PRETHODNO PRIOPĆENJE

DOI: 10.59245/ps.32.4.3
UDK: 621.391
Primljeno: kolovoz 2022.

KRUNOSLAV ARBANAS*

Vrednovanje kulture informacijske sigurnosti operatora ključnih usluga

Sažetak

Relevantna literatura već godinama ističe kako je informacijska sigurnost prestala biti isključivo tehničko i postala prije svega poslovno pitanje s posebnim naglaskom na ljudski čimbenik. Tim pomakom u razmišljanju mijenja se i fokus s isključivo tehničkih mjera zaštite informacijske sigurnosti prema organizacijsko-sociološkim elementima zaštite, čime do izražaja dolazi kultura informacijske sigurnosti. Upravo dobro uspostavljena kultura informacijske sigurnosti koja, uz uspostavljene tehničke mjere, u obzir uzima sociološke čimbenike i organizacijske mjere, može ne samo pridonijeti zaštiti informacija nego i promijeniti razmišljanje zaposlenika tako da prestanu promatrati informacijsku sigurnost kao smetnju u svakodnevnom radu. Ovaj rad predstavlja rezultate empirijskog istraživanja kulture informacijske sigurnosti na temelju uspostavljenih sigurnosnih praksi, provedenog na 239 zaposlenika organizacija iz osam sektora koji predstavljaju operatore ključnih usluga u Republici Hrvatskoj.

Ključne riječi: *informacijska sigurnost, kibernetička sigurnost, kultura informacijske sigurnosti, sigurnosna kultura, kritična infrastruktura, operatori ključnih usluga.*

UVOD

Povijesno gledano, problematika informacijske sigurnosti redovito se proučavala u tehnološkom kontekstu (Soomro i sur., 2016) gdje su organizacije slijedile tehnički usmjerenu strategiju informacijske sigurnosti koja naglašava ključnu ulogu tehnologije u oblikovanju učinkovitih sigurnosnih rješenja. Međutim, novo je gledište uravnoteženost strategije informacijske sigurnosti, naglašavajući važnost tehnologije, ali također uključujući sociološko-organizacijski kontekst kako bi u konačnici bila uspješna.

* dr. sc. Krunoslav Arbanas, Hrvatska energetska regulatorna agencija, Zagreb.

Različiti autori (Tang i sur., 2016), (Soomro i sur., 2016) slažu se da se informacijska sigurnost treba tretirati kao poslovno pitanje jer nije više samo „tehnički" nego i „ljudski" problem s obzirom na to da informacijska sigurnost počinje i završava s ljudima (Snyman i sur., 2018) koji su ključni čimbenik u upravljanju informacijskom sigurnošću (Tang i sur., 2016), (Yildirim, 2016), (Stewart i Jürjens, 2017) i nerijetko njezina „najslabija karika" (Soomro i sur., 2016), (Mahfuth i sur., 2017a), (Parsons i sur., 2017), (Wiley i sur, 2020). Tako istraživanje koje su proveli IBM Security i Ponemon Institute (IBM Security i Ponemon Institute, 2021) otkriva da su kompromitirane vjerodajnice i napadi lažnim predstavljanjem radi krađe identiteta (engl. *Phishing*) uzroci 37% analiziranih povreda podataka u cijelom svijetu u 2021. godini. Također, istraživanje provedeno u Južnoj Africi (Kritzinger i sur., 2023) identificiralo je tri čimbenika koja izazivaju zabrinutost kada je riječ o zaštiti informacija zaposlenika unutar organizacija, a to su korištenje interneta, sigurno korištenje e-pošte i korištenje društvenih mreža.

Kao što se može zaključiti iz navedenog, informacijska sigurnost uvelike ovisi o ponašanju zaposlenika koje može ojačati ili oslabiti sigurnost, zbog čega istraživači predlažu njegovanje kulture informacijske sigurnosti koja potiče prihvatljivo i obeshrabruje neprikladno sigurnosno ponašanje (Nasir i sur., 2019) kako bi informacijska sigurnost postala svačija odgovornost. Uspostavljanje kulture informacijske sigurnosti uključuje sigurnost u ponašanje zaposlenika, čime informacijska sigurnost postaje normalan dio njihova svakodnevnog ponašanja u organizaciji (Sherif i Furnell, 2015). Preispitivanjem informacijske sigurnosti kao sastavnog dijela navika i ponašanja zaposlenika, kultura informacijske sigurnosti postaje čimbenik koji omogućuje učinkovitu sigurnosnu praksu uklapajući je u svakodnevni rad (ENISA, 2017), (Tolah i sur., 2021).

Dodatno, kultura čiji je cilj osigurati informacijsku sigurnost kao odgovornost svih zaposlenika (AlHogail i Mirza, 2015), (Kritzinger i sur., 2023) promiče odgovornost pojedinaca u provedbi informacijske sigurnosti u organizacijama u kojima se, u idealnom slučaju, svi zaposlenici pridržavaju politika informacijske sigurnosti, čak i kada nitko nije u blizini te kada se njihovo ponašanje ne prati.

1. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

Kako bi se smanjile posljedice namjernih ili nenamjernih ljudskih radnji kao najveće prijetnje informacijskoj sigurnosti organizacije (Stewart i Jürjens, 2017), devedesetih godina 20. stoljeća pojavila se kultura informacijske sigurnosti kao mjera za promicanje sigurnog ponašanja zaposlenika u organizacijama. U literaturi se mogu pronaći brojne definicije kulture informacijske sigurnosti različite složenosti, a jedna od najjednostavnijih navodi kako kultura informacijske sigurnosti predstavlja *percepcije, stavove i pretpostavke koji se prihvaćaju i potiču u organizaciji – dakle način na koji se stvari rade u organizaciji radi zaštite informacijske imovine* (Alnatheer, 2014).

Bez obzira na različitu složenost, formulaciju i pristup pojedinih autora, u definicijama se može primijetiti isticanje važnosti dosljednog ponašanja ljudi u skladu s pravilima definiranim sigurnosnim politikama s obzirom na to da je cilj kulture informacijske sigurnosti

zaštititi informacijsku imovinu (Tolah i sur., 2017) promicanjem opreznog i sigurnog ponašanja zaposlenika (Mahfuth i sur., 2017a), čime se smanjuje vjerojatnost narušavanja sigurnosti (Masrek i sur., 2017).

