običajno z vsebino v polomljeni angleščini, kjer napadalec žrtvi obljublja finančno korist. Obstaja več različic, najbolj znana je tista o okradenemu prijatelju v tujini. Več v Modic (2010, 85–95).
[7] V slovenskem jeziku še ni ustreznega prevoda pojma.

neupoštevanja ali nepoznavanja varnostne politike. Nekaj pogostih nezavednih kršitev, ki jih povzročajo zaposleni, so:

- nezaklenjena vrata delovnih prostorov (pisarn) in zapustitev računalnika brez nadzora;
- upravljanje gesel: neredna menjava gesel, deljenje (ali souporaba) gesel z drugimi, uporaba privzetih uporabniških imen in gesel, ki jih je mogoče uganiti,
- razkrivanje (objava) podatkov na napačen elektronski naslov;
- neprimerna izmenjava datotek med zaposlenimi;
- izpisovanje občutljivih podatkov;
- izguba naprave (npr. USB ključ, snemalnik zvoka, prenosni računalnik);
- uporaba osebnih mobilnih naprav za povezavo v organizacijsko omrežje (Cisco 2014).

Pri vseh naštetih grožnjah in napakah imajo odločilno vlogo zaposleni, ki s svojimi neprevidnimi (in pogostokrat nezavednimi) dejanji vplivajo na tveganje informacijske varnosti celotne organizacije in tako predstavljajo najranljivejši del sistema.

3.2 VLOGA ZAPOSLENIH

Raziskave v preteklosti so pokazale, da sta »medsebojna interakcija zaposlenih ter njihovo vedenje oziroma odnos do informacijskih sredstev najšibkejša člena informacijske varnosti organizacije« (Da Veiga in drugi 2007, 148). Tudi kasneje so raziskovalci ugotavljali, da zaposleni še vedno povzročajo visok odstotek varnostnih incidentov, čeprav je v zadnjem desetletju zavest o pomembnosti informacijske varnosti močno narasla (Paulsen in Coulson 2011).

Eden izmed standardov ISO (27005 2011) predstavlja podroben seznam ter opis ranljivosti in napak, ki jih zaposleni storijo pri svojem delu, najpogostejše pa so uporaba šibkih gesel ali neustrezno varovanje gesel (zapisovanje gesel), nepravilna uporaba interneta (ogled nedovoljenih vsebin ali sumljivih spletnih strani) in programskih licenc (piratstvo), nenadzorovano odpiranje priponk v elektronskih sporočilih ter nerazumevanje ali nepoznavanje varnostne politike (malomarno ravnanje z računalnikom). Ranljivosti pa se pojavljajo tudi na ravni informacijskih oddelkov, kjer naj bi za informacijsko varnost skrbeli usposobljeni strokovnjaki. Tu gre predvsem za pomanjkanje varnostnih kopij, slabo varnost računalniške opreme (preverjanje delovanja protivirusnih programov in ostale zaščite), slabo komunikacijo z ostalimi zaposlenimi ter pomanjkanje nadzora nad aktivnostmi zaposlenih. Na vodstveni ravni

pa se napake in nepravilnosti nanašajo na oblikovanje ustrezne varnostne politike (ki mora biti praktična in razumljiva), pomanjkanje politike za e-pošto ter odgovornost za splošno pomanjkanje zavedanja informacijske varnosti zaposlenih (Bojanc in drugi 2014; Krausz 2014).

Za zmanjšanje napak človeškega faktorja organizacija lahko poskrbi z učinkovitim sistemom informacijske varnosti, za kar pa je potreben sistematičen pristop (Brezavšček in Moškon 2009). Upravljanje varnostnih tveganj[8] (angl. *security risk management*) je proces ugotavljanja in ocenjevanja tveganj na področju informacijske varnosti ter oblikovanje ukrepov za njihovo zmanjšanje (Alberts in Dorofee 2002). Sem v prvi vrsti spadajo varnostna politika, postopki, zaščitni ukrepi in protiukrepi, ki morajo biti natančno definirani. Taka varnostna kontrola je lahko učinkovita le takrat, kadar se zaposleni zavedajo teh ukrepov in se jih držijo pri vsakodnevnem opravljanju svojega dela (Spears in Barki 2010, 504).

3.3 POMEN INFORMACIJSKE VARNOSTNE KULTURE

Ustvarjanje varnostne kulture v organizaciji zahteva sistematično postavljanje ciljev in motiviranje zaposlenih za doseganje teh ciljev. Za varno organizacijo velja, da v njej obstaja informacijska varnostna kultura, kar pomeni, da njeni zaposleni sprejemajo dobre in pravilne odločitve v smislu varnosti. O visoki stopnji varnostne kulture govorimo, kadar imajo vsi zaposleni aktiven odnos do zaščite osebnih in zaupnih podatkov, kar zahteva znanje informacijske varnosti ter se kaže z zavestnim vedenjem v dani situaciji (Rančigaj in Lobnikar 2012, 2). Stabilna in močna informacijska varnostna kultura je v določeni meri odvisna tudi od vodstva organizacije, ki z obvladovanjem tveganj ter različnimi pristopi motiviranja zaposlenih, kot so nagrade, pohvale in bonitete (ter kazni na drugi strani) poskrbijo za čim boljši sistem zagotavljanja informacijske varnosti (Paulsen in Coulson 2011).

Glavni namen informacijske varnostne kulture je zmanjšati tveganja, ki jih predstavlja vedenje zaposlenih glede uporabe informacijskih sredstev (Da Veiga in Eloff 2010). Hkrati pa je cilj kulture vzpostaviti dejstvo, da je informacijska varnost celotne organizacije odgovornost prav vsakega zaposlenega (AlHogail 2015a, 569). V tem kontekstu sta že pred leti Schlienger in Teufel (2003) poudarjala, da mora varnostna kultura odražati ponotranjeno stališče varnostnega vedenja pri vsakodnevnih dejavnostih vseh zaposlenih.

[8] Za izraz se uporablja tudi pojem obvladovanje tveganj.

Po pregledu literature lahko izpostavimo, da so najpomembnejše komponente, ki dokazano pozitivno vplivajo na informacijsko varnostno kulturo, predvsem varnostna politika, vedenje zaposlenih ter njihovo zavedanje informacijske varnosti (Da Veiga in Eloff 2010; Martins in Da Veiga 2014; Roer in Petrič 2017). Slednje pa se da pridobiti in nadgraditi z usposabljanjem ter ustreznim upravljanjem z zaposlenimi (Martins in Da Veiga 2014; Parsons in drugi 2017). Vsi omenjeni dejavniki so torej ključnega pomena pri oblikovanju informacijske varnostne kulture, obstajajo pa še nekateri drugi organizacijski dejavniki, ki bi prav tako lahko pomembno prispevali k večji stopnji varnostne kulture (npr. komunikacija/interakcija med zaposlenimi, znanje o informacijski varnosti, odnos). V zadnjem času vse več raziskovalcev upošteva znanje kot zelo pomemben dejavnik informacijske varnosti (Rančigaj in Lobnikar 2012; Parsons in drugi 2014; Safa in Von Solms 2016; Roer in Petrič 2017). Dejstvo je, da se informacijska varnostna kultura zaradi številnih novih dejavnikov nenehno spreminja, zato je za ohranjanje želene stopnje ključnega pomena prilagajanje novim vplivom (Rančigaj in Lobnikar 2012, 7).

Stopnja informacijske varnosti je za organizacijo zelo pomembna. Večja kot je stopnja informacijske varnostne kulture, manj je verjetnosti za varnostni incident oziroma zunanji napad na organizacijsko varnost. Za ugotavljanje stopnje varnostne kulture v organizaciji pa je potrebno redno spremljanje in merjenje le-te.

4 MERJENJE INFORMACIJSKE VARNOSTNE KULTURE

Merjenje informacijske varnostne kulture organizaciji prinaša povratno informacijo o varnostnem delovanju (v smislu znanja, vedenja, odnosa, zavedanja) njenih zaposlenih, prav tako pa se z merjenjem identificira šibke točke, ki jih organizacija posledično lahko izboljša. Bernik in Prislan (2016) ugotavljata, da je merjenje informacijske varnosti v praksi slabo razvito ter da so obstoječe usmeritve in priporočila preveč kompleksna za marsikatero organizacijo.

V družboslovnem raziskovanju ločimo med kvalitativnim in kvantitativnim pristopom raziskovanja določenega pojava. V literaturi obstaja tako kvalitativni kot kvantitativni pristop raziskovanja različnih konceptov informacijske varnosti. Nekateri raziskovalci striktno zagovarjajo kvalitativni pristop obravnavanja informacijske varnosti (Johnsen in drugi 2006; Bernik in Prislan 2016), drugi pa večje prednosti vidijo v kvantitativnem načinu merjenja (Kruger in Kearney 2006; Da Veiga in Eloff 2010; AlHogail in Mirza 2015; Roer in Petrič 2017). Obstaja tudi kombiniran način merjenja z uporabo mešanih metod obeh pristopov, kjer

kvalitativni način običajno poveča veljavnost in zanesljivost kvantitativnega načina raziskovanja (Safa in drugi 2015; Parsons in drugi 2017).

4.1 KVALITATIVNI PRISTOP

Kvalitativni pristop se v raziskovanju uporablja takrat, kadar želimo k raziskovanemu problemu pristopiti bolj poglobljeno, se osredotočiti na pomen, razumevanje in iskanje razlage s strani vpletenih. Predmet analize so ponavadi besede (oziroma besedilo), ki ga dobimo preko različnih kvalitativnih metod zbiranja podatkov (npr. poglobljeni intervju, opazovanje z udeležbo, fokusne skupine) (Bryman 2001).

Obravnavanje informacijske varnostne kulture na kvalitativen način zaposlenim omogoča, da izrazijo svoja stališča, strahove in videnje informacijske varnosti v organizaciji (Johnsen in drugi 2006). Tak način zbiranja podatkov lahko poteka v obliki poglobljenih intervjujev ali fokusnih skupin, kar pa je časovno zamudno, še posebej kadar gre za veliko organizacijo.

Bernik in Prislan (2016) pravita, da je s kvalitativnim načinom raziskovanja informacijske varnosti možno oblikovati modele, ki vsebujejo različne vedenjske, organizacijske in kriminološke teorije in s tem pojasniti, kako organizacijski in osebnostni dejavniki, družbeni kontekst, medosebni odnosi, okolje in ostali vidiki vplivajo na varnostno vedenje zaposlenih in posledično prispevajo k informacijski varnosti (oziroma kulturi). Analiza in ugotavljanje stopnje informacijske varnostne kulture pa je na ta način pogostokrat subjektivno, saj končne ugotovitve temeljijo na podlagi intuicije ali pristranske logike.

Smiselno je, da se informacijska varnostna kultura obravnava na vseh zaposlenih, saj napadalci vedno iščejo najšibkejši člen, pogostokrat pa je to (predvsem v velikih organizacijah) neizvedljivo. V osnovi se kvalitativno raziskovanje naslanja na ontološka in epistemološka izhodišča, ki izhajajo iz humanistične ali interpretativne paradigme in se zaradi načina raziskovanja obravnava manjše število enot, kar pa v večini primerov raziskovanja informacijske varnostne kulture ni uporabno.

Zdi se, da za merjenje informacijskih varnostnih konceptov kvalitativen pristop ni najbolj primeren. Informacijska varnostna kultura je kompleksen pojav z več dimenzijami, ki jih je vse težko zajeti v eno analizo, ponovitev take analize pa je praktično nemogoča. Za učinkovito

spremljanje stopnje varnostne kulture potrebujemo orodje, ki bo rezultate podalo v sorazmeroma kratkem času in bodo po ponovnem merjenju ti med seboj primerljivi.

4.2 KVANTITATIVNI PRISTOP

Kvantitativni pristop raziskovanja v osnovi pomeni zbiranje številčnih podatkov večjega števila enot s standardiziranim merskim inštrumentom (npr. anketa), kjer na podlagi vzorca s statistično analizo lahko sklepamo o ugotovitvah na celotno populacijo (Bryman 2001).

Da Veiga in Martins (v AlHogail in Mirza 2015, 287) omenjata kar nekaj prednosti kvantitativnega načina merjenja informacijske kulture. Že sam vprašalnik in dejstvo, da ga bodo izpolnjevali vsi zaposleni, je lahko eden izmed načinov za krepitev zavedanja informacijske varnosti zaposlenih. S tem začutijo, da so del skupnega procesa in tako se poveča njihova pripadnost organizaciji. Stroški izvedbe in analize takega merjenja so relativno nizki, raziskava pa se z enakim vprašalnikom da ponoviti v katerem koli časovnem obdobju. Prav tako standardiziran proces merjenja organizaciji omogoča ugotoviti trenutno stopnjo varnostne kulture ter doseči želeno stopnjo s tem, ko se z rezultati prepozna šibke točke, ki jih je z dodatnimi ukrepi mogoče izboljšati. Tak merski inštrument je učinkovito orodje za primerjanje stopnje varnostne kulture ter ocenjevanje izvajanja njenih aktivnosti in nadaljnjih potreb za doseganje večje varnosti informacijskih sredstev (Da Veiga in Martins 2015b, 173). Glede na enostranske in zanesljive statistične analize so nadaljnje odločitve vodstva lažje in učinkovitejše (Da Veiga in Eloff 2010, 203).

Poleg tega pa kvantitativno merjenje organizacijske informacijske varnostne kulture omogoča tudi primerjave, kot npr. stopnja varnostne kulture med oddelki, razlike glede na spol in starost, medsektorske primerjave ali medkulturne primerjave v multinacionalkah. Roer in Petrič (2017, 12–13) sta tako med drugim ugotovila, da so ženske bolj zaskrbljene glede varnostnih napadov, moški pa so pokazali višjo stopnjo znanja in razumevanja. Sicer pa so ženske bolj dosledne pri izpolnjevanju norm in bolj odprte za sprejemanje varnostnih predpisov. Pomembno vlogo ima tudi starost, namreč z leti se razumevanje in zavedanje odgovornosti za informacijsko varnost povišuje. Taki izsledki imajo za organizacijo veliko pojasnjevalno moč, saj se usposabljanja in druge aktivnosti za izboljšanje informacijske varnosti lahko prilagodijo posameznim podskupinam glede na ugotovljene šibke dimenzije varnostne kulture.

Iz omenjenih dejstev sledi ugotovitev, da je merjenje informacijske varnostne kulture zelo pomembno. Pri analizi človeškega dejavnika informacijske varnosti v organizaciji je ključnega pomena ravno to, da ugotovimo, kateri del (ali kolikšen odstotek) zaposlenih je problematičen z vidika doseganja višje stopnje informacijske varnosti. Zato je relevanten kvantitativni pristop raziskovanja informacijske varnostne kulture. Pojavlja pa se problem anketnega merjenja, saj v praksi ni razvitih veliko takih merskih inštrumentov. Prav tako še ni pregleda merskih inštrumentov, ki se sploh uporabljajo. Pri merjenju varnostne kulture lahko prihaja do težav z neveljavnimi in nezanesljivimi merskimi inštrumenti, pristranskosti odgovarjanja zaradi družbene zaželenosti (ljudje odgovarjajo v skladu s pričakovanji in ne v skladu z dejanskimi ravnanji) ter drugih ovir, na katere so raziskovalci velikokrat premalo pozorni.

5 EMPIRIČNI DEL: METAANALIZA

V empiričnem delu naloge je predstavljena izvedba metaanalize anketnih merskih inštrumentov za merjenje informacijske varnostne kulture in nekaterih sorodnih konceptov. S tem želimo zajeti vse relevantne anketne merske inštrumente (vprašalnike) ter jih analizirati predvsem z vidika kvalitete (veljavnosti in zanesljivosti) ter primernosti za nadaljnjo uporabo. Ker gre za relativno novo področje raziskovanja v družboslovju, merski inštrumenti še niso uveljavljeni in pogosto tudi niso poimenovani.

5.1 OPREDELITEV STATISTIČNE METODE

Metaanaliza je dandanes popularno statistično orodje sekundarne analize podatkov na raziskovalnem področju družboslovja. Sprva se je uporabljala predvsem na področju pedagogike in psihologije, nato pa se je razširila tudi v ostale znanstvene vede družboslovnega raziskovanja (Cheung 2013, 704).

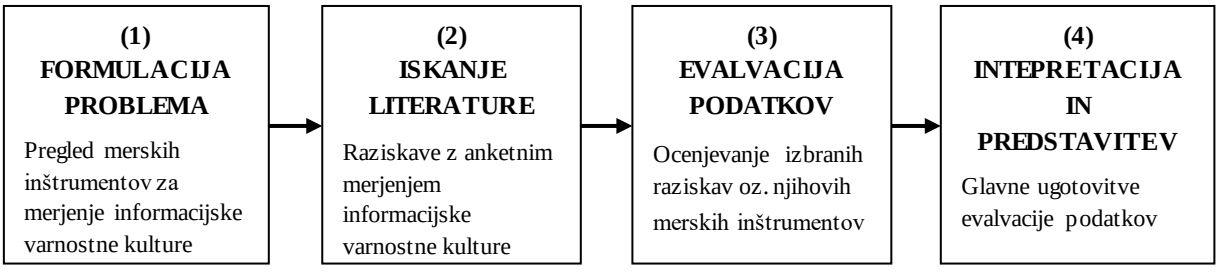
Metaanaliza je statistična metoda, ki s sistematičnim pregledom literature združuje rezultate študij s podobnim raziskovalnim problemom. Na ta način omogoča širši vpogled v raziskovalni problem, teoretični ali empirični zaključki ter končne ugotovitve metaanalize pa dajejo večjo težo znanju na določenem področju znanstvenega raziskovanja (Kastrin 2008, 26).

Utemeljitelj metode metaanalize je ameriški statistik in raziskovalec v pedagoški psihologiji Gene V. Glass, ki je leta 1976 zapisal natančno definicijo: »Metaanaliza se nanaša na analizo

analize. Termin uporabljam za statistično analizo velike zbirke rezultatov posameznih študij z namenom integracije novih spoznanj. Predstavlja močno alternativo dosedanji vzročni in pripovedni razlagi rezultatov in se uporablja kot podpora pri osmišljanju velike količine raziskovalnih podatkov« (Glass 1976, 3). Glass med drugim zagovarja dejstvo, da ustrezno izvedena metaanaliza ponuja pregled nad metodologijo izvedenih študij, daje sistematične, hitre in zanesljive odgovore na raziskovalna vprašanja oziroma hipoteze ter povečuje moč statističnega sklepanja zaradi večje količine podatkov (Smith in Glass 1977). Cooper in Hedges (2009, 11–15) pojem metaanalize opredelita kot opis kvantitativnih postopkov, ki jih raziskovalec uporablja kot statistično združitev rezultatov več študij. V tem kontekstu se metaanaliza nanaša na pregled končnih statističnih izračunov in iz tega izpeljanih relevantnih ugotovitev. Avtorja opredeljujeta tudi stopnje oziroma korake metaanalize, in sicer formulacija problema, iskanje literature, evalvacija/ocena podatkov, analiza podatkov (opcijsko; gre za statistično analizo podatkov metaanalize z računanjem velikosti učinka in uporabo inferenčne statistike), interpretacija rezultatov in predstavitev rezultatov.

