■ *Pregledni znanstveni članek*

Samanta Mikuletič, Brigita Skela Savič

Informacijska varnostna kultura v zdravstvu – sistematični pregled literature

Povzetek. Kršitve na področju varovanja podatkov največkrat izhajajo iz kraje ali izgube podatkov, nepooblaščenih dostopov, razkritja in vdiranja. Zaradi strahu pred razkritjem lahko pacient ne poda natančne anamneze, saj bi razkritje podatkov lahko povzročilo socialno stigmo in diskriminacijo. Močna informacijska varnostna kultura pripomore k učinkovitejšemu soočanju z varnostmi tveganji. Gre za niz značilnosti varovanja informacij in eno od vrednot organizacije, ki jo razvijejo zaposleni. Preko informacijske varnostne kulture se razvijejo norme, stališča in vedenja. Izvedli smo sistematičen pregled literature na to temo. Uporabili smo naslednje ključne besede: informacijska varnostna kultura, informacijska varnost, varovanje podatkov, zdravstveni podatki/pacientovi podatki in zdravstvo/zdravstveni delavci. V podatkovnih zbirkah DiKul, COBIB.SI, CINAHL, MEDLINE in ProQuestDissertations & Theses Global smo iskali slovenske in angleške znanstvene raziskave, objavljene od leta 2008 do leta 2018. Iskalni nabor je dal 1457 zadetkov. V končno analizo je bilo vključenih 6 raziskav. Identificirali smo 40 kod in 4 glavne kategorije: varnostna praksa, znanje/usposabljanje/izkušnje, zavedanje/odnos/stališče in dejavniki tveganja/zaupanje. Pregled je pokazal, da obstaja vrzel v odnosu in stališčih in da imajo različne poklicne skupine zdravstvenih delavcev različen pristop do varovanja informacij. Organizacije razmeroma malo ali skoraj nič ne vlagajo v izobraževanje zaposlenih in tako posledično ne razvijajo potrebne informacijske varnostne kulture.

Information Security Culture in Health Care – a Systematic Review

Abstract. Data protection violations mostly result from theft or loss of data, unauthorized data access, disclosure and security breaches. Due to the fear of disclosure, the patient may not give a detailed anamnesis, as the disclosure of the data could lead to social stigma and discrimination. A strong information security culture contributes to more effective management of security risks. It is reflected in information security characteristics and represents one of the organisational values developed by the employees. In order to achieve good information security, norms, positions and knowledge should be developed. A literature review and thematic synthesis were performed on this topic. We used the following keywords: information security culture, information security, data protection/data security, health data/patient data, and healthcare/healthcare professionals. The COBIB.SI, CINAHL, MEDLINE, ProQuest Dissertations & Theses Global, and DiKul databases were searched for scientific publications in Slovene and English from 2008 to 2018. Among the 1457 hits, six studies were included in the final analysis. We identified 40 codes and 4 main categories: security practice; knowledge, training, experience; awareness, behaviour and risk factors, trust. The review showed that there are differences in attitudes of different professional groups and that different health professional have a different approach to protecting information. Health organizations do not invest enough into education of their employees, and do not develop a good information security culture.

■ **Infor Med Slov** 2018; 23(1-2): 26-33

Institucija avtoric / Authors' institution: Fakulteta za zdravstvo Angele Boškin, Jesenice.

Kontaktna oseba / Contact person: Samanta Mikuletič, mag. zdr. nege, Fakulteta za zdravstvo Angele Boškin, Spodnji Plavž 3, 4270 Jesenice. E-pošta / E-mail: samanta.mikuletic@gmail.com.

Prispelo / Received: 4. 10. 2018. Sprejeto / Accepted: 21. 12. 2018.

Uvod

Informacijska varnostna kultura je »duša« organizacije in jo razumemo kot predpostavko o tem, kaj v zvezi z informacijsko varnostjo je spremenljivo in kaj ni. Pojem informacijske varnosti je povezan z preprečevanjem nepooblaščenega ali neželenega uničenja, spreminjanja, naključne ali namerne uporabe informacijskih virov. Informacijska varnostna kultura zajema socialne, kulturne in etične ukrepe za izboljšanje varnostnega ravnanja zaposlenih in velja za subkulturo organizacijske kulture. Vzpostavitev kulture varnosti informacij je nujna za učinkovito informacijsko varnost.[1]