(AlHogail i Mirza, 2015) primjećuju kako je jedan od načina mjerenja stanja kulture informacijske sigurnosti organizacije upotreba anketnih upitnika radi stjecanja razumijevanja čimbenika koji utječu na sigurnosno ponašanje zaposlenika. Međutim, iako su anketni upitnici najčešće korišten alati za mjerenje kulture informacijske sigurnosti (Orehek i Petrič, 2020), postoji i oprez zbog činjenice da su potrebne dinamičnije mjere za mjerenje ponašanja u svakodnevnim zadacima (Uchendu i sur., 2021), a provedena analiza (da Veiga i sur., 2020) pokazala je da su znanstvena tumačenja čimbenika kulture informacijske sigurnosti mnogo šira nego što ih industrija razumijeva.

U literaturi je prepoznato kako su postojeća istraživanja uvelike teorijska, odnosno opisna, kao i da postoji određen nedostatak znanja o prepoznavanju čimbenika kulture informacijske sigurnosti te mjerenju utjecaja koje ti čimbenici imaju na samu kulturu (Nasir i sur., 2017), čime se istodobno javlja potreba za sveobuhvatnim empirijskim istraživanjima iz tog područja (Mahfuth i sur., 2017b; Nasir i sur., 2019; Arbanas, 2020). (Nævestad i sur., 2023) pokazali su na primjeru jedne organizacije kako je ona tijekom dvogodišnjeg razdoblja sustavnim radom na upravljanju informacijskom sigurnošću, među ostalim i na redovnom podizanju svijesti zaposlenika, uspjela poboljšati kulturu informacijske sigurnosti, što je u konačnici dovelo do poboljšanja ponašanja zaposlenika u kontekstu informacijske sigurnosti. Tome u prilog idu i rezultati istraživanja provedenog u zdravstvenom sektoru (Gioulekas i sur., 2022) koji upućuju na to kako su se implementacija programa podizanja sigurnosne svijesti i sigurnosne edukacije pokazale nužnima.

S druge strane, kibernetički napadi koji su uslijed globalne umreženosti postali svakodnevica posebno dolaze do izražaja u sektorima čiji prekid djelovanja može imati ozbiljne posljedice na sigurnost i ekonomsku stabilnost neke države s obzirom na to da je riječ o kritičnoj nacionalnoj infrastrukturi ili ključnim uslugama. Takvi sektori nisu u jednakoj mjeri ranjivi na sve vrste sigurnosnih prijetnji, pa se tako može vidjeti da su, primjerice, organizacije iz financijskog sektora sklonije sigurnosnim prijetnjama koje uključuju krađe ili prijevare, dok su organizacije iz sektora energetike ranjivije na prijetnje poput aktivizma ili terorizma (Sas i sur., 2021).

Pregled literature (Evripidou i sur., 2022) vezan uz sigurnosnu kulturu u organizacijama koje ne koriste samo informacijsku tehnologiju (IT) nego i operativnu tehnologiju (OT), odnosno sustave koji kontroliraju i nadziru industrijske procese, pokazao je kako se često naglašavaju nedostatak svijesti i znanja o informacijskoj sigurnosti i odsutnost podrške najvišeg menadžmenta kao čimbenika koji utječu na sigurnosnu kulturu organizacije. Tome u prilog idu i rezultati istraživanja sigurnosne kulture organizacija koje upotrebljavaju operativnu tehnologiju (Evripidou, 2023), a pokazali su kako su tri ključne organizacijske prepreke razvoju sigurnosne kulture: upravljanje sigurnošću na najvišoj razini, nedostatak komunikacije između različitih funkcija u organizaciji, kao i nedostatak stručnog znanja o kibernetičkoj sigurnosti operativne tehnologije.

Da bi pojedini javni ili privatni subjekt bio određen kao operator ključnih usluga u Republici Hrvatskoj, takav subjekt, sukladno s člankom 6. Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18.), mora pružati neku od ključnih usluga određenih Zakonom, gdje pružanje ključne usluge ovisi o mrežnim i informacijskim sustavima, a pojava incidenta imala bi znatan negativan učinak na pružanje ključne usluge (Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/18.).

Spomenuti Zakon nastao je na temelju tzv. NIS direktive (Direktiva (EU) 2016/1148) Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194/1.) koja propisuje sedam sektora operatora ključnih usluga. Ti sektori su *energetika, prijevoz, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba vodom za piće i njezina distribucija* te *digitalna infrastruktura*, pri čemu je Republika Hrvatska u nacionalni Zakon dodala i osmi sektor koji predstavljaju *poslovne usluge za državna tijela*.

Imajući u vidu važnost informacijske sigurnosti u organizacijama iz sektora ključnih usluga, provedeno je empirijsko istraživanje kojim se željelo provjeriti stanje kulture informacijske sigurnosti na temelju uspostavljenih sigurnosnih praksi u organizacijama koje predstavljaju operatore ključnih usluga, gdje su sudionici istraživanja bili zaposlenici tih organizacija.

2. METODOLOGIJA ISTRAŽIVANJA

Istraživanje opisano u ovom radu provedeno je u tri glavne faze. Prva se faza sastoji od izrade anketnog upitnika, druga od prikupljanja podataka putem izrađenog anketnog upitnika, a završna faza odnosi se na analizu podataka dobivenih empirijskim istraživanjem.

Tijekom prve faze, nakon pregleda relevantne literature, razvijen je anketni upitnik koji predstavlja mjerni instrument za mjerenje stvarnog stanja implementiranih kontrola dobre prakse informacijske sigurnosti u organizacijama uzimajući u obzir holističku prirodu kulture informacijske sigurnosti, odnosno organizacijske mjere, tehničke mjere i sociološke čimbenike (Arbanas, 2021.). Nakon izrade anketnog upitnika, u drugoj fazi provedeno je empirijsko istraživanje čiji su sudionici bili zaposlenici organizacija koje predstavljaju operatore ključnih usluga u skladu sa Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18.). U konačnici, završna faza uključivala je analizu prikupljenih podataka nakon provedenog empirijskog istraživanja gdje je za objašnjenje rezultata korištena uobičajena deskriptivna statistička analiza.

3. REZULTATI ISTRAŽIVANJA

3.1. Anketni upitnik

U početnoj fazi izrađeno je ukupno 10 pitanja koja su obuhvaćala tri prepoznate kategorije kulture informacijske sigurnosti, odnosno organizacijske mjere, sociološke čimbenike i tehničke mjere te je radi provjere sadržajne valjanosti mjernog instrumenta, kontaktirano 15

eksperata koji imaju domensko znanje dokazivo međunarodnim certifikatima (CISM, CISA, CISSP ili slično) i relevantno radno iskustvo. Svaki stručnjak trebao je provjeriti relevantnost i jasnoću pojedinog pitanja, kao i preformulirati postojeća, ali i predložiti neka dodatna. Od ukupno 15 kontaktiranih eksperata, njih 11 (šestorica muškaraca i pet žena) vratilo je popunjenu tablicu. Kad je o radnom iskustvu riječ, većina stručnjaka (njih 7 ili 64%) ima pet do devet godina radnog iskustva na području informacijske sigurnosti, dva stručnjaka imaju više od 20 godina radnog iskustva, a preostala dva imaju radno iskustvo iz područja informacijske sigurnosti između 10 i 14 godina.

