CENTER ZA METODOLOGIJO IN INFORMATIKO
FAKULTETA ZA DRUŽBENE VEDE
UNIVERZA V LJUBLJANI

Priporočila in smernice za spodbujanje zdrave informacijskovarnostne kulture

Povzetek relevantnih znanstvenih študij in strokovnih poročil

Dr. Gregor Petrič, Zara Novak, Dr. Špela Orehek

Gradivo je del *projekta Ocenjevanje in krepitev informacijskovarnostne kulture pri izvajalcih bistvenih storitev: Analiza organizacijskih dejavnikov v odpornosti na kibernetske grožnje* (L5-50163), ki ga (so)financira Javna agencija za raziskovalno dejavnost Republike Slovenije (ARIS).

Ljubljana, januar 2025

Povzetek

Namen tega dokumenta je pregled ključnih priporočil in smernic za spodbujanje zdrave informacijskovarnostne kulture v organizacijah. Le-to ponazarjajo jasne in s strani zaposlenih ponotranjene informacijskovarnostne politike, močna zavezanost vodstva k prednjačenju informacijske varnosti v vseh organizacijskih in poslovnih procesih, pozitivna stališča in norme zaposlenih do informacijske varnosti ter odgovorno vedenje zaposlenih. Na podlagi analize 23 znanstvenih člankov in 20 strokovnih poročil dokument ponuja praktične usmeritve za strateško upravljanje politik, usposabljanje zaposlenih, integracijo tehnoloških rešitev v organizacijsko kulturo in implementacijo socio-tehnične perspektive za nenehno izboljšavo informacijsko-varnostne kulture. Cilj dokumenta je pomagati organizacijam izboljšati človeško plat organizacijske informacijske varnosti in okrepiti odpornost proti informacijskovarnostnim tveganjem na vseh ravneh organizacije. Dokument je primarno namenjen organizacijskim vodstvenim strukturam in odgovornim za informacijsko varnost v organizacijah. Pri tem je potrebno omeniti, da je dokument potrebno jemati predvsem kot niz posplošenih, znanstveno in strokovno utemeljenih ohlapnih priporočil, ki pa jih je za konkretne implementacije in delovanja potrebno prilagoditi v odnosu do specifičnih organizacijskih kontekstov in specifik posamičnih organizacij in podjetij.

Kazalo

1) STRATEŠKO UPRAVLJANJE ORGANIZACIJSKIH POLITIK ZA ZDRAVO INFORMACIJSKOVARNOSTNO KULTURO

- **Vzpostavite formalne in neformalne nadzorne mehanizme** (npr. politike in regulativnih ukrepov) za krepitev usklajenosti strategij informacijske varnosti z organizacijskimi cilji. Na primer:
    - Izvedite letne interne revizije politik kibernetske varnosti, da zagotovite skladnost z internimi standardi in zunanjimi predpisi, kot je NIS2. Prepričajte se, da pravilniki pokrivajo ključna področja, kot so ravnanje z informacijsko-komunikacijsko tehnologijo, nadzor dostopa, varstvo podatkov in odzivanje na incidente.
    - Vključite zunanjega revizorja za oceno ranljivosti s penetracijskimi testi in za pridobitev nepristranskega pregleda varnostnih vrzeli.

- **Podpora vodstva:** Aktivno vključite višje vodstvo v spodbujanje in podporo varnostnih ukrepov. To vključuje motiviranje vodstva za prevzem odgovornosti pri varnostnih kontrolah in mehanizmih. Na primer:
    - Razvijte strateški načrt, s pristopom od zgoraj navzdol, usmerjen v spremembo organizacijske kulture. Zagotovite zavzetost vodstva in vključite ambasadorje varnosti, ki bodo med sodelavci spodbujali varno ravnanje.
    - Organizirajte četrtletne informativne sestanke za vodstvo, kjer upravni odbor pregleda stanje kibernetske varnosti organizacije in sodeluje pri odločanju glede dodeljevanja sredstev za varnostne pobude.
    - Ustanovite formalno platformo za upravljanje tveganj, skladnosti in vodenja (GRC), kjer lahko najvišje vodstvo spremlja varnostne metrike in nadzira izvajanje politik. Ta platforma naj bo vključena v redne sestanke vodstva, kjer se razpravlja o varnostnih izboljšavah.

