PREGLEDNI ZNANSTVENI ČLANAK

UDK: 004.056
Primljeno: rujan 2020.

KRUNOSLAV ARBANAS*

Ključni čimbenici kulture informacijske sigurnosti

Sažetak

Novija istraživanja pokazuju da je za pravilno upravljanje informacijskom sigurnošću, osim odavno prepoznatih tehničkih mjera, potrebno uzeti u obzir i ne-tehničke mjere s posebnim naglaskom na ljudskome čimbeniku. Jedna od tih mjera jest i kultura informacijske sigurnosti koja, ako je dobro uspostavljena i podržana od višeg rukovodstva, može značajno pridonijeti zaštiti informacijske imovine pretvaranjem ljudi, kao prepoznatog problema informacijske sigurnosti, u rješenje tog problema. Potreba za uspostavom dobre kulture informacijske sigurnosti posebno dolazi do izražaja u slučaju organizacija koje predstavljaju tzv. kritičnu nacionalnu infrastrukturu koja je u današnje vrijeme sve češća meta kibernetičkih napada, a prvi je korak u uspostavi kulture informacijske sigurnosti identifikacija čimbenika koji čine tu kulturu. Cilj je ovoga rada sažeti najcitiranije ključne čimbenike kulture informacijske sigurnosti identificirane na temelju pregleda znanstvenih članaka indeksiranih u relevantnim bazama podataka te na kraju navesti utvrđene nedostatke u istraživanjima i pružiti čitateljima moguće smjernice za daljnja istraživanja.

Ključne riječi: *informacijska sigurnost, kultura informacijske sigurnosti, sigurnosna kultura, kritična nacionalna infrastruktura, ključni čimbenici.*

UVOD

Istraživači već stanovito vrijeme naglašavaju da se u borbi za postizanje informacijske sigurnosti više ne može oslanjati samo na tehničke kontrole i mjere zaštite (Yildirim, 2016), već se mora rabiti i ne-tehničke mjere, s posebnim naglaskom na ljudskome čimbeniku (Glaspie i Karwowski, 2018; AlHogail, 2015; Sherif i sur., 2015; Choi i sur., 2018).

Sigurnosni incidenti i kršenja sigurnosti često su uzrokovani neznanjem, stavom zaposlenika ili nedostatkom svijesti o informacijskoj sigurnosti (Mahfuth i sur., 2017a), čime se

* Krunoslav Arbanas, dipl. inf., Hrvatska energetska regulatorna agencija, Zagreb; Sveučilište u Zagrebu, Fakultet organizacije i informatike, Varaždin, Republika Hrvatska.

stavlja fokus na ne-tehničke mjere poput edukacije, obuke i osviještenosti o informacijskoj sigurnosti, osiguravajući time razumijevanje odgovornosti zaposlenika za svoje ponašanje prema informacijskoj sigurnosti (Chen i sur., 2015) i pretvarajući na taj način ljude iz prijetnji u rješenje (Mahfuth i sur., 2017a), ujedno naglašavajući činjenicu da je zaštita organizacijskih informacija odgovornost svih zaposlenika (Metalidou i sur., 2014).

Budući da je cilj zaštite informacija često u određenoj mjeri u sukobu s uobičajenim poslovnim ciljevima smanjenja troškova i maksimiziranja produktivnosti, potrebno je izgraditi odnos prema informacijskoj sigurnosti na takav način da informacijska sigurnost postaje prirodni dio svakodnevne rutine svih zaposlenika (Choi i sur., 2018) osiguravajući pritom da uspostavljene sigurnosne kontrole nisu pretjerane već razmjerne stvarnim rizicima unutar organizacije - odnosno da su smislene i što manje nametljive (Metalidou i sur., 2014). Sukladno s tim, zaključak je da primjerena razina informacijske sigurnosti u organizacijama zahtijeva višedimenzionalni holistički pristup (Yildirim, 2016). Iz tog razloga, Panguluri i suradnici (Panguluri i sur., 2017) uspoređuju takav pristup sa svojevrsnim tronošcem u kojem su *tehničke mjere*, kao što su vatrozid, antivirusni softver, enkripcija i sl., bitan element zaštite informacijske imovine, ali predstavljaju samo jednu „nogu“ spomenutog tronošca i samostalno nisu dovoljne bez drugih dviju „nogu“ - *ljudi* i *procesa*. Yildrim (Yildrim, 2016) vidi *tehnologiju*, *ljude* i *edukaciju* kao tri komponente holističkog pristupa, dok su za AlHogaila i Mirzu (AlHogail i Mirza, 2014) te kritične komponente *ljudi*, *organizacija* i *tehnologija*.

U konačnici to znači da, čak i ako organizacija uspostavi sustav upravljanja informacijskom sigurnošću prema preporukama sigurnosnih normi, nije zajamčeno sigurnosno prihvatljivo ponašanje zaposlenika što dovodi do potrebe za uspostavom primjerene kulture informacijske sigurnosti unutar organizacije, kao ključnim elementom za upravljanje ljudskim čimbenicima uključenim u informacijsku sigurnost koji može značajno doprinijeti zaštiti informacijske sigurnosti tako da ljude, iz prepoznatog problema informacijske sigurnosti, pretvori u rješenje tog problema.