Kao rezultat, eksperti su preformulirali pet pitanja kako bi se jasnije stvorila slika što se traži od ispitanika te su predložili dva dodatna pitanja kojima bi se mjerilo stvarno stanje u organizaciji kad je riječ o implementiranim mjerama informacijske sigurnosti (*U mojoj organizaciji postoji interna funkcija (jedna ili više osoba ili odjel) zadužena za informacijsku sigurnost* i *U zadnjih 12 mjeseci prijavio sam incident informacijske sigurnosti ili sumnju na isti*), čime je ukupan broj pitanja u anketnom upitniku bio 12. U slučaju dorade pitanja nije bilo potrebe za ponovnim usuglašavanjem eksperata jer je bila riječ samo o drugačijoj formulaciji pitanja bez mijenjanja njihova smisla (primjerice, pitanje *U zadnjih 12 mjeseci bio/bila sam* ***upozoren/a*** *na prijetnje vezane uz otvaranje sumnjivih mailova i privitaka u njima* preformulirano je u *U zadnjih 12 mjeseci bio/bila sam* ***informiran/a*** *o prijetnjama vezanim uz otvaranje sumnjivih elektroničkih poruka i privitaka u njima*).

3.2. Prikupljanje podataka

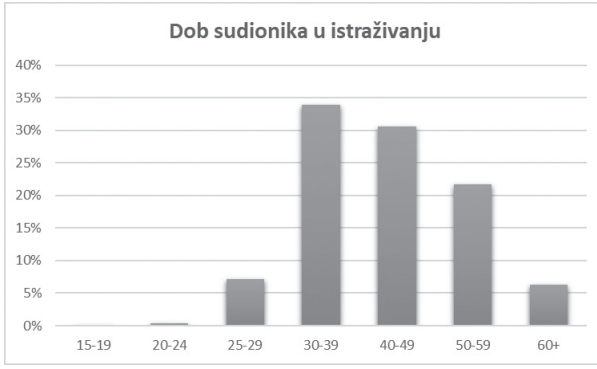
Kako bi se podaci mogli prikupljati online, mjerni instrument prebačen je u oblik online upitnika s pomoću alata LimeSurvey. Uz 12 pitanja koja se odnose na objektivne metrike stvarnog stanja sigurnosne prakse u organizaciji, online upitnik sastojao se od dodatnih sedam pitanja vezanih uz spol, dob, stupanj obrazovanja, radno iskustvo u postojećoj organizaciji, ukupno radno iskustvo, veličinu organizacije i djelatnost u kojoj je sudionik istraživanja zaposlen. Anketnim upitnikom nisu se prikupljali nikakvi osobni podaci, uključujući IP adresu, čime je zajamčena anonimnost sudionika, dok je sudjelovanje u istraživanju bilo dobrovoljno te je u bilo kojem trenutku bilo moguće odustati od ankete. Sudionici tog istraživanja definirani su kao zaposlenici organizacija koje predstavljaju operatore ključnih usluga u skladu s odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18.) koji koriste informacijski sustav organizacije. Veliki problem u provođenju istraživanja bio je u činjenici da je za određivanje statistički značajnog uzorka sudionika bilo potrebno imati podatke o veličini i karakteristikama cjelokupne populacije. Navedeni Zakon ne definira eksplicitno o kojim je organizacijama riječ kad se govori o operatorima ključnih usluga, nego samo navodi djelatnosti koje predstavljaju ključne usluge te kriterije za određivanje operatora tih ključnih usluga, zbog čega nije bilo moguće primijeniti jednu od metoda neprobabilističkog uzorkovanja. Ta činjenica smanjuje mogućnost generalizacije rezultata i predstavlja najveće ograničenje ovog istraživanja. Imajući to ograničenje u vidu, autor je za prikupljanje podataka odabrao metodu snježne grude (*engl. snowball method*) u kojoj se od sudionika tražilo da proslijede link na anketni upitnik drugim potencijalnim sudionicima kako bi se postigla najveća moguća veličina uzorka.

Kako bi se prikupili sudionici istraživanja, poslan je e-mail s kratkim opisom istraživanja i poveznicom na anketni upitnik na javne e-mail adrese organizacija za koje nije bilo sumnje da predstavljaju operatore ključnih usluga. Poziv za sudjelovanje u istraživanju ponovno je poslan još dvaput u razmaku od nekoliko tjedana. Istodobno, putem poslovne društvene mreže LinkedIn kontaktirani su potencijalni sudionici koji rade u predloženim organizacijama. U tom razdoblju u istraživanju je sudjelovalo ukupno 506 ispitanika, od kojih je 239 upitnika bilo ispunjeno u potpunosti i pogodno za daljnju analizu.

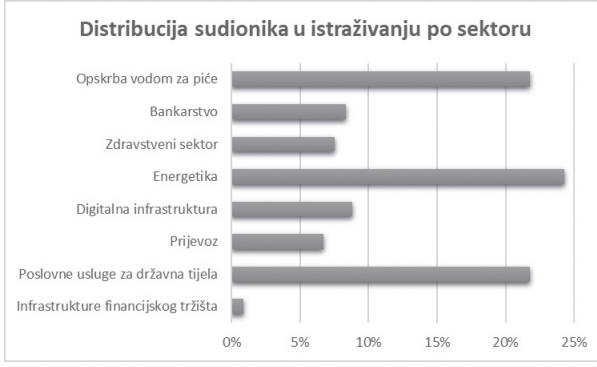
3.3. Analiza prikupljenih podataka

Od ukupnog broja sudionika bilo je 116 (49%) muškaraca i 123 (51%) žene. Najveći postotak sudionika (64,4%) bio je u dobi od 30 do 49 godina (Grafikon 1.), dok je najveći broj sudionika (157) imao visoku stručnu spremu. Najviše sudionika bilo je iz sektora energetike (24%), sektora opskrbe vodom za piće i njezine distribucije (22%) i sektora poslovnih usluga za državna tijela (22%), a najmanje (samo 1%) iz sektora infrastrukture financijskog tržišta (Grafikon 2.).