Razvoj informacijske varnosti

Razvoj informacijske varnosti je potekal v več valovih – doslej v štirih in trenutno se nahajamo v petem. Prvi ali *tehnični val* se je začel v osemdesetih letih 20. stoletja in je zajemal predvsem tehnična vprašanja informacijske varnosti. Z razvojem interneta je nastopil drugi ali *menedžerski val*. Organizacije so se začele zavedati pretečih se nevarnosti in dale večji pomen varnosti. Začele so oblikovati varnostne politike in postopke. Tretji, *institucionalni val* se je začel v devetdesetih letih 20. stoletja. Nakazal je potrebe po določenih oblikah standardizacije, merjenja in nadzora informacijske varnosti. Takrat se je začel razvoj informacijske varnostne kulture. Četrti ali *upravljavski val* se je začel leta 2000 s poudarkom na področju upravljanja informacijske varnosti. V petem valu ali *kibernetskem valu* se nahajamo danes. Osredotoča se na zaščito računalnikov in računalniške opreme pred nepooblaščenim dostopom.[2,3,4]

Tehnični in ne-tehnični vidik zagotavljanja varovanja informacij

Pri zagotavljanju varnosti informacijskih virov so tehnološke metode (požarni zidovi in gesla) varovanja informacij učinkovite do določene mere. Ne-tehnična vprašanja so enako pomembna kakor tehnična. Tehnični varnostni nadzor je potrebno natančno določiti, oblikovati, razviti, implementirati, konfigurirati in vzdrževati, za kar je v prvi vrsti pomemben človek.[5]

Merjenje informacijske varnostne kulture

Orehek[6] je z meta-analizo ugotavljala obstoj in kakovost merskih instrumentov za merjenje informacijske varnostne kulture. Kakovostnih vprašalnikov, veljavnih in zanesljivih, ki naj bi merili ta koncept, ni, obstaja pa več merskih instrumentov, ki merijo sorodne koncepte. Pri tem navaja, da se z anketnim merjenjem informacijske varnostne kulture ukvarja le peščica raziskovalcev iz Južne Afrike, Avstralije in Azije, ter da je v evropskem prostoru čutiti primanjkljaj.[6]

Faktorji, ki vplivajo na informacijsko varnostno kulturo za področje zdravstva

Kršitve varnosti zdravstvenih informacij imajo pomemben vpliv na paciente in na zdravstvene organizacije. Noor in Zuraini[7] sta razvila konceptualni model faktorjev, ki vplivajo na informacijsko varnostno kulturo za področje zdravstva. Izpostavila sta jih šest: vedenje zaposlenih, upravljanje sprememb, informacijsko varnostno zavedanje, varnostna priporočila, organizacijski sistem in znanje.[7]

Zlorabe zdravstvenih podatkov

V ZDA je o zlorabah podatkov poročalo 43 % zdravstvenih organizacij. Preučevanje incidentov kaže na pomembnost človeškega dejavnika pri zagotavljanju varovanja informacij. Zdravstveni sektor je izpostavljen kot najranljivejši glede stroškov razkritih zapisov.[8] Od leta 2009 do 2013 je število zabeleženih kršitev v ZDA doseglo 27 milijonov. Oddelek za zdravstvo in državljanske storitve (US Department of Health and Human Services) na spletnem portalu redno objavlja kršitve, povezane z varovanje zdravstvenih informacij. Viri razkritja so računalniški sistemi in omrežja, osebni računalniki, prenosni računalniki, podatki na papirju, elektronska pošta, elektronski zdravstveni zapisi in prenosne naprave (CD-ji, USB-ji, rentgenske slike).[9] V Sloveniji tovrstne analize izvaja skupina SI-CERT, ki deluje v okviru akademske raziskovalne mreže Arnes. Poročilo o omrežni varnosti kaže, da se vsak dan v letu v Sloveniji v povprečju prijavi 11 incidentov. Arnes veliko prizadevanj vlaga v ozaveščanje javnosti preko projektov, kot sta »Varni na internetu« in »Safe.si«.[10]

Posebnost zdravstvenega sektorja je zasebnost obravnav ter načelo odnosa med pacientom in zdravstvenim osebjem. Zaradi strahu pred razkritjem podatkov lahko pacient ne poda natančne anamneze (duševne bolezni, HIV ipd.), saj bi razkritje teh podatkov lahko povzročilo socialno stigmo in diskriminacijo.[11]

Namen in cilj

Namen raziskave je bil s sistematičnim pregledom literature preučiti koncept informacijske varnostne kulture v zdravstvu in možne metodološke pristope, ki so bili uporabljeni pri raziskovanju tega koncepta. Cilj pregleda je bil opredeliti komponente koncepta ter iz obstoječih raziskave povzeti, kaj so razlogi za

neupoštevanje informacijske varnosti in koliko je le-ta poznana med zdravstvenim osebjem.