Magistrsko delo se osredotoča na metaanalizo anketnih merskih inštrumentov za merjenje informacijske varnostne kulture. Statistično preverjanje dobljenih rezultatov posameznih raziskav pri tem ni ključnega pomena, zato smo ta korak metaanalize izpustili. Prav tako smo združili zadnje dva koraka analize, in sicer interpretacijo ter predstavitev rezultatov. Izvedbo metaanalize po korakih prikazuje naslednja slika.

Slika 4.1: Aplikacija korakov metaanalize merjenja informacijske varnostne kulture po modelu Cooper in Hedges



Vir: Cooper in Hedges (2009, 11–14), prikaz: lastno delo.

V literaturi se kot sinonima za metaanalizo uporabljata tudi pojma sinteza raziskovanja (angl. *research synthesis*) ter pregled raziskav (angl. *research review*) in se nanašata na aktivnosti evalvacije oziroma ocenjevanja kvalitete raziskav iz določenega področja. Med omenjene aktivnosti sodijo pregled literature, pregled in utemeljitev oziroma argumentacija relevantnih

teorij, kritična analiza tematike, reševanje konflikta empirije s teorijo in opredelitev glavnih opornih točk za nadaljnje raziskovanje (Cooper in Hedges 2009, 6). Rezultati metaanalize pogosto opredeljujejo usmeritve nadaljnje analize na obravnavanem področju, saj se s širšim pregledom znanja ugotovi tudi potrebe po dodatnem raziskovanju manj raziskanih pojavov (Hunter in Schmidt 2004, 21).

Eden izmed ključnih namenov metode metaanalize je analizirati kakovost podatkov in njihove analize. V kvantitativnem raziskovanju se kakovost raziskovanja nanaša na vidika veljavnosti in zanesljivosti, saj to pripomore k bolj natančni oceni merskega inštrumenta raziskovalnega okvirja posamezne študije nasploh, ne nazadnje pa so izsledki takih študij bolj objektivni (Kogovšek 2005, 262). Koncept zanesljivosti merjenja (angl. *reliability*) se nanaša predvsem na konsistentnost oziroma ponovljivost, in sicer je »merski postopek (inštrument) zanesljiv, kadar pri ponovnem merjenju pri enakih pogojih daje enake rezultate« (Ferligoj in drugi 1995, 12). Veljavnost (angl. *validity*) pa se nanaša relevantnost empiričnega raziskovanja v smislu utemeljevanja teoretičnih konceptov (konstruktov). Kot veljavno merjenje torej opredeljujemo vsako merjenje, kjer raziskujemo (merimo) tisto, kar dejansko želimo meriti glede na opredeljene cilje, raziskovalni problem oziroma predmet raziskovanja (Ferligoj in drugi 1995, 64). Merski inštrument je lahko zanesljiv, brez da je veljaven, vendar pa ne more biti veljaven, če ni tudi zanesljiv (Kimberlin in Winterstein 2008, 2278).

5.2 IZBOR IN SELEKCIJA PRIMERNIH RAZISKAV

Pri izboru in selekciji primernih raziskav za analizo smo se najprej osredotočili na primarne kriterije izbire, ki jih morajo študije oziroma raziskave izpolnjevati, in sicer:

- odprt dostop ali omogočen dostop študentom Univerze v Ljubljani (DiKUL)[9]
- spletni empirični strokovni ali znanstveni članek
- kvantitativno merjenje pojma informacijska varnostna kultura z anketnim vprašalnikom.

Iskanje primernih strokovnih in znanstvenih člankov je v prvi fazi potekalo preko portala Digitalne knjižnice Univerze v Ljubljani (DiKUL), kjer je uporabnikom na voljo veliko število

[9] Odprt dostop (»*open-access*«) se nanaša na spletne rezultate raziskav, ki so prosto dostopni v različnih bazah podatkov in uporabnikom na voljo za uporabo brez avtorskih oziroma licenčnih omejitev. Omogočen dostop študentom Univerze v Ljubljani pa pomeni brezplačen dostop do članka zaradi članstva v UL.

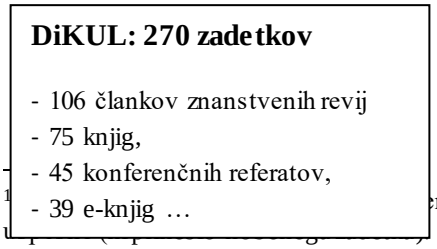
elektronskih knjig in revij, vključno z zbirkami podatkov najpomembnejših svetovnih založnikov (Digitalna knjižnica UL). V drugi fazi je iskanje primernih člankov potekalo na internetu preko iskalnika Google Scholar, v tretji fazi pa je bil izveden pregled seznama literature pridobljenih člankov iz prve in druge faze.

Na dan 16. 5. 2017 je portal DiKUL pri naprednem iskanju s ključnimi besedami »*information security culture*« in »*measurement*«[10] vrnil 270 zadetkov, od tega med drugim 106 člankov iz znanstvenih revij, 75 knjig, 45 konferenčnih referatov, 39 e-knjig in drugo[11]. Po pregledu vseh zadetkov (naslov, povzetek in krajši pregled) je bilo glede na zgoraj omenjene kriterije izbire relevantnih 29 virov. Iskanje ustreznih virov smo z enakimi ključnimi besedami kontrolirali s pregledom zadetkov preko iskalnika Google Scholar[12], kjer smo našli en dodaten ustrezen vir. Po pregledu seznama literature vseh 30 člankov smo identificirali še tri dodatne ustrezne vire. Skupaj je bilo tako v širši nabor virov izbranih 33 virov, ki ustrezajo izbirnim kriterijem.

Sledilo je poglobljeno analiziranje člankov, osredotočali pa smo se predvsem na metodološka poglavja in anketno merjenje informacijske varnostne kulture, kar je glavni namen tega magistrskega dela. Upoštevali smo tudi pristop mešanih metod (kvalitativno in kvantitativno raziskovanje), če smo ocenili, da anketno merjenje predstavlja večji del raziskave in ima torej večjo težo pri izsledkih raziskave. Poleg osnovnega koncepta informacijske varnostne kulture smo upoštevali tudi sorodne koncepte, ki so opredeljeni v teoretičnem delu.

Izmed 33 relevantnih virov smo v tem koraku najprej izločili 15 virov (12 virov zaradi neizpolnjevanja kriterija kvantitativnega merjenja in tri vire zaradi neustrezne tematike). V ožjem izboru je bilo 18 virov, zaradi podobnosti raziskav in merskih inštrumentov smo nadalje izločili še šest virov. Na tak način smo za analizo izbrali 12 raziskav oziroma merskih inštrumentov, ki so podrobno predstavljeni in analizirani v naslednjih poglavjih.

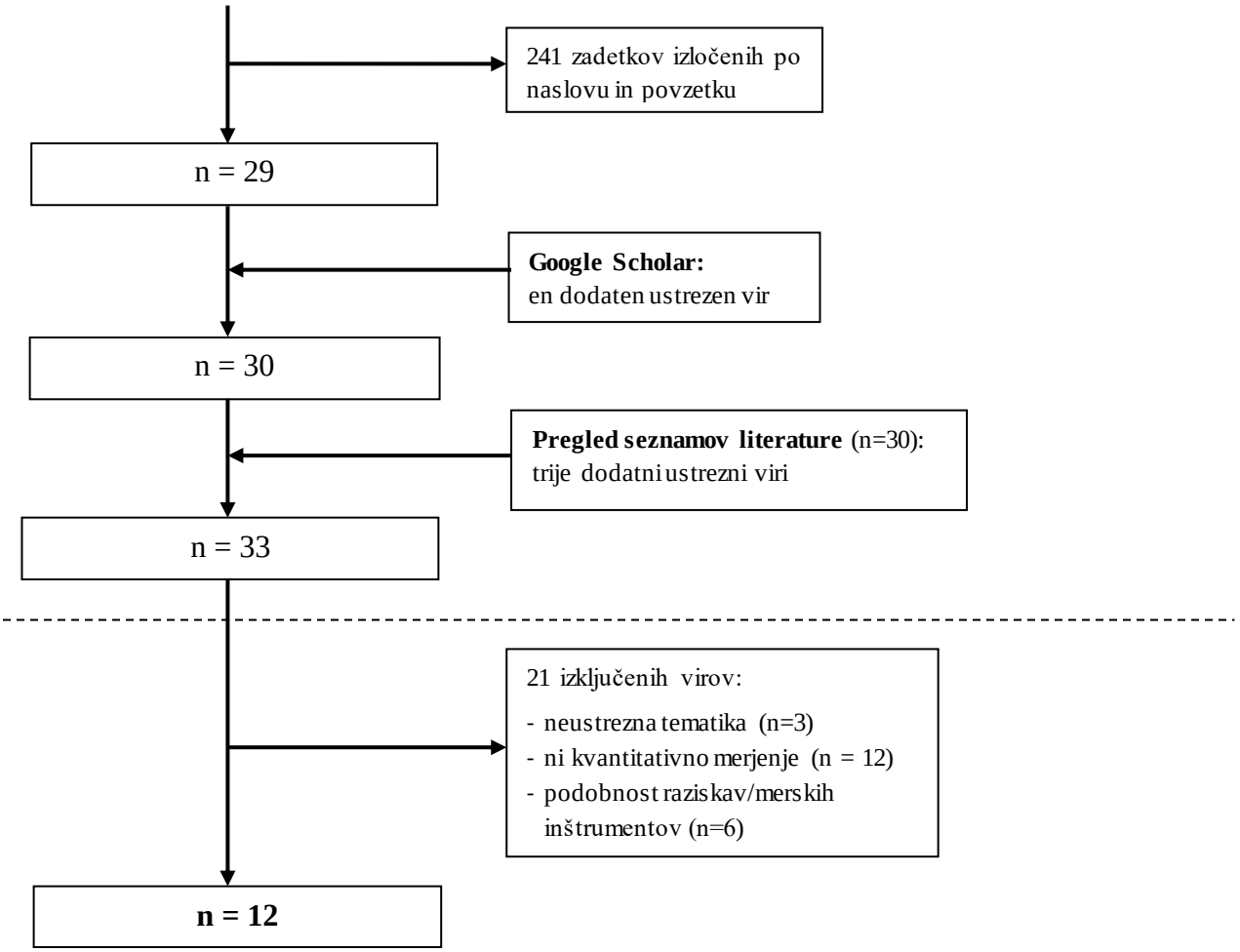
Slika 4.2: Potek izbire relevantnih raziskav za ocenjevanje merskih inštrumentov



[10] V slovenskem jeziku (»*informacijska varnostna kultura*« in »*merjenje*«) ni bilo

[11] Vsi relevantni zadetki (270): 106 znanstvenih revij, 75 knjig, 45 konferenčnih referatov, 39 e-knjig, 13 revij, deset panožnih periodik, pet poročil, tri novice in ena disertacija/diplomska naloga, en elektronski vir in ena recenzija.

[6] Iskanje na dan 3. 6. 2017 je iskalnik vrnil približno 1.090.000 zadetkov, pregledanih pa je bilo prvih 40 strani zadetkov.



5.3 PREGLED IZBRANIH RAZISKAV

V tem poglavju želimo predstaviti osnovne informacije o izbranih raziskavah. Pregled posamezne raziskave vsebuje opis namena raziskave, metodologije, analize in ugotovitev ter omejitev raziskave. Predstavitev analize in ugotovitev se nanaša predvsem na kvaliteto merskega inštrumenta in manj na vsebinske ugotovitve, pri omejitvah pa so povzete kritične točke raziskave, ki so jih avtorji navedli po zaključeni analizi. Osnovne značilnosti izbranih raziskav pa prikazuje spodnja tabela.

Tabela 5.1: Predstavitev izbranih raziskav za metaanalizo

Avtor	Leto	Naslov	Država[13]

[13] Država se nanaša na lokacijo raziskovanja oziroma delovanja raziskovalne skupine (avtorjev).

Da Veiga, Martins in Eloff	2007	Information security culture – validation of an assessment instrument	Južnoafriška republika
Da Veiga in Eloff	2010	A framework and assessment instrument for information security culture	Južnoafriška republika
Da Veiga in Martins	2015	Improving the information security culture through monitoring and implementation actions illustrated through a case study	Južnoafriška republika
Da Veiga in Martins	2015	Information security culture and information protection culture: A validated assessment instrument	Južnoafriška republika
Alnatheer, Chan in Nelson	2012	Understanding And Measuring Information Security Culture	Avstralija
AlHogail	2015	Cultivating and assessing an organizational information security culture: an empirical study	Savdska Arabija
Safa, Sookhak, Von Solms, Furnell, Ghani in Herawan	2015	Information security culture and information protection culture: A validated assessment instrument	Malezija, Južnoafriška republika, Združeno kraljestvo
Rocha Flores in Ekstedt	2016	Shaping intention to resist social engineering through transformational leadership, information security culture and awareness	Švedska
Narain Singh, Gupta in Ojha	2014	Identifying factors of organizational information security management	Indija
Parsons, Calic, Pattinson, Butavicius, McCormac in Zwaans	2017	The human aspects of information security questionnaire (HAIS-Q): Two further validation studies	Avstralija
Ahlan, Lubis in Lubis	2015	Information security awareness at the knowledge-based institution: its antecedents and measures	Malezija, Indonezija
Aurigemma in Mattson	2017	Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls.	Združene države Amerike

1. Da Veiga, Martins in Eloff (2007): Information security culture – validation of an assessment instrument

Namen: Namen raziskave je preveriti merski inštrument za ocenjevanje informacijske varnostne kulture (ki sta ga razvila Martins in Evans) z vidika veljavnosti in zanesljivosti ter tako zagotoviti ustrezen merski inštrument na področju raziskovanja informacijske varnosti in psihologije.

Metodologija: Empirična raziskava je bila izvedena v finančni organizaciji iz Južnoafriške republike, ki zaposluje več kot 12000 ljudi. Uporabljeno je bilo orodje za spletno anketiranje Survey Tracker. Vzorec raziskave je 4735 enot. Vprašalnik je bil razdeljen na tri vsebinske

sklope, in sicer informacijska varnostna kultura, ki vsebuje 42 trditev (indikatorjev), sklop vprašanj o znanju informacijske varnosti ter sklop vprašanj o demografskih podatkih. Zbiranje podatkov je potekalo štiri mesece. Zagotovljeno je bilo spremljanje stopnje odgovora za pridobitev statistično reprezentativnega vzorca za posamezne oddelke zaposlenih v organizaciji (za osem od 12 oddelkov je bila reprezentativnost vzorca glede na določene demografske podatke zagotovljena).

Analiza in ugotovitve: Dvostopenjska eksploratorna faktorska analiza je pokazala, da informacijsko varnostno kulturo lahko razdelimo na šest dimenzij[14], čeprav so pred analizo avtorji predvideli osem dimenzij. Z analizo faktorskih uteži in notranje konsistence je vseh šest dimenzij doseglo zadovoljive ocene veljavnosti in zanesljivosti.

Omejitve raziskave: Po analizi so avtorji ugotovili, da bi se določeni deli vprašalnika lahko še izboljšali, da bi v večji meri zadostili potrebam na različnih področjih industrije. Večji poudarek naj bi bil na znanju, zavedanju in odnosu zaposlenih do informacijske varnosti, saj bi to omogočalo poglobljeno analizo povezanosti vseh dimenzij.

2. Da Veiga in Eloff (2010): A framework and assessment instrument for information security culture

Namen: Namen raziskave je predlagati okvir za razvijanje informacijske varnostne kulture v organizaciji in ponazoriti njegovo uporabo. Ključno vprašanje pri tem je, kako vzpostaviti informacijsko varnostno kulturo v organizaciji, da se bodo zmanjšala tveganja, ki jih predstavlja vedenje zaposlenih v zvezi z uporabo komunikacijskih sredstev. Predlagajo okvir ISCF (Information Security Culture Framework) s sedmimi kategorijami informacijske varnostne kulture, za vsak sklop pa so oblikovane trditve, ki merijo stopnjo informacijske varnostne kulture. Osnovni cilj predlaganega koncepta je preverjanje njegove veljavnosti.

[14] Faktorska analiza je bila izvedena v dveh korakih, in sicer v prvi fazi je analiza pokazala štiri faktorje, na enega izmed njih se je uvrstilo večje število trditev. Zato so avtorji v drugi fazi posebej analizirali ta faktor, v analizi pa se je izkazalo, da gre še za tri nove dimenzije znotraj enega faktorja. Skupno število dimenzij je torej 6, in sicer: upravljanje informacijske varnosti, upravljanje uspešnosti, odgovornost, komunikacija, vodenje in sposobnost.

Metodologija: Empirična raziskava je bila izvedena v podjetju, ki opravlja revizijske in svetovalne naloge iz Južnoafriške republike in zaposluje približno 3000 ljudi. Uporabljeno je bilo orodje za spletno anketiranje Survey Tracker. Vzorec raziskave je 1085 enot. Vprašalnik je sestavljen iz 85 trditev na petstopenjski Likertovi lestvici, ki meri stopnjo strinjanja (oziroma nestrinjanja), izpolnjevali pa so ga zaposleni iz vseh organizacijskih ravni. V štirih izmed petih oddelkov zaposlenih vzorec ni reprezentativen zaradi nizke stopnje odgovora.

Analiza in ugotovitve:Izvedena konfirmatorna faktorska analiza (s sedmimi vnaprej določenimi komponentami informacijske varnostne kulture po okviru ISCF [15]) je pokazala visoko veljavnost in zanesljivost merskega inštrumenta.

Omejitve raziskave: Smiselna bi bila nadaljnja analiza z eksploratorno faktorsko analizo, s čimer bi se ugotavljalo, ali se trditve morda razvrstijo v drugačne dimenzije informacijske varnostne kulture, kot je bilo to predvideno z okvirjem ISCF, kar bi dalo še dodatno težo ugotovitvam raziskave. Z uporabo kompleksnejših tehnik modeliranja strukturiranih enačb bi se lahko oblikoval statistični model za komponente informacijske varnostne kulture, kar bi pripomoglo k ugotavljanju medsebojne povezanosti komponent.

3. Da Veiga in Martins (2015a): Improving the information security culture through monitoring and implementation actions illustrated through a case study

Namen: Raziskava se osredotoča na merjenje vpliva usmerjenega usposabljanja in ozaveščanja zaposlenih o informacijski varnostni kulturi. Gre za primerjalno študijo, katere namen je ugotoviti stopnjo informacijske varnostne kulture med različnimi oddelki zaposlenih v določenih časovnih točkah ter ali se le-ta spreminja oziroma izboljšuje, če zaposlene načrtno vključimo v trening veščin, ki bi po osmih oziroma devetih osnovnih dimenzijah informacijske

[15] Sedem dimenzij po ISCF: vodenje in upravljanje, upravljanje varnosti, varnostna politika, program upravljanja varnosti, upravljanje zaposlenih, zaščita tehnologije in spremembe.

varnostne kulture[16] pripomogle k znanju in vedenju zaposlenih na področju informacijske varnosti.

Metodologija: Empirična raziskava je bila izvedena v mednarodni finančni organizaciji, ki deluje v dvanajstih državah in ima več kot 8000 zaposlenih. Merjenje informacijske varnostne kulture je potekalo v štirih intervalih v obdobju osmih let, velikost vzorca pa se je vsako leto spreminjala[17]. Uporabljeno je bilo orodje za spletno anketiranje Survey Tracker. Vprašalnik, ki sta ga avtorja poimenovala ISCA (Information Security Culture Assessment), je nadgradnja vprašalnika iz prejšnje raziskave[18]. Zbiranje podatkov je vsako leto merjenja potekalo štiri do šest mesecev (odvisno od leta raziskave). Stopnja odgovora je znašala med 28 % in 39 % (odvisno od leta raziskave).