Grafikon 1: *Distribucija sudionika u istraživanju prema dobi*



Grafikon 2: *Distribucija sudionika u istraživanju prema sektoru*



Kao što je vidljivo iz Tablice 1., najveći broj sudionika u istraživanju (33,5%) imao je ukupno 10 do 20 godina radnog staža, a samo tri sudionika manje od dvije godine. Kada govorimo o radnom iskustvu u trenutačnoj organizaciji, 13 sudionika tamo je kraće od godinu

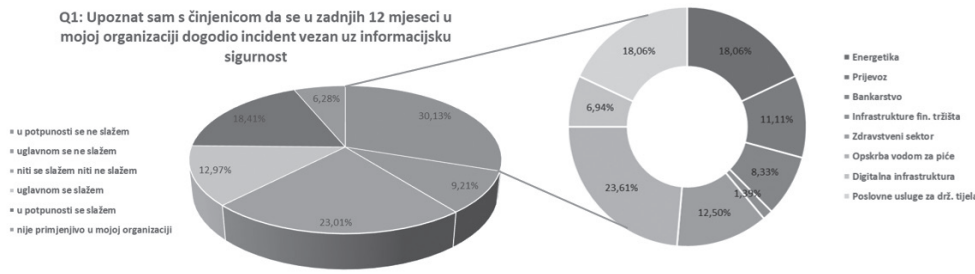
dana dok je najveći broj sudionika (28%) u trenutačnoj organizaciji proveo između 10 i 20 godina.

Tablica 1: *Radno iskustvo u trenutačnoj organizaciji i ukupno radno iskustvo sudionika*

Radno iskustvo u trenutačnoj organizaciji (god.)	Broj	Postotak	Ukupno radno iskustvo (god.)	Broj	Postotak
< 1	13	5,4%	< 1	1	0,4%
1 – 2	18	7,5%	1 – 2	2	0,8%
2 – 3	18	7,5%	2 – 3	12	5,0%
3 – 5	24	10,0%	3 – 5	14	5,9%
5 – 10	42	17,6%	5 – 10	35	14,6%
10 – 20	67	28,0%	10 – 20	80	33,5%
20 – 30	31	13,0%	20 – 30	53	22,2%
30+	26	10,9%	30+	42	17,6%

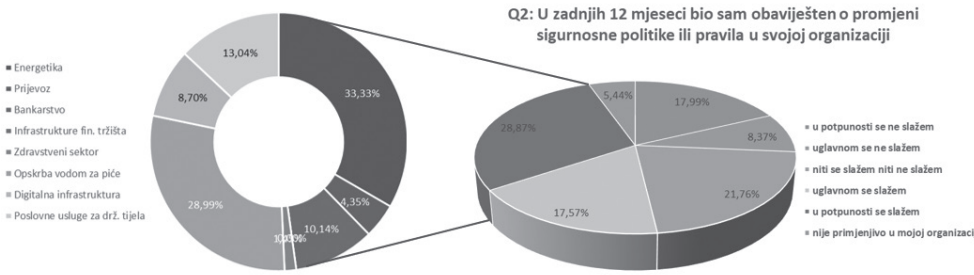
Podaci dobiveni empirijskim istraživanjem analizirani su na temelju distribucije odgovora za sve sektore zajedno, kao i za svaki sektor pojedinačno, po pojedinom pitanju. Distribucija odgovora zajedno za sve sektore, kao i pojedinačni udio po sektoru za najčešći odgovor, dani su u nastavku (Grafikoni 3. – 14.).

Grafikon 3: *Ukupna distribucija odgovora na 1. pitanje s udjelom po sektoru za najčešći odgovor*



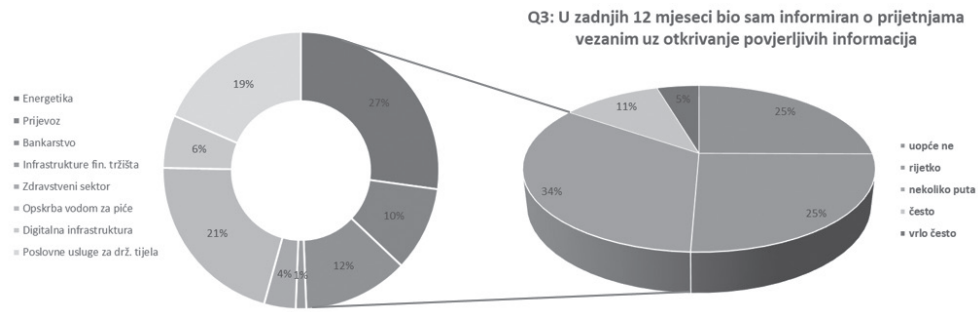
Kao što je vidljivo iz Grafikona 3., tek nešto više od 31% svih sudionika uglavnom se ili u potpunosti složilo s tvrdnjom da su upoznati s činjenicom da se u posljednjih 12 mjeseci dogodio sigurnosni incident u njihovoj organizaciji, što se može protumačiti dvojako – ili uistinu nije bilo pojave sigurnosnog incidenta u tom razdoblju ili organizacija nema uspostavljene mehanizme kojima bi se, nakon što se incident dogodio, utvrdio njegov uzrok i otklonilo ga se te obavijestilo sve zaposlenike o neželjenom događaju radi podizanja svijesti zaposlenika o informacijskoj sigurnosti, kao i sprječavanju njegova pojavljivanja ili sličnog događaja.

Grafikon 4: *Ukupna distribucija odgovora na 2. pitanje s udjelom po sektoru za najčešći odgovor*



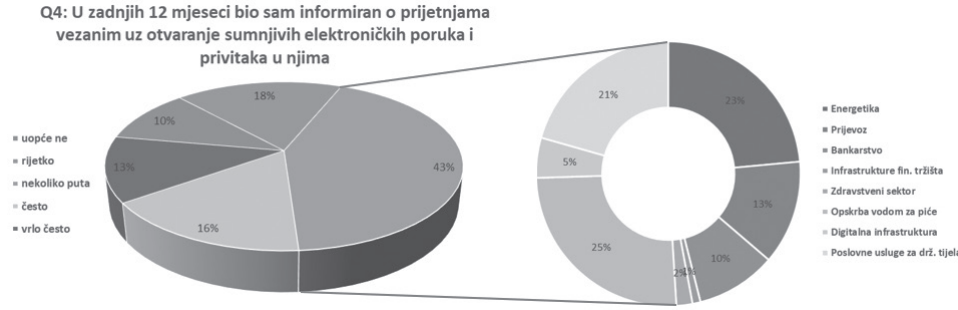
Grafikon 4. pokazuje kako se nešto više od 46% svih sudionika uglavnom ili u potpunosti slaže da su u posljednjih 12 mjeseci bili obaviješteni o promjeni sigurnosne politike u svojoj organizaciji, čime se pokazuje zrelost takvih organizacija kada je riječ o uvođenju i održavanju organizacijskih mjera informacijske sigurnosti, a samim time i doprinosu sigurnosne kulture.

