ELEKTROTEHNIŠKI VESTNIK 85(1-2): 13-22, 2018
IZVIRNI ZNANSTVENI ČLANEK

Model samozaščite v kibernetskem prostoru

Anže Mihelič, Simon Vrhovec

Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana, Slovenija
E-pošta: mihelic.anze@gmail.com, simon.vrhovec@fvv.uni-mb.si

Povzetek. Za zagotavljanje informacijske varnosti katerekoli organizacije, še zlasti tistih, ki izhajajo iz podatkovno občutljivih in intenzivnih sektorjev, je poglavitnega pomena, da kibernetske grožnje prepoznava in se z njimi sooča sleherni zaposleni, ki se povezuje v kibernetski prostor. Kljub ustreznim tehničnim ukrepom so namreč zaposleni neposredno izpostavljeni grožnjam in s tem predstavljajo najšibkejši člen v verigi zagotavljanja informacijske varnosti organizacije kot celote. Temu velja nameniti posebno pozornost, saj so posledice opustitve ustreznega informacijsko-varnostnega ukrepanja posameznikov za organizacijo vsaj neugodne, v mejnih primerih pa tudi kritične, in negativno vplivajo na njihovo poslovanje, npr. z izgubo zaupanja strank in poslovnih partnerjev. V prispevku je na podlagi spoznanj varnostno-motivacijske teorije, teorije izogibanja tehnološkim grožnjam in psihološke reaktance zasnovan model samozaščitnega vedenja, ki pojasnjuje, zakaj se uporabniki kibernetskega prostora odločajo za samozaščito pred kibernetskimi grožnjami. Razumevanje predlaganega modela informacijsko-varnostnim managerjem ponuja vpogled v dejavnike, ki vplivajo na samozaščitno vedenje zaposlenih v kibernetskem prostoru. Informacijsko-varnostni managerji s pomočjo predlaganega modela bolje razumejo, katere informacije in na kakšen način je treba podati zaposlenim, da bi spodbudili čim višjo raven samozaščitnega vedenja posameznih zaposlenih in s tem posledično dosegli večjo informacijsko varnost organizacije kot celote.

Ključne besede: Informacijska varnost, samovarovanje, organizacije, zaznavanje groženj, soočanje z grožnjami

A model of self-protection in the cyberspace

To ensure information security of an organization, it is important that all its employees accessing the cyber space recognize and deal with cyber-threats individually. Despite taking appropriate technical cyber-security measures, the employees are still directly exposed to cyber-threats and are one of the key weak points of ensuring information security of the organization. This needs to be payed special attention as avoidance of adequate cyber-security measures can be embarrassing for the organization and in some cases it can critically affect its business, losing their customers and business partners trust. In this paper we propose a new model of self-protective behavior based on the protection-motivation theory, technology threat avoidance theory, and psychological reactance. Using the proposed model, information-security managers get an insight into factors affecting self-protection of their employees in the cyber space and enables them to understand which information and in which way it should be delivered to their employees to encourage a higher degree of their self-protection behavior and, in turn, a higher degree of information security for the organization.

Keywords: Information security, self-protection, organization, threat detection

1 UVOD

Informacijsko-komunikacijske tehnologije (IKT) in z njimi kibernetski prostor so postali pomemben del vsakdana slehernega pravnega subjekta, najsi bo posameznika ali organizacije. Pri zadnjih je adopcija sodobnih tehnologij, ki se povezujejo prek kibernetskega prostora, še zlasti pomembna, saj so organizacije čedalje bolj vpete v elektronsko poslovanje na vseh ravneh [1], kar pričakujejo poslovni partnerji, državni organi in odjemalci. Razvoj IKT je s tem povzročil še pred tremi desetletji nesluteno razširjenost uporabe. Spletne aplikacije so nepogrešljivi komunikacijski kanali, ki jih podjetja, posamezniki in državni organi uporabljajo za manipulacijo (objavljanje, izmenjavo, hranjenje in obdelovanje) z vsebinami, namenjenimi zainteresirani javnosti. Pestrost različnih informacij zahteva kompleksno tehnološko infrastrukturo, s povečevanjem kompleksnosti tehnične infrastrukture pa eksponentno narašča tudi težavnost zagotavljanja ustrezne varnosti pred potencialno kibernetsko kriminaliteto [2]. Finančne izgube podjetij na svetovni ravni se merijo v stotinah milijard evrov in so se tako pred nekaj leti gibale med 0,4 in 1,4 odstotka bruto svetovnega proizvoda [3]. V letu 2016 se letna izguba približuje dvema odstotkoma bruto svetovnega proizvoda in z 21-odstotno rastjo dosega povprečno 9,5 milijona ameriških dolarjev letne izgube na posamezno podjetje [4].

Razširjenost in prenosnost sodobnih tehnologij, ki omogočajo vstop v kibernetski prostor, povzroča zameglitev še pred dobrima dvema desetletjema jasne meje med delovanjem posameznika v zasebnem življenju in delovanjem v imenu in za organizacijo, v kateri je zaposlen [5]. Za informacijsko varnost organizacije je odgovorna predvsem organizacija sama

Prejet 12. november, 2017
Odobren 21. januar, 2018

– z ustrezno tehnično zaščito in sprejemanjem ter izvajanjem preostalih politik zagotavljanja informacijske varnosti v organizaciji. Z najrazličnejšimi tehnikami socialnega inženiringa, pogosto v povezavi s tehnično bolj ali manj zahtevnim hekanjem, nevarno rabo računalniških naprav [6] od doma iz domačega omrežja, pa so organizacije lahko žrtve kibernetske kriminalitete tudi posredno, prek informacijsko-varnostno slabo ali povsem neozaveščenih zaposlenih. Na primer: ko se uporabnik prijavi v intranet organizacije, v kateri je zaposlen, z domačega računalnika, na katerem je nameščena zlonamerna programska oprema, lahko s tem razkrije dostopne podatke in omogoči dostop nepooblaščenim osebam, ki s tem lahko pridobijo zaupne podatke in povzročijo materialno škodo. Širjenje dostopa do interneta in nerazumevanje delovanja tehnologije za zaslonom je močno orodje za lažje zlonamerno izkoriščanje sistemskih ranljivosti IKT, znanja uporabnikov in posledično omogoča multiplikacijo socialnih in ekonomskih negativnih posledic [7]–[9].

V tem prispevku predlagamo nov model samozaščite v kibernetskem prostoru na podlagi pregleda literature na relevantnih področjih. Predlagani model postavlja teoretični okvir, ki združuje najbolj relevantne teorije, in sicer varnostno-motivacijsko teorijo, teorijo izogibanja tehnološkim grožnjam in teorijo psihološke reaktance. V prispevku predlaganega modela ne testiramo, a kljub temu podajamo smernice, kako bi ga lahko empirično preverili, pri čemer navajamo ključne izzive, s katerimi se pri tem soočamo.