Međutim, primjerena kultura informacijske sigurnosti ne može se uspostaviti bez formalno dokumentiranih sigurnosnih politika i procedura (Panguluri i sur., 2017), iako ne postoji jedinstveni pristup za upravljanje sigurnosnim politikama i procedurama (Kam i sur., 2020). Tome u prilog govore i rezultati istraživanja koje je provela Da Veiga koja je empirijski potvrdila hipotezu kako se broj sigurnosnih incidenata smanjio, odnosno s vremenom se poboljšala kultura informacijske sigurnosti, u organizacijama u kojima su zaposlenici upoznati s politikama informacijske sigurnosti (Da Veiga, 2016). Također, dosljedna podrška rukovodstva ključna je za stvaranje podržavajućeg okruženja u organizaciji (Glaspie i Karwowski, 2018) kako bi se podigla svijest o sigurnosti u zaposlenika (Yoo i sur., 2019) i kako bi se svi zaposlenici uključili u zahtjeve informacijske sigurnosti, čime se njeguje kultura informacijske sigurnosti (Panguluri i sur., 2017) koja može ili pridonijeti zaštiti informacijske imovine ili stvoriti rizike informacijske sigurnosti (Da Veiga, 2018) - odnosno pozitivno ili negativno oblikovati sâmo okruženje informacijske sigurnosti (Kam i sur., 2020).

Ovaj rad predstavlja istraživanje koje donosi pregled relevantne literature o kulturi informacijske sigurnosti kao i stavljanje kulture informacijske sigurnosti u kontekst kritične nacionalne infrastrukture. Opći je cilj ovog rada pružiti pregled trenutačnih istraživanja kulture informacijske sigurnosti dok je posebni cilj - pružiti pregled ključnih čimbenika koji čine kulturu informacijske sigurnosti kako to vide istraživači iz domene informacijske sigurnosti.

1. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

Pretraživanjem ključnih pojmova „secur* AND culture“ u bazama znanstvenih članaka *Web of Science (WoS), Science Direct, Emerald Insight, Springer Link, IEEE Xplore Digital Library* i *Google Scholar*, moguće je utvrditi da je informacijska sigurnost izrazito aktualna tema, i u stručnom i u znanstvenom krugu; što je rezultiralo brojnim istraživanjima u spomenutoj domeni. Sama kultura informacijske sigurnosti kao specifična tema u ovoj širokoj domeni u velikoj je mjeri zastupljena u znanstvenim istraživanjima, no ona se izričito ne odnosi na istraživanja povezana s kritičnom nacionalnom infrastrukturom iako postoje neki radovi (Yoo i sur., 2019) koji implicitno povezuju te dvije domene.

1.1. Kultura informacijske sigurnosti

Kultura informacijske sigurnosti pojavila se krajem 90-ih godina 20. stoljeća kao mjera za promicanje ponašanja zaposlenika u organizacijama koje je u skladu s propisanim pravilima informacijske sigurnosti zbog činjenice da se ljudi u literaturi često nazivaju „najslabijom karikom u sigurnosnom lancu“ (Mahfuth i sur., 2017a; Yoo i sur., 2019; Metalidou i sur., 2014) budući da, namjerno ili iz nehaja, predstavljaju najveću prijetnju informacijskoj sigurnosti organizacije (Mahfuth i sur., 2017a; Stewart i Jürjens, 2017). Zorni primjer izravnog ljudskog utjecaja na povećane rizike zbog curenja podataka ili njihova gubitka jest takozvana „skrivena informacijska tehnologija“ (engl. *Shadow IT*) koja se odnosi na „*uporabu rješenja i sustava informacijske tehnologije bez prethodnog izričitog odobrenja organizacije*“ (Sillic, 2019) gdje nekontrolirana instalacija softvera, priključivanje neprovjerene USB memorije u računalo ili omogućavanje nepoznate makronaredbe može nanijeti nepopravljivu štetu organizacijskim podacima.

Postoje brojne definicije kulture informacijske sigurnosti, primjerice da je to „*proces integracije vjerovanja, percepcija, stavova, vrijednosti, pretpostavki i znanja koja vode, usmjeravaju i upravljaju percepcijama i stavovima zaposlenika čime se utječe na njihovo sigurnosno ponašanje*“ (Mahfuth i sur., 2017a). S druge pak strane, (Da Veiga, 2018) proširuje ovu definiciju i tvrdi da kultura informacijske sigurnosti predstavlja „*stavove, pretpostavke, vjerovanja, vrijednosti i znanje koje zaposlenici/dionici koriste za interakciju s organizacijskim sustavima i procedurama u bilo kojem trenutku, gdje interakcija rezultira prihvatljivim ili neprihvatljivim ponašanjem koje se očituje u artefaktima i tvorbama koji postaju dio načina na koji se stvari rade u organizaciji radi zaštite informacijske imovine*“.

Kao što je očito iz gore navedenih definicija, veliki naglasak stavljen je na zaposlenike, što je i razumljivo zbog činjenice da se sadašnji i bivši zaposlenici smatraju jednim od glavnih uzroka incidenata vezanih uz informacijsku sigurnost (Da Veiga i Martins, 2015; Choi i sur., 2018). Tome u prilog govori i istraživanje koje je proveo PwC u Singapuru (PwC, 2018); gdje su 2017. godine ispitanici kao izvore sigurnosnih incidenata na prva dva mjesta postavili trenutačne (38 %) i bivše zaposlenike (32 %), dok su treće mjesto (30 %) zauzele ostale vanjske organizacije i aktivisti koji su godinu dana ranije bili rangirani na prvome mjestu sa 32 %, a sadašnji ili bivši zaposlenici dijelili su drugo mjesto sa 25 %.