- **Prilagojeni pristopi:** Prilagodite varnostne programe specifičnim potrebam organizacije, namesto da uporabljate univerzalne rešitve. Politike naj upoštevajo kulturno in organizacijsko edinstvenost. Na primer:
    - Razvijte smernice za kibernetsko varnost, specifične za posamezne sektorje, ki so vsakih šest mesecev pregledane in posodobljene. Identificirajte glavna in prednostna področja delovanja organizacije, pri čemer ustrezno prilagodite varnostne politike. Na primer, v zdravstvu se osredotočite na zasebnost podatkov in varno ravnanje s podatki pacientov, medtem ko v finančnih institucijah poudarite zaznavanje goljufij in varnost transakcij.
    - Prilagodite program upravljanja varnosti na podlagi resničnih incidentov. Po vdoru ali *phishing* napadu posodobite pravilnike tako, da naslovijo specifične ranljivosti, ki so jih incidenti razkrili. Te spremembe nato predstavite vsem zaposlenim prek interaktivnih delavnic.
- **Nacionalni in sektorski premisleki:** Strategije varnostne kulture morajo vključevati nacionalne kulturne dejavnike, zlasti v mednarodnih organizacijah ali sektorjih z različnimi kulturnimi normami. Na primer:

- Gostite letne delavnice za sodelovanje z lokalnimi strokovnjaki iz industrije in predstavniki vlade, da svoje mednarodne varnostne modele prilagodite nacionalnemu in sektorskemu kontekstu Slovenije.

- **Vzpostavite jasno komuniciranje politik in strategij:**
  - Poenostavite varnostne politike, pripravite pregleden povzetek navodil in protokolov (sploh če so dokumenti varnostnih politik obširni) in jih predstavite v razumljivem jeziku, tako da vsi zaposleni razumejo svojo vlogo pri zaščiti organizacije. Za boljšo dostopnost politik uporabite vizualne pripomočke kot so plakati v pisarnah in kontekstualni namigi (npr. plakati z napisom "Premisli, preden klikneš!" v bližini delovnih postaj).
  - Vzpostavite jasno opredeljene procese za poročanje o varnostnih incidentih in jih redno preizkušajte, da zagotovite, da zaposleni vedo, kako ukrepati v primeru kršitve. Uvedite anonimne kanale za poročanje o incidentih, s čimer boste zaposlenim omogočili, da brez strahu pred povračilnimi ukrepi prijavijo težave, hkrati pa pazite, da se tovrstni sistemi poročanja ne zlorabljajo.
  - Spodbujajte kulturo odgovornosti tako, da zaposlenim pokažete, kako njihovo vedenje neposredno vpliva na varnost organizacije. Izpostavite zgledna ravnanja, ki se dosledno držijo varnostnih protokolov.
  - Uporabite komunikacijska orodja kot so glasila, videoposnetki in *phishing* simulacije, da postane in ostane varnost ključna prioriteta za zaposlene. Ponudite spodbude in nagrade za sodelovanje v varnostnih dejavnostih z uporabo t.i. gamification tehnik. V komunikacijsko strategijo vključite več interaktivnih orodij (npr. kratke video vodiče, kvize in platforme za povratne informacije v realnem času), *ki bodo sporočila naredile privlačnejše in težje pozabljive.*
  - Vzpostavite stalno komuniciranje namesto enkratnih obvestil. Pri tem bodite inovativni in uporabite več različnih kanalov in načinov obveščanja.
  - Uporabite vizualne pripomočke in kontekstualne namige (kot so plakati, ozadja namizja ali pozivi za prijavo), da pri zaposlenih ohranite varnost na prvem mestu, ne da bi jih s tem preveč obremenjevali.

2) USPOSABLJANJE ZAPOSLENIH, SPREMEMBA VEDENJA, OPOLNOMOČENJE ZAPOSLENIH IN KREPITEV OZAVEŠČENOSTI O INFORMACIJSKI VARNOSTI