Analiza in ugotovitve: Vprašalnik je bil v smislu kvalitete analiziran predvsem z vidika vsebinske veljavnosti, s katero sta avtorja potrdila visoko stopnjo veljavnosti in s tem povečala veljavnost vprašalnika v skladu s statističnimi analizami prejšnjih raziskav. Izvedena je bila tudi regresijska analiza, s katero je pojasnjena medsebojna povezanost dimenzij informacijske varnostne kulture, kar omogoča boljšo zasnovo teoretskega modela.

Omejitve raziskave: Veljavnost in zanesljivost merskega inštrumenta statistično ni bila preverjena, avtorja se namreč opirata na izsledke prejšnjih raziskav, čeprav je bila opravljena določena prilagoditev vprašalnika, kar lahko vpliva na veljavnost in zanesljivost.

4. Da Veiga in Martins (2015b): Information security culture and information protection culture: A validated assessment instrument

Namen: Namen raziskave je predstaviti pojem kulture varovanja informacij, ki zajema koncept informacijske varnostne kulture in načela zasebnosti ter ugotoviti, ali je vprašalnik ISCA primeren za merjenje omenjenega pojma.

[16] Avtorja sta pojem informacijske varnostne kulture razdelila na osem dimenzij (upravljanje informacijskih sredstev, upravljanje informacijske varnosti, upravljanje sprememb, upravljanje zaposlenih, varnostna politika, program informacijske varnosti, zaupanje, vodenje informacijske varnosti), pri merjenju leta 2010 in 2013 pa sta dodala še deveto dimenzijo (zavedanje in usposabljanje).

[17] Merjenje je potekalo v letih 2006, 2007, 2010 in 2013. Velikost vzorcev po letih je naslednja: 2006: 1941 enot, 2007: 1571 enot, 2010: 2320 enot in 2013: 2159 enot.

[18] Vprašalnik ISCA se nanaša na vprašalnik iz raziskav Da Veiga, Martins in Eloff (2007) in Da Veiga in Eloff (2010) – glej opis pod prvo in drugo točko poglavja 5.3, str. 41–42.

Metodologija: Empirična raziskava je bila izvedena v mednarodni finančni organizaciji, ki deluje v dvanajstih državah in ima več kot 8000 zaposlenih, merjenje kulture varovanja informacij pa je potekalo v dveh valovih, leta 2010 in 2013[19]. Vzorec obsega 2320 enot za leto 2010 in 2159 za leto 2013, stopnja odgovora za leto 2010 je 28 %, leta 2013 pa 38 %. Vprašalnik, ki sta ga avtorja poimenovala IPCA, tokrat obsega 55 trditev na petstopenjski Likertovi lestvici, dodana pa so še vprašanja za preverjanje znanja informacijske varnostne kulture zaposlenih in demografska vprašanja.

Analiza in ugotovitve: Analiza podatkov je pokazala, da je vprašalnik ISCA kot osnova primeren za merjenje kulture varovanja informacij, saj sta avtorja v teoriji utemeljila odnos med kulturo varovanja informacij in informacijsko varnostno kulturo. Faktorska analiza je oblikovala šest dimenzij[20] novega konstrukta, avtorja pa trditve, ki merijo teh šest dimenzij, predlagata kot osnovo za vprašalnik IPCA *(Information Protection Culture Assessment*).

Omejitve raziskave: ISCA vprašalnik ne pokriva merjenja določenih značilnosti informacij, ki bi bile lahko relevantne za merjenje kulture varovanja informacij. Za večjo vsebinsko veljavnost bi torej morale biti dodane nove trditve v skladu z OECD smernicami o zasebnosti, prav tako pa bi se morala preveriti veljavnost konstrukta in izvesti novo oceno zanesljivosti.

5. Alnatheer, Chan in Nelson (2012): Understanding And Measuring Information Security Culture

Namen: Namen raziskave je oblikovati merski inštrument za merjenje informacijske varnostne kulture, saj je analiza literature pokazala na pomanjkanje jasne konceptualizacije in razlikovanja med dejavniki, ki oblikujejo varnostno kulturo ter dejavniki, ki vplivajo nanjo.

[19] Metodologija je enaka kot v raziskavi Da Veiga in Martins (2015a) – glej tretjo točko poglavja 5.3, le da so pri tej raziskavi v analizo vključeni samo podatki iz leta 2010 in 2013.
[20] Šest dimenzij kulture varovanja informacij: predanost informacijski varnosti, zavzetost vodstva, nujnost in pomembnost informacijske varnosti, učinkovitost varnostne politike, odgovornost za informacijsko varnost in dojemanje uporabe informacij.

Metodologija: Empirična raziskava je bila izvedena na zaposlenih v 200 organizacijah iz Savdske Arabije, ki je pokrila vse regije ter tipe in velikosti organizacij. Vprašalnik je bil poslan preko pošte, za boljšo stopnjo odgovora pa so avtorji uporabili tudi spletno anketiranje. Zbiranje podatkov je potekalo od marca do maja 2010, končno število enot v vzorcu je 254 (iz 64 organizacij). Stopnja odgovora je znašala 32 %. Vprašalnik je bil sestavljen s pomočjo ekspertne ocene in kvalitativnih intervjujev, končna verzija pa obsega 19 trditev na petstopenjski Likertovi lestvici strinjanja preko petih sklopov (dimenzij) informacijske varnostne kulture.

Analiza in ugotovitve: Analiza je pokazala, da na informacijsko varnostno kulturo vplivajo trije dejavniki, in sicer podpora vodstva, varnostna politika in usposabljanje, poleg tega pa sta komponenti informacijske varnostne kulture po tem modelu še odgovornost do varnosti in zavedanje informacijske varnosti. Avtorji so ugotovili, da večji poudarek na dejavnikih informacijske varnostne kulture, izboljšuje stopnjo le-te. Poglobljena statistična analiza nakazuje na visoko veljavnost in zanesljivost merskega inštrumenta in postopek operacionalizacije.

Omejitve raziskave: Raziskava nima bistvenih omejitev. Avtorji so predlagali ponovitev raziskave v različnih okoljih z različnimi demografskimi skupinami posebej. Ugotovili so tudi, da je pomemben element, ki konceptualizira informacijsko varnostno kulturo tudi skladnost z informacijsko varnostjo, ki jo je potrebno v prihodnjih raziskavah nujno upoštevati kot sestavni del informacijske varnostne kulture.

6. AlHogail (2015a): Cultivating and assessing an organizational information security culture: an empirical study

Namen: Namen raziskave je ponazoriti uporabo okvirja ISCF za merjenje informacijske varnostne kulture, ki sestoji iz petih dimenzij[21], oceniti stopnjo informacijske varnostne kulture v izbranih organizacijah ter integrirati pomen človeškega dejavnika v informacijski varnosti.

Metodologija: Empirična raziskava je bila izvedena v treh organizacijah iz Savdske Arabije (v vladni organizaciji, ki se ukvarja s financami, v manjšem do srednjem podjetju in v multinacionalki). Podatki za merjenje informacijski varnostne kulture so bili zbrani z vprašalnikom, ki so ga izpolnjevali zaposleni, veljavnost anketnih rezultatov pa je avtor nadalje preverjal s kvalitativnimi intervjuji s strokovnjaki iz izbranih organizacij. Vprašalnik je sestavljen iz sklopa demografskih vprašanj in sklopa merjenja informacijske varnostne kulture preko šestih dimenzij, trditve pa so oblikovane od dvostopenjske do petstopenjske Likertove lestvice, ki merijo stopnjo strinjanja zaposlenih s trditvijo. Velikost vzorca se razlikuje glede na organizacijo[22], stopnja odgovora pa znaša med 13 % in 40 %. Nato je bilo izvedenih še sedem intervjujev (tri v eni in po dva v drugih dveh organizacijah), od tega pet osebnih in dva telefonska intervjuja.

Analiza in ugotovitve: Statistična analiza je pokazala, da je merski inštrument zanesljiv in veljaven, na informacijsko varnostno kulturo pa statistično značilno vplivata dva dejavnika, in sicer IT (pred)znanje in delovno mesto v informacijskem oddelku organizacije. Stopnja informacijske varnostne kulture v treh izbranih podjetjih je nizka oziroma ni zadovoljiva. Avtor prav tako ugotavlja, da obstaja pozitivna povezanost med količino znanja in vedenjem zaposlenih ter količino znanja in stopnjo informacijske varnostne kulture. Raziskava dokazuje, da je nizka stopnja informacijske varnostne kulture posledica neprimernega procesa upravljanja sprememb v organizaciji.

Omejitve raziskave: Raziskovalni okvir ISCF, ki ga je razvil avtor sam, ima pet dimenzij, ki z empirično analizo niso bile preverjene oziroma dokazane (ni izvedene faktorske analize).

7. Safa, Sookhak, Von Solms, Furnell, Ghani in Herawan (2015): Information security conscious care behaviour formation in organizations

[21] Pet dimenzij po raziskovalnem okviru ISCF–AlHogail: strategija, tehnologija, organizacija, ljudje in okolje.
[22] Vzorec po organizacijah znaša: A – 52 enot, B – 20 enot, C – 22 enot.

Namen: Namen raziskave je zmanjšati tveganje za informacijske varnostne grožnje z vidika človeškega dejavnika delovanja v organizaciji. Glavni razlog za to je nizka stopnja primernega vedenja zaposlenih v smislu informacijske varnosti, kot to dokazujejo prejšnje raziskave. Cilj raziskave je spremeniti (izboljšati) vedenje zaposlenih na višjo raven skrbi za zavedno vedenje na področju informacijske varnosti.

Metodologija: Empirična raziskava obsega pristop mešanih metod, in sicer kvalitativno za oblikovanje relevantnih faktorjev s pregledom literature in intervjuji s strokovnjaki (metoda delfi[23]) ter kvantitativno z anketnim vprašalnikom za merjenje dimenzij informacijskega varnostnega zavednega vedenja zaposlenih. Raziskava je bila izvedena v več organizacijah v Maleziji z zaposlenimi v IT oddelkih. Vprašalnik obsega 43 trditev na petstopenjski Likertovi lestvici, ki meri stopnjo strinjanja zaposlenih in je bil pilotno testiran. Vzorec obsega 212 enot.

Analiza in ugotovitve: Analiza je pokazala, da skrb za zavedno informacijsko varnostno vedenje zmanjšuje tveganje za napačno ravnanje s podatki, zavedanje oziroma ozaveščenost pa ima znaten učinek na odnos do informacijske varnosti. Primerna varnostna politika ima pomemben vpliv na norme in prepričanja glede informacijske varnosti v organizaciji. Rezultati kažejo, da izkušnje z informacijsko varnostjo vplivajo na zaznan vedenjski nadzor, ta pa ne vpliva na skrb za zavedno informacijsko vedenje. Na slednjo imata neposreden in pomemben vpliv ocena grožnje informacijske varnosti in samoučinkovitost zaposlenih. Ugotovitve so relevantne, saj merski inštrument dosega visoke ocene veljavnosti in zanesljivosti.

Omejitve raziskave: Vprašalnik so izpolnjevali zaposleni v informacijskih oddelkih, ki imajo praviloma več znanja o informacijski varnosti in konceptih, zato posploševanje ugotovitev na celotno organizacijo ni možno.

8. Rocha Flores in Ekstedt (2016): Shaping intention to resist social engineering through transformational leadership, information security culture and awareness

[23] Delfi metoda je tehnika pridobivanja skupinskega konsenza skupine strokovnjakov na določenem področju. Uvršča se med tehnike ustvarjalnega mišljenja, saj gre za izmenjavanje idej in zamisli v kratkem časovnem obdobju (Linstone in Turoff 1975).

Namen: Raziskava je namenjena identificiranju organizacijskih in individualnih dejavnikov, ki vplivajo na preprečevanje socialnega inženiringa[24] med zaposlenimi v organizaciji. Ena izmed osmih komponent analize je tudi informacijska varnostna kultura.

Metodologija: Empirična raziskava je bila izvedena v več organizacijah na Švedskem. Vprašalnik je bil sestavljen na podlagi izsledkov iz teorije, nato so ga ocenili strokovnjaki, testiran pa je bil s pilotno raziskavo. Končna verzija vprašalnika ima 35 trditev na 11-stopenjski Likertovi lestvici strinjanja. Uporabljeno je bilo orodje za spletno anketiranje Survey Monkey. Zbiranje podatkov je potekalo osem mesecev. Vzorec za analizo obsega 1583 enot, stopnja odgovora znaša 37 %.

Analiza in ugotovitve: Empirična analiza modela je pokazala, da ima odnos zaposlenih najmočnejši neposreden vpliv na prepoznavanje socialnega inženiringa. Informacijska varnostna kultura ima znaten učinek na odnos zaposlenih in normativna prepričanja glede socialnega inženiringa, obenem pa se je izkazalo, da je učinek informacijske varnostne kulture na vedenje zaposlenih šibek. Merski inštrument dosega visoke ocene zanesljivosti in veljavnosti, ki je bila še posebej podrobno analizirana. Glavna ugotovitev raziskave je, da sta odnos zaposlenih in njihova namera delovanja najpomembnejša prediktorja varnega informacijskega vedenja, ki hkrati povečujeta motivacijo zaposlenih, da se naučijo nadzorovati spletne grožnje in nevarnosti tudi v praksi.

Omejitve raziskave: Dejavniki (faktorji) v modelu, ki pojasnjujejo varianco, imajo šibko pojasnjevalno moč, zato bi moral model vsebovati več dejavnikov oziroma teoretskih konstruktov, s katerimi bi povečali vpliv. Prav tako raziskava ne upošteva značilnosti organizacije (velikost in industrija, v kateri deluje), kjer bi lahko prišlo do razlik.

9. Narain Singh in drugi (2014): Identifying factors of organizational information security management

[24] Opredelitev pojma se nahaja na str. 28.

Namen: Avtorja nakazujeta na pomanjkanje literature in razkorak med teoretičnim in praktičnim pristopom na področju informacijske varnosti. Namen raziskave je opredeliti dejavnike upravljanja informacijske varnosti (angl. *information security management*), ki se nanašajo na organizacijske izzive informacijske varnosti, s katerimi se v zadnjem času soočajo strokovnjaki. Cilj raziskave je preverjanje statistične veljavnosti dobljenih rezultatov.

Metodologija: Empirična raziskava je bila izvedena s pristopom mešanih metod, in sicer kvalitativno z analizo ključnih besed in mnenj strokovnjakov in kvantitativno z anketnim vprašalnikom. Z analizo ključnih besed iz raziskovalnih člankov treh najbolj relevantnih znanstvenih revij sta avtorja identificirala deset ključnih dejavnikov upravljanja informacijske varnosti, ki sta jih nato raziskovala kvantitativno. Vprašalnik v prvem sklopu obsega 53 trditev na petstopenjski Likertovi lestvici, ki meri stopnjo strinjanja zaposlenih s posamezno trditvijo, v drugem sklopu pa osnovna demografska vprašanja. Anketo so izpolnjevali zaposleni z različnih področij industrije v Indiji. Vzorec je 152 enot, stopnja odgovora pa znaša 17,6 %.

Analiza in ugotovitve: Analiza je pokazala, da obstaja deset ključnih dejavnikov upravljanja informacijske varnosti, med katere spada tudi informacijska varnostna kultura. Dejavniki pokrivajo vse tri organizacijske aspekte (strateškega, taktičnega in operativnega). Analiza je potrdila veljavnost in zanesljivost vprašalnika.

Omejitve raziskave: Velikost vzorca ne omogoča dovolj velike statistične moči za podajanje zanesljivih ugotovitev. Raziskava se osredotoča le na identificiranje ključnih dejavnikov, ne pokaže pa, kako so ti dejavniki povezani drug z drugim, s čimer bi se lahko vzpostavil celovit okvir upravljanja informacijske varnosti.

10. Parsons, Calic, Pattinson, Butavicius, McCormac in Zwaans (2017): The human aspects of information security questionnaire (HAIS-Q): Two further validation studies

Namen: Namen raziskave je dodatno testirati in povečati veljavnost vprašalnika HAIS-Q (*Human Aspects of Information Security Questionnaire*), ki je bil s prejšnjimi raziskavami prepoznan kot učinkovit inštrument za merjenje informacijskega varnostnega zavedanja.

Metodologija: Empirična raziskava je bila razdeljena na dva dela, prva študija je zajemala eksperiment z načrtno krajo podatkov in kasnejše izpolnjevanje vprašalnika HAIS-Q, drugi del pa panelno anketiranje zaposlenih z enakim vprašalnikom (ob določenih pogojih profila anketiranca). Obe študiji sta bili izvedeni v Avstraliji. Vsebinski del vprašalnika HAIS-Q obsega 63 trditev, ki na petstopenjski Likertovi lestvici strinjanja merijo sedem komponent informacijske varnostne ozaveščenosti. Prva študija ima vzorec 112 enot (univerzitetnih študentov), druga pa 505 enot (zaposlenih ljudi iz Avstralije).

Analiza in ugotovitve:Rezultati prve študije so pokazali, da so se tisti, ki so dosegli boljšo oceno po vprašalniku HAIS-Q, tudi bolje odrezali na eksperimentalnem testu kraje podatkov, kar pomeni, da vprašalnik HAIS-Q lahko napoveduje vedenjske vidike ljudi glede informacijske varnosti. Analiza druge študije pa je pokazala, da znotraj sedmih komponent informacijskega varnostnega zavedanja obstajajo trije vidiki ozaveščanja zaposlenih v organizaciji, in sicer njihovo znanje, stališče (odnos) in vedenje, ki so med seboj močno pozitivno povezani. Merski inštrument dosega visoke ocene veljavnosti in zanesljivosti.

Omejitve raziskave: Izbran vzorec anketiranih v drugi študiji je vključeval določene predpostavke, in sicer starost nad 18 let, uporaba računalnika vsaj 20 % delovnega časa in delo v organizaciji z izoblikovano (formalno ali neformalno) informacijsko varnostno politiko. Prav tako se je izkazalo, da je nekaj ljudi odgovarjalo z družbeno zaželenimi odgovori. Te omejitve pa onemogočajo posploševanje ugotovitev.

11. Ahlan, Lubis in Lubis (2015): Information security awareness at the knowledge-based institution: its antecedents and measures

Namen: Namen raziskave je podrobno razjasniti vlogo informacijskega varnostnega zavedanja in predhodne stopnje merjenja tega koncepta. Osredotoča se na kvantitativno anketno merjenje,

ki daje konsistentne rezultate in prispeva k boljšemu razumevanju uporabnikovega dojemanja omenjenega koncepta.

Metodologija: Empirična raziskava je bila izvedena med študenti in zaposlenimi na dveh univerzah v Indoneziji. Vprašalnik je sestavljen iz 39 vsebinskih trditev na petstopenjski Likertovi lestvici in petih demografskih vprašanj in je bil predhodno testiran. Zbiranje podatkov je potekalo po metodi PAPI[25]. Vzorec za raziskavo obsega 103 enote.