Istraživanje koje je provela tvrtka EY (EY, 2017) utvrdilo je da se postotak ispitanika koji su, kao izvor sigurnosnih ranjivosti, prepoznali nemarne ili neupućene zaposlenike,

u 2017. godini povećao na 60 % u odnosu na prethodne dvije godine kada je taj postotak bio 44 %. Također, 64 % sudionika istraživanja identificiralo je zlonamjerni softver (engl. *Malware*) i lažno predstavljanje radi krađe identiteta (engl. *Phishing*) kao izvor sigurnosnih prijetnji za organizacije, u usporedbi s postotkom od 44 % za zlonamjerni softver i 43 % za lažno predstavljanje, u istraživanju dvije godine ranije. To ne čudi, jer su napadi socijalnog inženjeringa, od kojih je jedan lažno predstavljanje radi krađe identiteta, već neko vrijeme prepoznati kao glavna sigurnosna prijetnja zbog svoje prirode ciljanja na ljudske ranjivosti iskorištavanjem karakteristika i ponašanja ljudi (Metalidou i sur., 2014).

U relevantnim istraživanjima iz područja kulture informacijske sigurnosti autori su se bavili temama koje uključuju procjenu i mjerenje kulture informacijske sigurnosti (Masrek, 2017; Sas i sur., 2020; Alnatheer, 2014) te njezino prihvaćanje u organizacijama (Mokwetli i Zuva, 2018); zatim identificiranje čimbenika kulture informacijske sigurnosti (Masrek, 2017; Hassan i Ismail, 2012; Mahfuth i sur., 2017b; Sherif i sur., 2015; Alnatheer, 2015; Nasir i sur., 2017), kao i razvoj okvira kulture informacijske sigurnosti (AlHogail i Mirza, 2014; AlHogail, 2015). Također, zamijećeno je i nekoliko sustavnih pregleda literature (Karlsson i sur., 2015; Mahfuth i sur., 2017a; AlHogail i Mirza, 2014; Hassan i sur., 2015; Nasir i sur., 2019; da Veiga i sur., 2020).

Rezultati tih istraživanja prepoznali su činjenicu da su postojeća istraživanja uvelike filozofska, opisna ili teorijska, kao i činjenicu da nedostaje znanje o prepoznavanju čimbenika kulture informacijske sigurnosti i mjerenju njihova utjecaja na kulturu informacijske sigurnosti (Nasir i sur., 2017) te da postoji potreba za sveobuhvatnim empirijskim istraživanjima iz navedena područja (Mahfuth i sur., 2017b; Karlsson i sur., 2015; Nasir i sur., 2019), posebno u dijelu definiranja sveobuhvatnog okvira za uspostavu kulture informacijske sigurnosti u organizaciji (AlHogail i Mirza, 2014). Tome u prilog govori i pregled literature o objavljenim radovima iz područja kulture informacijske sigurnosti između 2003. i 2013. godine koji su proveli AlHogail i Mirza (AlHogail i Mirza, 2014) i otkrili da je samo 14 radova (22 % od ukupno objavljenih radova) predstavilo neku vrstu okvira za uspostavu kulture informacijske sigurnosti, a samo su 2 od 13 istraživačkih modela, koje je Alnatheer (Alnatheer, 2014) prepoznao u svojem pregledu literature, osigurala validirani instrument za vrednovanje kulture informacijske sigurnosti. S tim u vezi, osnovna pretpostavka za izradu neke vrste okvira za uspostavu kulture informacijske sigurnosti jest identifikacija ključnih čimbenika kulture informacijske sigurnosti – stoga tablica 1 prikazuje najčešće citirane ključne čimbenike kulture informacijske sigurnosti u relevantnoj literaturi.

Tablica 1: Ključni čimbenici kulture informacijske sigurnosti pronađeni u relevantnoj literaturi