Grafikon 5: *Ukupna distribucija odgovora na 3. pitanje s udjelom po sektoru za najčešći odgovor*



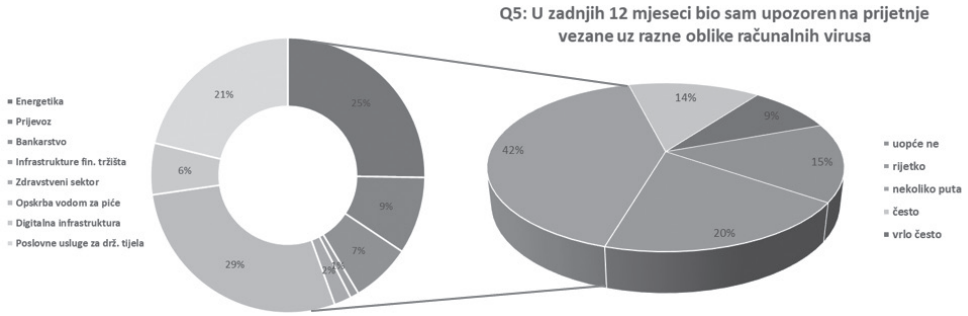
Iz Grafikona 5. vidljivo je kako je tek 16% svih sudionika rijetko ili uopće nije bilo informirano o prijetnjama vezanim uz otkrivanje povjerljivih informacija u posljednjih 12 mjeseci, čime se također pokazuje visoka razina svijesti o informacijskoj sigurnosti u ovim organizacijama te time izravno utječe na mogućnost sprječavanja sigurnosnih incidenata.

Grafikon 6: *Ukupna distribucija odgovora na 4. pitanje s udjelom po sektoru za najčešći odgovor*



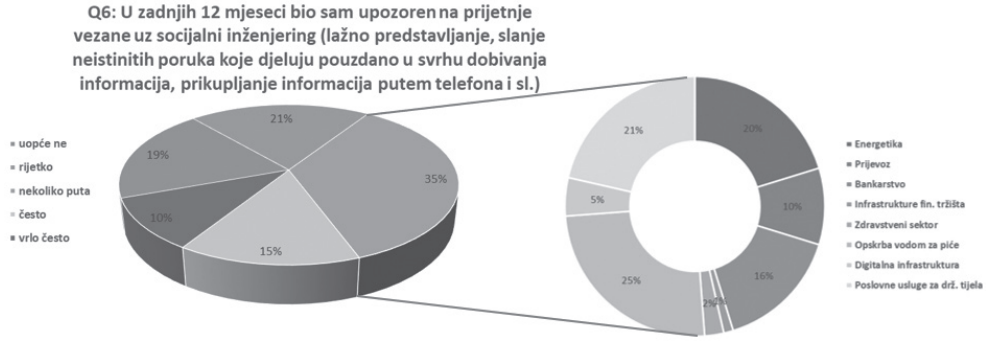
Kao što je vidljivo iz Grafikona 6., 72% svih ispitanika barem je nekoliko puta bilo informirano o prijetnjama vezanim uz otvaranje sumnjivih elektroničkih poruka i privitaka u njima, čime se pokazuje kako promatrane organizacije rade na podizanju svijesti o informacijskoj sigurnosti i sprječavanju pojave takvog oblika sigurnosnih incidenata.

Grafikon 7: *Ukupna distribucija odgovora na 5. pitanje s udjelom po sektoru za najčešći odgovor*



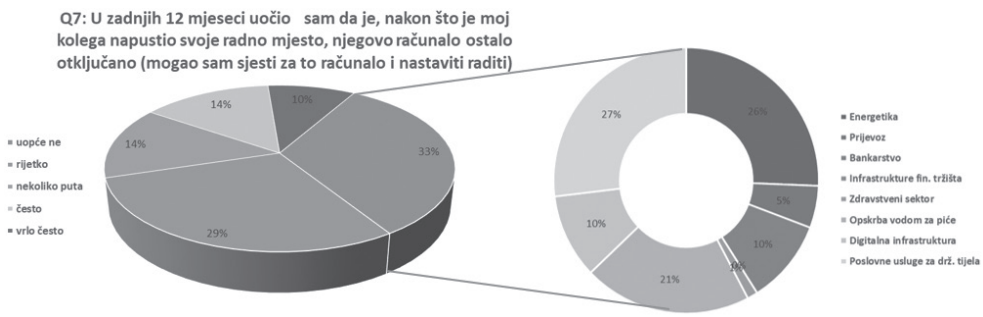
Grafikon 7. pokazuje kako je trećina (35%) svih sudionika izjavila da su u proteklih 12 mjeseci rijetko ili uopće nisu bili upozoreni na prijetnje vezane uz razne oblike računalnih virusa. Time se pokazuje kako se, čak i ako postoji formalno razrađen proces upozoravanja zaposlenika na ugroze putem računalnih virusa, ta praksa ne provodi sustavno te bi taj segment zahtijevao određena poboljšanja kako bi se povećala svijest zaposlenika o informacijskoj sigurnosti, čime bi se u konačnici i povećala zrelost kulture informacijske sigurnosti u samoj organizaciji.

Grafikon 8: *Ukupna distribucija odgovora na 6. pitanje s udjelom po sektoru za najčešći odgovor*



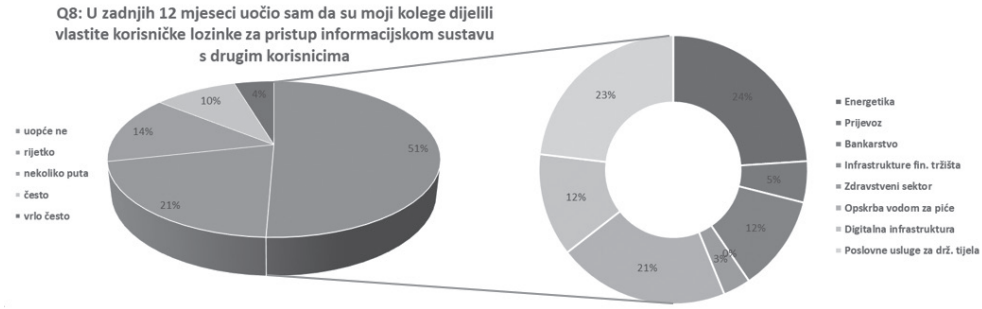
Iz Grafikona 8. vidljivo je kako je 60% svih sudionika barem nekoliko puta u posljednjih 12 mjeseci bilo upozoreno na prijetnje vezane uz socijalni inženjering. Iako je riječ o visokom postotku, to bi područje trebalo biti predmet poboljšanja u organizacijama s obzirom na to da je socijalni inženjering jedna od sigurnosnih prijetnji koja je svake godine u porastu zbog učestalog mijenjanja načina zavaravanja krajnjeg korisnika.