V naslednjem poglavju so predstavljeni rezultati pregleda relevantne literature. V tretjem poglavju je predstavljen predlagani model. V zadnjem poglavju je predstavljena diskusija, vključno s smernicami za empirično testiranje predlaganega modela, in ključni sklepi prispevka.

2 TEORETIČNA IZHODIŠČA

Za namene oblikovanja predlaganega teoretičnega modela je bil opravljen sistematičen pregled znanstvene literature, ki obravnava tematiko informacijske varnosti, usvajanja informacijskih tehnologij, samo-varovanja, varnostno-zaščitnega vedenja, psiholoških dejavnikov odločanja, prepoznavanja groženj in soočanja z njimi. S tem smo identificirali relevantne teorije ter oblikovali ključne konstrukte za graditev lastnega modela. Pregled je bil opravljen februarja 2017 v bazi Web of Science. Iskanje je bilo opravljeno s ključnimi besedami in njihovimi kombinacijami: *information system* AND threat* (n = 45); *protect* motivat* AND information** (n = 8); *technolog* AND threat** (n = 310); *information security AND threat** (n = 73); *computer AND threat** (n = 109); *resistance AND technolog** (n = 651); *psychological reactance* (n = 118); *efficacy AND information* technolog** (n = 30); *psychological reactance AND information system** (n = 2); *psychological reactance AND threat** (n = 37).

Tabela 1: Kriteriji za vključitev/izključitev iz pregleda literature

Kriterij za vključitev	**Kriterij za izključitev**
Tematska ustreznost	Tematska neustreznost
Članek ne spada na področje informacijske varnosti, vendar pripomore k razumevanju naslovne tematike	Članek ne spada na področje informacijske varnosti in ne pripomore k razumevanju naslovne tematike
Omogočen dostop do celotnega besedila članka prek sistema UKM	Dostop le do povzetka članka
Izvirni znanstveni članek v znanstveni reviji	Ni izvirni znanstveni članek v znanstveni reviji

Zadetki so bili razvrščeni po citiranosti, od najpogosteje citiranega do najredkeje citiranega, in ročno pregledani. Iskanje ni bilo omejeno z letnico objave. Na podlagi kriterijev, predstavljenih v tabeli 1, smo v pregledu literature uporabili le izbrane zadetke. V pregled literature smo uvrstili tudi članke, ki jih nismo izločili neposredno z opisanim iskalnim postopkom, a so nanje referenčno nakazovali drugi članki, vključeni v naš pregled. Končno število relevantnih člankov je 44. Pregled teoretičnih konstruktov, ki smo jih identificirali v relevantnih člankih, predstavljamo v tabeli 2.

Tabela 2: Pregled teoretičnih konstruktov in virov

Konstrukt	**Viri**
Verjetnost uresničitve grožnje	[5], [8], [10]–[20]
Posledice uresničitve grožnje	[5], [8], [10]–[20]
Strah	[10], [11], [13], [21]–[23]
Stopnja zaskrbljenosti	[12], [15]
Pričakovane koristi	[19], [24]–[26]
Pričakovane izgube	[5], [10], [11], [13], [15]–[17], [19]–[21], [24]
Neto koristi	[24], [25]
Samoučinkovitost	[5], [8], [10]–[21], [23], [27]–[33]
Prepričanje o učinkovitosti ukrepov	[10]–[13], [15], [16], [18]–[20], [23], [28], [33], [34]
Ogrožanje posameznikove svobode	[35]–[55]
Nagnjenost k psihološki reaktanci	[35]–[55]
Psihološka reaktanca	[35]–[55]

Čeprav organizacije, da bi zagotovile zaupnost, integriteto in razpoložljivost informacij, v zadnjem času namenjajo čedalje več sredstev za razvoj tehnologije in procese za izvajanje informacijsko-varnostnih ukrepov, pri ohranjanju varnega računalniškega okolja igrajo pomembno vlogo ljudje. Kljub ustreznim tehničnim ukrepom so namreč zaposleni neposredno izpostavljeni grožnjam (tako v službenem kot v domačem okolju) in so tako najšibkejši člen v verigi zagotavljanja informacijske varnosti organizacije kot celote [1], [8]. Ključna pozornost pri prizadevanju zagotoviti boljšo informacijsko varnost mora biti tako usmerjena v iskanje načinov, kako končne uporabnike (npr.

zaposlene) motivirati za varno rabo IKT, da bi s tem zaščitili osebna in organizacijska informacijska sredstva [11]. Avtorji [1], [13], [15]–[18], [56], [57], ki so v zadnjem času s teoretičnimi pristopi skušali prikazati samozaščitne procese za potrebe informacijske varnosti ali v povezavi z njo (najsi bo s soočanjem ali z odmikom), so svoje modele najpogosteje opirali na *varnostno-motivacijsko teorijo* [23]. Med (za naš prispevek) pomembnejšimi je tudi *teorija izogibanja tehnološkim grožnjam* [17]. Da bi lahko bolje predvidevali samovarovanje zaposlenih v organizacijah, je omenjenim modelom treba dodati še element odnosov med nadrejenimi in podrejenimi v podjetju in vpliv prepričevalnega komuniciranja. Gre za ključni dejavnik pri odločitvah posameznikov o varnostnem ukrepanju, saj se na podlagi načina komunikacije in medsebojnih odnosov v organizacijah posamezniki odločajo, kako in v kolikšni meri bodo sledili navodilom nadrejenih. Zaradi teh predvidevanj v svoj model vključujemo *element psihološke reaktance* kot psihološko reakcijo posameznika, ki nastane, ko posameznik meni, da je bilo njegovo svobodno vedenje ogroženo [35], [47], [58].

2.1 Varnostno-motivacijska teorija

Varnostno-motivacijska teorija (angl. *protection motivation theory* – PMT) [10], [22] je bila sprva uporabljena za razumevanje in spreminjanje posameznikovega odnosa do zdravja in odzivanje na sporočila o zdravstvenih tveganjih. Na splošno predvideva dva glavna kognitivna procesa: *ocenjevanje ogroženosti* in *ocenjevanje obvladovanja / spoprijemanja* in sestoji iz šestih komponent, ki vplivajo na zavzemanje ali opuščanje motivacije za varnostno vedenje: 1. zaznana resnost grožnje (uporabnikovo prepričanje o kritičnosti posledic oz. obsegu potencialne škode), 2. zaznana verjetnost uresničitve grožnje (uporabnikovo prepričanje o stopnji ranljivosti varnostnih napadov), 3. zaznana učinkovitost preventivnih ukrepov, 4. zaznana samoučinkovitost posluževanja preventivnih ukrepov (ocenjevanje sposobnosti za učinkovito spoprijemanje z grožnjo z ovrednotenjem (samo)učinkovitosti varnostnih ukrepov), 5. izkupiček varnostnega odzivanja in 6. stroški z odzivanjem na grožnje. V prvotnem modelu [22], ki še vedno ostaja (pogosto napačno) najpogosteje citiran in je bil razvit na podlagi konceptov pričakovane vrednosti (angl. *expectancy-value concepts*), so bile predstavljene le prve tri komponente. Model je bil dopolnjen s tremi dodatnimi komponentami v reviziji [10].