Analiza in ugotovitve: Analiza je pokazala, da obstaja 10 dimenzij koncepta informacijskega varnostnega zavedanja, ki so strukturirane z individualnega, organizacijskega in institucionalnega vidika. Izkazalo se je, da na informacijsko varnostno zavedanje najbolj vplivata program usposabljanja in strokovna uspešnost[26].

Omejitve raziskave: Velikost vzorca za analizo je precej majhna, ugotovitve pa so relevantne za področje univerzitetnega okolja. Merski inštrument ne dosega zadovoljivih ocen z vidika zanesljivosti, zato je tudi njegova veljavnost vprašljiva.

12. Aurigemma in Mattson (2017): Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls

Namen: Namen raziskave je ugotoviti, kako položaj zaposlenih v hierarhični strukturi organizacije vpliva na njihovo obvladovanje informacijske varnostne politike v smislu

[25] PAPI (angl. *Paper-and-Pencil Interviewing*): vrsta osebnega anketiranja, kjer anketar označuje odgovore anketiranca na papirnat vprašalnik.
[26] Strokovna uspešnost (angl. *peer performance*): koncept ocenjevanja zaposlenih s strani nadrejenih po vnaprej pripravljenih kriterijih (v tem primeru gre za ocenjevanje strokovne uspešnosti na področju informacijske varnosti).

varnostnih groženj in nadzora, natančneje gleda napada nepooblaščenega zunanjega uporabnika.

Metodologija: Empirična raziskava je bila izvedena na Ministrstvu za obrambo v Združenih državah Amerike, ki je zelo hierarhično organizirana vladna enota in zato omogoča raziskovanje zastavljenega problema. Vsebinski del vprašalnika obsega 17 trditev na 7-stopenjski Likertovi lestvici strinjanja, ki meri šest vidikov informacijske varnostne politike, dodane pa so tri kontrolne (demografske) spremenljivke. Vprašalnik je bil dvakrat pilotno testiran. Anketiranje je po izbiri udeležencev potekalo na spletu ali v klasični obliki na papirju. Vzorec za analizo je 239 enot, stopnja odgovora pa 23 %.

Analiza in ugotovitve: Analiza je pokazala, da ima status oziroma položaj zaposlenega na zaznano vedenjsko obvladovanje pozitiven učinek na tiste zaposlene, ki poročajo o povprečni in nadpovprečni stopnji nadzora sodelavcev ter hkrati negativen učinek za tiste zaposlene, ki poročajo o podpovprečni stopnji nadzora sodelavcev. Obenem pa višji položaj zaposlenega ne pomeni višje stopnje samoučinkovitosti v smislu vedenjskega (samo)nadzora glede preprečevanja napada nepooblaščenega zunanjega uporabnika. Sicer pa analiza nakazuje, da nadzor sodelavcev lažje izvajajo moški kot ženske ter da imajo zaposleni z boljšim znanjem računalništva višjo stopnjo zavedanja informacijskih varnostnih groženj. Merski inštrument dosega visoke ocene veljavnosti in zanesljivosti, zato ugotovitve lahko smatramo kot relevantne.

Omejitve raziskave: Model je primeren le za organizacije s hierarhično strukturo, čeprav bi se ga dalo implicirati tudi na druge vrste struktur (npr. ravno). Vprašalnik je v veliki meri prilagojen specifično na situacije, povezane z napadom nepooblaščenega zunanjega uporabnika, ampak bi se vsaj določene trditve (oziroma komponente) dalo posplošiti in s tem razširiti njegovo uporabno vrednost.

5.4 EVALVACIJA MERSKIH INŠTRUMENTOV IZBRANIH RAZISKAV

Evalvacija merskih inštrumentov izbranih raziskav je potekala po vnaprej pripravljenih ocenjevalnih kriterijih, pri ocenjevanju merskih inštrumentov pa smo izbrali tiste kriterije, za katere menimo, da so relevantni in potrebni za kakovostno merjenje nekega teoretskega

konstrukta, v našem primeru informacijske varnostne kulture. Sledi tudi podroben opis posameznih kriterijev.

Izbrani ocenjevalni kriteriji so naslednji:

(1) Definicije teoretskih pojmov in komponent
(2) Vzorčenje in stopnja (ne)odgovora
(3) Merjenje komponent teoretskega konstrukta
(4) Opisne statistike
(5) Korelacijska analiza
(6) Faktorska analiza
(7) Veljavnost konstrukta
(8) Pragmatična veljavnost
(9) Zanesljivost
(10) Dostopnost merskega inštrumenta

(1) *Definicije teoretskih pojmov in komponent* so pogoj za veljavno operacionalizacijo oziroma oblikovanje merskih inštrumentov v raziskovalnem procesu. Pri tem je natančnost opredeljevanja teoretskih konstruktov in njihovih komponent ključnega pomena, saj le teoretsko utemeljene definicije omogočajo kvalitetno izvedeno operacionalizacijo (Ferligoj in drugi 1995, 63). Law in drugi (1998) so prav tako prišli do ugotovitev, da teoretski konstrukt, ki nima opredeljenih posameznih dimenzij in njihove medsebojne povezave, ni dobro definiran, zato pogoj za operacionalizacijo ni izpolnjen.

Iz zgornje utemeljitve sledi, da je merski inštrument kot produkt operacionalizacije ustrezen ob temeljitem pregledu raziskovalnega pojava, ki vključuje tudi razjasnitev osnovnih pojmov. Informacijska varnostna kultura (in tudi drugi koncepti za merjenje informacijske varnosti) je teoretski konstrukt, ki ga sestavlja več dimenzij. Teoretični del (ozadje) izbranih raziskav mora za veljavno operacionalizacijo torej vsebovati opredelitev pojma, pri čemer pa mora biti definirana tudi vsaka izmed njegovih dimenzij.
Pri tem kriteriju se osredotočamo na opredelitev informacijske varnostne kulture (ali konstrukte sorodnih konceptov) in njenih komponent v teoretičnem delu (ozadju) izbranih raziskav.

(2) *Vzorčenje in stopnja (ne)odgovora* se nanašata na opis vzorčnega okvira raziskave, kjer se pričakujejo podatki o načinu vzorčenja, metodi anketiranja, številu enot, stopnji (ne)odgovora,

strukturi vzorca (demografske značilnosti npr. spol, starost in status anketiranca) in dodatnih karakteristikah ali metodoloških opombah raziskave v zvezi z raziskovalnim okvirjem. V literaturi se pojavlja več opredelitev za minimalno velikost vzorca v raziskavi s faktorsko analizo, in sicer glede na minimalno absolutno število enot ter glede na koeficient STV[27]. Pri minimalnem številu enot obstaja več pravil (vsaj 100 do vsaj 500 enot), Hair in drugi (2014) pa so kot spodnjo mejo sprejemljivosti vzorca opredelili najmanj 100 enot. Tudi pri koeficientu STV imajo raziskovalci različne poglede na zadovoljivo število enot v vzorcu, in sicer se ta giblje med 2 in 20 (MacCallum in drugi 1999, 90–92). Martins (v Da Veiga 2010, 204) je predlagal, da je sprejemljiv kriterij minimalne velikosti vzorca najmanj 100 enot ali koeficient STV vsaj 5 (kar pomeni, da je velikost vzorca ustrezna, kadar je število enot petkratnik števila indikatorjev v vprašalniku). Sicer pa je za večjo relevantnost analize in ugotovitev zaželena vrednost koeficienta STV vsaj 10 oziroma minimalno število enot v vzorcu vsaj 500 (MacCallum in drugi 1999, 84). Kot zadovoljiva stopnja odgovora pri spletnem anketiranju (s poslanim vabilom preko elektronske pošte) šteje povprečno med 30 % in 40 %, za anketiranje preko elektronske pošte 40 % in navadne pošte 50 %, pri anketiranju preko telefona in pri osebnem anketiranju pa zadovoljiva stopnja odgovora znaša 70 %, dobra pa nad 80 % (Dillman in drugi 2014; Callegaro in drugi 2015).

(3) *Merjenje komponent teoretskega konstrukta* je povezano z definicijami teoretskih pojmov. Tu nas zanima, ali so raziskovalci upoštevali komponente informacijske varnostne kulture (oziroma drugih konceptov informacijske varnosti) iz teorije in jih kot take neposredno merili v anketnem vprašalniku. Gre torej za jasnost postopka oblikovanja indikatorjev po posameznih komponentah, ki vključuje različne tehnike operacionalizacije (npr. oblikovan širši nabor indikatorjev, posvetovanje in testiranje z eksperti, izvedena pilotna raziskava itd.). Ta kriterij je namenjen tudi kontroli relevantnega raziskovanja z upoštevanjem teoretičnih izhodišč.

(4) *Opisne statistike* dajejo osnoven pregled nad podatki analize. S tem se bralcu predstavijo glavne skupne lastnosti podatkov oziroma statistike, ki kažejo variabilnost spremenljivk kot npr. mere srednjih vrednosti (aritmetična sredina, mediana, modus), mere razpršenosti (varianca, standardni odklon, variacijski razmik, kvartilni odklon itd.) ter mere asimetrije in sploščenosti (Ferligoj in drugi 2015).

[27] STV (angl. *subject-to-variable*): koeficient razmerja med številom enot v vzorcu in številom indikatorjev v merskem inštrumentu (vprašalniku).

(5) *Korelacijska analiza* podatkov je možna, kadar so spremenljivke merskega inštrumenta ordinalnega, intervalnega ali razmernostnega tipa. To pomeni, da je anketni vprašalnik sestavljen iz lestvic, ki merijo strinjanje, prepričanja, stališča, zadovoljstvo, pogostost in ostalih merljivih kategorij. V osnovi je korelacijska analiza povezanost med dvema ali več spremenljivkami, običajno interpretirana s koeficienti medsebojne povezanosti glede na tip merske lestvice (Trochim 2001). S tem kriterijem želimo preveriti, ali so bili raziskovalci znotraj merskega inštrumenta pozorni na medsebojno povezanost posameznih komponent informacijske varnostne kulture, kar je tudi osnova za regresijsko analizo in ugotavljanje odvisnosti vplivov posameznih dejavnikov. S tem se prepričamo, da merski inštrument vsebuje vsaj ordinalni tip merskih lestvic, kar pomeni, da omogoča tudi izvedbo faktorske analize.

(6) *Faktorska analiza* je multivariatna statistična metoda za redukcijo podatkov z namenom pojasnjevanja večjega števila indikatorjev z manjšim številom faktorjev, ki predstavljajo skupne razsežnosti spremenljivk. Najpomembnejši statistični podatki za tak postopek so vrednosti korelacijskih koeficientov (Dillon in Goldstein 1984, 53). Glede na tip raziskovanja ločimo eksploratorno in konfirmatorno faktorsko analizo. Namen eksploratorne faktorske analize je odkriti latentno strukturo in ugotoviti povezanost spremenljivk brez predhodne teoretične podlage za obstoj oziroma nastanek posameznih faktorjev. Uporablja se bolj pogosto kot konfirmatorna faktorska analiza, kjer se preverja vnaprej predvidena faktorska struktura na podlagi obstoječe teorije, torej je število faktorjev fiksno določeno, pri tem pa lahko predvidevamo, katere spremenljivke se bodo uvrstile v posamezni faktor (Child 2006, 6–8). Ta način faktorske analize je velik bolj strog kar se tiče izpolnjevanja predpostavk, zahteva pa tudi dobro postavljen in utemeljen teoretski model. Obe vrsti faktorske analize morata izpolnjevati določene predpostavke, še posebej je potrebno upoštevati primernost podatkov za izvedbo faktorske analize (npr. predpostavka o normalni porazdelitvi – Bartlettov test sferičnosti[28], prileganje vzorčnih podatkov – Keiser-Meyer-Olkin test[29] pri eksploratorni faktorski analizi in različni indeksi prileganja pri konfirmatorni faktorski analizi) ter vrednosti faktorskih uteži za skladnost modela s podatki (Williams 2010, 5).

[28] Bartlettov test sferičnosti: test, ki preverja smiselnost uporabe (eksploratorne) faktorske analize, in sicer opazovane latentne spremenljivke med seboj ne smejo biti odvisne.
[29] Keiser-Meyer-Olkin (KMO) test: test, ki se uporablja za ocenjevanje primernosti podatkov za izvedbo (eksploratorne) faktorske analize, temelji pa na predpostavki ustreznega vzorčenja posameznih spremenljivk in celotnega modela.

Pri tem kriteriju analize podatkov se osredotočamo na izračune posameznih vrednosti uteži faktorjev, kjer so zaželene čim višje vrednosti, ter statistike za ocenjevanje skladnosti modela. S tako analizo dobimo vpogled v kompleksnost merskega inštrumenta, ki jo je mogoče pojasniti z enostavnejšim modelom. V kolikor faktorski model daje dobre rezultate, je to eden izmed kazalnikov ustrezno zastavljenega merskega inštrumenta.

(7) *Veljavnost konstrukta* je ena izmed več razsežnosti merjenja veljavnosti po Splichalu (1990, 188) in se nanaša na validacijo, kar pomeni, da s tem ugotavljamo ustreznost raziskovalnega postopka oziroma umeščenost konstrukta v teoretični okvir raziskovalnega problema. Z drugimi besedami gre za preizkušanje učinkovitosti merjenja določene lastnosti spremenljivke, s čimer pridemo do veljavnih izsledkov raziskave (Ferligoj in drugi 1995). Pod veljavnost konstrukta spada konvergentna veljavnost, ki kaže, ali so različni merski postopki nadomestljivi, in je pomembna predvsem za uvajanje novih merskih inštrumentov. V analizi podatkov se konvergentna veljavnost kaže pri faktorskih utežeh, kjer naj bi se koeficient veljavnosti za višjo stopnjo veljavnosti čim bolj približal vrednosti 1. Na splošno je merski inštrument konvergentno veljaven, če so vrednosti faktorskih uteži nad 0,3 (Dillon in Goldstein 1984; Child 2006), nekateri avtorji pa konvergentno veljavnost opredeljujejo s faktorskimi utežmi nad 0,5 (Hair in drugi 2014). Izbira mejne vrednosti faktorskih uteži je samovoljna odločitev raziskovalca, dejstvo pa je, da višje uteži nakazujejo večjo (konvergentno) veljavnost (DiStefano in drugi 2009, 3). Drug vidik veljavnosti konstrukta je diskriminantna veljavnost, ki je opredeljena kot »stopnja, do katere se teoretični pojem razlikuje od drugih teoretičnih pojmov« (Ferligoj in drugi 1995, 89). Diskriminantno veljavnost se preverja preko korelacijskih koeficientov med faktorji, ki morajo biti statistično značilno različni od 1 (oziroma imeti čim nižjo vrednost) (Trochim 2001). Pri analizi konfirmatorne faktorske analize pa je diskriminantna veljavnost dosežena takrat, ko je kvadratni koren povprečne variance (angl. *Average variance extracted* – AVE) večji od medsebojnih korelacij faktorjev ter faktorske uteži večje od vseh njihovih križnih vrednosti (Hair in drugi 2014). Veljavnost konstrukta se pri konfirmatorni faktorski analizi sicer lahko preverja tudi s strukturnim modeliranjem enačb (SEM[30] analizo), kjer visoke (χ^2, GFI, AGFI, CFI) oziroma nizke vrednosti koeficientov

[30] SEM (angl. *Structural Equation Modeling*): modeliranje strukturnih enačb je multivariatna statistična metoda z naprednejšo obdelavo medsebojno koreliranih podatkov (npr. regresijska in faktorska analiza, variančno-kovariančna analiza). Več o metodi v Ramlall (2016).

(RMR/RMSEA itd.)[31] nakazujejo na dobro prileganje teoretskega modela in empiričnih podatkov, kar je osnovni pogoj validacije (Child 2006; Ramlall 2016).

Pri preverjanju veljavnosti konstrukta v izbranih raziskavah smo v analizi iskali omenjene statistike za preverjanje konvergentne in diskriminantne veljavnosti, v kolikor sta bili ti analizirani.

(8) *Pragmatična veljavnost* je ena izmed več razsežnosti merjenja veljavnosti po Splichalu (1990, 188) in se nanaša na vindikacijo, kar pomeni, da s tem preverjamo ustreznost izbire metode. Pri pragmatični veljavnosti se osredotočamo na vsebinsko veljavnost in kriterijsko veljavnost. Vsebinska veljavnost je preprost, vendar subjektivni način preverjanja veljavnosti, raziskovanje po tem kriteriju pa je veljavno, kadar je merski inštrument sestavljen v skladu z dosedanjimi izsledki raziskav oziroma literature (Ferligoj in drugi 1995, 69–70). Ker se ne nanaša na statistično preverjanje oziroma vrednosti, je zelo težko določiti stopnjo veljavnosti in njeno sprejemljivost, običajno gre za (subjektivno) oceno raziskovalca (Kimberlin in Winterstein 2008, 2278). Pod pragmatično veljavnost spada tudi kriterijska veljavnost. Ločimo med napovedno veljavnostjo (angl. *predictive validity*), kjer s kriterijsko spremenljivko ocenjujemo možnosti napovedovanja vrednosti merjene spremenljivke in njenih učinkov v prihodnosti. Oceno veljavnosti napovedovanja predstavlja koeficient napovedne veljavnosti, ki meri korelacijo med merjeno in kriterijsko spremenljivko, pri čemer visoka vrednost koeficienta pomeni višjo stopnjo veljavnosti. Drug vidik pragmatične veljavnosti je sočasna veljavnost (angl. *concurrent validity*), kjer veljavnost proučevane spremenljivke (konstrukta) preverjamo s pomočjo druge (podobne) spremenljivke, ki ni vključena v merski postopek[32]. (Ferligoj in drugi 1995, 74–79). Kriterijsko veljavnost se poleg korelacijske analize lahko preverja tudi z metodo regresijske analize, ki je poleg napovedovanja vpliva uporabna tudi za opis porazdelitve spremenljivk ter oceno distribucij, ki bi jih imele te spremenljivke pod hipotetičnimi pogoji (Stolzenberg 2004,165).

Kot dopolnitev veljavnosti konstrukta smo pri tem kriteriju poskušali zajeti še druge vidike veljavnosti, saj pragmatična veljavnost po našem mnenju dodaja težo večji veljavnosti merskega inštrumenta nasploh. V analizah izbranih raziskav smo bili pozorni na oceno in utemeljitev vsebinske veljavnosti ter testiranje kriterijske veljavnosti.

[31] Razlaga oznak koeficientov in meje sprejemljivih vrednosti se nahajajo v prilogi.
[32] Poleg osnovnega merjenja poteka še vzporedno merjenje s kriterijsko spremenljivko, na podlagi katerega se enako kot pri napovedni veljavnosti izračuna koeficient sočasne veljavnosti.

(9) *Zanesljivost* merskega inštrumenta je ocena, ki nam pove, v kolikšni meri merski inštrument (v tem primeru anketni vprašalnik oziroma trditve in lestvice v vprašalniku) ob ponovnih merjenjih daje vedno enake rezultate. Zanesljivost lahko merimo na več načinov, in sicer (Ferligoj in drugi 1995, 31–47):

- z vidika mer enakovrednosti[33]: z notranjo metodo konsistentnosti (angl. *internal consistency*) in z metodo razpolovitve (angl. *split-half*),
- z vidika mer stabilnosti rezultatov[34]: s ponovnim testom (angl. *test-retest*) in z metodo alternativne oblike (angl. *alternative form*).