Metode

Najprej smo razvili *Protokol sistematičnega pristopa k pregledu literature*, povzet po Booth in sod.[12] Analizo podatkov smo izvedli po metodi tematske integrativne analize. Gre za kvalitativno vsebinsko analizo rezultatov dveh ali več primarnih kvalitativnih in kvantitativnih raziskav, pri kateri se lahko uporabi dve ali več iskalnih strategij. Tovrstna analiza je ustvarjalna, a kritična, in je ključna za prepoznavanje in primerjanje pomembnih vzorcev in tem. Uporablja najširšo vrsto raziskovalnih metod, ki omogočajo vključitev eksperimentalnih in neeksperimentalnih raziskav, vse z namenom, da bi bolje razumeli raziskovalni problem.[12]

Metode pregleda literature

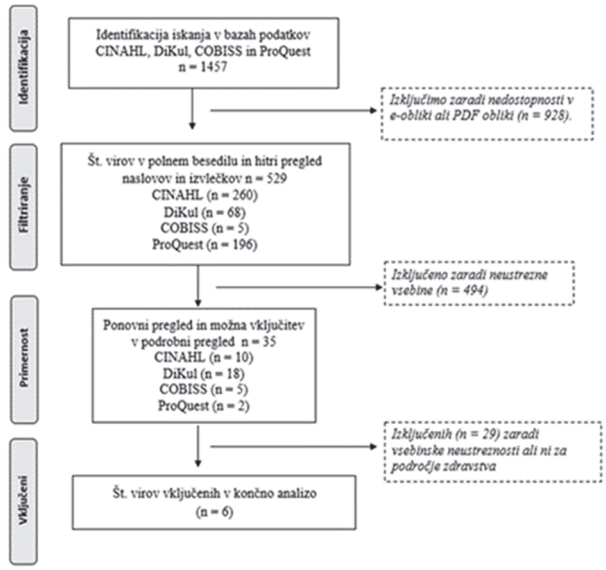
S pomočjo odgovorov na vprašanja PICO smo tvorili ključne besede: informacijska varnostna kultura (angl. *information security culture*), informacijska varnost (angl. *information security*), varovanje podatkov (angl. *data protection / data security*), zdravstveni podatki / pacientovi podatki (angl. *health data / patient data*) in zdravstvo / zdravstveni delavci (angl. *helathcare / helathcare professionals*). Ključne besede smo z uporabo Boolovimih operatorjev AND, OR in NOT združevali v iskalne nize v različnih elektronskih bibliografskih podatkovnih zbirkah. Iskali smo v zbirkah COBIB.SI, DiKul, CINAHL in ProQuest. Zadetke smo zožili z omejitvenimi kriteriji: obdobje objave (od 2010 do 2018), angleški in slovenski jezik, znanstvene revije, doktorske disertacije in magistrska dela dostopna v obliki PDF. V pregled smo vključili randomizirane in nerandomizirane kvantitativne in kvalitativne raziskave.

Potek pregleda

Skupno smo v podatkovnih zbirkah identificirali 1457 zadetkov (slika 1). Izbranih zadetkov za pregled v polnem besedilu in morebitno vključitev v rezultate je bilo 35. V končni pregled literature smo vključili 6 raziskav. Uporabili smo metodo PRISMA – mednarodni standard za prikaz rezultatov pregleda literature.

Ocena kakovosti pregleda

Izbor literature je temeljil na aktualnosti, vsebinski ustreznosti in dostopnosti virov. Oceno kakovosti pregleda smo podali na podlagi hierarhije dokazov v znanstveno raziskovalnem delu.[13] Izbrane raziskave za smo analizirali v skladu s smernicami STROBE in COREQ.



Slika 1 Diagram PRISMA (potek iskanja, pregleda in vključenosti virov).

Obdelava podatkov iz pregleda literature

Uporabili smo deskriptivno metodo in metodo tabeliranja. Podatke smo obdelali s tematsko integrativno analizo. Kvalitativno sintezo smo naredili na podlagi znanstvenih vsebin, ki smo jih kodirali in kasneje združili po kategorijah. Pred analizo vsebine izbranih raziskav smo zbrali podatke o značilnosti vsake posamezne raziskave (avtorji, država, raziskovalni načrt, vzorčenje, raziskovalni instrument, preučevane spremenljivke, ključne ugotovitve).

Rezultati

V končni pregled literature smo vključili šest raziskav, ki se navezujejo na obravnavano tematiko (tabeli 1 in 2).

Tabela 1 Raziskave, vključene v končni pregled.