Prvotna različica varnostno-motivacijske teorije skuša določati medsebojne odnose glavnih komponent predstavljenega varnostno-motivacijskega modela, z namenom razumevanja vpliva sporočilne komunikacije, ki povzroča strah ciljne publike. Omenjena sporočila so sestavljena iz dveh osnovnih delov: 1. zbujanje strahu in 2. priporočila za vedenje. Avtorji so tako izvorno predvidevali, da povzročanje oziroma izzivanje strahu o neki zdravstveni nevarnosti in dovzetnosti za bolezni določene ciljne populacije ter priporočila o vedenju s predlogi varnostnega ukrepanja zmanjšuje ali celo odpravlja tveganje za okužbo z določeno boleznijo [23]. Motivacija za zaščito se pojavi, ko so ljudje izpostavljeni nevarnosti za svoje zdravje ali življenje. Izpostavljenost nevarnosti za zdravje sproži dva kognitivna procesa ocenjevanja, ki izhajata iz Lazarus-Folkmanove teorije spoprijemanja s stresom [59]. Gre za procesa 1. ocenjevanja ogroženosti (kognitivna ocena, ki določa, zakaj in do kakšne mere je določena situacija za posameznika stresna) in 2. spoprijemanja s stresom (proces, s katerim posameznik ureja situacijske odnose in uravnava čustva) [60]. Omenjena procesa vodita do prilagoditvenega ali neprilagoditvenega odzivanja [61] (slika 1).

Motivacije za varnostno ukrepanje ni mogoče meriti neposredno, zato je v raziskavah mogoče pogosto zaslediti konstrukt namere za varnostno ukrepanje/vedenje, ki je pomemben napovedovalec človekovega vedenja [62].

Dojemanje in razumevanje nevarnosti sta sestavljena iz dveh dejavnikov: subjektivne zaznave verjetnosti grožnje oziroma ranljivosti in subjektivne zaznave ovrednotenja grožnje (zaznava resnosti grožnje). To pomeni, da posameznik pri presoji nevarnosti zase najprej oceni resnost grožnje in verjetnost njene uresničitve, nato pa jih primerja s koristmi, ki jih ima z

Slika 1: Grafični prikaz modela varnostno-motivacijske teorije [10]

neprilagoditvenim odzivanjem. Posameznik lahko spremeni svoje obstoječe vedenje in/ali pa ga spremeni, kar je odvisno od vrste nevarnosti, lastnega dojemanja ranljivosti ter notranjih in zunanjih zadovoljstev, povezanih s spremembami vedenja [61].

Preden posameznik začne spreminjati lastno vedenje, se mora zavedati, da je izpostavljen tveganjem, katerih koristi ne odtehtajo nevarnosti posledic, če nadaljuje s svojim obstoječim neželenim vedenjem. Ko posameznik opazi nevarnost situacije in se posledic ustraši, se začne iskanje različnih strategij soočanja z grožnjo. Pri tehtanju izgub in koristi ob prilagoditvenem ali neprilagoditvenem vedenju se v povezavi z zaznano učinkovitostjo predlaganega vedenja (tj. zaznana učinkovitost), zaznano sposobnostjo, da se predlagano vedenje izvrši (tj. zaznana samoučinkovitost) in z ocenjenimi izgubami (tj. izgube), povezanimi s spremembami vedenja [10], [63].

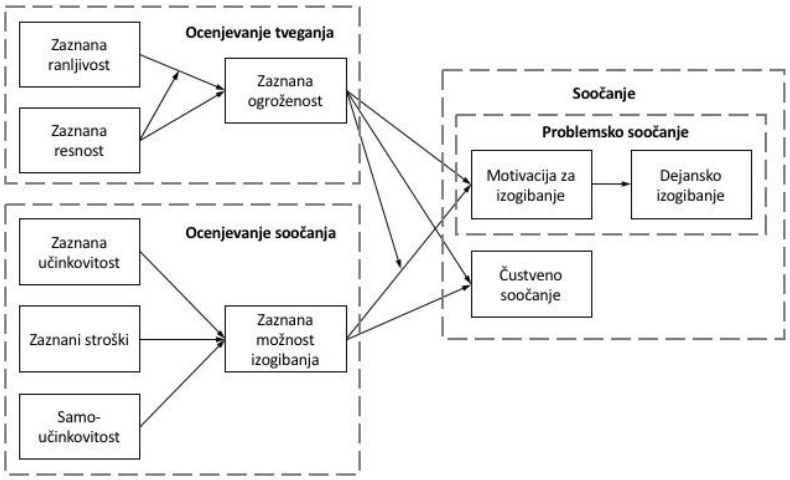
Učinkovitost varnostnega ukrepanja in samoučinkovitost povečujeta verjetnost spreminjanja vedenja (tj. varnostnega ukrepanja), medtem ko ocena izgub v smislu izgube časa in vloženega truda sproži odzivanje in sredstva, potrebna za varnostno ukrepanje, s čimer se verjetnost reakcije posameznika na tveganje (tj. namera za varnostno ukrepanje) zmanjšuje. Teorija predvideva, da je razmerje med omenjenimi elementi procesa soočanja z grožnjami linearno in dopolnjujoče [10], [23]. Model prav tako predvideva, da kombinacija navedenih dejavnikov narekuje moč motivacije za varnostno ukrepanje. Dejavniki morajo biti podani kumulativno. Odsotnost kateregakoli elementa pripelje do pomanjkanja motivacije za soočanje z grožnjo.

Varnostno-motivacijska teorija je zaradi svoje vsestranskosti skozi različne predelave prerasla v splošno teorijo vedenja pri soočanju s potencialnimi grožnjami, med drugimi na področjih varnostno usmerjenega vedenja v organizacijah [15], varovanja informacijskih sistemov [20], [27] in samovarovanja v kibernetskem prostoru [16], [21].