Pri notranji metodi konsistentnosti gre za ugotavljanje zanesljivosti medsebojne konsistentnosti komponent določenega teoretskega konstrukta. Najbolj pogosto uporabljena mera za določanje zanesljivosti notranje konsistentnosti je koeficient Cronbach alfa, ki se giblje na intervalu med 0 in 1. Vrednosti med 0,7 in 0,8 nakazujejo na zadovoljivo oceno zanesljivosti, medtem ko vrednosti med 0,8 in 0,9 pomenijo že zelo dobro oceno zanesljivosti (Nunnally in Bernstein 1994; Bland in Altman 1997; Miller 2009; Hair in drugi 2014). Nekateri avtorji kot zadovoljivo oceno sprejemajo tudi vrednosti koeficienta nad 0,6 (Brewerton in Millward 2001; Trochim 2001). Alternativni koeficient merjenja zanesljivosti pa je koeficient CR (angl. *composite reliability*), ki se uporablja predvsem pri SEM analizi, pri čemer vrednosti nad 0,6 nakazujejo na ustrezno oceno zanesljivosti (Allen in Yen 2002).

Ocenjevanje zanesljivosti z metodo razpolovitve je primerno, kadar teoretično spremenljivko (konstrukt) merimo z več enakovrednimi indikatorji. Pri tem merjene indikatorje razdelimo v dve skupini in vsako izmed njih obravnavamo kot sestavljeno spremenljivko (kot seštevek vrednosti vseh indikatorjev v eni skupini), korelacija med obema skupinama indikatorjev pa daje oceno zanesljivosti. Mera za določanje zanesljivosti z metodo razpolovitve je Spearman-Brownov obrazec, njegova opredelitev ocene zanesljivosti pa je zaradi standardiziranih vrednosti koeficientov enaka kot pri koeficientu Cronbachove alfe – glej zgoraj (Ferligoj in drugi 1995; Eisinga in drugi 2013).

[33] Mere enakovrednosti se ne nanašajo na ponovljivost, temveč na merjenje »v istem času« (angl. *cross-sectional measuring*). Ocene zanesljivosti temeljijo na izračunanih koeficientih korelacij med merjenimi spremenljivkami, zato obstaja predpostavka, da so izbrane spremenljivke enakovredne (Ferligoj in drugi 1995, 39).
[34] Mere stabilnosti se nanašajo na ponovne (enake) postopke merjenja na istih enotah v določenem časovnem razmiku (Ferligoj in drugi 1995, 31). Uporabne so predvsem za ocene zanesljivosti pri longitudinalnih študijah.

Ponovni test (metoda retesta) zahteva ponovitev merjenja na istih enotah v določenem časovnem razmiku ob nespremenjenih pogojih (npr. v tem času anketiranec ni prejel dodatnih informacij o analizirani tematiki). Oceno zanesljivosti dajejo koeficienti korelacije med spremenljivkami, ki so merjene v različnih časovnih intervalih. Višje vrednosti koeficientov odražajo tudi boljšo zanesljivost, podobno kot pri ostalih koeficientih merjenja zanesljivosti (Ferligoj in drugi 1995; Allen in Yen 2002; Kimberlin in Winterstein 2008). Med manj uporabljenimi pa je metoda alternativne oblike, kjer je prav tako potrebno ponovno merjenje istega konstrukta, vendar v drugačni obliki (alternativna vprašanja, druga merska lestvica), pri tem pa moramo zagotoviti, da bo drug merski inštrument še vedno meril isto dejansko spremenljivko (problem veljavnosti). Oceno zanesljivosti daje koeficient korelacije med obema meritvama (Ferligoj in drugi 1995; Hair in drugi 2014).

Pri tem kriteriju se osredotočamo na enega (katerega koli) od zgoraj omenjenih načinov merjenja zanesljivosti, pomembno pa je, da iz analize dobimo povratno informacijo o oceni zanesljivosti merskega inštrumenta. V kolikor je ocena zadovoljiva, smo lahko prepričani, da je merski inštrument kvalitetno zastavljen in uporaben za nadaljnje raziskovanje.

(10) *Dostopnost merskega inštrumenta* se nanaša na obliko in posredovanje anketnega vprašalnika, ki je bil uporabljen v analizi. Pri tem je sprejemljivih več možnosti, in sicer objavljena celotna verzija merskega vprašalnika v prilogi raziskave (oziroma znanstvenega članka) ali prost dostop do vprašalnika na svetovnem spletu. Bolj strokovno ustrezna je prva možnost, slednja je praviloma izjema. Ena izmed možnosti je tudi, da se avtor ali avtorji novega merskega inštrumenta odločijo za omejen dostop, pri čemer morajo raziskovalci prositi za dovoljenje oziroma plačati za uporabo merskega inštrumenta. V tej točki nas torej zanima, ali je anketni vprašalnik dostopen širšemu krogu raziskovalcev z namenom ponovne uporabe, saj k širjenju znanosti najbolj prispeva prav princip odprtega dostopa podatkov.

Naslednja tabela prikazuje podatke in statistike glede kvalitete merskih inštrumentov izbranih raziskav. V analizi merskih inštrumentov se osredotočamo predvsem na tiste ocenjevalne kriterije, ki v največji meri prispevajo k zagotavljanju veljavnega in zanesljivega merjenja. Prvih šest merskih inštrumentov se nanaša na merjenje informacijske kulture, ostali pa merijo podoben koncept ali pa se v njih pojavljajo komponente informacijske varnostne kulture.

Tabela 5.2: Analiza kvalitete merskih inštrumentov izbranih raziskav

Raziskava / merski inštrument	Ocenjevalni kriteriji									
	Definicije pojma in komponent	**Vzorčenje**	**Merjenje komponent**	**Opisne statistike**	**Korelacijska analiza**	**Faktorska analiza**	**Veljavnost konstrukta**	**Pragmatična veljavnost**	**Zanesljivost**	**Dostopnost**
Da Veiga, Martins in Eloff (2007)	Ni definicije ISC, naštete komponente ISC, vendar brez opredelitve	Način: spletno anketiranje Vzorec: 4735 enot Stopnja odgovora: 37,7 % Struktura: kraj bivanja, vrsta zaposlenih, delovne izkušnje	8 komponent; proces oblikovanja vprašalnika, testiranje, pilotna raziskava	n.p.	n.p.	Eksploratorna FA Ni faktorskih uteži (vrednosti nad 0,3)	Konvergentna veljavnost: faktorske uteži nad 0,3	n.p.	Cronbachov alfa: 0,677–0,956	n.p.
Da Veiga in Eloff (2010) / ISCA vprašalnik	Definicija ISC in 7 komponent ISC (nekatere definirane)	Način: spletno anketiranje Vzorec: 1085 enot Stopnja odgovora: 36,2 % Struktura: kraj bivanja, vrsta zaposlenih, delovne izkušnje	7 komponent; 85 indikatorjev; ekspertna ocena vprašalnika	n.p.	n.p.	Konfirmatorna FA GFI: 0,9982 AGFI: 0,9981 RMR: 0,0798 Ni faktorskih uteži	Konvergentna veljavnost: GFI: 0,9982 RMR: 0,0798	Vsebinska veljavnost: razvit model ISCF	Cronbachov alfa: 0,740–0,946	n.p. (najden na internetu)
Da Veiga in Martins (2015a) / ISCA vprašalnik	Definicije ISC in 8 (oziroma 9) komponent ISC	Način: spletno anketiranje Vzorec: 1571-2320 enot Stopnja odgovora: 28-38,8 % Struktura: kraj bivanja, vrsta zaposlenih	8/9 komponent; 44 indikatorjev; prilagajanje indikatorjev v vprašalniku	n.p.	Analiza variance; Pearsonovi koeficienti korelacije: 0,346–0,754 ($p<0,01$)	n.p.	n.p.	n.p.	n.p.	n.p.
Da Veiga in Martins (2015b) / IPCA vprašalnik	Definicije ISC, ISPr in 10 komponent	Način: spletno anketiranje Vzorec: 2159-2320 enot Stopnja odgovora: 28-38,8 %	10 komponent	Povprečje in %Da za vsako dimenzijo	n.p.	Eksploratorna FA (metoda PCA, rotacija varimax) (vrednosti nad 0,3); KMO in Bartlettov test: ustrezni rezultati (ni vrednosti)	Konvergentna veljavnost: faktorske uteži nad 0,3	n.p.	Cronbachov alfa: 0,764–0,887	n.p.
Alnatheer, Chan in Nelson (2012)	Definicija ISC in 5 komponent	Način: spletno anketiranje, anketiranje po pošti Vzorec: 254 enot Stopnja odgovora: 32 % Struktura: tip in velikost organizacije, vrsta industrije	5 komponent; 19 indikatorjev; ekspertna ocena in intervjuji za prilagajanje indikatorjev v vprašalniku, pilotna raziskava	Povprečje, standardni odklon, standardna napaka	Korelacije faktorjev: 0,320–0,467	Eksploratorna FA Faktorske uteži: 0,549–0,818 KMO test: 0,932 Bartlettov test: $p<0,001$ Varianca: 68 % Konfirmatorna FA Faktorske uteži: 0,621–0,886	Konvergentna veljavnost: faktorske uteži nad 0,5; Diskriminantna veljavnost: AVE: 0,654–0,784	n.p.	Cronbachov alfa: 0,820-0,906 CR: 0,883–0,936	Vprašalnik z indikatorji v analizi

AlHogail (2015a) / ISCF vprašalnik	Definicije ISC in 6 komponent	Način: spletno anketiranje Vzorec: 22-52 enot Stopnja odgovora: 13-40 % Struktura: spol, starost, izobrazba, delovne izkušnje, vrsta zaposlenih, znanje IT	6 komponent	Povprečje, standardni odklon, standardna napaka, interval zaupanja	Spearmanovi koeficienti korelacije: 0,551–0,957; Kruskal-Wallis test: 0,0297–0,947	n.p.	Konvergentna veljavnost: GFI: 0,902–0,969	n.p.	Cronbachov alfa: 0,619–0,928	n.p.
Safa in drugi (2015) / ISCCB vprašalnik	Definicije ISCCB in ostalih 9 konstruktov	Način: spletno anketiranje, PAPI Vzorec: 212 enot Stopnja odgovora: n.p. Struktura: spol, starost (razredi), izobrazba, vrsta industrije, delovne izkušnje	9 komponent; 43 indikatorjev; metoda delfi za oblikovanje trditev in pilotna raziskava	n.p.	Korelacije faktorjev: 0,186–0,612	Konfirmatorna FA Faktorske uteži: 0,527–0,923 $x^2 = 1006,89$ ^{2}/df: 1,89 GFI: 0,963 AGFI: 0,936 CFI: 0,921 IFI: 0,914 NFI: 0,938 RMSEA: 0,072	Konvergentna veljavnost: faktorske uteži nad 0,5; Diskriminantna veljavnost: korelacije med konstrukti (faktorji) pod 0,9	n.p.	Cronbachov alfa: 0,720–0,862	Vprašalnik z indikatorji v analizi
Rocha Flores in Ekstedt (2016)	Ni definicije konstrukta, ampak samo komponent	Način: spletno anketiranje Vzorec: 1583 enot Stopnja odgovora: 37 % Struktura: spol, starost (razredi), računalniške izkušnje, vrsta industrije, velikost podjetja	8 komponent; ekspertna ocena oblikovanja indikatorjev, pilotna raziskava vprašalnika	n.p.	Korelacije faktorjev: 0,218–0,637	Konfirmatorna FA Faktorske uteži: 0,688–0,940 Varianca: 42,0 %	Konvergentna veljavnost: faktorske uteži nad 0,7; Diskriminantna veljavnost: AVE: 0,594–0,873	Vsebinska veljavnost: metoda razvrščanja indikatorjev	Cronbachov alfa: 0,830–0,952 CR: 0,911–0,965	Vprašalnik z indikatorji v prilogi članka
Narain Singh in drugi (2014)	Definicije ISM in 10 komponent	Način: spletno anketiranje Vzorec: 152 enot Stopnja odgovora: 17,6 % Struktura: delovno mesto, delovne izkušnje, vrsta industrije	10 komponent; analiza ključnih besed, ekspertna ocena, pilotna raziskava vprašalnika	n.p.	n.p.	Eksploratorna FA (metoda PCA, rotacija varimax); Faktorske uteži: 0,504–0,816 KMO test: 0,91 Bartlettov test: p<0,001 Varianca: 68,8 %	Konvergentna veljavnost: faktorske uteži nad 0,5	n.p.	Cronbachov alfa: 0,740–0,915	Vprašalnik z indikatorji v analizi
Parsons in drugi (2017) / HAIS-Q vprašalnik	Definicije ISA in 7 komponent (nekatere definirane)	Način: panelno spletno anketiranje Vzorec: 505 enot	7 komponent; ekspertna ocena za oblikovanje indikatorjev	Povprečje, standardni odklon, minimum in maksimum za vsako dimenzijo	Pearsonovi koeficienti korelacije: 0,30–0,40	Eksploratorna FA Faktorske uteži: 0,500-0,780 KMO test: 0,96 Bartlettov test: p<0,001 Varianca: 54 %	Konvergentna veljavnost: faktorske uteži nad 0,5	Vsebinska veljavnost: poglobljeni intervjuji	Cronbachov alfa: 0,750–0,820	Vprašalnik z indikatorji v analizi
Ahlan in drugi (2015)	Definicija ISA, 11 komponent	Način: PAPI Vzorec: 103 enote	11 komponent; ekspertna ocena trditev v	n.p.	Korelacije faktorjev: 0,004–0,475	Eksploratorna FA Faktorske uteži: -0,052–0,880	Konvergentna veljavnost: nekatere	n.p.	Cronbachov alfa: 0,056–0,681	Vprašalnik z indikatorji v

	(preučevano s treh vidikov)		vprašalniku v smislu jasnosti in enostavnosti				faktorske uteži pod 0,2; Diskriminantna veljavnost: AVE: 0,257–0,595		CR: 0,430–0,815	prilogi članka
Aurigemma in Mattson (2017)	Definicija ISP, 6 komponent (nekatere definirane)	Način: spletno anketiranje, PAPI Vzorec: 239 Stopnja odgovora: 23 % Struktura: spol, računalniško znanje, delovna funkcija zaposlenega	6 komponent ISP v analizi	Povprečje, standardni odklon	Korelacije faktorjev: 0,088–0,737	Konfirmatorna FA Faktorske uteži 0,753–0,991 CFI: 0,928–0,963 SRMR: 0,049–0,059	Konvergentna veljavnost: faktorske uteži nad 0,7 Diskriminantna veljavnost: AVE: 0,679–0,899	n.p.	CR: 0,850–0,964	Vprašalnik z indikatorji v analizi

Legenda: n.p. – ni podatka

ISA – zavedanje informacijske varnosti
ISC – informacijska varnostna kultura
ISCCB – skrb za zavedno informacijsko vedenje
ISM – upravljanje informacijske varnosti
ISP – informacijska varnostna politika
ISPr – kultura varovanja informacij

Merski inštrument v raziskavi Da Veiga, Martins in Eloff (2007) je eden izmed prvih oblikovanih anketnih vprašalnikov za merjenje informacijske varnostne kulture. Ima nekoliko slabše teoretsko ozadje, saj ne vsebuje definicij informacijske varnostne kulture in komponent. Temu sledi dejstvo, da je postopek operacionalizacije z vidika veljavnosti morda vprašljiv. Oblikovanje vprašalnika je sicer potekalo v projektni (raziskovalni) skupini kot prilagoditev že obstoječega vprašalnika, ki ga je razvil eden izmed avtorjev. Vprašalnik je bil nato testiran na majhni skupini zaposlenih v izbrani organizaciji z namenom spremljanja obraznih reakcij ob izpolnjevanju vprašalnika. Po analizi so ga nekoliko prilagodili in poenostavili. Končna verzija vprašalnika je bila preko spletnega orodja Survey Tracker posredovana vsem zaposlenim v organizaciji, 38% stopnja odgovora pa pomeni 4735 enot v vzorcu. Na zbranih podatkih je bila izvedena dvostopenjska eksploratorna faktorska analiza, prikazani rezultati pa so pomanjkljivi. Avtorji niso podali vrednosti faktorskih uteži, njihovih medsebojnih korelacij in drugih karakteristik za prileganje modela, ampak so ustreznost analize zgolj z besedami omenili v interpretaciji, zato je veljavnost konstrukta vprašljiva. Omeniti velja tudi nizke (mejne) vrednosti koeficientov Cronbachove alfe za oceno zanesljivosti pri dveh dimenzijah (približno 0,68).

Nadgradnja omenjenega merskega inštrumenta je vprašalnik ISCA, ki sta ga oblikovala Da Veiga in Eloff (2010). Vprašalnik temelji na njunem ISCF modelu informacijske varnostne kulture s sedmimi komponentami, kjer so podane natančne definicije pojma in nekaterih komponent (vendar ne vseh). Kljub temu, da je bila različica prejšnjega vprašalnika že pilotno testirana, so avtorji izvedli ekspertno oceno z namenom prilagoditve vprašalnika za boljše razumevanje indikatorjev. Končna verzija vprašalnika je bila prav tako posredovana preko spletnega orodja Survey Tracker, stopnja odgovora je znašala približno 36%, velikost vzorca pa 1085 enot. Konfirmatorna faktorska analiza kaže na zelo dobro skladnost modela s podatki (indeksi prileganja: GFI=0,998; AGFI=0,998; RMR=0,08), zato lahko sklepamo na visoko stopnjo konvergentne veljavnosti, čeprav vrednosti faktorskih uteži niso eksplicitno zapisane. Na podlagi teoretsko utemeljenega ISCF modela, ki izhaja iz zgoraj omenjene raziskave in merskega inštrumenta, so avtorji utemeljili tudi vsebinsko veljavnost. Vrednosti koeficientov Cronbachove alfe se gibljejo med 0,740 in 0,946, kar kaže na visoko oceno zanesljivosti. Vprašalnik ISCA v raziskavi ni bil v celoti predstavljen, vendar je dotična verzija vprašalnika objavljena na internetu.

V raziskavi Da Veiga in Martins (2015a) je bil prav tako uporabljen vprašalnik ISCA, ki sta ga avtorja dopolnila še z dvema komponentama informacijske varnostne kulture. Podala sta tudi

ustrezno definicijo pojma in pojasnila pomen vseh devetih komponent. Vprašalnik je nekoliko prilagojen in vsebuje občutno manj indikatorjev (prej 85, sedaj 44), saj se je po ekspertni oceni izkazalo, da je prvotni vprašalnik precej kompleksen. Novejša verzija vprašalnika ISCA je primerna za merjenje informacijske varnostne kulture v vseh organizacijah ne glede na področje delovanja. Zbiranje podatkov je potekalo podobno kot v prejšnji raziskavi, saj gre za isto raziskovalno skupino avtorjev. V analizi so predstavljene opisne statistike ter rezultati analize variance in povezanosti faktorjev. Pearsonov koeficient korelacije med faktorji znaša med 0,346 in 0,754 pri manj kot 1% stopnji statistične značilnosti. Vrednosti koeficientov so ustrezne (niso večje od 0,8), zato lahko rečemo, da je model stabilen. V primeru visokih korelacij med faktorji se nakazuje problem multikolinearnosti, saj imajo visoko korelirani faktorji podoben vpliv na teoretski konstrukt in jih je zato bolje izločiti iz modela. Ker ni bilo izvedene faktorske analize, ne moremo sklepati o veljavnosti in zanesljivosti te različice merskega inštrumenta ISCA.