R. br.	Ključni čimbenik	Referenca
1.	**Svijest o informacijskoj sigurnosti**	Masrek, 2017; Hassan i sur., 2015; Alnatheer, 2015; Glaspie i Karwowski, 2018; Mahfuth i sur., 2017a; Hassan i Ismail, 2012; Mahfuth i sur., 2017b; Sherif i sur., 2015; Da Veiga i Martins, 2015; Yoo i sur., 2019; Nasir i sur., 2017; Choi i sur., 2018; Sillic, 2019.
2.	**Podrška rukovodstva**	Masrek, 2017; Hassan i sur., 2015; Alnatheer, 2015; Mahfuth i sur., 2017a; Glaspie i Karwowski, 2018; Mahfuth i sur., 2017b; Panguluri i sur., 2017; Da Veiga, 2016; Nasir i sur., 2017.
3.	**Politike i procedure informacijske sigurnosti**	Masrek, 2017; Hassan i sur., 2015; Alnatheer, 2015; Glaspie i Karwowski, 2018; Mahfuth i sur., 2017a; Mahfuth i sur., 2017b; Sherif i sur., 2015; Da Veiga i Martins, 2015; Panguluri i sur., 2017; Yoo i sur., 2019; Nasir i sur., 2017; Choi i sur., 2018.
4.	**Obuka**	Alnatheer, 2015; Glaspie i Karwowski, 2018; Mahfuth i sur., 2017a; Mahfuth i sur., 2017b; Da Veiga i Martins, 2015; Stewart i Jürjens, 2017; Yoo i sur., 2019; Nasir i sur., 2017; Choi i sur., 2018.
5.	**Usklađenost**	Masrek, 2017; Alnatheer, 2015; Mahfuth i sur., 2017a; Mahfuth i sur., 2017b; Stewart i Jürjens, 2017; Yoo i sur., 2019; Nasir i sur., 2017.
6.	**Znanje**	Hassan i sur., 2015; Hassan i Ismail, 2012; Mahfuth i sur., 2017a; Mahfuth i sur., 2017b; Nasir i sur., 2017.
7.	**Sigurnosno ponašanje**	Hassan i sur., 2015; Hassan i Ismail, 2012; Mahfuth i sur., 2017b; Sherif i sur., 2015; Nasir i sur., 2017.
8.	**Uloge i odgovornosti**	Mahfuth i sur., 2017b; Panguluri i sur., 2017; Chen i sur., 2015; Yoo i sur., 2019.
9.	**Uvjerenja**	Hassan i sur., 2015; Mahfuth i sur., 2017b; Yoo i sur., 2019; Nasir i sur., 2017.
10.	**Procjena i analiza rizika**	Alnatheer, 2015; Mahfuth i sur., 2017a; Mahfuth i sur., 2017b; Nasir i sur., 2017.
11.	**Etičko ponašanje**	Alnatheer, 2015; Mahfuth i sur., 2017a; Mahfuth i sur., 2017b; Nasir i sur., 2017.
12.	**Edukacija**	Alnatheer, 2015; Sherif i sur., 2015; Yoo i sur., 2019.
13.	**Povjerenje**	Hassan i sur., 2015; Mahfuth i sur., 2017b; Nasir i sur., 2017.
14.	**Upravljanje promjenama**	Hassan i Ismail, 2012; Mahfuth i sur., 2017b
15.	**Tehnologija**	Masrek, 2017; Mahfuth i sur., 2017b

Kao što je vidljivo, različiti autori navode različite čimbenike koji utječu na kulturu informacijske sigurnosti što dovodi do zaključka kako ne postoji konsenzus u postojećim istraživanjima oko toga koji su to zapravo ključni čimbenici kulture informacijske sigurnosti.

1.2. Kritična nacionalna infrastruktura

Izraz „kritična infrastruktura“ obično se rabi za opisivanje infrastrukture, sustava i imovine koji su toliko važni za društvo i gospodarstvo da bi nedostupnost ili uništenje takve infrastrukture moglo dovesti do velikih poremećaja u društvu i gospodarstvu (Thacker i sur., 2017) - gdje bi učinci spomenutih poremećaja mogli negativno utjecati ne samo na lokalno, regionalno ili nacionalno, već potencijalno čak i na globalno gospodarstvo (Maglaras i sur.,

2018). U hrvatskom Zakonu o kritičnim infrastrukturama (NN 56/13.) članak 3. navodi kako su nacionalne kritične infrastrukture *„sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti"*.

Različite države u svijetu identificirale su različite sektore koji čine njihovu kritičnu infrastrukturu. U Ujedinjenom je Kraljevstvu kritična nacionalna infrastruktura razvrstana u 13 sektora: komunikacije, hitne službe, energetika, financijske usluge, hrana, državna uprava, zdravstvo, prijevoz, vodno gospodarstvo, obrana, civilna nuklearna industrija te svemirska i kemijska industrija (Chaurasia i sur., 2016; The Parliamentary Office of Science and Technology, 2017). U SAD-u je Ministarstvo za unutarnju sigurnost identificiralo 16 ključnih infrastrukturnih sektora, od kojih 12 odgovara kategorizaciji nacionalne infrastrukture u Velikoj Britaniji, a dodatni su sektori komercijalni sektor, kritična proizvodnja, brane i informacijska tehnologija (Chaurasia i sur., 2016). Njemačka i Kanada imaju po 10 kritičnih sektora, od kojih je osam zajedničko (informacijsko-komunikacijska tehnologija, energetika, financije, državna uprava, javno zdravstvo, promet i vodno gospodarstvo), a razlikuju se u sektorima hitnih službi i kulturne baštine za Njemačku (Federal Republic of Germany, 2009); odnosno sektorima proizvodnje i zaštite za Kanadu (Her Majesty the Queen in Right of Canada, 2009). Australija je identificirala osam sektora kritične infrastrukture koje čine telekomunikacije, energetika, vodno gospodarstvo, državna uprava, promet, zdravstvo, bankarstvo i financije te hrana (Australian Government i Critical Infrastructure Centre, 2019).