Grafikon 9: *Ukupna distribucija odgovora na 7. pitanje s udjelom po sektoru za najčešći odgovor*



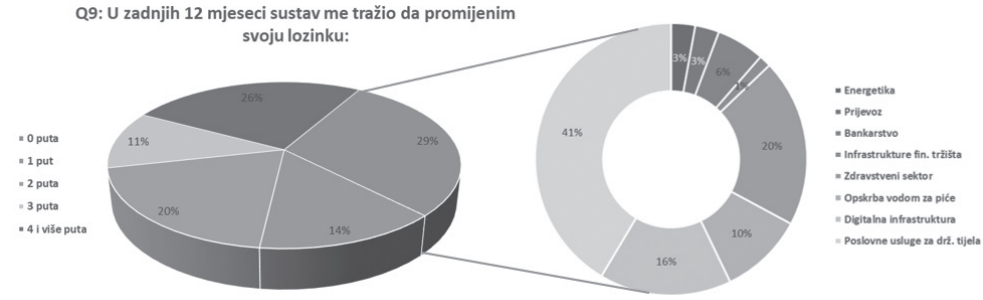
Grafikon 9. pokazuje da je gotovo četvrtina (24%) svih ispitanika izjavila kako su u posljednjih 12 mjeseci uočili da su njihovi kolege ostavili otključano računalo nakon napuštanja radnog mjesta. Taj postotak nije zanemariv i promatrane organizacije trebale bi poraditi na tome, pogotovo zato što se ovdje, uz obaveznu organizacijsku mjeru podizanja sigurnosne osviještenosti, radi i o tehničkoj mjeri nametanja obaveznog zaključavanja zaslona računala nakon određenog razdoblja neaktivnosti, što je jednostavno primijeniti na svim računalima.

Grafikon 10: *Ukupna distribucija odgovora na 8. pitanje s udjelom po sektoru za najčešći odgovor*



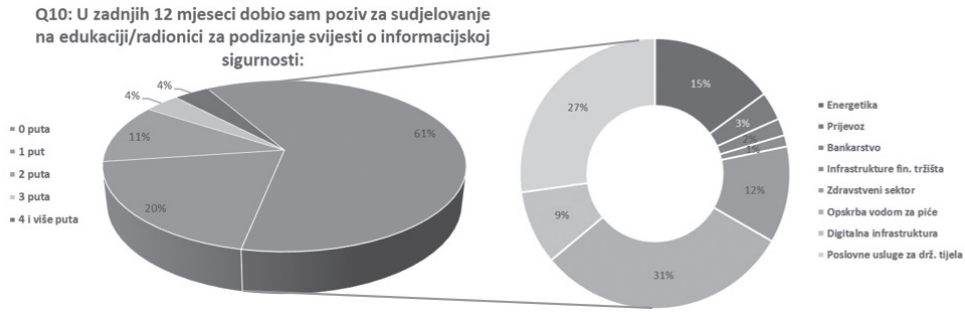
Kao što je vidljivo iz Grafikona 10., čak 73% svih sudionika tvrdilo je kako su rijetko ili uopće nisu uočili da su njihovi kolege u zadnjih 12 mjeseci dijelili vlastite korisničke lozinke za pristup informacijskom sustavu s drugim korisnicima. Time se, s jedne strane, pokazuje zrelost organizacije kada je riječ o informacijskoj sigurnosti, ponajviše zbog sigurnosne osviještenosti o tom pitanju, no istodobno otvara pitanje kolika je zapravo razina te osviještenosti zbog činjenice da je čak četvrtina ispitanika uočila dijeljenje lozinki, što može upućivati na ozbiljne sigurnosne propuste i nezadovoljavajuću razinu osviještenosti u organizaciji. Posebno zanimljivo vezano uz ovakve rezultate bilo bi vidjeti o kojim je odjelima u organizaciji bila riječ, što bi ujedno pokazalo gdje bi organizacije trebale usmjeriti napore u obliku dodatnih edukacija radi podizanja svijesti o informacijskoj sigurnosti.

Grafikon 11: *Ukupna distribucija odgovora na 9. pitanje s udjelom po sektoru za najčešći odgovor*



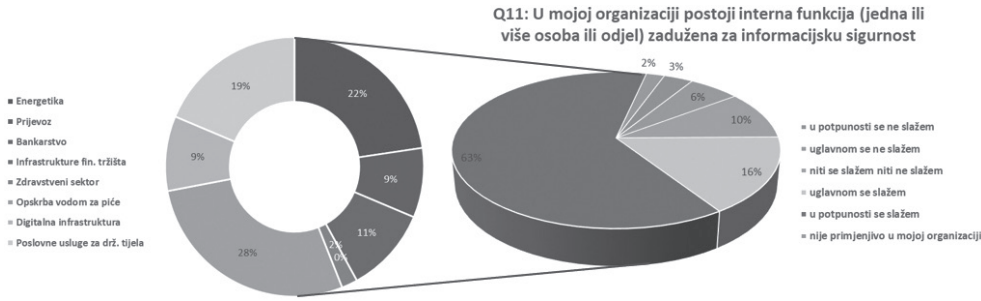
Iz Grafikona 11. vidljivo je da je nešto manje od trećine (29%) svih sudionika izjavilo kako ih u posljednjih 12 mjeseci sustav nije tražio da promijene lozinku, što je mogući indikator kako je u tim organizacijama postavljena slaba ili nikakva politika lozinki, čime se te organizacije izlažu nepotrebnom riziku kompromitacije pristupa informacijskom sustavu organizacije, a samim time i osjetljivim podacima. Iako je preporučljivo mijenjati lozinke barem jednom godišnje, ako je politika lozinki podešena tako da je rijetko mijenjanje lozinke kompenzirano njezinom povećanom kompleksnošću (veća duljina uz korištenje velikih slova, malih slova, brojeva i/ili posebnih znakova), tada se taj rizik smanjuje.