Avtorji	Leto objave	Država
Gebrasilase in Lessa[14]	2011	Etiopija
Kwon in Johnson[15]	2013	ZDA
Agaku, Ayo-Yusuf in Connoly[16]	2014	ZDA
He in Johnson[17]	2017	Kitajska
Noor idr.[18]	2017	Malezija
Božić[19]	2016	Slovenija

Skupno smo identificirali 40 kod, ki smo jih glede na lastnosti in medsebojno povezanost združili v štiri vsebinske kategorije (tabela 3).

Tabela 3 Povzetek rezultatov.

Raziskava	Namen raziskave	Raziskovalni načrt	Vzorec in metoda vzorčenja	Raziskovalni instrument	Proučevane spremenljivke	Ključne ugotovitve
Gebrasilase & Lessa, 2011, Etiopija[14]	Izboljšati prakso varovanja informacij in identificirati dejavnike, ki vplivajo na informacijsko varnostno kulturo v bolnišnici Hawassa.	Mešani raziskovalni načrt. Izvedba ankete, poglobljenih intervjujev in pregled/analiza dokumentov.	564 enot (zdravniki, medicinske sestre, laboranti, farmacevti, študenti, administratorji in drugi zaposleni, ki prihajajo v stik z zdravstvenimi podatki). Najprej startificiran vzorec, nato tehnika enostavnega naključnega vzorčenja (tehnika loterije).	Uporabili so obstoječ vprašalnik za oceno informacijske kulture, ki je bil preveden v amharsko različico.	Znanje, odnos, prepričanje, ukrepi, ki se jih poslužujejo zaposleni v zvezi z informacijsko varnostno kulturo.	Zaznano pomanjkanje zavesti med zaposlenimi, pomanjkanje zavezanosti in podpore vodstva za delovanje in izvajanje informacijske varnosti. Odsotnost ozaveščenosti je najverjetneje posledica odsotnosti usposabljanja. Ozaveščenosti lahko ovira vodstvo, premalo sredstev za izvajanje informacijske varnosti. Večina zaposlenih nikoli ni bila na usposabljanju.
Kwon & Johnson, 2013, ZDA[15]	Preučiti varnost pacientovih podatkov v zdravstvenih ustanovah v ZDA.	Randomizirana kvantitativna raziskava. Izveden t-test, faktorska analiza, diskriminantna analiza, preverjena zanesljivosti in veljavnosti konstrukta.	Iz vsake od 250 bolnišnic so izbrali po eno osebo, (upravljavci IT oddelkov, direktorji IT, glavni varnostni akterji). Zaradi manjkajoči vrednosti so iz vzorca izpustili 46 bolnišnic, tako, da je realizirani vzorec obsegal 204 bolnišnice.	Podatke so zbirali s telefonsko anketo med zaposlenimi, ki so skrbeli za zasebnost in varnost zdravstvenih podatkov v bolnišnicah.	Vzorci varnostnih praks in odnosi med vzorci in skladnostjo s predpisi. Klasifikacija zdravstvenih ustanov na podlagi varnostnih praks s pomočjo združevanja v skupine (clustering).	204 bolnišnice so razvrstili v tri skupine, ki so imele podobno prakso skladnosti. Vse skupine so sprejemale tehnične prakse. Uravnotežile so varnostno prakso preko varovanja, revizije, upravljanja s človeškimi viri in upravljanja varnosti tretjih oseb.
Agaku, Adisa, Ayo-Yusuf & Connoly, 2014, ZDA[16]	Oceniti dojemanje in vedenje odraslih v ZDA na področju varovanja in zaščite zdravstvenih informacij.	Kvantitativni načrt, presečna raziskava. Gre za prvo od štirih ponovljenih anket (*Health Information National Trends Survey).* Izvedena multipla logistična regresija.	3959 respondentov – odrasli prebivalci ZDA.	Nacionalna reprezentativna anketa. Vprašalnik poslan po pošti. Stopnja odzivnosti 37 %.	Zaznavanje zaščitnih ukrepov; varnost in zasebnost informacij; nadzor nad zbiranjem, uporabo in izmenjavo informacij.	Zaskrbljenost respondentov zaradi kršitve varnosti zdravstvenih podatkov, predvsem pri pošiljanju dokumentov preko faksa ali elektronsko. Približno 12 % anketirancev je zaradi varnostnih pomislekov zdravstvenim delavcem zamolčalo določene informacije.