Istega leta sta omenjena avtorja ponovno izvedla analizo merjenja informacijske varnostne kulture z merskim inštrumentom ISCA (Da Veiga in Martins 2015b). Sicer sta vprašalnik prilagodila za merjenje koncepta kulture varovanja informacij s poudarkom na načelih zasebnosti in delom z osebnimi podatki (od tu spremenjeno ime – vprašalnik IPCA), vendar se vsebinsko bistveno ni spremenil. Temelji na osnovni definiciji informacijske varnostne kulture, iz katere izhaja definicija kulture varovanja informacij. Prejšnji verziji sta dodala še eno komponento (skupaj 10), ki za merjenje informacijske varnostne kulture ne bi bila relevantna, kljub temu pa bi bil merski inštrument za merjenje le-te primeren (brez sklopa trditev za deseto komponento). Rezultati eksploratorne faktorske analize so potrdili skladnost modela (sklicujoč na ustrezne vrednosti KMO testa in Bartlettovega testa sferičnosti, vendar le-te niso zapisane). Prav tako ponovno ni navedenih vrednosti faktorskih uteži, zato težko ocenjujemo konvergentno veljavnost. Vrednosti koeficienta Cronbachove alfe se gibljejo med 0,764 in 0,887, kar kaže na zanesljivost merskega inštrumenta.

Alnatheer in drugi (2012) so v svoji raziskavi predstavili merski inštrument informacijske varnostne kulture, ki je utemeljen z raziskovalnim modelom. Merski inštrument vsebuje definicije varnostne kulture in petih pripadajočih komponent. Avtorji so podrobno predstavili njegovo operacionalizacijo. Z metodo prilagajanja indikatorjev in poglobljenimi intervjuji so oblikovali prvo verzijo vprašalnika, ki so ga nato po ekspertni oceni še prilagodili. Končno verzijo, ki ima 19 trditev na petstopenjski Likertovi lestvici strinjanja, so testirali s pilotno raziskavo. Zbiranje podatkov je potekalo preko poslanih vprašalnikov po pošti v kombinaciji s

spletnim anketiranjem. Študija je bila zastavljena precej obsežno, saj so vanjo sistematično vključili 200 organizacij, tako da so pokrili vse regije ter velikost in vrsto organizacije glede na industrijo. Vzorec znaša 254 zaposlenih iz 63 različnih organizacij. Stopnja odgovora je bila 32%. Korelacije faktorjev znašajo med 0,320 in 0,467, kar kaže na stabilnost modela. Izvedeni sta bili tako eksploratorna kot konfirmatorna analiza podatkov. Vrednost KMO testa znaša 0,932, statistična značilnost Bartlettovega testa sferičnosti pa manj kot 0,001 (0,1 %), zato lahko sklepamo na zelo dobro skladnost modela s podatki. To kaže tudi visoka variabilnost vseh pet faktorjev skupaj, ki znaša približno 68%. Vrednosti faktorskih uteži pri eksploratorni analizi znašajo med 0,549 in 0,818, s čimer lahko potrdimo visoko stopnjo konvergentne veljavnosti. Z namenom podkrepitve rezultatov eksploratorne analize so avtorji uporabili tudi konfirmatorno faktorsko analizo za nadaljnje izboljšanje veljavnosti modela. Konfirmatorna faktorska analiza je bila izvedena ločeno za dejavnike, ki po modelu vplivajo na varnostno kulturo ter za preostali dve komponenti, ki jo po njihovem mnenju oblikujeta. Vrednosti faktorskih uteži znašajo od 0,621 do 0,886, kar ponovno potrjuje konvergentno veljavnost. Tudi indeksi prileganja obeh modelov kažejo na dobro prileganje s podatki[35]. Diskriminantno veljavnost so utemeljili z analizo vrednosti AVE, ki znašajo od 0,654 do 0,784. Poleg veljavnosti konstrukta so avtorji analizirali tudi nomološko veljavnost, ki je v tem delu ne obravnavamo. Vrednosti Cronbachove alfe po posameznih faktorjih znašajo med 0,820 in 0,906, kar kaže na zelo dobro notranjo konsistentnost merskega inštrumenta, njegovo visoko stopnjo zanesljivosti pa opredeljuje tudi CR koeficient (vrednosti med 0,883 in 0,936). Vprašalnik je objavljen skupaj z analizo raziskave.

AlHogail (2015a; 2015b) je na podlagi svojega modela informacijske varnostne kulture oblikoval vprašalnik ISCF. Merski inštrument vsebuje definicije informacijske varnostne kulture in šestih komponent, postopek operacionalizacije merskega vprašalnika pa v raziskavi ni opisan. Zbiranje podatkov je potekalo preko spletnega anketiranja v treh različnih organizacijah, velikost vzorcev pa znaša 52, 20 in 22 enot (stopnja odgovora 13–40%). V analizi so predstavljene opisne statistike (povprečje, standardni odklon, standardna napaka, interval zaupanja) ter vrednosti Spearmanovega koeficienta korelacije, ki nakazujejo pozitivno povezanost med komponentami (vrednosti od 0,551 do 0,957). Statistično značilnost

[35] Model dejavnikov: χ^2=94,5, χ^2/df=2,305; GFI=0,939; AGFI=0,901, NFI=0,913, CFI=0,964; IFI=0,964; RMSEA=0,072;
Model komponent: χ^2=31,16, χ^2/df=2,397; GFI=0,966; AGFI=0,926, NFI=0,973, CFI=0,984; IFI=0,984; RMSEA=0,074.

demografskih spremenljivk je avtor preverjal s pomočjo Kruskall-Wallisovega testa[36]. Izkazalo se je, da pri manj kot 5% stopnji statistične značilnosti na informacijsko varnostno kulturo v vseh treh organizacijah vpliva vrsta zaposlenih (delo v IT oddelkih), v dveh organizacijah pa še IT znanje[37] zaposlenih ter raven zaposlitve. Glede na predstavitev rezultatov o veljavnosti in zanesljivosti merskega inštrumenta sklepamo, da je bila na podatkih izvedena konfirmatorna faktorska analiza, čeprav eksplicitno to ni zapisano. Veljavnost merskega inštrumenta avtor utemeljuje z metodo SEM. Indeks prileganja GFI pri vseh treh študijah primera znaša nad 0,9, zato lahko zaključimo, da je model skladen s podatki. Ker nimamo podatka glede vrednosti faktorskih uteži (ali vrednosti AVE), težko sklepamo o konvergentni veljavnosti. Koeficienti Cronbachove alfe znašajo med 0,619 in 0,928. Zanesljivost tehnološke komponente je v vseh treh organizacijah nizka (0,62–0,72), zato je notranja konsistentnost merskega inštrumenta vprašljiva.

Skrb za zavedno informacijsko varnostno vedenje je teoretsko zelo podoben koncept informacijski varnostni kulturi, saj glavni konstrukt sestavljajo pomembnejše komponente informacijske varnostne kulture (glej str. 25–26). Merski inštrument ISCCB so oblikovali Safa in drugi (2015) na podlagi lastnega teoretskega modela. Vsebuje definicijo pojma in devetih pripadajočih komponent, kar je osnova za veljavno operacionalizacijo. Pri oblikovanju vprašalnika so uporabili metodo delfi (usklajevanje indikatorjev s konsenzom skupine strokovnjakov), nato pa je bil vprašalnik testiran s pilotno raziskavo. Zbiranje podatkov je potekalo s spletnim anketiranjem in metodo PAPI, velikost vzorca znaša 212 enot, o stopnji odgovora pa nimamo podatka. Korelacije faktorjev znašajo med 0,186 in 0,612, kar pomeni, da je model stabilen. Izvedena je bila konfirmatorna faktorska analiza z natančno analizo skladnosti in veljavnost modela (metoda SEM). Faktorske uteži znašajo od 0,527 do 0,923, kar kaže na zadovoljivo stopnjo konvergentne veljavnosti. Vsi navedeni indeksi prileganja kažejo na visoko skladnost modela s podatki, in sicer χ^2=1006,89, χ^2/df=1,89 (kar je manj od kritične vrednosti 3), GFI=0,96, AGFI=0,936, CFI=0,921, IFI=0,914, NFI=0,938 (vsi nad kritično vrednostjo 0,9 oziroma AGFI nad 0,8), RMSEA=0,072 (pod kritično vrednostjo 0,1). Diskriminantno veljavnost so avtorji utemeljili z vrednostmi vseh parov korelacij med faktorji pod 0,9, po teoriji naj bi bile te vrednosti čim bolj različne od 1. V tem primeru je pogoju zadoščeno, saj najvišja vrednost korelacije med dvema faktorjema znaša 0,612. Merski

[36] Kruskall-Wallis test je neparametrična testna statistika za primerjavo dveh (ali več) neodvisnih vzorcev – kadar porazdelitev na vzorcu ni normalna.
[37] Pod IT znanje štejemo razvojne storitve, kot so razvoj programske opreme, spletnih aplikacij in portalov, naprednejše delo z bazami podatkov in komunikacijskimi orodji.

inštrument ocenjujemo kot zanesljiv, saj vrednosti koeficienta Cronbachove alfe znašajo med 0,720 in 0,862. Celoten vprašalnik ISCCB s posameznimi indikatorji se nahaja v omenjeni raziskavi.

Rocha Flores in Ekstedt (2016) sta preučevala model zaznavanja socialnega inženiringa v organizaciji. V model sta vključila tudi informacijsko varnostno kulturo in nekatere njene komponente (zavedanje informacijske varnosti, stališča, norme in prepričanja, varnostno politiko). Merski inštrument nima konkretne opredelitve konstrukta, vsebuje pa definicije vseh ostalih vključenih konstruktov. Avtorja sta izvedla ekspertno oceno oblikovanja indikatorjev, s čimer sta optimizirala vprašalnik in ga nato pilotno testirala. Zbiranje podatkov za analizo je potekalo preko spleta, vzorec znaša 1583 enot, stopnja odgovora pa 37%. V raziskavi je bila izvedena konfirmatorna faktorska analiza, s katero so raziskovalci dosegli visoko stopnjo konvergentne veljavnosti (vrednosti faktorskih uteži med 0,688 in 0,940). Če se osredotočimo samo na omenjene komponente informacijske varnostne kulture, opazimo, da so vrednosti faktorskih uteži teh komponent zelo visoke (0,828–0,940). Večjo težo veljavnosti konstrukta poleg konvergentne veljavnosti daje še utemeljitev diskriminantne veljavnosti z vrednostmi koeficienta AVE med 0,594 in 0,873. Vsebinsko veljavnost so avtorji dokazali z metodo razvrščanja indikatorjev. Korelacije med faktorji znašajo med 0,218 in 0,637, kar nakazuje na stabilnost modela, faktorji pa skupaj pojasnijo 42% variabilnosti. Vrednosti koeficienta Cronbachove alfe znašajo med 0,830 in 0,952, vrednosti koeficienta CR pa med 0,911 in 0,965, kar pomeni, da ima merski inštrument poleg visoke veljavnosti tudi visoko stopnjo zanesljivosti. Indikatorji po posameznih konstruktih se nahajajo v prilogi omenjene raziskave.

Narain Singh in drugi (2014) so se osredotočili na merjenje koncepta upravljanje informacijske varnosti, po njihovem modelu pa ta vsebuje tudi nekatere komponente informacijske varnostne kulture (informacijska varnostna politika, usposabljanje in zavedanje informacijske varnosti, skladnost), zato ga je smiselno analizirati. Merski inštrument vsebuje definicijo glavnega konstrukta ter vseh desetih pripadajočih komponent. Sestavljen je bil z metodo ključnih besed za iskanje ustreznih komponent in ekspertno oceno, na koncu pa testiran s pilotno raziskavo. Končna verzija vprašalnika vsebuje 53 indikatorjev. Zbiranje podatkov je potekalo preko spletnega anketiranja, velikost vzorca znaša 152 enot, stopnja odgovora pa 17,6%. Na podatkih je bila izvedena eksploratorna faktorska analiza s podrobno analizo pripadajočih statistik. Vrednost KMO testa znaša 0,91, statistična značilnost Bartlettovega testa sferičnosti pa manj kot 0,001 (0,1 %), kar pomeni, da se podatki zelo dobro prilegajo modelu. Metoda glavnih osi (rotacija varimax) je podala visoke vrednosti faktorskih uteži, ki se gibljejo med 0,504 in 0,816,

vseh 10 faktorjev pa skupaj pojasnjuje skoraj 70% variabilnosti. To pomeni, da so faktorji zajeli precejšen del vpliva na glavni konstrukt. Visoke vrednosti faktorskih uteži nakazujejo na konvergentno veljavnost modela, zadovoljive vrednosti koeficienta Cronbachove alfe (0,740–0,915) pa opredeljujejo tudi dobro zanesljivost merskega inštrumenta. Indikatorji po posameznih komponentah se nahajajo v analizi omenjene raziskave.

Naslednji merski inštrument v naši analizi je HAIS-Q, ki meri stopnjo zavedanja informacijske varnosti (Parsons in drugi 2017). Ker gre za eno izmed glavnih komponent informacijske varnostne kulture, vprašalnik HAIS-Q predstavlja pomemben del pri merjenju le-te. Merski inštrument vsebuje definicijo glavnega pojma in nekaterih pripadajočih komponent. Sestavljen je bil s pomočjo ekspertne ocene, s čimer so avtorji dosegli ustrezno oblikovanje indikatorjev. Zbiranje podatkov je potekalo preko spletnega anketiranja (panelna raziskava), vzorec pa je znašal 505 enot. V analizi so predstavljene opisne statistike (povprečje, standardni odklon, minimum in maksimum) za vsako izmed sedmih komponent. Vrednosti Pearsonovega koeficienta korelacije znašajo med 0,30 in 0,40 (pozitivna linearna povezanost). Nadalje je bila izvedena eksploratorna faktorska analiza. Vrednost KMO testa znaša 0,96, statistična značilnost Bartlettovega testa sferičnosti pa pod 0,001 (0,1 %), zato sklepamo na visoko skladnost modela s podatki. Vrednosti faktorskih uteži znašajo med 0,500 in 0,780, s čimer je zagotovljena konvergentna veljavnost merskega inštrumenta. Vsebinsko veljavnost so avtorji utemeljili z izvedbo poglobljenih intervjujev za ocenjevanje natančnosti in ustreznosti indikatorjev. Vrednosti koeficienta Cronbachove alfe znašajo med 0,750 in 0,820, kar kaže na zanesljivost merskega inštrumenta. Vprašalnik HAIS-Q z vsebinskimi indikatorji je dostopen v analizi omenjene raziskave.

Merjenje informacijskega varnostnega zavedanja so se lotili tudi Ahlan in drugi (2015), ki so v svoj merski inštrument vključili 11 komponent. Podali so definicijo konstrukta, medtem ko komponent niso definirali. Merski inštrument je bil sestavljen s pomočjo ekspertne ocene, pri čemer so se osredotočili predvsem na jasnost in enostavnost indikatorjev. Končna verzija vprašalnika vsebuje 39 indikatorjev. Zbiranje podatkov je potekalo z metodo PAPI, vzorec pa znaša 103 enote. Izvedena je bila eksploratorna faktorska analiza, vrednosti faktorskih uteži znašajo med -0,052 in 0,880, kar nakazuje na problematičnost nekaterih indikatorjev in posledično vprašljivo konvergentno veljavnost. Korelacije faktorjev sicer znašajo med -0,004 in 0,475, zato lahko sklepamo, da je model stabilen. Avtorji so analizirali tudi diskriminantno veljavnost, ki pa prav tako ni zadovoljiva, saj vrednost AVE znaša med 0,257 in 0,595 in pri nekaterih indikatorjih ne dosega minimalne vrednosti 0,5. Vrednosti koeficienta Cronbachove

alfe prav tako ne dosegajo zadovoljivih vrednosti (0,056–0,681) in niti pri enem faktorju ne presegajo kritične vrednosti 0,7, zato lahko zaključimo, da merski inštrument ni zanesljiv.

Pomembno komponento informacijske varnostne kulture sta obravnavala Aurigemma in Mattson (2017), ki sta vzpostavila merski inštrument za merjenje informacijske varnostne politike. Merski inštrument vsebuje definicijo pojma in nekaterih komponent (ne vseh). Zbiranje podatkov je potekalo z metodo PAPI in spletnim anketiranjem, število enot v vzorcu znaša 239, stopnja odgovora pa 23%. Korelacije faktorjev znašajo približno od 0,1 do 0,7. Izvedena je bila konfirmatorna faktorska analiza, rezultati pa kažejo na visoko veljavnost merskega inštrumenta. Vrednosti faktorskih uteži znašajo nad 0,7 (med 0,753 in 0,991), indeksi prileganja (CFI med 0,928 in 0,963 ter SRMR med 0,049 in 0,059) pa kažejo na odlično skladnost modelov s podatki[38]. Analiza je pokazala tudi na visoko diskriminantno veljavnost merskega inštrumenta, saj se vrednost AVE giblje med 0,679 in 0,899. Prav tako so visoke vrednosti Cronbachove alfe za oceno zanesljivosti, ki znašajo med 0,850 in 0,964, kar dokazuje dobro notranjo konsistentnost vprašalnika. Vprašalnik z indikatorji se nahaja v analizi omenjene raziskave.

Podrobnejša analiza merskih inštrumentov daje vpogled v kvaliteto merjenja v smislu operacionalizacije, oblikovanja vprašalnikov ter karakteristik veljavnosti in zanesljivosti. Za ovrednotenje in primerjavo merskih inštrumentov potrebujemo natančno opredeljene kriterije, saj taki standardizirani kriteriji omogočajo nepristransko ocenjevanje. V osnovi smo opredelili deset ocenjevalnih kriterijev, nekateri izmed njih so precej obširni in zajemajo več vidikov znotraj enega kriterija. Zaradi kompleksnosti kriterijev, ki vsebujejo več karakteristik, smo določene osnovne kriterije razdelili na več podkriterijev. Naslednja tabela v okviru glavnih kriterijev prikazuje podkriterije in njihove (mejne) vrednosti za sprejetje posameznega podkriterija.

[38] Avtorja sta s strukturnim modeliranjem enačb analizirala več modelov in predstavila rezultate vseh osmih modelov, na katere se nanašajo vrednosti indeksov prileganja.