Grafikon 12: *Ukupna distribucija odgovora na 10. pitanje s udjelom po sektoru za najčešći odgovor*



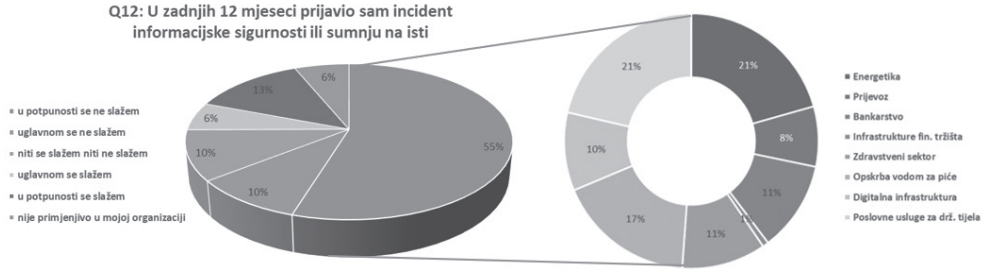
Grafikon 12. pokazuje kako više od polovice (61%) svih ispitanika u posljednjih 12 mjeseci nije dobilo poziv za sudjelovanje na edukaciji ili radionici za podizanje svijesti o informacijskoj sigurnosti, što svakako predstavlja dodatno područje za unapređenje. Podizanje svijesti o informacijskoj sigurnosti jedan je od ključnih elemenata kulture informacijske sigurnosti, a redovitim održavanjem takvih edukacija podiže se razina kultura informacijske sigurnosti u samoj organizaciji te ujedno i smanjuje vjerojatnost pojave sigurnosnih incidenata vezanih uz ljudski čimbenik.

Grafikon 13: *Ukupna distribucija odgovora na 11. pitanje s udjelom po sektoru za najčešći odgovor*



Kao što je vidljivo iz Grafikona 13., samo 9% svih sudionika tvrdi da u njihovoj organizaciji ne postoji interna funkcija zadužena za informacijsku sigurnost, što govori kako su organizacije prepoznale važnost informacijske sigurnosti kao nezaobilazne funkcije u današnjem turbulentnom okruženju temeljenom na pravodobnim informacijama i njihovoj zaštiti.

Grafikon 14: *Ukupna distribucija odgovora na 12. pitanje s udjelom po sektoru za najčešći odgovor*



Iz Grafikona 14. vidljivo je da je 65% svih sudionika izjavilo kako se uglavnom ili u potpunosti slaže s izjavom da u posljednjih 12 mjeseci nisu prijavili sigurnosni incident ili sumnju na njega. Taj podatak može se dvojako tumačiti – ili nije bilo pojave (potencijalnog) sigurnosnog incidenta ili zaposlenici nisu upoznati s procesom upravljanja incidentima informacijske sigurnosti. Međutim, svakako bi trebalo obratiti pozornost na činjenicu da je 6% svih sudionika izjavilo kako prijava sigurnosnih incidenata ili sumnje na njih nije primjenjiva na njihovu organizaciju. Ta činjenica otvara sumnju na to da te organizacije nisu primijenile mjere i standarde informacijske sigurnosti zahtijevane Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18.), što znači da taj dio predstavlja područje kojem je potrebno unapređenje u obliku jedne ili više mjera, poput primjerice formalne uspostave procesa upravljanja sigurnosnim incidentima (politika, procedura, određivanje uloga i odgovornosti), obavješćivanje svih zaposlenika o mogućnostima i načinima prijave incidenata ili redovito podizanje svijesti svih zaposlenika o tom pitanju.

4. ZAKLJUČAK I SMJERNICE ZA BUDUĆA ISTRAŽIVANJA

Relevantna literatura potvrdila je važnost tehnoloških rješenja u oblikovanju učinkovitih sigurnosnih rješenja, ali i naglasila potrebu za uravnoteženim pristupom na tom području, uključujući sociološko-organizacijski kontekst. Kako informacijska sigurnost više nije „tehničko pitanje“, nego više „ljudski problem“, koji zahtijeva uključenje višeg rukovodstva, raste potreba za holističkim proučavanjem kulture informacijske sigurnosti. Imajući to u vidu, cilj ovog istraživanja bio je provjeriti stanje kulture informacijske sigurnosti na temelju uspostavljenih sigurnosnih praksi, provedenog na 239 zaposlenika organizacija iz osam sektora koji predstavljaju operatore ključnih usluga u Republici Hrvatskoj.

Tumačeći dobivene rezultate na promatranom uzorku, možemo zaključiti da će u slučaju razvijene kulture informacijske sigurnosti biti prisutna provedba odgovarajućih mjera i standarda informacijske sigurnosti. Iako su rezultati ovog istraživanja pokazali kako je kultura informacijske sigurnosti u promatranim organizacijama na zadovoljavajućoj razini, također su uočena određena područja koja bi zahtijevala unapređenje. Ta područja bila su vezana uz neučestala upozorenja zaposlenicima na prijetnje vezane uz razne oblike računalnih virusa, ostavljanje otključanog računala nakon napuštanja radnog mjesta, rijetko mijenjanje korisničke lozinke, nedobivanja poziva za sudjelovanje na radionicama za podizanje svijesti o informacijskoj sigurnosti te naposljetku neinformiranost o postojanju mogućnosti prijave

sigurnosnih incidenata. U pravilu, sva ova područja mogu se adresirati redovnim održavanjem radionica za podizanje svijesti o informacijskoj sigurnosti na kojima bi se obradile te teme, čime bi se povećala uspješnost uspostavljenih sigurnosnih mjera te posljedično i zrelost sigurnosne kulture u organizaciji.

Teorijske implikacije ovog istraživanja upućuju na potrebu holističkog pristupa kulturi informacijske sigurnosti u obliku važnosti ne samo organizacijskih i tehničkih mjera nego i sociooloških čimbenika s obzirom na to da je ovo empirijsko istraživanje proizašlo na temelju teorijskog okvira koji se sastoji od navedena tri elementa. S druge strane, praktične implikacije istraživanja upućuju na mogućnost korištenja dobivenih rezultata kako bi se, prilikom organiziranja programa podizanja svijesti o informacijskoj sigurnosti u organizaciji, dodatni fokus stavio na identificirane probleme.

Glavno ograničenje ovog istraživanja jest nemogućnost korištenja probabilističkih metoda uzorkovanja zbog nedostupne informacije o cjelokupnoj veličini populacije, ali su rezultati istraživanja otvorili mogućnosti i za buduća istraživanja. Tako bi istraživanjem koje uključuje više sudionika, posebno ako bi se njihov odabir temeljio na probabilističkom uzorkovanju, mogla znatno povećati mogućnost generaliziranja zaključaka. Također bi bilo korisno provesti takva istraživanja u drugim sektorima, koji ne predstavljaju operatore ključnih usluga, kako bi se mogli usporediti rezultati u različitim industrijama i dati neke specifičnosti pojedine industrije, kao i vidjeti usporedbu stanja uspostavljenih mjera informacijske sigurnosti za organizacije kojima je to zakonska obveza, kao i onih kojima nije.