- **Programi ozaveščanja:** Oblikujte ciljno usmerjene programe usposabljanja, ki krepijo razumevanje zaposlenih o njihovi vlogi pri zagotavljanju informacijske varnosti. Osredotočite se na etiko, zasebnost in ključni pomen zaščite občutljivih podatkov. Na primer:
    - Izvajajte obvezna polletna usposabljanja za ozaveščanje o kibernetski varnosti, ki vključujejo simulacije *phishinga*, kvize in primere iz resničnega sveta, prilagojene specifičnim tveganjem v posameznih sektorjih (npr. *ransomware* v zdravstvu, finančne goljufije v bančništvu). Poslužujte se različnih inovativnih pristopov izobraževanja kot je npr. učenje skozi igro.
    - Izvajajte četrtletne varnostne delavnice z uporabo interaktivnih orodij, ki simulirajo grožnje iz resničnega življenja (npr. *phishing* napade). Spremljajte stopnjo udeležbe zaposlenih in njihovo uspešnost pri teh simulacijah, da identificirate tiste, ki potrebujejo dodatno usposabljanje.
    - Usposabljajte zaposlene, da prepoznajo, se izognejo in poročajo o taktikah potencialnih napadalcev. Konstantno posodabljajte usposabljanja, da boste dohajali nenehno razvijajoče se grožnje.
    - Spodbujajte zaposlene, da prijavijo morebitne grožnje, tako da zagotovite jasna in lahko dostopna orodja za poročanje, kot je gumb za prijavo *phishinga*.

- **Vpliv družbenih in poklicnih norm:** Za določene sektorje (npr. zdravstvo) naj intervencije poudarijo poklicno etiko in družbene norme za spodbujanje varnega vedenja. Programi naj prav tako spremljajo odnos zaposlenih in ravni družbenega vpliva, da se usposabljanja ustrezno prilagodijo.
    - Uporabite anonimne ankete za merjenje dojemanja zaposlenih varnostne kulture, družbenih norm in vedenja sodelavcev glede varnostnih praks. Na podlagi povratnih informacij prilagodite kampanje ozaveščanja, da odpravite vrzeli, kot je npr. pomanjkanje odgovornosti med sodelavci.
    - Na skupinskih srečanjih spodbujajte krepitev informacijskovarnostne kulture s primeri dobrih praks zglednega varnostnega vedenja zaposlenih. Nagrajujte oddelke, ki dosledno in pravočasno zaključujejo varnostna usposabljanja z manjšimi spodbudami ali pohvalami na sestankih širšega vodstva.

- **Spodbujanje medosebnega zaupanja:** Ustvarite zaupanje med zaposlenimi preko platform, ki spodbujajo interakcijo in sodelovanje, kar lahko okrepi spoštovanje varnostnih praks.
    - Razvijte interno platformo ali forum, kjer lahko zaposleni delijo svoje skrbi in dobre prakse glede varnosti. Spodbujajte oddelke k sodelovanju in izmenjavi izkušenj glede varnosti, na četrtletnih sestankih.

- Uporabljajte platforme za sodelovanje (npr. Teams, Slack), za spodbujanje odprtega dialoga o informacijski varnosti. Ustvarite posebne kanale, kjer lahko zaposleni prijavijo sumljive aktivnosti, delijo znanje in zastavljajo vprašanja o informacijski varnosti v varnem in sodelovalnem okolju.
- Vzpostavite anonimne in varne kanale kjer lahko zaposleni prijavijo skrbi glede varnosti brez strahu pred povračilnimi ukrepi. Te kanale promovirajte prek opomnikov po elektronski pošti in med usposabljanji.
- Ne kaznujte zaposlenih za prijave incidentov, ki se izkažejo kot neobstoječa grožnja. To spodbuja kulturo, kjer se varnostni pomisleki obravnavajo brez strahu pred sankcijami. Izogibajte se sistemom obtoževanja ali kaznovanja zaposlenih, saj to negativno vpliva na varnostno kulturo. Varnostni pomisleki in napake naj se obravnavajo brez strahu pred sankcijami. Zavzemajte se za konstruktivno reševanje pomislekov, skrbi in napak v zvezi z informacijsko varnostjo z osredotočanjem na učenje in izboljšave, kar krepi zaupanje in varnostno kulturo.
- Prepoznajte in nagrajujte zaposlene, ki izkazujejo varnostno ozaveščena vedenja in s tem krepite njihovo zavzetost in zavezanost informacijski varnosti.

- **Spodbujanje individualne odgovornosti:** Spodbujajte odgovorno uporabo informacijsko-komunikacijskih tehnologij kot so računalniki, pametni telefoni, tablice in druge naprave. Usposabljajte zaposlene ne le o tem, kako uporabljati varnostna orodja, temveč tudi zakaj so ta orodja ključna za njihovo vlogo pri zaščiti organizacijskih podatkov. Spodbujajte uporabo pristopov, ki povezujejo tehnološke nadzorne ukrepe (npr. šifriranje, nadzor dostopa) z resničnimi situacijami, s katerimi se zaposleni srečujejo, ter jasno prikazujejo povezavo med tehnologijo in človeško odgovornostjo.