Republika Hrvatska svojim Zakonom o kritičnim infrastrukturama (NN 56/13.) identificirala je 10 sektora koji se smatraju nacionalnom kritičnom infrastrukturom. Radi se o sljedećim sektorima: *energetika*, *komunikacijska i informacijska tehnologija*, *promet*, *zdravstvena zaštita*, *vodno gospodarstvo*, *hrana*, *financije*, *proizvodnja, skladištenje i prijevoz opasnih tvari*, *javni sektor* te *nacionalni spomenici i vrijednosti*. Kao dodatni, jedanaesti sektor, Vlada Republike Hrvatske 2013. godine u svojoj je Odluci o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura (NN 56/2013.) - navela znanost i obrazovanje. Sama provedba spomenuta Zakona nije zaživjela u željenome opsegu zbog činjenice da je izostala identifikacija konkretnih infrastruktura u navedenim sektorima, kao i određivanje sigurnosnih zahtjeva prema njima (Ured Vijeća za nacionalnu sigurnost, 2018.) što je djelomično riješeno donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18.); a djelomično i zato što spomenuti Zakon o kibernetičkoj sigurnosti raspisuje kriterije za identifikaciju konkretnih organizacija operatora ključnih usluga iz manje (8) sektora negoli što to propisuju Zakon o kritičnoj infrastrukturi i pripadajuća Odluka Vlade Republike Hrvatske (11).

Kao što je vidljivo iz tablice 2, od spomenutih 11 sektora iz jednoga odnosno 8 sektora iz drugoga Zakona, njih šest podudara se u oba Zakona (energetika, digitalna infrastruktura, prijevoz, zdravstveni sektor, opskrba vodom za piće i njezina distribucija te bankarstvo). S druge pak strane, pet sektora (hrana, proizvodnja, skladištenje i prijevoz opasnih tvari, javne službe, nacionalni spomenici i vrijednosti te znanost i obrazovanje) prisutno je u Zakonu o kritičnim infrastrukturama i pripadajućoj Odluci Vlade Republike Hrvatske, a nisu u Zakonu o kibernetičkoj sigurnosti, odnosno obrnuto, dva sektora (infrastrukture financijskog tržišta i poslovne usluge za državna tijela), nalaze se u Zakonu o kibernetičkoj sigurnosti, a ne zatiču se u Zakonu o kritičnim infrastrukturama i pripadajućoj Odluci Vlade Republike Hrvatske.

Tablica 2: Identificirani sektori koji čine kritičnu nacionalnu infrastrukturu Republike Hrvatske

	Zakon o kritičnim infrastrukturama (NN 56/13.)	**Zakon o kibernetičkoj sigurnosti (NN 64/18.)**
Sektor	Energetika	Energetika
	Komunikacijska i informacijska tehnologija	Digitalna infrastruktura
	Promet	Prijevoz
	Zdravstvo	Zdravstveni sektor
	Vodno gospodarstvo	Opskrba vodom za piće i njezina distribucija
	Hrana	
	Financije	Bankarstvo
	Proizvodnja, skladištenje i prijevoz opasnih tvari	
	Javne službe	
	Nacionalni spomenici i vrijednosti	
	Znanost i obrazovanje*	
		Infrastrukture financijskog tržišta
		Poslovne usluge za državna tijela
∑	**11**	**8**

* Na temelju Odluke Vlade Republike Hrvatske (NN 108/2013.)

Izvor: vlastiti prikaz na temelju Zakona o kritičnim infrastrukturama (NN 56/13.), Odluci o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura (NN 56/2013.) i Zakona o kibernetičkoj sigurnosti operatora ključnih usluga u davatelja digitalnih usluga (NN 64/18.)

Kibernetički napadi često iskorištavaju tehničke ranjivosti u računalnim sustavima, ali također i nedostatak svijesti među ljudima koji koriste te sustave, pa često nije izuzetak da napadi ciljaju oboje (The Parliamentary Office of Science and Technology, 2017). Tako su primjerice organizacije iz sektora energetike osjetljivije na terorizam ili aktivizam dok su u financijskom sektoru izraženije sigurnosne prijetnje kao što su prijevare ili krađe (Sas i sur., 2020). Prema istraživanju koje je proveo PwC (PwC, 2018), tri glavna područja na kojima se događaju kibernetički incidenti jesu: iskorištavanje ranjivosti u mobilnim uređajima, lažno predstavljanje radi krađe identiteta (engl. *Phishing*) i iskorištavanje slabosti zaposlenika.

Također, iako su ljudi prepoznati kao ključni čimbenik (ne)uspješnog upravljanja informacijskom sigurnošću u organizacijama (Yildirim, 2016), još se uvijek događa sve veći broj incidenata informacijske sigurnosti uzrokovanih ljudima. Stavimo li činjenicu da kultura informacijske sigurnosti može ili pridonijeti zaštiti informacija ili stvoriti rizik (Da Veiga, 2018) u kontekst kritične nacionalne infrastrukture - potreba za razvojem općeg i sveobuhvatnog okvira za procjenu i uspostavu kulture informacijske sigurnosti postaje još izraženija zbog toga što su upravo te organizacije u današnje vrijeme sve češće mete različitih oblika incidenata vezanih uz informacijsku sigurnost a zbog svoje strateške važnosti za pojedinu državu.