Raziskava	Namen raziskave	Raziskovalni načrt	Vzorec in metoda vzorčenja	Raziskovalni instrument	Proučevane spremenljivke	Ključne ugotovitve
He & Johnson, 2017, Kitajska[17]	Raziskati ovire, pri uporabi učenja iz incidentov kršenja varnosti zdravstvenih informacij.	Kvalitativni raziskovalni načrt –študija primera ene zdravstvene organizacije na terciarni ravni. Izvedeni so bili polstrukturirani intervjuji in pregledi oz. analiza dokumentov.	V vzorec ene zdravstvene ustanove je bilo izbranih 10 zdravstvenih delavcev (6 zdravnikov in 4 medicinske sestre) in 5 strokovnjakov za IT.	Vprašalnik z demografskimi vprašanji, polstrukturirani intervju.	Vprašanja o zbiranju podatkov oz. evidentiranju varnostnih incidentov; pridobivanje znanja o incidentih in povratne informacije.	Obravnave varnostnih incidentov z nizko stopnjo resnosti so se osredotočile na tehnične vidike, in manj poudarile pridobivanje znanja iz teh izkušenj. Podrobnosti ob ravnanju z incidenti niso bile ali so bile slabo dokumentirane. Organizacija ni imela strukturiranega načina za pridobivanje znanja iz nastalih incidentov.
Noor idr., 2017, Malezija[18]	Pregledati dejavnike, ki lahko vplivajo na informacijsko varnostno kulturo v okolju informatike v zdravstvu.	Izveden kvalitativni pristop, izvedba polstrukturiranega intervjuja.	7 zdravnikov, 5 medicinskih sester, 3 farmacevti in 4 administratorji. Merili za izbor udeležencev v študijo sta bili zaposlitev v zdravstveni organizaciji vsaj eno leto in uporaba IS.	Polstrukturiran vprašalnik. Pridobljeni podatki so bili urejeni z orodjem Atlas.	Identifikacija dvanajstih kategorij glede na pridobljene odgovore anketirancev.	Osveščenost o varnosti, varnostno znanje in varnostno vedenje so trije najpomembnejši dejavniki, ki ustvarjajo kulturo informacijske varnosti. Za te tri dejavnike je potrebna visoka zaveza glavnega vodstva, da se kultura informacijske varnosti oblikuje med zdravstvenimi delavci.
Božić, 2016, Slovenija[19]	Predstaviti učinek in pomen ozaveščanja zaposlenih pri vzpostavljanju in izvajanju varovanja informacijske varnosti.	Mešani raziskovalni načrt. Analiza tveganja, izveden družbeni inženiring in 10 delavnic ozaveščanja.	*Analiza tveganja*: eno svetovalno podjetje. *Družbeni inženiring:* naključna izbira 86 malih in srednje velikih organizacij (javni, zdravstveni in bančni sektor) v osrednjeslovenski regiji. *Vprašalnik in delavnice*: 253 zaposlenih v zdravstveni ustanovi.	*Analiza tveganja* z orodjem SBR. *Izvedba družbenega inženiringa* (nadzor nad poslanim USB ključkom organizacijam –kontrola uporabe ključka). *Vprašalnik* za zaposlene v zdravstveni ustanovi v Ljubljani pred začetkom delavnic.	*Analiza tveganja:* ocenitev tveganja informacijske varnosti. *Družbeni inženiring:* avtomatizirana analitika evidentiranja, iz katere je bilo razvidno, kdaj je določena organizacija odprla datoteke s ključka.	*Analiza tveganja:* človeški dejavnik je odgovoren za več kot polovico incidentov, povezanih z varovanjem informacij v organizaciji. *Izvedba družbenega inženiringa:* 90 % organizacij je ključek uporabilo, le v 11 % je prišel v roke IT-službe; 7 % organizacij je zanikalo, da bi prejeli pošiljko, čeprav so ključek uporabili. Zaposleni slabo poznajo varnostne politike; 22 % jih je že bilo priča varnostnemu incidentu. Večina uporablja premalo različnih gesel; 36 % gesla deli med seboj.

Tabela 2 Prikaz rezultatov po kodah in kategorijah.