- **Motiviranje varnostnih ambasadorjev:**
  - Prepoznajte in usposabljajte t. i. "varnostne ambasadorje" v vsakem oddelku, ki naj bodo odgovorni za spodbujanje varnostnih praks, odgovarjanje na vprašanja in poročanje o morebitnih varnostnih težavah. Vsak mesec izvedite srečanja z njimi, da pridobite povratne informacije in zagotovite, da aktivno angažirajo zaposlene.
  - Določite varnostne ambasadorje, ki so usposobljeni za osnovne varnostne prakse in služijo kot stična točka oddelku, v katerem delujejo. Spodbujajte jih, da delijo to znanje med timskimi sestanki.

3) INTEGRACIJA TEHNOLOŠKIH REŠITEV V ORGANIZACIJSKO KULTURO

- **Integracija tehnologije in kulture:** Bistveno je zmanjšati neskladje med varnostnimi protokoli in obstoječimi vzorci ravnanja zaposlenih in njihovimi prepričanji. Prilagodite varnostno tehnologijo, da se ujema z obstoječim potekom dela in komunikacijskimi vzorci v organizaciji. Na primer, uvedite varna orodja za sodelovanje, ki izboljšajo, ne pa motijo, že uveljavljene prakse v timih, ter spodbujajo varnost na način, ki je naraven in ne obremenjujoč.
    - Dovolj zgodaj vključite zaposlene: vključite zaposlene v razpravo o uvajanju določenih rešitev, še preden jih uvedete. Zberite povratne informacije o njihovem načinu dela in identificirajte morebitne točke trenja v njihovih vsakodnevnih rutinah.
    - Prilagodite uvedbo: prilagodite uvedbo rešitve čim bolj gladko. Na primer, integrirajte MFA v obstoječa orodja za sodelovanje (kot sta Slack ali Teams), ki jih zaposleni že uporabljajo, tako da se dodaten varnostni korak zdi naraven in ne prisiljen.
    - Ponudite prilagodljivost: zagotovite možnosti, ki so v skladu z željami zaposlenih, na primer možnost, da izbirajo med različnimi metodami. S tem se spoštuje delovne navade zaposlenih, hkrati pa ohranja močno varnost.
    - Komunicirajte jasno, enostavno in upoštevajoč odnose med zaposlenimi: predstavite prednosti rešitve v skladu s kulturo sodelovanja v organizaciji. Na primer, razložite, kako določen ukrep ščiti ne le posamezne račune, ampak skupna prizadevanja celotne organizacije pred kibernetskimi grožnjami.

- **Premostitev vrzeli med tehnologijo in vedenjem:**
    - Zagotovite, da so varnostna orodja (npr. zaznavanje *phishinga*, platforme za varen dostop) uporabniku prijazna in da jih zaposleni dobro razumejo. To je mogoče doseči z vključitvijo povratnih informacij zaposlenih v izbiro in uporabo tehničnih orodij, s čimer zagotovite, da podpirajo širšo varnostno kulturo, namesto da ustvarjajo trenja.

- **Spremljanje in analitika:** Uvedite tehnološka orodja, ki omogočajo spremljanje informacijskovarnostne kulture, kot so sistemi, ki spremljajo angažiranost zaposlenih z varnostnimi protokoli in učinkovitosti usposabljanj.
    - Uporabite avtomatizirane varnostne nadzorne plošče za sledenje angažiranosti zaposlenih z varnostnimi protokoli (npr. odziv na simulacije *phishinga*, posodobitve gesel).
    - To dopolnite z izvedbo letne ankete za merjenje varnostne kulture v organizaciji, pri čemer primerjajte rezultate s sistemskimi podatki, da ocenite učinkovitost varnostnih usposabljanj.

- Uporabite metrike za sledenje zrelosti varnostne kulture, vključno z angažiranostjo zaposlenih pri usposabljanju, spoštovanjem varnostnih politik in pogostostjo prijav incidentov.
- Uvedite platforme, ki omogočajo anonimno prijavo skrbi zaposlenih glede informacijske varnosti, da spodbudite transparentnost in zgodnje odkrivanje tveganj.
- Redno pregledujte varnostne prakse preko notranjih ali zunanjih ocen, da prepoznate vrzeli in področja za izboljšave.