LITERATURA

1. AlHogail, A. i Mirza, A. (2015). *Organizational Information Security Culture Assessment*. U: The 2015 International Conference on Security and Management (pp. 286-292).
2. Alnatheer, M. A. (2014). *A Conceptual Model to Understand Information Security Culture*. International Journal of Social Science and Humanity, 4(2), 104-107.
3. Arbanas, K. (2020). *Ključni čimbenici kulture informacijske sigurnosti*. Policija i sigurnost, 29(4), 376-388.
4. Arbanas, K. (2021). *Radni okvir za procjenu i unapređenje kulture informacijske sigurnosti.* Doktorska disertacija. Varaždin: Fakultet organizacije i informatike.
5. Da Veiga, A., Astakhova, L. V., Botha, A. i Herselman, M. (2020). *Defining organisational information security culture – Perspectives from academia and industry*. Computers and Security, 92.
6. Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194/1.
7. ENISA. (2017). *Cyber Security Culture in organisations*.
8. Evripidou, S., Ani, U. D., D McK. Watson, J., Hailes, S. (2022). *Security Culture in Industrial Control Systems Organisations: A Literature Review*. U: Clarke, N., Furnell, S. (urednici) Human Aspects of Information Security and Assurance. HAISA 2022. IFIP Advances in Information and Communication Technology, vol. 658. Springer.

9. Evripidou, S., Ani, U. D., Hailes, S. i D McK. Watson, J. (2023). *Exploring the Security Culture of Operational Technology (OT) Organisations: The Role of External Consultancy in Overcoming Organisational Barriers*. U: Proceedings of the Nineteenth Symposium on Usable Privacy and Security. Anaheim, CA, SAD.
10. Gioulekas, F. i suradnici. (2022). *A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures*. Healthcare 2022, 10, 327.
11. IBM Security & Ponemon Institute. (2021). *Cost of Data Breach Report 2021*.
12. Kritzinger, E., Da Veiga, A. i van Staden, W. (2023). *Measuring organizational information security awareness in South Africa*. Information Security Journal: A Global Perspective, 32(2), 120-133.
13. Mahfuth, A., Yussof, S., Baker, A. A. i Ali, N. (2017a). *A systematic literature review: Information security culture.* U: International Conference on Research and Innovation in Information Systems, ICRIIS (pp. 1-6). Langkawi, Malezija.
14. Mahfuth, A., Yussof, S., Bakar, A. A., Ali, B. i Abdallah, W. (2017b). *A Conceptual Model for Exploring the Factors Influencing Information Security Culture*. International Journal of Security and Its Applications, 11(5), 15-26.
15. Masrek, M. N., Harun, Q. N. i Zaini, M. K. (2017). *Information Security Culture for Malaysian Public Organization: a Conceptual Framework*. U: 4Th International Conference on Education and Social Sciences 2017 (pp. 156-166). Istanbul, Turska.
16. Nasir, A., Arshah, R. A. i Ab Hamid, M. R. (2017). *Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture*. U: Proceedings of the 2017 International Conference on Information System and Data Mining (str. 56-60). Charleston, SAD: ACM New York, SAD.
17. Nasir, A., Abdullah Arshah, R. i Ab Hamid, M. R. (2019). *A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions.* Inf. Security Journal, 28(3), 55-80.
18. Nasir, A., Arshah, R. A., Hamid, M. R. A. i Fahmy, S. (2019). *An analysis on the dimensions of information security culture concept: A review*. Journal of Information Security and Applications, 44, 12-22.
19. Nævestad, T.-O., Honerud, J. H., Meyer, S. F. (2023). *Information Security Behaviour in an Organisation Providing Critical Infrastructure: A Pre-post Study of Efforts to Improve Information Security Culture*. U: Le Coze, JC., Antonsen, S. (urednici) Safety in the Digital Age. SpringerBriefs in Applied Sciences and Technology. Springer.
20. Orehek, Š. i Petrič, G. (2020). *A systematic review of scales for measuring information security culture.* Information and Computer Security.
21. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. i Zwaans, T. (2017). *The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies*. Computers and Security, 66, 40-51.
22. Sas, M., Hardyns, W., van Nunen, K., Reniers, G. i Ponnet, K. (2021). *Measuring the security culture in organizations: a systematic overview of existing tools*. Security Journal, 34, 340-357.
23. Sherif, E. i Furnell, S. (2015). *A Conceptual Model for Cultivating an Information Security Culture*. International Journal for Information Security Research, 5(2), 565-573.

24. Snyman, D. P., Kruger, H. i Kearney, W. D. (2018). *I shall, we shall, and all others will: paradoxical information security behaviour.* Inf. and Computer Security, 26(3), 290-305.
25. Soomro, Z. A., Shah, M. H. i Ahmed, J. (2016). *Information security management needs more holistic approach: A literature review*. International Journal of Information Management, 36(2), 215-225.
26. Stewart, H. i Jürjens, J. (2017). *Information security management and the human aspect in organizations*. Information and Computer Security, 25(5), 494-534.
27. Tang, M., Li, M. i Zhang, T. (2016). *The impacts of organizational culture on information security culture: a case study.* Information Technology and Management, 17(2), 179-186.
28. Tolah, A., Furnell, S. M. i Papadaki, M. (2017). *A Comprehensive Framework for Cultivating and Assessing Information Security Culture*. U: The Eleventh International Symposium on Human Aspects of Information Security & Assurance, 52-64.
29. Uchendu, B., Nurse, J. R. C., Bada, M. i Furnell, S. (2021). *Developing a cyber security culture: Current practices and future needs*. Computers and Security, 109.
30. Wiley, A., McCormac, A. i Calic, D. (2020). *More than the individual: Examining the relationship between culture and Information Sec. Awareness*. Comp. and Security, 88.
31. Yildirim, E. (2016). *The importance of information security awareness for the success of business enterprises.* U: Advances in Intelligent Systems and Computing (pp. 211-222).
32. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne novine br. 64/18.

Summary

Krunoslav Arbanas

Evaluation of Information Security Culture of Key Service Operators

Relevant literature has been pointing out for many years that information security has ceased to be exclusively technical and has become primarily a business issue with a particular emphasis on the human factor. With this shift in thinking, the focus changes from exclusively technical security measures to organizational and sociological protection elements, bringing information security culture into focus. A well-established information security culture, which, in addition to established technical measures, considers sociological factors and organizational measures, can not only contribute to the protection of information but also change the way employees think so that they stop viewing information security as an obstacle in their daily work. This paper presents the results of empirical research of information security culture based on established security practices conducted on 239 employees of organizations from 8 sectors representing key service operators in the Republic of Croatia.

Keywords: information security, cybersecurity, information security culture, security culture.