Noviji primjer kibernetičkih napada na nacionalnu infrastrukturu jest pad elektroenergetske mreže u Ukrajini 2015. godine (koji se ponovio godinu dana kasnije) kada je napad na tri tvrtke za distribuciju električne energije izazvao prekid napajanja električnom energijom koji je zahvatio oko 225.000 korisnika. Vjeruje se da su napadači koristili lažne poruke elektroničke pošte za pristup ciljanim mrežama šest mjeseci prije napada, tijekom kojih su stekli sigurnosne vjerodajnice i znanje o infrastrukturi potrebno za dovršavanje napada (The Parliamentary Office of Science and Technology, 2017; Mansfield-Devine, 2018). Drugi je primjer napad zlonamjernog softvera Stuxnet (Maglaras i sur., 2018), koji je uspio uništiti centrifuge u iranskoj nuklearnoj elektrani, iako njezina računalna mreža nije bila spojena s vanjskim mrežama, na način da je preuzeo kontrolu nad Siemensovim programibilnim logičkim kontrolerima (PLC-ima) (Mansfield-Devine, 2018).

Najpoznatiji su hrvatski primjeri kibernetičkih napada *phishing* napadi na državni i javni sektor 2018. godine, koji su tada postali nadaleko poznati po primjeru grada Đakova, čiji je zaposlenik uplatio 50.000 € na račun Johna Smitha bez provjere autentičnost elektroničke pošte koju je zaprimio, kako se činilo prema zaglavlju elektroničke poruke, od svojeg šefa, gradonačelnika (Novi list, 2018.). Drugi poznati domaći primjer kibernetičkog napada koji je odjeknuo u javnosti bio je nedavni napad na naftnu kompaniju INA d.d. koji je započeo na Valentinovo 2020. godine i trajao bez prekida nekoliko dana. Službene izjave koje su se tih dana mogle dobiti od INA-e bile su šture i uključivale su samo obrazloženje o tome kako se radi o napadima uskraćivanja usluge (engl. *Denial of Service*); dok su službeni uzrok, razmjer i posljedice ovoga napada ostali nepoznati (Ivezić, 2020).

Iz navedenih primjera vidljivo je kako je zajednički nazivnik svih tih napada upravo ljudski čimbenik, što još jednom potvrđuje tvrdnju koja je u više navrata spomenuta u ovome radu, a to je da su ljudi kritični element informacijske sigurnosti o kojem je svakako potrebno voditi brigu prilikom planiranja primjerenog upravljanja informacijskom sigurnošću.

2. ZAKLJUČAK I SMJERNICE ZA BUDUĆA ISTRAŽIVANJA

Pitanje sigurnosti informacijskih sustava, a samim time i informacija kao ključnih resursa u današnjem informacijskom društvu, nešto je s čime se u nekom obliku suočava svaka organizacija neovisno o tome o kojem se sektoru poslovanja radi. Informacijska sigurnost više nije isključivo tehnički problem, već ponajprije problem upravljanja koji zahtijeva uključivanje višeg rukovodstva u uspostavljanje sigurnosnih politika, procedura i organizacijske strukture za upravljanje informacijskom sigurnošću, a zahtijeva i edukaciju, obuku i podizanje svijesti o informacijskoj sigurnosti kod zaposlenika.

Istraživanja iz domene informacijske sigurnosti dosljedno pokazuju da zaposlenici predstavljaju najveću prijetnju informacijskoj sigurnosti i stoga predstavljaju presudni čimbenik u procesu upravljanja informacijskom sigurnošću. No isto tako, iako su zaposlenici dio problema informacijske sigurnosti, oni su također i dio rješenja (Mahfuth i sur., 2017a), budući da se razina informacijske sigurnosti u organizaciji može povećati edukacijom, obukom i podizanjem svijesti o sigurnosti informacija. Drugim riječima, uspostavljanjem kulture informacijske sigurnosti u kojoj je sigurnost informacija odgovornost svih zaposlenika može se umanjiti vjerojatnost incidentnih i neželjenih situacija koje imaju za posljedicu narušavanje povjerljivosti, integriteta ili dostupnosti tih informacija.

Aktualna literatura također prepoznaje činjenicu da su postojeća istraživanja u velikoj mjeri opisna ili teorijska, kao i da postoji nedostatak znanja u prepoznavanju čimbenika i mjerenju njihova utjecaja na kulturu informacijske sigurnosti te se javlja potreba za empirijskim istraživanjem (Mahfuth i sur., 2017b; Karlsson i sur., 2015), posebno u dijelu definiranja sveobuhvatnog okvira za uspostavu kulture informacijske sigurnosti u organizaciji (AlHogail i Mirza, 2014). Dodatni je problem činjenica da u literaturi ne postoje široko prihvaćene dimenzije kulture informacijske sigurnosti što nas dovodi u situaciju da različita istraživanja kulture informacijske sigurnosti rabe različite perspektive i koncepte, odnosno različite dimenzije i čimbenike (Nasir i sur., 2017), koji se ne mogu usporediti. To predstavlja dvosmjerni problem: za istraživače je taj problem vidljiv u potrebi identificiranja stvarnih koncepata kulture informacijske sigurnosti kako se nalazi pojedinog istraživanja kulture sigurnosti informacija ne bi ograničavali te time onemogućavali daljnje generaliziranje i primjenu - dok praktičarima taj problem predstavlja nemogućnost njegovanja i procjene pozitivne kulture informacijske sigurnosti u organizaciji (Nasir i sur., 2019), budući da ne postoje usuglašeni stavovi oko ključnih čimbenika koji čine kulturu informacijske sigurnosti.