4) IMPLEMENTACIJA SOCIO-TEHNIČNE PERSPEKTIVE ZA NENEHNO IZBOLJŠAVO IN PRILAGAJANJE

- **Holistično razumevanje tehnologije kot socio-tehničnega sistema:** Implementirajte modele, ki upoštevajo tako tehnične kot družbene elemente informacijske varnosti. Ta pristop zagotavlja, da so varnostni sistemi usklajeni z načinom delovanja in interakcije ljudi v organizaciji.
    - Zgradite socio-tehnični varnostni okvir z vzpostavitvijo interdisciplinarne varnostne ekipo, ki vključuje tako IT strokovnjake kot tudi netehnične zaposlene (npr. sodelavci iz kadrovske službe, marketinga). Ekipa naj se srečuje mesečno, da razpravlja o interakciji med človekom in tehnologijo v organizaciji ter predlaga spremembe varnostnih praks na podlagi povratnih informacij netehničnih uporabnikov.

- **Povratne zanke:** Vzpostavite iterativne mehanizme, kjer se povratne informacije zaposlenih uporabljajo za izboljšanje varnostnih politik in praks. To ustvarja bolj dinamično in prilagodljivo informacijskovarnostno kulturo.
    - Vzpostavite četrtletne fokusne skupine, da zberete povratne informacije o učinkovitosti trenutnih varnostnih praks. Te vpoglede uporabite za izpopolnjevanje programov usposabljanja, politik in tehničnih ukrepov. Spremljajte spremembe skozi čas in prilagodite strategije na podlagi povratnih informacij.
    - Uvedite sistem nenehnega zbiranja povratnih informacij, kjer lahko zaposleni delijo svoja izkustva in izzive z varnostnimi protokoli prek anonimnih anket ali fokusnih skupin. Te povratne informacije uporabite za izboljšanje programov usposabljanja varnosti in tehničnih ukrepov.
    - Nenehno izpopolnjujte in prilagajajte varnostne cilje in metode na podlagi znanj, pridobljenih iz prejšnjih iniciativ. Uskladite strategije z aktualnim okoljem groženj in najboljšimi praksami.
    - Po vsakem varnostnem ukrepu (npr. novem programu usposabljanja ali spremembi politik) preglejte rezultate in prilagodite strategije, tako da rešite težave ali izkoristite uspehe.

- **Integracija kulture na več ravneh:** Zavedajte se, da informacijskovarnostna kultura deluje na več ravneh, od ravni posameznika do ravni skupine, organizacije in države. Pobude bi morale obravnavati vse te razsežnosti za spodbujanje močne informacijskovarnostne kulture.
    - Izvedite letno medoddelčno raziskavo, ki meri odnos zaposlenih do informacijske varnosti na ravni posameznika, skupine in organizacije. Na podlagi teh rezultatov razvijte prilagojene intervencije, kot so ciljno usmerjene delavnice za oddelke, ki kažejo nizko vključenost v varnostne protokole.
    - Izvedite četrtletne zelo kratke ankete, ki merijo ozaveščenost in odnos zaposlenih do varnosti. Na podlagi rezultatov organizirajte prilagojene delavnice za oddelke, ki dosegajo nižje rezultate pri meritvah, da odpravite specifične vrzeli v posamičnih

vidikih informacijskovarnostne kulture (npr. znanju, vedenju, stališčih, občutku odgovornosti).

- **Spodbujanje kulture tehnološkega prilagajanja**: Spodbujajte odprtost do novih tehnologij z ustvarjanjem okolja, v katerem se zaposleni počutijo udobno pri sprejemanju novih orodij in prilagajanju nanje. Redno zbirajte povratne informacije o tem, kako dobro se tehnologija integrira z vsakodnevnimi nalogami, in prilagodite strategije na podlagi teh povratnih informacij, da zagotovite ravnotežje med potrebami po varnosti in produktivnostjo zaposlenih.

5) METODA

V analizo literature je bilo vključenih 23 znanstvenih člankov in 20 strokovnih besedil, ki obravnavajo informacijsko varnostno kulturo (IVK) v organizacijah, objavljenih med leti 2020 in 2024.