Kategorija: varnostna praksa[15,17,18]
Varovanje – revizija – upravljanje s človeškimi viri – upravljanje varnosti tretjih oseb – preverjanje ozadja pred zaposlovanjem – prednost sprejemanju tehničnih rešitev pred postopki upravljanja varnosti – obravnave varnostnih incidentov z nizko stopnjo resnosti se osredotočajo na tehnične vidike – podrobnosti o ravnanju z incidenti so le delno ali sploh niso dokumentirane – občutljivost teme – izvajanje varnostne politike – potrebno je izboljšanje informacijske varnosti – zaposleni bi morali sodelovati pri izboljšanju informacijske varnosti – za dobro informacijsko varnost je potrebno sodelovanje – potrebna visoka zaveza glavnega vodstva, da se kultura informacijske varnosti razvije med zdravstvenimi delavci.
Kategorija: Znanje, usposabljanje, izkušnje[14,18]
Odsotnost usposabljanja vpliva na ozaveščenost – usposabljanje ovira vodstvo – ni zadosti sredstev za izvedbo izobraževanj in usposabljanj – večina zaposlenih nikoli ni prejela usposabljanja – zaposleni ne vedo, kaj je informacijska varnost – nepoznavanje organizacijske politike o informaciji varnosti – raven varnostnega znanja zaposlenih je nizka – potrebno motiviranje zaposlenih, da upoštevajo varnostne politike in postopke – izvajanje izobraževanja zaposlenih na področju varovanja informacij je na nizki stopnji – zaposleni razmeroma slabo poznajo varnostne politike – so priče varnostnemu incidentu – zlorabe gesel za dostop med zaposlenimi in študenti – uhajanje občutljivih podatkov novinarjem.
Kategorija: Zavedanje, odnos, stališče [14,18,19]
Pomanjkanje zavesti med zaposlenimi – odsotnost ozaveščenosti je najverjetneje posledica odsotnosti usposabljanja v bolnišnici – zaposleni želijo več izobraževanj in usposabljanj v zvezi z varnostjo informacij – stopnja zavedanja/ozaveščenosti je med zdravstvenimi delavci še vedno na srednji ravni – različne skupine zaposlenih imajo različen pristop do informacijske varnosti – zanikanje organizacije, da so uporabili nepoznano napravo za shranjevanje podatkov.
Kategorija: Dejavniki tveganja, zaupanje [14,16,19]
Pomanjkanje zavezanosti in podpore vodstva – zaposleni ne vedo, kaj je informacijska varnost – zaposleni ne poznajo vprašanj o varnosti informacij, povezanih z njihovim delovnim mestom – zaskrbljenost pacientov zaradi kršitve varnosti zdravstvenih podatkov – zaradi varnostnih pomislekov pacienti zdravstvenim delavcem zamolčijo določene informacije – človeški dejavnik je odgovoren za več kot polovico incidentov – nepravilna uporaba nepoznanih nosilcev podatkov – premalo različnih gesel – zaposlenih svoja gesla delijo med seboj.

Razprava

Organizacije razmeroma malo ali skoraj nič ne vlagajo v izobraževanja svojih zaposlenih s področja informacijske varnosti in tako posledično tudi ne razvijajo dobre informacijske varnostne kulture, ki je pomembna za vsakodnevno delovaje organizacije. Varnostna praksa organizacij ni na visokem nivoju, saj organizacije dajejo prednost sprejemanju tehničnih rešitev za zaščito in ne postopkom upravljanja varnosti, človeški dejavnik pa je vzrok za večino varnostnih tveganj ali kršitev.

Bolnišnice se raje poslužujejo preverjanja preteklosti pred zaposlovanjem kot pa organiziranju ali izvedbi izobraževanj. Ob varnostnih incidentih organizacije preidejo v reševanje tehničnih težav, pozabljajo pa na pozitivne strani pridobivanja znanja in ozaveščenosti, ki bi jih lahko bili deležni zaposleni.[17] Znanje, usposabljanje in izkušnje so pomembni dejavniki pri razvijanju dobre informacijske varnostne kulture v organizaciji, saj so zaposleni, pogosto zaradi pomanjkanja znanja, največja grožnja varnosti informacij.[20]