Na temelju prethodno iznesenih zapažanja identificirano je nekoliko mogućih pravaca za daljnja istraživanja kulture informacijske sigurnosti. Buduća istraživanja mogla bi istražiti dodatne ključne čimbenike kulture informacijske sigurnosti i analizirati odnose među njima kako bi se bolje razumjela njihova međusobnu povezanost. Drugo, mogao bi se predložiti sveobuhvatan okvir/model kulture informacijske sigurnosti, temeljen na utvrđenim ključnim čimbenicima koji bi pomogli uspostavi i/ili unapređenju kulture informacijske sigurnosti u organizacijama, posebno onima koje su prepoznate kao kritična nacionalna infrastruktura. Treće, kao što je navedeno već nekoliko puta prije, osobito je potrebna empirijska validacija predloženih teorijskih modela zbog nedostatka empirijskih dokaza o važnosti identificiranih ključnih čimbenika. Četvrto, bilo bi zanimljivo ispitati što dovodi do uspostavljanja identificiranih ključnih čimbenika kulture informacijske sigurnosti unutar organizacije, tj. što su prethodnici tih čimbenika. Posljednje, ali ne manje bitno, potrebno je provesti više istraživanja o odnosu kulture informacijske sigurnosti i sigurnosnim izazovima povezanim s novim tehnologijama, poput primjerice kognitivnog računarstva, pametnih mreža, robotizacije, interneta stvari (engl. *Internet of Things*) i sl.

Zaključno, potrebno je naglasiti kako će prepoznavanje ključnih čimbenika kulture informacijske sigurnosti i njihova validacija empirijskim istraživanjem u konačnici omogućiti rukovodstvu organizacije usmjeravanje ograničenih resursa na one elemente koji su ključni za održivu kulturu informacijske sigurnosti. Njegujući dobru kulturu informacijske sigurnosti unutar organizacije, zaposlenici se više neće doživljavati kao sigurnosni rizik već kao rješenje jednog ili više sigurnosnih pitanja istovremeno, povećavajući otpornost organizacije na različite oblike kibernetičkih napada i ugroza vezanih uz kompromitaciju povjerljivosti, integriteta i dostupnosti informacijske imovine organizacije.

LITERATURA

1. AlHogail, A. (2015). *Design and validation of information security culture framework*. Computers in Human Behavior, 49, 567-575.
2. Alhogail, A. i Mirza, A. (2014). *Information security culture: A definition and a literature review*. U: 2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014. Hammamet, Tunis: IEEE.
3. Alnatheer, M. A. (2014). *A Conceptual Model to Understand Information Security Culture*. International Journal of Social Science and Humanity, 4(2), 104-107.
4. Alnatheer, M. A. (2015). *Information Security Culture Critical Success Factors*. U: 2015 12th International Conference on Information Technology - New Generations (str. 731-735). Las Vegas, SAD.
5. Australian Government i Critical Infrastructure Centre. (2019). *Critical Infrastructure Centre Compliance Strategy*. (https://cicentre.gov.au/document/P10S011 - 02.09.2020.)
6. Chaurasia, P., Yogarajah, P., Condell, J., Prasad, G., McIlhatton, D. i Monaghan, R. (2016). *Countering terrorism, protecting critical national infrastructure and infrastructure assets through the use of novel behavioral biometrics*. Behavioral Sciences of Terrorism and Political Aggression, 8(3), 197-211.
7. Chen, Y., Ramamurthy, K., i Wen, K. W. (2015). *Impacts of comprehensive information security programs on information security culture*. Journal of Computer Information Systems, *55*(3), 11-19.
8. Choi, S. E., Martins, J. T. i Bernik, I. (2018). *Information security: Listening to the perspective of organisational insiders*. Journal of Information Science, 44(6), 752-767.
9. Da Veiga, A. (2016). *Comparing the information security culture of employees who had read the information security policy and those who had not*. Information and Computer Security, 24(2), 139-151.
10. Da Veiga, A. (2018). *An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture*. Information & Computer Security, 26(5), 584-612.
11. 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, 101713.
12. Da Veiga, A. i Martins, N. (2015). *Improving the information security culture through monitoring and implementation actions illustrated through a case study*. Computers and Security, 49, 162-176.
13. EY. (2017). *Cybersecurity regained: preparing to face cyber attacks - 20th Global Information Security Survey 2017-18*. (https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf - 02.09.2020.)
14. Federal Republic of Germany. (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. (https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile - 08.09.2020.)
15. Glaspie, H. W. i Karwowski, W. (2018). *Human Factors in Information Security Culture: A Literature Review*. U: D. Nicholson (urednik), Advances in Human Factors in Cybersecurity. AHFE 2017. Advances in Intelligent Systems and Computing, vol 593 (str. 269-280). Springer.