Tabela 5.3: Vrednosti ocenjevalnih kriterijev in podkriterijev

	Kriterij	Podkriterij	Vrednost
1	Definicije teoretskih pojmov in komponent	Definicija pojma	DA/NE
		Opredelitev in definicije komponent	
2	Vzorčenje in stopnja odgovora	Način vzorčenja / metoda anketiranja	DA/NE
		Število enot v vzorcu	Vsaj 100 enot ali 5x št. indikatorjev
		Stopnja odgovora	30-40% za spletno anketiranje[39]
		Struktura vzorca (spol, starost,…)	DA/NE
3	Merjenje komponent teoretskega pojma	Komponente pojma v vprašalniku	DA/NE
		Postopek oblikovanja indikatorjev	
4	Opisne statistike		DA/NE
5	Korelacijska analiza		DA/NE
6	Faktorska analiza	Prileganje podatkov / skladnost modela[40]	KMO test > 0,5; Bartlettov test: < 0,05 RMSEA/ RMR < 0,1; CFI/GFI > 0,9
		Faktorske uteži	Faktorske uteži > 0,3
7	Veljavnost konstrukta	Konvergentna veljavnost	Faktorske uteži > 0,4
		Diskriminantna veljavnost	Korelacije med faktorji statistično značilno različni od 1 (oziroma imeti čim nižjo vrednost) ali AVE > 0,5
8	Pragmatična veljavnost	Vsebinska veljavnost	DA/NE (subjektivna ocena raziskovalca)
		Kriterijska veljavnost	Korelacijski koeficient kriterijske spremenljivke > 0,5
9	Zanesljivost		Cronbachov alfa > 0,7 ali CR > 0,6
10	Dostopnost		DA/NE

Metodološko oceno kakovosti tako sestavlja 18 kriterijev, pri tem je devet kriterijev vsebinskih, preostalih devet pa številskih. Vsebinski kriteriji (definicija pojma, opredelitev in definicije komponent, način vzorčenja/metoda anketiranja, struktura vzorca, komponente pojma v vprašalniku, postopek oblikovanja indikatorjev, opisne statistike, korelacijska analiza ter dostopnost) so opredeljeni kot prisotnost oziroma odsotnost njihovih karakteristik v analizi. Številskim kriterijem (število enot v vzorcu, stopnja odgovora, prileganje podatkov/skladnost modela, faktorske uteži, konvergentna veljavnost, diskriminantna veljavnost, kriterijska veljavnost ter zanesljivost) pa smo določili mejne (kritične) vrednosti sprejemljivosti

[39] Pri večini izbranih raziskav gre za spletno anketiranje, zato navajamo le omejitev stopnje odgovora za ta način anketiranja. Pri ostalih pa smiselno upoštevamo mejne vrednosti, ki so navedene pri razlagi drugega osnovnega kriterija (str. 54).

[40] Kriterij se razlikuje glede na tip izvedene faktorske analize – pri eksploratorni faktorski analizi upoštevamo koeficienta KMO in Bartlettovega testa, pri konfirmatorni faktorski analizi pa izbrane koeficiente SEM analize.

posameznega kriterija glede na priporočila po teoriji. Število enot v vzorcu je sprejemljivo, če dosega vsaj 100 enot ali petkratno število indikatorjev v vprašalniku, stopnja odgovora za spletno anketiranje pa med 30% in 40% (za osebno anketiranje 70%). V okviru faktorske analize se način preverjanja kriterija skladnosti podatkov razlikuje glede na tip izvedene faktorske analize – pri eksploratorni faktorski analizi upoštevamo vrednost koeficienta KMO testa nad 0,5 in Bartlettovega testa sferičnosti pod 0,05, pri konfirmatorni faktorski analizi pa izbrane koeficiente SEM analize, in sicer vrednosti indeksov prileganja CFI/GFI nad 0,9 ter RMSEA/RMR pod 0,1. Za doseganje ustreznih vrednosti faktorskih uteži smo določili spodnjo mejo 0,3. Kriterij veljavnosti konstrukta smo razdelili na konvergentno veljavnost s kritično vrednostjo faktorskih uteži nad 0,4 ter diskriminantno veljavnost, pri kateri morajo biti korelacije med faktorji statistično značilno različne od 1 (oziroma imeti čim nižjo vrednost) ali pa mora vrednost koeficienta AVE znašati nad 0,5. Del kriterija pragmatične veljavnosti je poleg vsebinske veljavnosti še kriterijska veljavnost, kjer mora biti vrednost korelacijskega koeficienta kriterijske spremenljivke za doseganje kriterija večja od 0,5. Zadnji številski kriterij je zanesljivost, ki ga opredeljujemo z vrednostjo Cronbachove alfe nad 0,7 ali vrednostjo CR koeficienta nad 0,6.

Na ocenjevalnem listu so podane ocene izpolnjevanja posameznih kriterijev za 12 izbranih raziskav. V kolikor je raziskava zadostila kriteriju po zgornjem opisu, prikazujemo znak ✓, v nasprotnem primeru pa znak X' oziroma znak X, če ni podatka. Končna ocena merskega inštrumenta je seštevek točk izpolnjenih kriterijev.

Tabela 5.4: Ocenjevalni list kakovosti merskih inštrumentov izbranih raziskav

	(1)		(2)				(3)		(4)	(5)	(6)		(7)		(8)		(9)	(10)	
	Definicija pojma	Opredelitev in definicije komponent	Način vzorčenja	Število enot v vzorcu	Stopnja odgovora	Struktura vzorca	Komponente pojma v vpr.	Postopek oblikovanja indikatorjev	Opisne statistike	Korelacijska analiza	Prileganje podatkov	Faktorske uteži	Konvergentna veljavnost	Diskriminantna veljavnost	Vsebinska veljavnost	Kriterijska veljavnost	Zanesljivost	Dostopnost	Skupaj
Da Veiga, Martins in Eloff (2007)	X	X	✓	✓	✓	✓	✓	✓	X	X	X	✓	X'	X	X	X	X	X	7
Da Veiga in Eloff (2010)	✓	X	✓	✓	✓	✓	✓	✓	X	X	✓	X	?	X	✓	X	✓	✓	11
Da Veiga in Martins (2015a)	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	X	X	X	X	X	X	X	X	9
Da Veiga in Martins (2015b)	✓	✓	✓	✓	✓	X	✓	X	✓	X	?	?	X	X	X	X	✓	X	8
Alnatheer in drugi (2012)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X	✓	✓	16
AlHogail (2015a)	✓	✓	✓	X	X	✓	✓	X	✓	✓	X	X	?	X	X	X	X'	X	7
Safa in drugi (2015)*	✓	✓	✓	✓	X	✓	✓	✓	X	✓	✓	✓	✓	✓	X	X	✓	✓	14
Rocha Flores in Ekstedt (2016)*	X	✓	✓	✓	✓	✓	✓	✓	X	✓	?	✓	✓	✓	✓	X	✓	✓	14
Narain Singh in drugi (2014)*	✓	✓	✓	✓	X	✓	✓	✓	X	X	✓	✓	✓	X	X	X	✓	✓	12
Parsons in drugi (2017)*	✓	X	✓	✓	X	X	✓	✓	✓	✓	✓	✓	✓	X	✓	X	✓	✓	13
Ahlan in drugi (2015)*	✓	✓	✓	✓	X	X	✓	✓	X	✓	X	X'	X'	X'	X	X	X'	✓	8
Aurigemma in Mattson (2017)*	✓	X	✓	✓	X	✓	✓	X	✓	✓	✓	✓	✓	✓	X	X	✓	✓	13

Legenda:
✓– kriterij je izpolnjen
X – kriterij ni izpolnjen, ker ni podatka / X' – ne dosega mejnih vrednosti
? – vprašljiv kriterij - ni številčnega podatka, ampak samo vsebinska interpretacija, zato se pojavlja dvom o ustreznem izpolnjevanju kriterija
* – ni merjen koncept informacijske varnostne kulture, ampak informacijska varnostna kultura kot dimenzija drugega (sorodnega) koncepta ali pa posamezna komponenta informacijske varnostne kulture

Prvih šest člankov na ocenjevalnem listu se nanaša na merjenje informacijske varnostne kulture. Opazimo lahko, da pojem informacijske varnostne kulture raziskujejo predvsem Da Veiga, Martins in Eloff, ki dominirajo na tem področju. Izmed omenjene skupine raziskovalcev je najboljšo oceno merskega inštrumenta dosegla raziskava Da Veiga in Eloff (2010) – 11 točk, anketni vprašalnik pa je kot edini prosto dostopen, čeprav ni bil objavljen skupaj z raziskavo. Merski inštrument (prva verzija vprašalnika ISCA) dosega vsebinsko vejavnost ter visoko oceno zanesljivosti. Pri analizi sicer ni navedenih vrednosti faktorskih uteži, kar zmoti preglednost in relevantnost rezultatov. Zaradi tega tudi ne moremo oceniti konvergentne veljavnosti, ki jo merski inštrument morda celo dosega. Boljšo oceno merskega inštrumenta bi omenjena raziskava lahko dobila z analizo veljavnosti konstrukta (konvergentna in diskriminantna veljavnost) ter analizo korelacijskih koeficientov za ugotavljanje stabilnosti modela. Kasnejši raziskavi Da Veiga in Martins (2015a) in Da Veiga in Martins (2015b), ki temeljita na enakem merskem inštrumentu oziroma je le-ta nadgradnja predhodnega vprašalnika, vsebujeta tudi pregled opisnih statistih in korelacijsko analizo. Razlika med vsemi tremi verzijami vprašalnika je v številu dimenzij informacijske varnostne kulture – v raziskavi Da Veiga in Eloff (2010) je uporabljenih sedem dimenzij, v kasnejši raziskavi Da Veiga in Martins (2015a) sta dodani še dve novi dimenziji ter v raziskavi Da Veiga in Martins (2015b) še ena, vendar kot smo že omenili, ta ne bi bila primerna za merjenje varnostne kulture.

Sodeč po oceni – 16 točk, so najboljši merski inštrument za merjenje informacijske varnostne kulture oblikovali Alnatheer in drugi (2012), ki ga odlikuje odličen proces operacionalizacije, saj izpolnjuje vse kriterije, ki se nanjo nanašajo. Izmed vseh kriterijev nista bila raziskana samo vsebinska in kriterijska veljavnost, na tem mestu pa je potrebno ponovno opozoriti, da so avtorji v analizi obravnavali tudi nomološko veljavnost. To pomeni, da je merski inštrument visoko veljaven in zanesljiv, prav tako pa je dostopen v analizi. Kljub temu bi ga avtorji z utemeljitvijo vsebinske in kriterijske veljavnosti lahko še izboljšali.

Med ostalimi avtorji, ki ne pripadajo omenjeni raziskovalni skupini, se z anketnim merjenjem informacijske varnostne kulture ukvarja AlHogail s svojimi akademskimi sodelavci, vendar njegov merski inštrument ISCF sodeč po rezultatih evalvacije ni najbolj kvaliteten (ocena 7). Manjka predvsem faktorska analiza, s katero bi lahko ocenili porazdelitev in variabilnost faktorjev, skladnost modela s podatki in različne tipe veljavnosti. Prav tako analize načeloma ne moremo ponoviti, saj anketni vprašalnik ni javno dostopen.

V ocenjevalni list kakovosti merskih inštrumentov smo vključili tudi ostale raziskave, ki informacijsko varnostno kulturo merijo bodisi kot komponento širšega pojma oziroma je v merjenje vključena le posamezna komponenta informacijske varnostne kulture ali pa gre za merjenje podobnega koncepta.

Na splošno lahko opazimo, da merski inštrumenti teh raziskav dosegajo boljšo metodološko oceno kot tisti za merjenje informacijske varnostne kulture. Pri tem najbolj izstopata raziskavi Safa in drugi (2015) ter Rocha Flores in Ekstedt (2016). Prva se nanaša na merjenje sorodnega koncepta skrbi za zavedno vedenje na področju informacijske varnosti, druga pa se osredotoča na merjenje organizacijskih in individualnih dejavnikov, ki vplivajo na preprečevanje socialnega inženiringa. Oba merska inštrumenta sta dosegla najvišjo oceno med vsemi – 14 točk. Merski inštrument ISCCB v raziskavi Safa in drugi (2015) dosega visoko stopnjo skladnosti modela in veljavnosti konstrukta, še večjo težo veljavnosti pa bi avtorji lahko opredelili z utemeljitvijo vsebinske ali kriterijske veljavnosti. Dokazovanje vsebinske veljavnosti je lahko zaradi dokaj mladega področja raziskovanja sicer precej težavno. Merski inštrument dosega tudi zadovoljivo oceno zanesljivosti. Na drugi strani pa je merski inštrument v raziskavi Rocha Flores in Ekstedt (2016) prav tako konvergentno in diskriminantno veljaven, avtorja pa sta utemeljila tudi vsebinsko veljavnost. V analizi sicer manjkajo podatki o indeksih prileganja modela s podatki, vendar po visokih ocenah veljavnosti konstrukta sklepamo na skladnost modela. Podobno kot pri prejšnji raziskavi ima tudi ta merski inštrument zadovoljivo stopnjo zanesljivosti. Oba anketna vprašalnika sta bila v raziskavah objavljena skupaj z analizo oziroma v prilogi. Glede na podobnost koncepta skrbi za zavedno vedenje na področju informacijske varnosti in informacijske varnostne kulture ocenjujemo, da je večji del merskega inštrumenta ISCCB primeren za merjenje informacijske varnostne kulture. Ta bi sicer potreboval malenkostne prilagoditve pri indikatorjih v smislu navezovanja na informacijsko varnostno kulturo. V primerjavi z ISCA vprašalnikom ima ISCCB za približno polovico manj indikatorjev (ISCA jih ima 85, ISCCB pa 43 indikatorjev), kar pomeni, da je manj kompleksen in hitrejši za izpolnjevanje. Prav tako je za merjenje informacijske varnostne kulture uporaben del vprašalnika iz raziskave Rocha Flores in Ekstedt (2016), ki se nanaša na njene komponente. Možno je tudi združevanje indikatorjev iz obeh omenjenih vprašalnikov po komponentah informacijske varnostne kulture, s čimer bi lahko računali na visoko veljavnost in zanesljivost novega merskega inštrumenta.

Visoko oceno kakovosti merskih inštrumentov dosegajo še tri raziskave, in sicer Narain Singh in drugi (2014) – 12 točk ter Parsons in drugi (2017) in Aurigemma in Mattson (2017) – 13 točk. Pri prvi raziskavi gre podobno kot pri zgoraj omenjenih raziskavah prav tako za merjenje nekaterih komponent informacijske varnostne kulture v okviru drugega koncepta. Glede na visoke vrednosti kazalnikov veljavnosti in zanesljivosti sklepamo, da gre za kvaliteten merski inštrument. Raziskava Parsons in drugi (2017) pa se osredotoča samo na merjenje zavedanja informacijske varnosti, ki je eden izmed pomembnejših delov informacijske varnostne kulture in prepoznan kot ena njenih glavnih komponent. Slabost merskega inštrumenta HAIS-Q je v tem, da nima opredeljenih komponent glavnega konstrukta, vendar za merjenje informacijske varnostne kulture to ni problematično, saj je predvsem važno, da je definiran pojem zavedanja informacijske varnosti. Merski inštrument je z vidika veljavnosti in zanesljivosti zelo kvaliteten. Z merjenjem zavedanja informacijske varnosti so se ukvarjali tudi Ahlan in drugi (2015), vendar zaradi pomanjkljive analize predvsem z vidika veljavnosti in zanesljivosti merski inštrument ni priporočljiv za uporabo. V tem kontekstu deluje tudi raziskava Aurigemma in Mattson (2017), ki meri informacijsko varnostno politiko, ki je prav tako ena vidnejših komponent informacijske varnostne kulture. Njun merski inštrument dosega zelo visoke ocene veljavnosti in zanesljivosti, manj pa se osredotoča na samo operacionalizacijo, kjer bi ga bilo mogoče še izboljšati. Omenjeni dejavniki implicirajo kakovostno zasnovo vseh treh merskih inštrumentov, zato se indikatorji, ki se nanašajo na informacijsko varnostno kulturo, prav tako lahko uporabijo pri nadaljnjem raziskovanju.

5.5 UGOTOVITVE

Po pregledu obstoječe literature o merjenju informacijske varnostne kulture smo ugotovili, da gre za dokaj neraziskano področje, saj se z anketnim merjenjem omenjenega pojma ukvarja le peščica raziskovalcev. Gre za raziskovalno skupino treh raziskovalcev iz Južne Afrike[41], ki so do sedaj objavili največ izsledkov in poskusov merjenja. Po ena študija prihaja tudi iz Avstralije in azijskega predela, dejstvo pa je, da je v evropskem prostoru čutiti primanjkljaj na področju raziskovanja informacijske varnostne kulture. Glede na to, da gre za enega bolj pomembnih

[41] V to skupino spadajo Adele Da Veiga, Jan H. P. Eloff in Nico Martins (Univerza v Južni Afriki – UNISA, Pretoria).

organizacijskih vidikov današnjega časa, lahko rečemo, da je opazen razkorak med teorijo in merjenjem dejanske stopnje informacijske varnosti v organizacijah.

Iz analize je razvidno, da uveljavljenega inštrumenta na področju merjenja informacijske varnostne kulture trenutno ni. Kot edini relevanten in kakovostno zasnovan se je izkazal merski inštrument iz raziskave Altanheer in drugi (2012), ki dosega visoke ocene veljavnosti in zanesljivosti, poleg tega pa temelji na kvalitetno zasnovani operacionalizaciji. Glede poglobljene analize z vidika kvalitete je lahko zgled bodočim raziskavam na tem področju. Delno zadovoljivo kakovost pa je dosegel merski inštrument na podlagi raziskovalnega modela ISCF, ki so ga avtorji poimenovali ISCA (kar v prevodu pomeni ocena informacijske varnostne kulture). Ta ima sicer nekaj pomanjkljivosti, vendar kljub temu predstavlja solidno osnovo za nadaljnje raziskovanje. Predvsem veljavnosti (veljavnost konstrukta, kamor spadata konvergentna in diskriminantna veljavnost) bi bilo v prihodnje potrebno nameniti več pozornosti. S prevodom trditev in manjšimi metodološkimi spremembami (manjše število trditev, drugačno oblikovanje trditev) bi lahko oblikovali modificiran merski inštrument. S tem bi ohranili kakovost, poskušali pa bi ga čim bolj generalizirati in organizacijam približati kot uporabno vrednost glede merjenja stopnje njihove informacijske varnostne kulture.

Poleg informacijske varnostne kulture pa obstajajo tudi sorodni koncepti, ki se osredotočajo na informacijsko varnost v organizacijah. Denimo, informacijska varnostna kultura je lahko merjena kot del širšega koncepta informacijskega varnostnega zavedanja. Dober primer je vprašalnik HAIS-Q, kar v prevodu pomeni vprašalnik človeških vidikov informacijske varnosti. Sicer je precej obsežen, vendar bi za oblikovanje novega merskega inštrumenta lahko izluščili le nekaj indikatorjev posameznega sklopa, ki dosegajo najvišje ocene veljavnosti in zanesljivosti. Na podoben način bi relevantne indikatorje po komponentah informacijske varnostne kulture lahko uporabili iz merskih inštrumentov v raziskavah Safa in drugi (2015), Narain Singh in drugi (2014), Aurigemma in Mattson (2017) ter Rocha Flores in Ekstedt (2016), ki so se izkazali za zelo kvalitetne. S tem bi ustvarili nov merski inštrument s pričakovano visoko stopnjo veljavnosti in zanesljivosti, ki bi ga morali sprva utemeljiti s teoretskim modelom in ustreznimi definicijami.

Opažamo tudi, da noben izmed izbranih merskih inštrumentov ni bil analiziran z vidika kriterijske (prediktivne) veljavnosti, prav tako sta bili v manjši meri analizirani diskriminantna in vsebinska veljavnost. Pri merskih inštrumentih informacijske varnostne kulture je zaskrbljujoče dejstvo, da samo eden izmed njih dosega veljavnost konstrukta, ocene pa so slabe

tudi glede pragmatične veljavnosti in skladnosti modelov. Na drugi strani pa so avtorji v raziskavah, ki merijo sorodne koncepte, pomanjkljivo navedli nekatere osnovne podatke o vzorčenju, tu imamo v mislih predvsem stopnjo odgovora, ki je prav tako kot analiza veljavnosti pomemben podatek za ocenjevanje relevantnosti merskega inštrumenta. Vsa našteta dejstva dokazujejo, da je na področju kvantitativnega (anketnega) merjenja varnostne kulture še precej prostora za izboljšave in nove idejne zasnove merskih inštrumentov.