S pregledom smo ugotovili, da večina zdravstvenih delavcev nikoli ni bila deležna izobraževanj ali usposabljanj, kar se je pokazalo tudi v tem, da jih večina ni poznala varnostne politike. V veliki meri je bilo za takšno stanje odgovorno vodstvo, ker ni vlagalo zanimanja ali sredstev. Odnos, prepričanje in ravnanje zaposlenih do informacij morajo biti sprejemljivi in morajo biti del vsakdanjega »življenja« organizacije. Ocenjevanje odnosa in znanja zaposlenih do informacijske varnosti lahko pomaga organizaciji razumeti vedenja in prepoznati probleme. Ugotovili smo, da obstaja vrzel v odnosu oziroma stališčih in da imajo različne poklicne skupine različen pristop do varovanja informacij, je pa stopnja zavedanja še vedno na srednji ravni. Iz raziskav, ki so bile opravljene na področju zdravstvene nege v tujini, je jasno, da je problematika informacijske varnosti slabo oziroma premalo obravnavana. Albarrak[21] v svoji raziskavi opozarja, da se medicinske sestre zavedajo problematike informacijske varnosti, a kljub temu njihove navade predstavljajo resno grožnjo za varnost in zaupnost pacientovih podatkov.[21] Niimi in Ota[22] sta ugotovila, da nekatere bolnišnice sledijo različnim varnostnim ukrepom, veliko medicinskih sester pa ni prepoznalo varnostnih vzdrževalnih ukrepov.[22] V Sloveniji je bila v letu 2016 izvedena serija desetih delavnic ozaveščanja za zaposlene v eni od zdravstvenih ustanov. Pred delavnicami je bila izvedena anketa z namenom pridobiti splošen vpogled v trenutno stanje ozaveščenosti. Zaposleni so slabo poznali varnostne politike; četrtina anketirancev jih je že bila priča varnostnemu incidentu (od zlorabe gesel za dostop med zaposlenimi in študenti do uhajanja občutljivih podatkov novinarjem). Večina zaposlenih uporablja premalo različnih gesel (gesla enaka za več sistemov); 36 % pa jih svoja gesla deli

med seboj, kar pomeni, da jih je ravno toliko bilo v prekršku glede varnostne politike uporabe gesel.[19]

Nove tehnologije lahko dodatno povečajo ranljivost zasebnih informacij, vključno z zdravstvenimi. Še večji problem je, da je možno te naprave izgubiti ali ukrasti in hranijo veliko pomembnih informacij. Skrb vzbuja to, da so respondenti v raziskavi (odrasli prebivalci ZDA) zaradi varnostnih pomislekov zdravstvenim delavcem zamolčali določene pomembne informacije.[16] Pojem informacijske varnostne kulture za področje zdravstva opisuje le ena raziskava,[14] ostale opisujejo podobne oziroma sorodne koncepte,[15-19] kot je varnost informacij ali informacijska varnost. Med zadetki je bilo zaslediti veliko dobrih raziskav na omenjeno temo, vendar za področje zdravstva malo. Spremenljivke, ki so bile znanstveno preučevane, so bile predvsem znanje, odnos, prepričanje o informacijski varnosti, vzorci varnostnih praks, skladnost s predpisi ter zaščitni ukrepi za zavarovanje zdravstvenih podatkov.

Omejitve

V raziskavi smo se osredotočili na pregled aktualnih raziskav, starih do 8 let, in sicer znanstvenih prispevkov, objavljenih v angleškem in slovenskem jeziku. Izbor jezika lahko povzroči pristranskost, zato bi bilo smiselno nadaljnje raziskovanje usmeriti v iskanje relevantnih prispevkov v drugih jezikih in iz drugih zbirk podatkov. Iskanje, pregled in izbor raziskav je opravil samo en raziskovalec. V bodoče bi lahko več raziskovalcev skupaj razvilo raziskovalno strategijo, jo uporabilo v različnih podatkovnih zbirkah in bi ločeno izbirali relevantne raziskave, čemur bi v primeru neskladja sledilo iskanje konsenza. Analizirane raziskave so se glede na raven dokazov[13] vse razen ene uvrstile nizko.

Zaključek

Za področje zdravstva je koncept informacijske varnostne kulture slabo raziskan, tako v Sloveniji kot v tujini. Informacije, ne glede na obliko, zahtevajo ustrezno zaščitno, njihovi uporabniki pa so ključni potencialni predstavniki groženj. Kršitve varnosti zdravstvenih informacij imajo pomemben vpliv ne le na paciente, ampak tudi na zdravstvene ustanove. Glede na večanje pogostosti zlorab podatkov, je tema aktualna in pomembna, vzpostavitev informacijske varnostne kulture pa nujna.

Sistematični pregled obstoječih dokazov je dal vpogled v trenutno situacijo. V končno analizo je bilo vključenih šest raziskav (eno magistrsko delo in pet drugih znanstvenih prispevkov). V prihodnje bi bilo potrebno bolj celostno raziskati stanje v slovenskih zdravstvenih ustanovah in za ta namen razviti kakovosten merski instrument, ki bi meril celoten koncept informacijske varnostne kulture. Za zaposlene v zdravstvenih organizacijah je potrebno organizirati kontinuirana izobraževanja in delavnice, prav tako poudariti pomembnost organiziranja izobraževanj pri vodstvu. Kako uspešne so bile izvedene delavnice, bi lahko preverili z izvedbo kvazieksperimenta.