16. Hassan, N. H. i Ismail, Z. (2012). *A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment*. Procedia - Social and Behavioral Sciences, 65, 1007-1012.
17. Hassan, N. H., Ismail, Z. i Maarop, N. (2015). *Information Security Culture: A Systematic Literature Review*. U: Proceedings of the 5th International Conference on Computing and Informatics (str. 456-463). Istanbul, Turska.
18. Her Majesty the Queen in Right of Canada. (2009). *National Strategy for Critical Infrastructure*. (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf - 08.09.2020.).
19. Ivezić, B. (1. ožujka 2020.). *Love ih policija i stručnjaci iz SAD-a: Kibernetički kriminalci ucijenili Inu za 100 milijuna kuna?* Poslovni dnevnik. (https://www.poslovni.hr/kolumne/velike-kompanije-u-strahu-zbog-ucjena-kibernetickih-kriminalaca-4215239 - 10.09.2020.).
20. Kam, H.-J., Mattson, T. i Kim, D.J. (2020), "The "Right" recipes for security culture: a competing values model perspective", Information Technology & People. https://doi.org/10.1108/ITP-08-2019-0438
21. Karlsson, F., Åström, J. i Karlsson, M. (2015). *Information security culture state-of-the-art review between 2000 and 2013*. Information and Computer Security, 23(3), 246-285.
22. Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A. i Cruz, T. J. (2018). *Cyber security of critical infrastructures*. ICT Express, 4(1), 42-45.
23. Mahfuth, A., Yussof, S., Baker, A. A. i Ali, N. (2017a). *A systematic literature review: Information security culture.* U: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) (str. 1-6). Langkawi, Malezija: IEEE.
24. 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.
25. Mansfield-Devine, S. (2018). *Critical infrastructure: understanding the threat*. Computer Fraud and Security, 2018(7), 16-20.
26. Masrek, M. N. (2017). *Assessing information security culture: The case of Malaysia public organization*. U: 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (str. 1-1). Semarang, Indonezija: IEEE.
27. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. i Giannakopoulos, G. (2014). *The Human Factor of Information Security: Unintentional Damage Perspective*. Procedia - Social and Behavioral Sciences, 147, 424-428.
28. Mokwetli, M. i Zuva, T. (2018). *Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa*. U: 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (str. 1-7). Durban, South
29. *Namagarčio ih lažnim e-mailom*. (15. rujna 2018.). Novi list. (http://www.novilist.hr/Vijesti/Crna-kronika/Namagarcio-ih-laznim-e-mailom-Grad-Dakovo-famoznom-Johnu-Smithu-uplatio-50.000-eura - 10.09.2020.)
30. 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.
31. 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.

32. *Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura*. Narodne novine, 56/2013.
33. Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). *Creating a Cyber Security Culture for Your Water/Waste Water Utility*. U: Clark R., Hakim S. (urednici) Cyber-Physical Security. Protecting Critical Infrastructure, vol 3. (str. 133-160). Springer, Cham.
34. PwC. (2018). *The Global State of Survey 2018 Singapore highlights*. (https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf - 02.09.2020.)
35. Sas, M., Hardyns, W., van Nunen, K., Reniers, G. i Ponnet, K. Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal* (2020). https://doi.org/10.1057/s41284-020-00228-4
36. Sherif, E., Furnell, S. i Clarke, N. (2015). *An Identification of Variables Influencing the Establishment of Information Security Culture*. U: T. Tryfonas & I. Askoxylakis (urednici), Proc. of the Third Int. Conf. on Human Aspects of Information Security, Privacy, and Trust (Vol. 9190, str. 436-448). Los Angeles, SAD: Springer.
37. Sillic, M. (2019). *Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context*. Computers and Security, 80, 108-119.
38. Stewart, H. i Jürjens, J. (2017). *Information security management and the human aspect in organizations*. Information and Computer Security, 25(5), 494-534.
39. Thacker, S., Barr, S., Pant, R., Hall, J. W. i Alderson, D. (2017). *Geographic Hotspots of Critical National Infrastructure*. Risk Analysis, 37(12), 2490-2505.
40. The Parliamentary Office of Science and Technology. (2017). *Cyber Security of UK Infrastructure*. Postnote 554. (http://researchbriefings.files.parliament.uk/documents/POST-PN-0554/POST-PN-0554.pdf - 08.09.2020.)
41. Ured Vijeća za nacionalnu sigurnost. (2018). *Izvješće o provedbi akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti u 2017. godini*. (https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvje%C5%A1%C4%87e%20o%20provedbi%20mjera%20Akcijskog%20plana%20za%20provedbu%20Nacionalne%20strategije%20kiberneti%C4%8Dke%20sigurnosti%20u%202017..pdf - 08.09.2020.)
42. Yildirim, E. (2016). *The importance of information security awareness for the success of business enterprises*. U: Advances in Intelligent Systems and Computing, vol. 501 (str. 211-222). Springer.
43. Yoo, H., Lee, J. H. i Chung, J. (2019). *An analysis of the survey results on nuclear security culture for personnel at nuclear facilities*. Progress in Nuclear Energy, 112, 75-79.
44. *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*. Narodne novine*,* 64/18.
45. *Zakon o kritičnim infrastrukturama*. Narodne novine*,* 56/13.

Summary

Krunoslav Arbanas

Key Factors of Information Security Culture

The recent research shows that to manage information security properly, one must consider not just widely-recognised technical measures but also non-technical measures with particular emphasis on the human factor. One of these measures is information security culture which, if well-established and supported by senior management, can significantly contribute to the protection of information assets by turning people from the recognised problem of information security into the mere solution to this problem. The need for establishing a sound information security culture is especially evident in the case of organisations that represent the so-called critical national infrastructure. Nowadays, it is an increasingly frequent target of cyber-attacks, and the first step in establishing an information security culture is to identify the factors that constitute that culture. The purpose of this paper is to summarise most cited key factors of information security culture identified in scientific articles indexed in relevant databases and, in the end, to state identified research gaps and provide readers with possible directions for further research.

Keywords: information security, information security culture, security culture, critical national infrastructure, key factors.