6 ZAKLJUČEK

Tveganja informacijske varnosti v današnjem času tehnoloških sprememb in razvoja predstavlja predvsem človeški dejavnik, ki je zaradi dovršene varnostne programske opreme najbolj ranljiv del organizacije. Pogosto so zaposleni tisti, ki s svojim neodgovornim in velikokrat nezavednim ravnanjem povzročajo varnostne incidente, česar se zlonamerneži dobro zavedajo in na ta način želijo izkoristiti njihovo malomarnost ali nevednost. Nevarnost predstavljajo informacijska sredstva, kjer so shranjeni občutljivejši podatki, ki imajo za organizacijo določeno vrednost.

Oblikovanje informacijske varnostne kulture je nujno za učinkovito upravljanje informacijske varnosti. Zajema celosten pristop obravnavanja informacijske varnosti z vedenjskega vidika zaposlenih. Vsaka organizacija je odgovorna za merjenje stopnje informacijske varnostne kulture, zato je pomembno, da tej temi posveti dovolj pozornosti in vzpostavi dober sistem spremljanja varnostne kulture, kajti le tako bo organizacija ohranila nadzor pred zunanjimi grožnjami.

Glede na predstavljena dejstva je za raziskovanje informacijske varnostne kulture najbolj učinkovito kvantitativno merjenje, ki organizaciji ne sme predstavljati stroška, temveč naložbo za varno delovanje v prihodnje. Varnostno kulturo je možno spremljati preko standardiziranih vprašalnikov, ki jih organizacija lahko pripravi v sodelovanju z zunanjimi strokovnjaki ali uporabi kakšnega od že razvitih vprašalnikov. Sistematičen pregled obstoječih merskih inštrumentov v tem magistrskem delu daje oceno njihove uporabnosti. Izkazalo se je, da trenutno noben izmed razvitih vprašalnikov še ni uveljavljen v tolikšni meri, da bi bil splošno uporaben, zato raziskovalci na tem področju uvajajo nove ideje in modele za merjenje tega pojma. Večinoma vprašalniki niso poimenovani, zato je preglednost njihove analize nekoliko omejena. Identificirali smo tri različne vprašalnike za merjenje informacijske varnostne kulture,

izmed katerih najvišjo oceno z vidika kvalitete dosega merski inštrument v raziskavi Altanheer in drugi (2012). V literaturi pa obstajajo tudi podobni koncepti informacijski varnostni kulturi, ki smo jih prav tako upoštevali v analizi. Splošno gledano so ti merski inštrumenti z vidika veljavnosti in zanesljivosti bolj kvalitetni, kar bi lahko izkoristili v nadaljnjem raziskovanju z izborom relevantnih indikatorjev in oblikovanjem novega modificiranega merskega inštrumenta.

Pregled merskih inštrumentov je sicer omejen na znanstveno literaturo, kar pa ne pomeni, da zajema vse relevantne merske inštrumente. Raziskovanje in merjenje informacijske varnostne kulture se pojavlja tudi na ravni strokovne literature in drugih področjih, zato nabor analiziranih merskih inštrumentov ni celosten. Ocenjevalni kriteriji so bili izbrani na podlagi subjektivne presoje glede kvalitete merskih inštrumentov, mejne vrednosti (številskih) kriterijev pa so bile določene na podlagi izsledkov iz teorije na področju statistike. Kljub temu lahko prihaja do manjših odstopanj pri vrednotenju obravnavanih merskih inštrumentov (relativno visoki pogoji za izpolnjevanje posameznega kriterija). Ne glede na to ocenjujemo, da je izvedena metaanaliza podala temeljit vpogled v tematiko merjenja informacijske varnostne kulture.

7 LITERATURA

1. Ahlan, Abdul Rahman, Muharman Lubis in Arif Ridho Lubis. 2015. Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science* 72: 361–373.

2. Alberts, Christopher in Audrey Dorofee. 2002. **Managing Information Security Risks: The OCTAVE^{SM} Approach**. Boston: Pearson Education. Dosotpno prek: TeamLiB.

3. Albrechtsen, Eirik in Jan Hovden. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security* 29 (4): 432–445.

4. AlHogail, Areej in Abdulrahman Mirza. 2015. Organizational Information Security Culture Assessment. *The 2015 International Conference on Security and Management, 286–292*. Dostopno prek: http://worldcomp-proceedings. com/proc/p2015/ SAM_contents.html (29. junij 2017).

5. --- 2015a. Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. *Information Journal of Security and Its Applications* 9 (7): 163–178.

6. --- 2015b. Design and validation of information security culture framework. *Computers in Human Behavior* 49: 567–575.

7. Allen, Mary J. in Wendy M. Yen. 2002. **Introduction to Measurement Theory**. Long Grove: Waveland Press. Dostopno prek: Google books.

8. Alnatheer, Mohammed, Taizan Chan in Karen Nelson. 2012. Understanding And Measuring Information Security Cuture. *Prispevek na konferenci PACIS 2012*, št. 144. Dostopno prek: http://www.pacis-net.org/file/2012/PACIS2012-005.pdf (27. julij 2017).

9. Aurigemma, Salvatore in Thomas Mattson. 2017. Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security* 66: 218–234.

10. Bernik, Ivan in Kaja Prislan. 2012. *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.

11. --- 2016. Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. *PLoS ONE*. Dostopno prek: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163050 (19. julij 2017).

12. BIS. 2015. *Information Security Breaches Survey: Technical report*. Dostopno prek: https://www.gov.uk/government/publications/information-security-breaches-survey-2015 (14. julij 2017).

13. Bland, Martin, J. in Douglas G. Altman. 1997. Statistics notes: Cronbach's alpha. *British Medical Journal* 314 (7080): 572.

14. Bojanc, Rok, Borka Jerman-Blažič in Metka Tekavčič. 2014. *Informacijska varnost v podjetniškem okolju: potrebe, ukrepi in ekonomika vlaganj*. Ljubljana: Ekonomska fakulteta.

15. Brewerton, Paul M. in Lynee J. Millward. 2001. *Organizational Research Methods*. London: SAGE.

16. Bryman, Alan. 2001. *Social research method*s. New York: Oxford University Press.

17. Callegaro, Mario, Katja Lozar Manfreda in Vasja Vehovar. 2015. *Web Survey Methodology*. Thousand Oaks: SAGE.

18. Cheung, Mike W.-L. 2013. Applied Meta-Analysis for Social Science Research by N. A. Card. *Structural Equation Modeling: A Multidisciplinary Journal* 20 (4): 704–707.

19. Child, Dennis. 2006. *The Essentials of Factor Analysis*. London: Continuum.

20. Cisco. 2014. *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*. San Jose: Cisco White Paper. Dostopno prek: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html (8. avgust 2017).

21. Cooper, Harris in Larry V. Hedges. 2009. Research synthesis as a scientific process. V *The handbook of research synthesis*. Druga izdaja, ur. Harris Cooper, Larry V. Hedges in Jeffrey C. Valentine, 3–36. New York: Russel Sage Foundation.

22. Da Veiga, Adele, Nico Martins in Jan H. P. Eloff. 2007. Information security culture – validation of an assessment instrument. *Southern African Business Review* 11 (1): 147–166.

23. --- in Jan H.P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29 (2): 196–207.

24. --- in Nico Martins. 2015a. Information security culture and information protection culture: A validated assessment instrument. *Computer Law and Security Review* 31 (2): 243–256.

25. --- 2015b. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security* 49: 162–176.

26. --- 2017. Defining and identifying dominant information security cultures and subcultures. *Computers & Security* 70: 72–94.

27. Dhillon, Gurpreet. 2001. Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security* 20 (2): 165–172.

28. *Digitalna knjižnica Univerze v Ljubljani*. Dostopno prek: http://dikul.uni-lj.si (10. maj 2017).

29. Dillman, Don A., Jolene D. Smyth in Leah Melani Christian. 2014. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. Četrta izdaja. New Jersey: Wiley & Sons.

30. Dillon, William R. in Matthew Goldstein. 1984. *Multivariate analysis: methods and applications*. New York: Wiley & Sons.

31. DiStefano, Christine, Min Zhu in Diana Mindrila. 2009. Understanding and Using Factor Scores: Considerations for the Applied Researcher. *Practical Assessment, Research & Evaluation* (14) 20: 1–11.

32. Eisinga, Rob, Manfred Grotenhuis in Ben Pelzer. 2013. The reability of a two-item scale: Pearson, Cronbach or Spearman-Brown? *International Journal of Public Health* 58 (4): 637–642.

33. Ferligoj, Anuška, Karmen Leskošek in Tina Kogovšek. 1995. *Merjenje zanesljivosti in veljavnosti*. Metodološki zvezki. Ljubljana: Fakulteta za družbne vede.

34. --- Katja Lozar Manfreda in Aleš Žiberna. 2015. *Osnove statistike na prosojnicah: študijsko gradivo pri predmetu Statistika*. Ljubljana: Fakulteta za družbene vede.

35. Glass, Gene V. 1976. Primary, secondary, and meta-analysis of research. *Educational Researcher* 5 (10): 3–8.

36. Hair, Joseph F, William C. Black, Barry J. Babin in Rolph E. Anderson. 2014. *Multivariate Data Analysis*. Sedma izdaja. Harlow: Pearson.

37. Hunter, John E. in Frank L. Schmidt. 2004. *Methods of meta-analysis: correcting error and biasin research findings*. Druga izdaja. Thousand Oaks: Sage.

38. *International Organization for Standardization*. 2017. Dostopno prek: https://www.iso.org/isoiec-27001-information-security.html (12. julij 2017).

39. *ISO/IEC 27000*. 2016. Dostopno prek: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en (14. julij 2017).

40. --- *27005*. 2011. Dostopno prek: https://www.iso.org/standard/56742.html (14. julij 2017).

41. Johnsen, Stig O., Christian Waale Hansen, Yngve Nordby in Maria B. Dahl. 2006. Measurement and improvement of information security culture. *Measurement and Control* 39 (2): 52-56.

42. Kastrin, Andrej. 2008. Metaanaliza in njen pomen za psihološko medicino. *Psihološka obzorja* 17 (3): 25–42.

43. Kimberlin, Carole L. in Almut G. Winterstein. 2008. Validity and reability of measurements used in research. *American Journal of Health-System Pharmacy* 65 (23): 2276–2284.

44. Kogovšek, Tina. 2005. Zanesljivost in veljavnost v kvalitativnem in kvantitativnem raziskovanju. *Teorija in praksa* 42 (1): 256–278.

45. Krausz, Michael. 2014. **Managing Information Security Breaches: Studies From Real Life**. Second edition. Cambridgeshire: IT Governance Publishing. Dostopno prek: EBSCO eBook Collection.

46. Kritzinger, Elmarie in Sebastiaan H. Von Solms. 2010. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security* 29 (8): 840–847.

47. Kuusisto, Rauno in Tuija Kuusisto. 2013. Strategic Communication for Cyber Security Leadership. V *12th European Conference on Information Warfare and Security 2013*, 167–172.

48. Law, Kenneth S., Chi-Sum Wong in William H. Mobley. 1998. Toward a taxonomy of multidimensional constructs. *Academy of Management Review* 23 (4): 741–755.

49. Lim, Joo S., Shanton Chang, Sean Maynard in Atif Ahmad. 2009. Exploring the Relationship between Organizational Culture and Information Security Culture. V *Australian Information Security Management Conference*, 88–97. Perth: Edith Cowan University.

50. Linstone, Harold A. in Murray Turoff. 1975. *The Delphi Method: Techniques and Applications*. London: Addison-Wesley Publishing Company.

51. MacCallum, Robert C., Keith F. Widaman, Shaobo Zhang in Sehee Hong. 1999. Sample size in factor analysis. *Psychological Methods* 4 (1): 84–99.

52. Marentič Požarnik, Barica. 2000. *Psihologija učenja in pouka*. Ljubljana: DZS.

53. Martins, Adele in Jan H. P. Eloff. 2002. Information security culture. V *Security in the Information Society*, ur. M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi in Heba K. Aslan, 203–214.Boston: Kluwer Academic Publishers.

54. Martins, Nico in Adele Da Veiga. 2014. Information Security Culture: A Comparative Analysis of Four Assessments. V *European Conference on Information Management and Evaluation* 8: 49–57.

55. McCormac, Agata, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius in Malcolm Pattinson. 2017. Individual differences and Information Security Awareness. *Computers in Human Behaviour* 69: 151–156.

56. Metalidou, Efthymia, Catherine Marinagi, Panagiotis Trivellas, Niclas Eberhagen, Christos Skourlas in Georgios Giannakopoulos. 2014. The Human Factor of Information Security:

Unintentional Damage Perspective. *Procedia – Social and Behavioral Sciences* 147 (214): 424–428.

57. Miller, Michael B. 2009. Coefficient alpha: a basic introduction from the perspectives of classical test theory and structural equation modeling. *Structural Equation Modeling: A Multidisciplinary Journa*l 2 (3): 255–273.

58. Modic, David. 2010. Nigerijska prevarantska pisma. V *Kriminaliteta in tehnologija: Kako računalniki spreminjajo nadzor in zasebnost ter kriminaliteto in kazenski pregon*, ur. Aleš Završnik, 85–95. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

59. Narain Singh, Abhishek, M. P. Gupta in Amitabh Ojha. 2014. Identifying factors of organizational information security management. *Journal of Enterprise Information Management* 27 (5): 644–667.

60. Nunnally, Jum C. in Ira H. Bernstein. 1994. **Psychometric theory**. Tretja izdaja. Univerza v Michiganu: McGraw-Hill. Dostopno prek: Google books.

61. Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson in Cate Jerram. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* 42: 165–176.

62. --- Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac in Tara Zwaans. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Science* 66: 40–51.

63. Paulsen, Celia in Tony Coulson. 2011. Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security. *Communications of the IIMA* 11 (3): 35–54.

64. Ramlall, Indranarain. 2016. **Applied Structural Equation Modelling for Researchers and Practitioners: Using R and Stata for Behavioural Research**. Bingley: Emerald Group Publishing. Dostopno prek: Google books.

65. Rančigaj, Katja in Branko Lobnikar. 2012. Vedenjski vidiki zagotavljanja informacijske varnosti: pomen upravljanja informacijske varnostne kulture. V *Konferenca Informacijska varnost: odgovori na sodobne izzive*, ur. Igor Bernik in Gorazd Meško, 1–12. Ljubljana: Fakulteta za varnostne vede.

66. Rhee, Hyeun-Suk, Cheongtag Kim in Young U. Ryu. 2009. Self efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security* 28 (8): 816–826.

67. Richardson, Robert. 2008. *CSI Computer Crime & Security Survey: The latest results from the longest-running project of its kind*. Dostopno prek: http://www.kwell.net/doc/FBI2008.pdf (16. julij 2017).

68. Rocha Flores, Waldo in Mathias Ekstedt. 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security* 59: 26–44.

69. Roer, Kai in Gregor Petrič. 2017. *Indepth insight into the human factor: The 2017 Security Culture Report*. Newark: CLTRe North America, Inc. Dostopno prek: https://get.clt.re/report/ (10. julij 2017).

70. Rusjan, Marko. 2010. Hekerstvo kot izziv in upor. V *Kriminaliteta in tehnologija: Kako računalniki spreminjajo nadzor in zasebnost ter kriminaliteto in kazenski pregon*, ur. Aleš Završnik, 69–84. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

71. Safa, Nader S., Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani in Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53: 65–78.

72. --- in Rossouw Von Solms.2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 57: 442–451.

73. Schein, Edgar H. 1987. *Organizational Culture and Leadership: A Dynamic View*. San Francisco: Jossey-Bass Publisshers.

74. Schlienger, Thomas in Stephanie Teufel. 2003. Information security culture – from analysis to change. *South African Computer Journal* 2003 (31): 46–*52*.

75. Shaw, Ruey Shiang, Charlie C. Chen, Albert L. Harris in Hui-Jou Huang. 2009. The impact of information richness on information security awareness training effectiveness. *Computers & Education* 52: 92–103.

76. *SI-CERT*. 2017. Dostopno prek: https://www.cert.si/si/varnostne-groznje/ (14. julij 2017).

77. Siponen, Mikko T. 2001. Five dimensions of information security awareness. *Computers and Society* 31 (2): 24–29.

78. Smith, Mary Lee in Gene V. Glass. 1977. Meta-analysis of psychotherapy outcome studies. *American Psychologist* 32 (9): 752–760.

79. Spears, Janine L. in Henri Barki. 2010. User Participation in Information Systems Security Risk Management. *MIS Quarterly* 34 (3): 503–522.

80. Splichal, Slavko. 1990. *Analiza besedil: statistična obravnava jezikovnih podatkov v družboslovnih raziskavah*. Metodološki zvezki 6. Ljubljana: Fakulteta za sociologijo, politične vede in novinarstvo.

81. Stolzenberg, Ross M. 2004. Multiple Regression Analysis. V *Handbook of data analysis*, ur. Melissa Hardy in Alan Bryman, 165–207. London: SAGE.

82. Tsohou, Aggeliki, Maria Karyda in Spyros Kokolakis. 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommednations for information security awareness programs. *Computers & Security* 52: 128–141.

83. Trochim, William M. K. 2001. *Research methods knowledge base*. Druga izdaja. Cincinnati: Atommic Dog Pub.

84. Van Niekerk, Jan Frederik in Rossouw Von Solms. 2010. Information security culture: A management perspective. *Computers & Security* 29 (4): 476–486.

85. Von Solms, Basie. 2000. Information Security – The Third Wave? *Computers & Security* 2000 (19): 615–620.

86. --- 2006. Information Security – The Fourth Wave. *Computers & Security* 2006 (25): 165–168.

87. Williams, Bret, Andrys Onsman in Ted Brown. 2010. Exploratory factor analysis: A five-step guide for novices. *Journal of Emergency Primary Health Care* 8 (3): 1–13.

PRILOGA: RAZLAGA OZNAK

Indeksi prileganja	**Razlaga**	**Sprejemljiva vrednost**
AVE (angl. *Average Variance Extracted*)	Povprečje izločenih varianc	> 0,5
χ^2 (angl. *Chi-square*)	Hi-kvadrat	$p \geq 0,05$
χ^2/df (angl. *Chi-square test with degree of freedom*)	Normirani hi-kvadrat	> 3

GFI (angl. *Goodness of Fit Index*)	Indeks skladnosti	> 0,9
AGFI (angl. *Adjusted Goodness of Fit Index*)	Prilagojen indeks skladnosti	> 0,8
CFI (angl. *Comparative Fit Index*)	Primerjalni indeks prileganja	> 0,9
IFI (angl. *Incremental Fit Index*)	Indeks postopnega prileganja	> 0,9
NFI (angl. *Normed Fit Index*)	Normiran indeks prileganja	> 0,9
RMR (angl. *Root Mean Square Residual*)	Kvadratni koren povprečnega reziduala	> 0,1
SRMR (angl. *Standardized Root Mean Squared Residual*)	Standardiziran kvadratni koren povprečnega reziduala	> 0,05
RMSEA (angl. *Root Mean Square Error of Approximation*)	Kvadratni koren povprečne napake približka	> 0,1