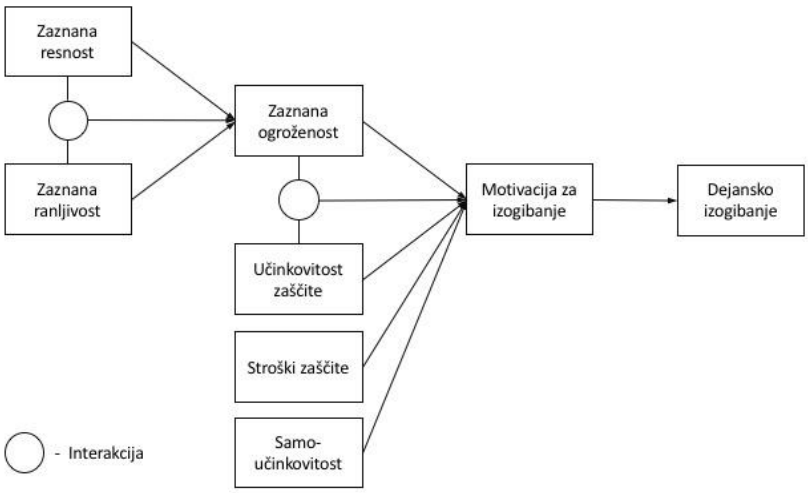
2.2 Teorija izogibanja tehnološkim grožnjam

Teorija izogibanja tehnološkim grožnjam (angl. *technology threat avoidance theory* – TTAT) [17] se pogosto napačno citira kot model PMT [11] in temelji na predpostavki, da je posameznik na eni strani ob zaznani tehnološki grožnji motiviran za aktivno izogibanje grožnji s sprejemanjem varnostnih ukrepov (če zazna, da se je grožnji mogoče s temi ukrepi izogniti), na drugi strani pa se z grožnjami sooča pasivno – s čustvenim odzivanjem [17]. PMT in TTAT si sicer delita oba osnovna kognitivna procesa [18], katerih komponente so v TTAT poimenovane nekoliko drugače, vsebinsko pa so domala nespremenjene: učinkovitost ukrepanja (angl. *response efficacy*) je tako preimenovana v varnostno učinkovitost (angl. *safeguard effectiveness*); stroški ukrepanja (angl. *response cost*) so preimenovani v stroške varovanja (angl. *safeguard cost*); motivacija za zaščito (angl. *protection motivation*) pa je preimenovana v motivacijo za izogibanje (angl. *avoidance motivation*) [5].

Kljub temu se omenjena modela pomembno razlikujeta v procesih soočanja, kjer se TTAT močno opira na teorijo spoprijemanja [59]. Soočanje z grožnjami TTAT deli v dve smeri: 1. čustveno soočanje z grožnjami (angl. *emotion focused coping*) in 2. problemsko soočanje z grožnjami (angl. *problem focused coping*). Grafični prikaz modela je razviden na sliki 2. V prvem primeru gre za situacijo, ko oseba na stresne dejavnike gleda kot odporne na spremembe, ki bi jih osebi uspelo povzročiti s svojim varnostnim vedenjem, in posledično začne prevladovati čustveno soočanje z grožnjami. V drugem primeru pa posameznik oceni, da se je mogoče z grožnjo soočiti z ukrepanjem; posledično začne prevladovati soočanje, usmerjeno v reševanje problemov [17], [59]. Zaradi tedanjega pomanjkanja velikega števila raziskav, povezanih z informacijsko-tehnološkimi grožnjami, je bila TTAT razvita s sintetiziranjem različnih raziskav s področja psihologije, zdravstvene nege, obvladovanja tveganj in informacijskih sistemov [64].



Slika 2: Grafični prikaz modela teorije izogibanja tehnološkim grožnjam [17]



Slika 3: Grafični prikaz modela TTAT, ki je bil empirično preverjen [5]

Avtorja sta svoja predvidevanja iz teoretičnega oblikovanja teorije skušala preveriti tudi z empirično raziskavo, izhajajoč iz modela, ki je razviden na sliki 3.

Kot je razvidno, se testirani model (slika 3) v bistvenih povezavah razlikuje od teoretičnega modela (slika 2). V teoretičnem modelu avtorja predvidevata, da na zaznano ogroženost vplivata zaznana resnost posledic in zaznana ranljivost za grožnje pri ocenjevanju tveganja, zaznana učinkovitost zaščitnih ukrepov, zaznani stroški ukrepanja in lastna učinkovitost pri ukrepanju pa vplivajo na zaznano možnost izogibanja pri ocenjevanju soočanja z grožnjo. Oba ciljna konstrukta (zaznana ogroženost in zaznana možnost izogibanja) nato vplivata na motivacijo za izogibanje pri problemsko usmerjenem soočanju z grožnjo in na čustveno usmerjeno soočanje. V testiranem modelu pa avtorja enako kot v teoretičnem modelu predvidevata, da na zaznano ogroženost neposredno vplivata zaznana resnost posledic in zaznana ranljivost za grožnje, preostali dejavniki pa skupaj z zaznano ogroženostjo vplivajo neposredno na motivacijo za izogibanje grožnji. Statistična analiza je pokazala statistično značilnost vseh vplivov, prikazanih na modelu, prikazanem na sliki 3 [5]. Avtorja sprememb in razlik v predvidevanjih o korelacijah in vplivih med različnimi konstrukti med teoretičnim in testiranim modelom v svojem prispevku ne pojasnita. Prav tako ne pojasnita, zakaj v empirično testiranje modela nista bila vključena konstrukta zaznane možnosti izogibanja grožnji in čustvenega soočanja z grožnjo.

2.3 Teorija psihološke reaktance

Osrednja novost v prispevku predlaganega vedenjskega modela je vključitev psihološke reaktance. Omenjenemu psihološkemu odzivu v slovenskem prostoru ni namenjene skorajda nikakršne pozornosti. Teorija psihološke reaktance je bila pri nas povezana s socialnim delom [65] in preiskovalno psihologijo [66]. Strokovnih in znanstvenih zapisov v slovenščini na drugih področjih skorajda ni mogoče zaslediti. Nekoliko obsežneje je omenjena teorija v smislu teoretsko-analitičnih pristopov, obravnavana v tuji literaturi, vendar se je tudi v tujini vprašanje psihološke reaktance in ravnanja oz. pristopanja k vedenju odpora šele dodobra začelo raziskovati s koncem osemdesetih in v začetku devetdesetih let prejšnjega stoletja [43], [49]. V nadaljevanju se osredinjamo na psihološko reaktanco v odnosih med nadrejenimi in podrejenimi zaposlenimi v organizacijah ter njenim vplivom na odzive podrejenih na navodila o informacijsko-varnostnem ukrepanju.

Oče teorije psihološke reaktance, ki jo nekateri slovenski avtorji prevajajo tudi kot teorijo reakcije nasprotovanja [65], je Jack W. Brehm, ki je teorijo zasnoval leta 1966 v monografiji Teorija psihološke reaktance (v izvirniku: *A theory of psychological reactance*) [67]. O psihološki reaktanci govorimo, ko subjekt oblikuje reakcijo nasprotovanja. Teorija predvideva, da ima vsak subjekt svobodo lastnega vedenja v kateremkoli trenutku. Če je katerokoli od teh vedenj ogroženo ali onemogočeno, subjekt oblikuje nasprotno reakcijo – protireakcijo [47]. Reakcija nasprotovanja, imenovana *psihološka reaktanca*, se pogosto oblikuje na način enega ali več različnih neposrednih ali posrednih vzorcev odgovorov, oblikovanih z namenom povrniti si ogroženo ali odvzeto svobodo [65]. Iz narave stvari izhaja, da je pogoj za nastanek psihološke reaktance stik med (najmanj) dvema subjektoma. Poudariti velja, da v dani situaciji ni nujno, da se povzročitelj stresa (omejevanja svobode) zaveda, da drugemu subjektu omejuje svobodo; pomembno je le, da dejanje kot tako (odvzemanje ali omejevanje njegove svobode) dojema tisti subjekt, ki je temu stresu izpostavljen.