Relevantni znanstveni članki so bili izbrani za analizo glede na kriterije:

- Članki so objavljeni v angleškem jeziku;
- Članki se nanašajo in pokrivajo temo informacijskovarnostne kulture v organizacijah ("*information security culture*") in sorodnih terminov (kot so kultura kibernetske varnosti oz. "*cybersecurity culture*" in varnostna kultura oz. "*security culture*");
- Članki vključujejo uporabna priporočila za spremembo ali izboljšanje IVK ali njenih posamičnih dimenzij.

Izvedeni sta bili dve ločeni poizvedbi za iskanje ustrezne znanstvene literature. Obe sta bili izvedeni na portalih Web of Science in Scopus, ki predstavljata največji in najbolj prepoznani bazi znanstvenih publikacij. Izvedlo se je iskanje po različnih ključnih besedah z namenom identifikacije čim večjega števila različnih člankov. Uporabljena je bila poizvedba s ključnimi besedami: "*security culture*" OR "*information security culture*" OR "*cybersecurity culture*".

Pri prvi poizvedbi je bil pri identifikaciji člankov poleg ključnih besed vključen tudi kriterij števila citiranj posameznega vira v drugih znanstvenih publikacijah. Iskanje je bilo izvedeno med julijem in avgustom 2024 in je vključevalo članke, objavljene med januarjem 2020 in avgustom 2024. Rezultati so bili razvrščeni in identificirani glede na število citiranj posameznega vira v drugih znanstvenih virih. Pregledani so bili tudi seznami virov izbranih člankov, za potencialno identifikacijo dodatnih relevantnih virov. Na ta način je bilo izbranih 12 najbolj ustreznih člankov, ki so ustrezali kriterijem in so bili največkrat citirani v drugih virih.

Druga poizvedba je vključevala enake ključne besede, identificirane članke pa smo razvrstili po datumu objave, kjer so v poštev prišli najnovejši članki. Drugo iskanje se je izvedlo z namenom pridobivanja najnovejših in aktualnih informacij in ugotovitev na področju upravljanja informacijskovarnostne kulture. V drugem iskanju je bilo tako izbranih in analiziranih 11 znanstvenih člankov. V primeru, da je bil članek identificiran že v prvi poizvedbi, se ta članek tu ni upošteval.

Po identifikaciji znanstvenih virov je sledila analiza besedil in identifikacija posameznih priporočil za izboljšanje IVK ali njenih posamičnih dimenzij v organizacijah. Identificiralo se je tudi, če se posamično priporočilo nanaša na specifičen tip organizacije (npr. zdravstvo), ali pa ta ni bil eksplicitno naveden.

Identifikacija strokovnih besedil za izluščenje in analizo priporočil je potekala preko spletnega iskanja, pri čemer so bila besedila izbrana na osnovi naslednjih kriterijev:

- Poročila so objavljena v angleškem ali slovenskem jeziku;
- Poročila se nanašajo na temo informacijskovarnostne kulture ("*information security culture*") v organizacijah in njenih sorodnih terminov kot so kultura kibernetske varnosti

("*cybersecurity culture*"*)* in varnostna kultura ("*security culture*") ter na temo izboljšanja človeškega dejavnika informacijske varnosti ("*human factor of information security*") v organizacijah.

Iskanje je bilo izvedeno na Google iskalniku. Zraven ključnih besed so poizvedbe iskanja vključevale pojme, povezane s priporočili, kot so "*how to change*" (kako spremeniti), "*how to improve*" (kako izboljšati) in "*recommendations for improving*" (predlogi za izboljšanje). Iskanje se je izvedlo v slovenskem in angleškem jeziku. Primerna poročila so se identificirala po prej naštetih kriterijih, letu objave (izbor glede na razvrstitev po datumu objave) ter prepoznavnosti in kvaliteti medija, na katerem je bilo poročilo objavljeno. Iskala so se poročila s čim bolj raznolikimi priporočili. Poročila, ki so imela priporočila podobna ali enaka ostalim, so bila izključena. Na tak način se je identificiralo 20 strokovnih poročil, objavljenih med decembrom 2022 in avgustom 2024. Na izbranih poročilih se je izvedla analiza besedila, tako da smo izluščili priporočila za izboljšanje IVK ali njenih posamičnih dimenzij v organizacijah.

Skupaj so tako v pregledu literature analizirana priporočila za izboljšanje IVK v organizacijah ali človeškega faktorja IVK v organizacijah iz 43 različnih virov; od tega 23 znanstvenih člankov in 20 strokovnih poročil.