Konflikt interesov

Del rezultatov je bil predstavljen na 11. Mednarodni znanstveni konferenci Fakultete za zdravstvo Angele Boškin (Bled, 7 .6. 2018).

Reference

1. Alnatheer M, Nelson K: Proposed framework for understanding information security culture and practices in the Saudi context. In: *Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1.-3. 12. 2009*. Perth 2009: Security Research Centre, School of Computer and Security Science, Edith Cowan University; 6-17.
2. Von Solms B: Information security – the third wave? *Comp Secur* 2000; 19(7), 615-620.
3. Von Solms B: Information security – the fourth wave? *Comp Secur* 2006, 25(165), 165-168.
4. Kuusisto R, Kuusisto T: Strategic communication for cyber security leadership. In: Kuusisto R, Kurkinen E (eds.), *Proceedings of the 12th European conference on information warfare and security, University of Jyvaskyla, Finland, 11.-12. 7. 2013*. UK 2013: Academic Conferences and Publishing International Limited; 167.
5. Williams PA: What does security culture look like for small organizations? In: *7th Australian Information Security Management Conference*. Perth, Western Australia 2009: Security Research Centre, School of Computer and Security Science, Edith Cowan University; 47-54. https://doi.org/10.4225/75/57b4029530dea (15. 12. 2018).
6. Orehek Š: *Merjenje informacijske varnostne kulture: metaanaliza anketnih merskih inštrumentov: magistrsko delo*. Ljubljana 2017: Univerza v Ljubljani, Fakulteta za družbene vede.
7. Noor H, Zuraini I: A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia Soc Behav Sci* 2012; 65: 1007-1012. https://doi.org/10.1016/j.sbspro.2012.11.234 (15. 12. 2018)
8. Ponemon Institute: *Cost of data breach study: global analysis*. [S. l.] 2015: Ponemon Institute. https://nhlearningsolutions.com/Portals/0/Documents/2015Cost-of-Data-BreachStudy.pdf (2. 12. 2017)
9. US Department of Health and Human Sercices, Office for Civil Rights: *Breach portal: notice to the secretary of HHS*

breach of unsecured protected health information. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (2. 12. 2017)
10. SI-CERT: *Poročilo o omrežni varnosti za leto 2015.* https://www.cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf (2. 12. 2017)
11. Appari A, Johnson E: Information security and privacy in healthcare: current state of research. *IJIEM* 2010; (6)4: 279-314.
12. Booth A, Sutton A, Papaioannou D: *Systematic approaches to a successful literature review*. Los Angeles: 2012 Sage; 59-60.
13. Polit D, Beck CT: *Essentials of nursing research: appraising evidence for nursing practice.* Philadelphia 2008: Lippincott Williams & Wilkins.
14. Gebrasilase T, Lessa LF: Information security culture in public hospitals: the case of Hawassa referral hospital. *Afr J Inf Syst* 2011; 3(3): 72-86.
15. Kwon J, Johnson ME: Security practices and regulatory compliance in the healthcare industry. *J Am Med Infor Assoc* 2013; 20(1): 44-51. https://doi.org/10.1136/amiajnl-2012-000906 (15. 12. 2018)
16. Agaku I, Adisa A, Ayo-Yusuf A, Connolly, N: Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *J Am Med Infor Assoc* 2014; 21(2): 374-378. https://doi.org/10.1136/amiajnl-2013-002079 (15. 12. 2018)
17. He Y, Johnson C: Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. *Inform Health Soc Care* 2017; 42(4): 393-408. https://doi.org/10.1080/17538157.2016.1255629 (15. 12. 2018)
18. Noor H, Norazen M, Maarop N, Ismail Z, Wardah A: Information security culture in health informatics environment: a qualitative approach. In: *International Conference on research and innovation in information systems (ICRIIS).* Langkawi, Malaysia 2017; 1-6. https://doi.org/10.1109/ICRIIS.2017.8002450 (16. 12. 2018)
19. Božić F: *Človeški dejavnik pri zagotavljanju informacijske varnosti: magistrsko delo.* Ljubljana 2016: Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.
20. Niekerk JF, Solms R: Information security culture: a management perspective. *Comp Secur* 2010; 29(4): 476-486. https://doi.org/10.1016/j.cose.2009.10.005 (16. 12. 2018)
21. Albarrak A: Information security behavior among nurses in an academic hospital. *HealthMED* 2012; 6(7): 2349-2354.
22. Niimi Y, Ota K: Privacy recognition by nurses and necessity of their information security education. In: Shaw T (ed.), *International conference on education reform and modern management.* Amsterdam 2014: Atlantis Press; 358-361.