Psihološka reaktanca je neposredna čustvena reakcija, ki sproži nasprotovanje situaciji, ki ogroža ali omejuje posamezna svobodna vedenja. Nastane tedaj, ko je nekdo resnično prisiljen sprejeti poglede ali

vstopiti v določene odnose in tako oblikuje vedenja, s katerimi si pribori svobodo nazaj (svobodo povrne v izhodiščno stanje). Subjekt, ki je izpostavljen stresu, lahko zaradi siljenja k sprejetju določenih stališč ali prepričanj zavzame ali okrepi *nasprotna stališča* in izkazuje odpor ob nadaljnjem prepričevanju [47]. Reaktanca lahko sproži tudi *vedenje*, s katerim subjekt, ki je stresu izpostavljen, nasprotuje zahtevam ali pričakovanjem [68] in ustvari negativen odnos do avtoritarno nastopajočega subjekta [55], [66].

Subjekti, ki so izpostavljeni stresu in čutijo omejevanje ali odvzemanje svobode, se lahko na nastalo situacijo odzovejo na različne načine – oblikujejo enega ali več različnih neposrednih ali posrednih vzorcev odgovorov. Rooney [69] te vzorce deli na:

1. *Poskus neposredne povrnitve svobode v izhodiščno stanje.* Gre za poseganje po neposrednih sredstvih povračanja v izhodiščno stanje, kar pomeni, da se subjekt ne ozira na posledice njegovega ravnanja.

2. *Poskus posredne povrnitve svobode – iskanje "luknje" v pravilu oz. zahtevi*. Gre za spoštovanje tehničnih pravil ob spodkopavanju vsebine in namena tega pravila. Takšno vedenje se pogosto označuje tudi kot pasivno-agresivno.

3. *Poskus zmanjševanja oblikovanja protireakcije z opazovanjem drugih ali spodbujanjem drugih, naj si znova pridobijo pravico.* Oblikovanje protireakcije se zmanjša bodisi z opazovanjem poskusov drugih subjektov v procesu povračanja svobode v izhodiščno stanje bodisi s poskusi spodbujanja drugih, da izvajajo prepovedana vedenja.

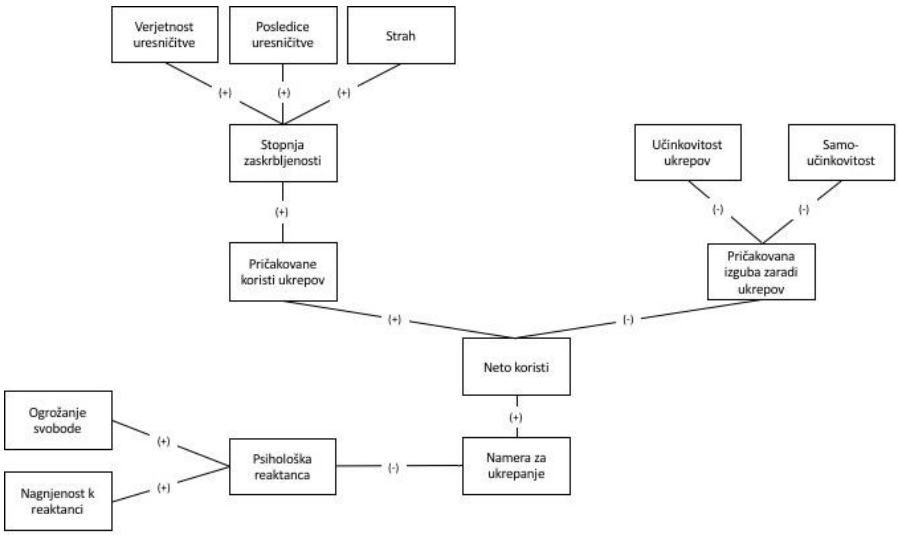
4. *Prepovedano vedenje postaja čedalje višje vrednoteno.* Če je subjektu posredno ali neposredno prepovedano izražanje njihove reaktance, se želja po prepovedanem vedenju še poveča. To lahko potrdijo posamezniki, katerim se je med odvajanjem zasvojenosti od cigaret želja po kajenju še povečala.

5. *Sovražnost ali agresivnost do vira groženj.* Reakcijo nasprotovanja lahko subjekt izrazi v obliki sovražnosti ali agresivnosti do vira ogrožanja, tudi tedaj,ko je malo verjetno, da bi subjektu uspelo povrniti svobodo v izhodiščno stanje. Raziskave na področju reaktance kažejo, da so k tovrstnim reakcijam najbolj nagnjeni adolescenti.

Navedene oblike odzivov (reaktance) se zdijo znane in spominjajo na vedenja, ki jih je mogoče razumeti kot slabšalno definicijo odpora. Teorija reaktance je tako podobna "preokvirjeni" definiciji odpora pri opisovanju odzivov na neko nezaželeno spremembo, v ustaljenem načinu vedenja. Gre namreč preko tega "preokvirjenega" pogleda, da bi ustvarila osnovo teoretičnim in empiričnim raziskavam, ki lahko pripomorejo k napovedovanju, kdaj bodo reakcije nasprotovanja nastale in kako jih je mogoče zmanjšati [69].

3 PREDLAGANI MODEL SAMOZAŠČITE

V tem prispevku predlagamo nov model samozaščite, ki temelji na predstavljenih rezultatih pregleda literature. Model samozaščite združuje predstavljene modele v enotno teorijo, ki razlaga, kako različni elementi predstavljenih modelov vplivajo na namero posameznikov za ukrepanje s tehtanjem koristi in izgub informacijsko-varnostnih ukrepov (neto koristi). Na sliki 4 so predstavljeni konstrukti, ki sestavljajo predlagani model samozaščite, in njihove teoretično predvidene medsebojne korelacije.