6) ZNANSTVENI VIRI

AlGhanboosi, B., Ali, S. in Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. *Computers in Human Behavior*, *144*(2). https://doi.org/10.1016/j.chb.2023.107702

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*(2). https://doi.org/10.1016/j.cose.2020.102003

Chen, H. in Hai, Y. (2024). Exploring the critical success factors of information security management: a mixed-method approach. *Information and Computer Security*, *5*, str. 545–572 . https://doi.org/10.1108/ICS-03-2023-0034

Choi, H., Park, S. in Kang, J. (2024). Enhancing participatory security culture in public institutions: An analysis of organizational employees' security threat recognition processes. *IEEE Access*, *12*, str. 47543–47558. https://doi.org/10.1109/ACCESS.2024.3383311

Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L. in Deibert, R. (2020). The information security cultures of journalism. *Digital Journalism*, *8*(8), str. 1068–1091. https://doi.org/10.1080/21670811.2020.1777882

Da Veiga, A. (2023). A model for information security culture with creativity and innovation as enablers – refined with an expert panel. *Information and Computer Security*, *31*(3), str. 281–303. https://doi.org/10.1108/ics-11-2022-0178

Dornheim, P. in Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information and Computer Security*, *32*(2), str. 179–196. https://doi.org/10.1108/ics-07-2023-0116

Georgiadou, A., Psarrou, A. M. in Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security*, *129*. https://doi.org/10.1016/j.cose.2023.103199

Hassandoust, F. in Johnston, A. C. (2023). Peering through the lens of high-reliability theory: A competencies driven security culture model of high-reliability organisations. *Information Systems Journal*, *33*(5), str. 1212–1238. https://doi.org/10.1111/isj.12441

Hoppe, F., Gatzert, N. in Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *Journal of Risk Finance*, *22*(3/4), str. 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Karlsson, M., Karlsson, F., Åström, J. in Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*, *30*(3), str. 382–401. https://doi.org/10.1108/ICS-06-2021-0073

Lin, C., Wittmer, J. L. in Luo, X. (2022). Cultivating proactive information security behavior and individual creativity: The role of human relations culture and IT use governance. *Information & Management*, *59*(6), str. 1–13. https://doi.org/10.1016/j.im.2022.103650

Mikuletič, S., Vrhovec, S., Skela-Savič B. in Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computer Security*, *136*(2). https://doi.org/10.1016/j.cose.2023.103489

Murray, G., Falkeling, M. in Gao, S. (2024). Trends and challenges in research into the human aspects of ransomware: a systematic mapping study. *Information & Computer Security.* https://doi.org/10.1108/ICS-12-2022-0195

Owusu Kwateng, K., Amanor, C. in Tetteh, F. K. (2022). Enterprise risk management and information technology security in the financial sector. *Information and Computer Security*, *30*(3), str. 422–451. https://doi.org/10.1108/ICS-11-2020-0185

Palanisamy, R., Norman, A. A. in Kiah, L. M. (2023). Employees' BYOD Security policy compliance in the public sector. *Journal of Computer Information Systems*, *64*(1), str. 1–16. https://doi.org/10.1080/08874417.2023.2178038

Sharma, S. in Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, *120*. https://doi.org/10.1016/j.cose.2022.102774

Solomon, G. in Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), str. 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217

Tejay, G. P. in Mohammed Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3). https://doi.org/10.1016/j.im.2022.103751

Tenzin, S., McGill, T. in Dixon, M. (2024). An Investigation of the factors that influence information security culture in government organizations in Bhutan. *Journal of Global Information Technology Management*, *27*(1), str. 37–62. https://doi.org/10.1080/1097198X.2023.2297634

Uchendu, B., Nurse, J. R., Bada, M. in Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*. https://doi.org/10.1016/j.cose.2021.102387

Wong, WP., Tan, K.H., Govindan, K., Li, D. in Kumar, A. (2023). A conceptual framework for information-leakage-resilience. *Annals of Operations Research*, *329*(1), str. 931–951. https://doi.org/10.1007/s10479-021-04219-5

Zyoud, B. in Lebai L. S. (2024). The role of information security culture in zero trust adoption: Insights from UAE organizations. *IEEE Access*, *12*, str. 72420–72444. https://doi.org/10.1109/ACCESS.2024.3402341

7) STROKOVNI VIRI

BARR Advisory. (2024, 8. januar). *How to implement an information security program in 9 steps.* https://www.barradvisory.com/resource/how-to-implement-an-information-security-program-in-9-steps-2/