Slika 4: Teoretična osnova samozaščitnega vedenja v kibernetskem prostoru v organizacijah

Prvi sklop: Zaznana verjetnost uresničitve grožnje, zaznana resnost posledic, stopnja zaskrbljenosti in strah

Na odziv na grožnje, ki ni nujno vedno usmerjen v varnostno ukrepanje, sta potrebni predvsem zaznava in pravilna identifikacija grožnje, kumulativno pa morata biti izpolnjena še dva pogoja: subjekt mora zaznati možnost, da lahko do uresničitve grožnje resnično pride, in prepoznati resnost njenih posledic. Količina identificiranih informacijsko-varnostnih groženj, visoka stopnja verjetnosti in resnost posledic uresničitve groženj zvišujejo stopnjo zaskrbljenosti pred potencialnimi izgubami uresničitve informacijsko-varnostnih groženj. Za potrebe našega modela stopnjo zaskrbljenosti razumemo kot raven, po kateri zaposleni verjame, da je njegovo informacijsko imetje ogroženo [15]. Ena pomembnejših komponent, ki jo je v svoj revidirani PMT-model vključil tudi Rogers [10], [23], pozneje pa v svoje modele, ki temeljijo na PMT ali pa njegove izvedenke [11], [13], je *strah*. Gre za vzvod, ki ga vodstveni delavci pogosto uporabljajo, da bi dosegli želeni učinek. Informacijsko-varnostni kadri si namreč prizadevajo za uskladitev ukrepov končnih uporabnikov (zaposlenih), z želeno varnostno držo skozi prepričevalno komuniciranje. Pogosto je v omenjeni komunikaciji vključeno prepričevanje z določeno mero strahu, čeprav z vidika informacijske varnosti še ni jasno, kako in ali sploh bodo ustrahovalna navodila sprejeta in kako bodo v končni posledici vplivala na dejanja končnih uporabnikov [13]. V predstavljenem modelu tako predvidevamo, da strah pred izgubami pozitivno vpliva na pričakovane koristi od varnostnega ukrepanja, saj se z večanjem strahu pred izgubami povečujejo tudi pričakovane koristi varnostnega ukrepanja. Omenjeni strah lahko razumemo na korporacijski ravni kot strah menedžmenta pred informacijskimi in finančnimi izgubami podjetja zaradi varnostnega neukrepanja ali pa na ravni končnih uporabnikov kot strah pred kaznovanjem s strani organizacije ali pa kot strah po izgubi lastne informacijske varnosti. Odsotnost kateregakoli elementa pri zaznavanju navadno rezultira v neodzivanju na grožnje. Celoten proces, predvsem elementa zaznane verjetnosti uresničitve in posledic uresničitve, je močno zaznamovan z žrtvino optimistično pristranskostjo, ki predvidoma pogosto pomeni oviro za nadaljevanje procesa – motivacijo za samovarovanje v obliki neto koristi (angl. *net benefits*) na eni strani ali neodzivanju na grožnje na drugi.

Drugi sklop: Psihološka reaktanca

Potencialna psihološka reaktanca je element, ki ga prvič vključujemo v model, katerega temelj je PMT. Teorija predvideva, da reaktanca nastane, ko posameznik občuti omejevanje svojih svobod, kar bi lahko razumeli, da se pojavlja ob vsakem omejevanju svobode, vendar pa se lahko razlikuje po intenzivnosti odziva [39], [42], [49]. Reaktanca je odvisna predvsem od razumevanja posameznika, da določeno svobodo ima in lahko s svobodo prosto razpolaga. Tako se lahko (izražena) reaktanca pojavi le v primeru ogrožanja tiste svobode, katere se posameznik zaveda in jo hkrati vrednoti. Med vrednotenjem določene svobode in reaktanco tako obstaja pozitivna korelacija – čim više je dotična svoboda vrednotena, tem močnejša bo reaktanca. Podobno bo reaktanca močnejša s stopnjevanjem pomembnosti ali edinstvenosti ogrožene svobode za zadovoljevanje posameznikovih potreb. [69]. Na drugi strani pa v model vključujemo nagnjenost posameznika k reaktančnim odzivom, torej predvidevamo obstoj individualnih razlik, ki vplivajo na pojavnost in moč psihološke reaktance. Kot primere lahko podamo raziskave dejavnikov, ki značilno vplivajo na omenjeno nagnjenost, in sicer na etnično pripadnost [54], [70], spol [43], [44], [71], [72], starost [43], [54] in čustveno inteligentnost [44]. S tem predvidevamo, da je potencialna psihološka reaktanca pozitivno povezana s pričakovano izgubo zaradi varnostnih ukrepov.

Tretji sklop: Samoučinkovitost in zaznana učinkovitost ukrepov

Zaradi informacijsko-varnostnega ukrepanja nastanejo tudi izgube, najsi bodo v obliki finančnih izdatkov, ali pa izgube časa, udobja in truda, in kot taki negativno vplivajo na motivacijo po varnostnem ukrepanju [15]. Na drugi strani učinkovitost izbranega varnostnega ukrepanja in visoka samo-učinkovitost zmanjšujeta pričakovano izgubo zaradi varnostnih ukrepov. Samoučinkovitost avtorji pogosto navajajo kot ključni dejavnik, ki vpliva na pogostnost odzivanja na grožnje [16], vključuje vedenja sprejemanja in spoprijemanja z grožnjami ter ima vzročni učinek v obeh procesih modela – zaznavanju in soočanju [1]. V procesu evalvacije samoučinkovitosti pri odločitvi, da bo subjekt sam pridobil ustrezna znanja, obstaja nevarnost zanke, kjer v nekem obdobju pridobljena znanja niso zadostna za uspešno soočanje z grožnjami. Zaradi več zaporednih neuspelih poskusov se subjekt lahko znajde v zanj brezizhodnem položaju, kar pripelje do neodzivanja na grožnje, in to kljub začetnemu interesu aktivnega soočanja z grožnjo. Gre za pojav priučene nemoči [73], ki temelji na prepričanju osebe, da dogodkov v svojem življenju ne more nadzorovati. Ta temelji na preteklih izkušnjah pomanjkanja nadzora nad dogajanjem in mnenju, da vsi napori vodijo k neuspehu. Na ta pojav morajo biti pozorne predvsem manjše organizacije/podjetja, kjer je delovno okolje pogosto označeno kot obremenjeno, hektično [74] z visoko stopnjo razdrobljenosti [75] in odločanjem, ki temelji na hevrističnem sistemu vodenja [76], [77].

4 RAZPRAVA IN SKLEP

V prispevku predlagani teoretični model združuje predstavljena teoretična izhodišča in prek treh vidikov zaznavanja in soočanja z grožnjami skuša oblikovati nov pogled na samovarovanje v kibernetskem prostoru v organizacijah. V nadaljnjem raziskovanju in empiričnem testiranju predlaganega modela predlagamo anketno raziskovanje v večjih organizacijah, kjer zaposleni, uporabniki IKT informacijske tehnologije uporabljajo vsakodnevno in so ključnega pomena za njihovo delo. Posebno pozornost je treba nameniti vidiku, ki se osredinja na odpor posameznika do informacijsko-varnostnega ukrepanja – psihološko reaktanco. Psihološka reaktanca namreč na namero za ukrepanje vpliva le, če je ukrepanje izrecno zahtevano ali pričakovano. In naprej, med psihološko reaktanco in katerimkoli drugim konstruktom ne smemo pričakovati linearne povezanosti ali linearnega vpliva. Zaradi narave omenjanega psihološkega pojava je treba pričakovati krivočrtno povezanost med psihološko reaktanco in namero za varnostno ukrepanje, pri čemer naj bi bili indikatorji, ki merijo namero za informacijsko-varnostno ukrepanje, vsebinsko neposredno usmerjeni v podrejeno-nadrejena razmerja in zahteve po varnostnem ukrepanju. Skozi merjenje dejanskega vedenja varnostnega ukrepanja oziroma namere za varnostno ukrepanje, ko so vključene zahteve po tovrstnem vedenju, bi lahko natančneje opazovali stopnjo reaktančnosti posameznikov in vplive med obveznostjo vedenja, namero za ukrepanje in dejanskim vedenjem ob pričakovanem (obveznem) ukrepanju.