Brother Nordics. (2024, 24. april). *Human factors: How can you build a robust cyber security culture?* https://www.brother.is/business-solutions/resource-hub/blog/security/2024/human-factor-as-security-threat

Calderon, D. (2023, 23. avgust). *Building a strong security culture for resilience and digital trust*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/building-a-strong-security-culture-for-resilience-and-digital-trust

Carpenter, P. (2024, 20. junij). *What happens when an organization suffers from a poor security culture?* Forbes Business Council. https://www.forbes.com/councils/forbesbusinesscouncil/2024/06/20/what-happens-when-an-organization-suffers-a-poor-security-culture/

Coursera (2023, 14. december). *9 cybersecurity best practices for businesses in 2024*. https://www.coursera.org/articles/cybersecurity-best-practices?utm_medium=sem&utm_source=gg&utm_campaign=B2C_EMEA__coursera_FTCOF_career-academy_pmax-multiple-audiences-country-multi&campaignid=20858198824&adgroupid=&device=c&keyword=&matchtype=&network=x&devicemodel=&adposition=&creativeid=&hide_mobile_promo&gad_source=1&gclid=CjwKCAjwxNW2BhAkEiwA24Cm9Jkl7DqHxf15kltswKZZ0Jkw3PIL9ZmHXUAkmJFvtGPUSsnr2k6E7hoCWPgQAvD_BwE

Durbin, S. (2024, 14. avgust). *Strategies for security leaders: Building a positive cybersecurity culture*. Help Net Security. https://www.helpnetsecurity.com/2024/08/20/cybersecurity-culture-strategies/

Friel, D. (b. d.). *Effective strategies to minimise cyber security risk*. MetaCompliance. https://www.metacompliance.com/blog/cyber-security-awareness/cyber-security-risk

Gallant, B. (2023, 29. april). *Creating a cyber security culture.* LinkedIn. https://www.linkedin.com/pulse/creating-cyber-security-culture-brett-gallant/

Hamayun, M. (2023, 20. november). *The human factor of cyber security* [blog]. https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/

Hart, J. (2023, 15. september). *How To cultivate a thriving security culture*. Forbes Technology Council. https://www.forbes.com/councils/forbestechcouncil/2023/09/15/how-to-cultivate-a-thriving-security-culture/

Hofmann, S. (2024, 24. januar). *The ultimate guide to a strong security culture* [blog]. https://www.cyberpilot.io/cyberpilot-blog/the-ultimate-guide-to-a-strong-security-culture

LinkedIn community. (b. d.). *How can you address the human factor in data security risks?* LinkedIn. https://www.linkedin.com/advice/1/how-can-you-address-human-factor-data-security

Murphy, J. (2024, 29. marec). *5 tips for building a cybersecurity culture at your company*. TechTarget Security. https://www.techtarget.com/searchsecurity/tip/5-tips-for-building-a-cybersecurity-culture-at-your-company

Nuñez, C. (2022, 15. december). *How to embed Gen Z in your organization's security culture*. Security Intelligence. https://securityintelligence.com/x-force/gen-z-cybersecurity-culture/

Phinsec. (b. d.). *Top 10 tips for minimizing human vulnerability* [blog]. https://www.phinsec.io/blog/top-10-tips-for-minimizing-human-vulnerability

Pryimenko, L. (2024, 20. februar). *12 cybersecurity best practices to prevent cyber attacks in 2024.* Ekran System. https://www.ekransystem.com/en/blog/best-cyber-security-practices

SaltyCloud. (2024, 5. februar). *Growing an information security culture*, *complete guide*. https://www.saltycloud.com/blog/growing-an-information-security-culture-complete-guide/

Security Mentor. (b. d.) *Tips to improve your organization's security culture.* https://blog.securitymentor.com/tips-to-improve-your-organizations-security-culture

Spivey, T. (2023, 30. november). *How to create a healthy security culture*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/how-to-create-a-healthy-security-culture?gad_source=1&gclid=CjwKCAjwuMC2BhA7EiwAmJKRrFy4sl13M6NsgW1nebL7KNKoCltMLb5lQxaV_kSGXc39xP7vlWdp4RoCrnUQAvD_BwE

Yacono, L. (2023, 21. februar). *4 ways to mitigate the human factors of cyber security* [blog]. https://www.cimcor.com/blog/3-ways-to-mitigate-the-human-factors-of-cyber-security