Z razumevanjem v prispevku predlaganega modela samozaščite v kibernetskem prostoru lahko organizacije prilagodijo politike zagotavljanja informacijske varnosti, komunikacijo, informacijsko-varnostna izobraževanja zaposlenih idr., saj informacijsko-varnostni memedžerji z njegovo pomočjo bolje razumejo, katere informacije in kako je treba podati zaposlenim, da bi spodbudili čim višjo raven samozaščitnega vedenja posameznih zaposlenih in s tem posledično dosegli višjo informacijsko varnost organizacije kot celote. Zaposleni v organizaciji se tako samoiniciativno bolje zavarujejo pred kibernetskimi grožnjami in s tem večajo informacijsko varnost organizacije kot celote in se s tem uspešneje izogibajo finančnim in drugim izgubam. Poudariti velja, da dvig stopnje informacijske varnosti ni odvisen izključno od izogibanja kibernetskim grožnjam, saj je za to treba zajeti tudi varnostno zavest, splošno varnostno obnašanje, fizično varovanje, nove tehnologije zaščite idr.

LITERATURA

[1] S. Browne, M. Lang, and W. Golden, "Linking Threat Avoidance and Security Adoption : A Theoretical Model For SMEs," in #eWellBeing, 2015, pp. 32–43.

[2] A. Mihelič and S. Vrhovec, "Soočanje z najpogostejšimi ranljivostmi spletnih aplikacij državnih organov," in Informatika v Javni Upravi, 2016.

[3] I. Bernik, "Cybercrime: The Cost of Investments into Protection," Varstvoslovje, vol. 16, no. 2, pp. 105–116, 2014.

[4] "2016 Cost of Cyber Crime Study & the Risk of Business Innovation," 2016.

[5] H. Liang and Y. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," J. Assoc. Inf. Syst., vol. 11, no. 7, pp. 394–413, 2010.

[6] S. Vrhovec, "Varna uporaba mobilnih naprav v kibernetskem prostoru," Elektroteh. Vestnik/Electrotechnical Rev., vol. 83, no. 3, pp. 144–147, 2016.

[7] A. Acquisti, A. Friedman, and R. Telang, "Is There a Cost to Privacy Breaches? An Events Study," in Fifth Workshop on the Economics of Information Security, 2006, pp. 1--20.

[8] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," MIS Q., vol. 34, no. 3, pp. 613–643, 2010.

[9] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," J. Comput. Secur., vol. 11, no. 3, pp. 431–448, 2003.

[10] R. W. Rogers, "Cognitive and physiological process in fear appeals and attitude change: a revised theory of protection motivation," in Social Psychophysiology: a source book, J. Cacioppo and R. Petty, Eds. New York: Guilford Press, 1983, pp. 153–176.

[11] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threaths and fear that motivate protective security behaviors," MIS Q., vol. 39, no. 4, pp. 837–864, 2015.

[12] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: a systematic review of quantitative studies," Inf. Manag. Comput. Secur., vol. 22, no. 1, pp. 42–75, 2014.

[13] B. A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," MIS Q., vol. 34, no. 3, pp. 549–566, 2010.

[14] H. S. Rhee, Y. U. Ryu, and C. T. Kim, "Unrealistic optimism on information security management," Comput. Secur., vol. 31, no. 2, pp. 221–232, 2012.

[15] T. Herath and H. R. Rao, "Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125, 2009.

[16] D. Lee, R. Larose, and N. Rifon, "Keeping our network safe: a model of online protection behaviour," Behav. Inf. Technol., vol. 27, no. 5, pp. 445–454, 2008.

[17] H. Liang and Y. Xue, "Avoidance of Information Technology Threats: A Theoretical Perspective," MIS Q., vol. 33, no. 1, pp. 71–90, 2009.

[18] Y. Chen and F. M. Zahedi, "Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China," MIS Q., vol. 40, no. 1, pp. 205–222, 2016.

[19] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," Comput. Human Behav., vol. 24, no. 6, pp. 2799–2816, 2008.

[20] P. Ifinedo, "Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory," Comput. Secur., vol. 31, no. 1, pp. 83–95, 2011.

[21] J. L. Jenkins, M. Grimes, J. G. Proudfoot, and P. B. Lowry, "Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals," Inf. Technol. Dev., vol. 20, no. 2, pp. 196–213, 2013.

[22] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," J. Psychol., vol. 91, pp. 93–114, 1975.

[23] J. E. Maddux and R. W. Rogers, "Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change," J. Exp. Soc. Psychol., vol. 19, pp. 469–479, 1983.

[24] H.-W. Kim and A. Kankanhalli, "Investigating user resistance to information systems implementation: A status quo bias perspective," MIS Q., vol. 33, no. 3, pp. 567–582, 2009.

[25] M. Carter and V. Grover, "Me , My Self , and I (T): Conceptualizing Information Technology (IT) Identity and its Implications Me , My Self , and I (T): Conceptualizing Information Technology (IT) Identity and its Implications," MIS Quaterly, 2015.

[26] B. B. Hughes, D. Bohl, M. Irfan, E. Margolese-Malin, and J. R. Solórzano, "ICT/Cyber benefits and costs: Reconciling competing perspectives on the current and future balance," Technol. Forecast. Soc. Change, vol. 115, pp. 117–130, 2017.

[27] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Inf. Manag., vol. 51, no. 1, pp. 69–79, 2013.

[28] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," J. Assoc. Inf. Syst., vol. 8, no. 7, pp. 386–408, 2007.

[29] T. Dinev, J. Goo, Q. Hu, and K. Nam, "User behaviour towards protective information technologies: The role of national cultural differences," Inf. Syst. J., vol. 19, no. 4, pp. 391–412, 2009.

[30] A. Beaudry and A. Pinsonneault, "Understanding User Responses to Information Technology: A Coping Model of User Adaptation," MIS Q., vol. 29, no. 3, pp. 493–524, 2005.

[31] A. Beaudry and A. Pinsonneault, "IT-induced adaptation and individual performance: a coping acts model," in International Conference on Information Systems, 2001, pp. 475–480.

[32] D. R. Compeau and C. A. Higgins, "Computer Self- Efficacy: Development of a Measure and Initial Test," MIS Q., vol. 19, pp. 189–211, 1995.

[33] D. Compeau, C. Higgins, and S. Huff, "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," MIS Q., vol. 23, no. 2, pp. 145–158, 1999.

[34] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," Decis. Support Syst., vol. 47, no. 2, pp. 154–165, 2009.

[35] S. S. Brehm and J. W. Brehm, Psychological Reactance: A Theory of Freedon and Control. New York: Academic Press, 1981.

[36] S. Dal Cin, M. P. Zanna, and G. T. Fong, Resistance and Persuasion. 2004.

[37] J. Compton, B. Jackson, and J. A. Dimmock, "Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes," Front. Psychol., vol. 7, no. February, pp. 1–9, 2016.

[38] S. A. Rains, "The Nature of Psychological Reactance Revisited: A Meta-Analytic Review," Hum. Commun. Res., vol. 39, pp. 47–73, 2013.

[39] R. E. Goldsmith and R. A. Clark, "Tendency to conform: A new measure and its relationship to psychological reactance," Psychol. Rep., no. 96, pp. 591–594, 2005.

[40] L. Shen, "Mitigating psychological reactance: The role of message-induced empathy in persuasion," Hum. Commun. Res., vol. 36, no. 3, pp. 397–422, 2010.

[41] A. J. Donnell, A. Thomas, and W. C. Buboltz, "Psychological Reactance: Factor Structure and Internal Consistency of the Questionnaire for the Measurement of Psychological Reactance," J. Soc. Psychol., vol. 14, no. 5, pp. 679–687, 2001.

[42] S. M. Hong and S. Page, "A Psychological Reactance Scale - Development, Factor Structure and Reliability," Psychol. Rep., vol. 64, no. 3, pp. 1323–1326, 1989.

[43] S. M. Hong, E. Giannakopoulos, D. Laing, and N. a Williams, "Psychological reactance: effects of age and gender.," J. Soc. Psychol., vol. 134, no. 2, pp. 223–228, 1994.

[44] J. Middleton, W. Buboltz, and B. Sopon, "The relationship between psychological reactance and emotional intelligence," Soc. Sci. J., vol. 52, no. 4, pp. 542–549, 2014.

[45] A. Brown, S. Finney, and M. France, "Examining the Dimensionality of the Hong Psychological Reactance Scale," James Madison Univ. Retrieved, pp. 1–35, 2010.

[46] T. Matthias, L. Miller, P. Caputi, R. Jayasuriya, and D. Willis, "Psychological reactance and information systems adoption," IFIP Int. Fed. Inf. Process., vol. 235, pp. 491–495, 2007.

[47] A. M. Miron and J. W. Brehm, "Reactance Theory - 40 Years Later," Zeitschrift für Sozialpsychologie, vol. 37, no. 1, pp. 9–18, 2006.

[48] M. Mikulincer, "The relationship of probability of success and performance following unsolvable problems: Reactance and helplessness effects," Motiv. Emot., vol. 12, no. 2, pp. 139–153, 1988.

[49] E. T. Dowd, C. R. Milne, and S. L. Wise, "The therapeutic reactance scale: A measure of psychological reactance.," Journal of Counseling & Development., vol. 69, no. 6. pp. 541–545, 1991.

[50] E. T. Dowd, F. Wallbrown, D. Sanders, and M. J. Yesenosky, "Psychological Reactance and Its Relationship to Normal Personality Variables," Cognit. Ther. Res., vol. 18, no. 6, pp. 601–612, 1994.

[51] K. Laurin, A. C. Kay, D. Proudfoot, and G. J. Fitzsimons, "Response to restrictive policies: Reconciling system justification and psychological reactance," Organ. Behav. Hum. Decis. Process., vol. 122, no. 2, pp. 152–162, 2013.

[52] L. Pavey and P. Sparks, "Reactance, autonomy and paths to persuasion: Examining perceptions of threats to freedom and informational value," Motiv. Emot., vol. 33, no. 3, pp. 277–290, 2009.

[53] B. L. Quick, "What is the Best Measure of Psychological Reactance? An Empirical Test of Two Measures," Health Commun., vol. 27, no. 1, pp. 1–9, 2012.

[54] K. M. P. Woller, W. C. Buboltz, and J. M. Loveland, "Psychological reactance: Examination across age, ethnicity, and gender," Am. J. Psychol., vol. 120, no. 1, pp. 15–24, 2007.

[55] C. H. Miller, L. T. Lane, L. M. Deatrick, A. M. Young, and K. A. Potts, "Psychological reactance and promotional health messages: The effects of controlling language, lexical concreteness, and the restoration of freedom," Hum. Commun. Res., vol. 33, pp. 219–240, 2007.

[56] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What Do Systems Users Have to Fear? Using Fear Appeals To Engender Threats and Fear that Motivate Protective Security Behaviours," MIS Q., vol. 39, no. 4, pp. 837–864, 2015.

[57] J. Jansen, "Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach," Proc. Ninth Int. Symp. Hum. Asp. Inf. Secur. Assur. (HAISA 2015) Stud., no. Haisa, pp. 120–130, 2015.

[58] D. A. Nesterkin, "Organizational change and psychological reactance," J. Organ. Chang. Manag., vol. 26, no. 3, pp. 573–594, 2013.

[59] R. Lazarus and S. Folkman, Stress, coping, and adaptation. New York: Springer-Verlag, 1984.

[60] T. Mitchell, "Stress, coping and appraisal in a hiv-seropositive rural sample: a test of the goodness of fit hypothesis," University of Ohio, 2004.

[61] K. Neuwirth, S. Dunwoody, and R. Griffin, "Protection Motivation and Risk Communication," Risk Anal., vol. 20, no. 5, pp. 721–734, 2000.

[62] I. Ajzen, "The theory of planned behavior," Organ. Behav. Hum. Decis. Process., vol. 50, no. 2, pp. 179–211, 1991.

[63] M. F. Flynn, R. D. Lyman, and S. Prentice-Dunn, "Protection motivation theory and adherence to medical treatment regimens for muscular dystrophy," J. Soc. Clin. Psychol., vol. 14, pp. 61–75, 1995.

[64] H. Rho and I. Yu, "The impact of information technology threat avoidance factors on avoidance behavior of user," Dep. Bus. Manag. Sunc. Natl. Univ., 2011.

[65] L. Šugman Bohic, "Ocenjevanje začetnih stikov v neprostovoljnih transakcijah." 2008.

[66] I. Areh, "Policijska zaslišanja skozi prizmo znanosti," Psihol. Obz., vol. 25, pp. 18–28, 2016.
[67] J. W. Brehm, A Theory of Psychological Reactance. New York: Academic Press, 1966.
[68] D. B. Buller, R. Borland, and M. Burgoon, "Impact of behavioural intention on effectiveness of message features: Evidence from the family sun safety project," Hum. Commun. Res., vol. 24, pp. 433–453, 1998.
[69] H. R. Rooney, Strategies for Work with Involuntary Clients, Second Edi. New York: Columbia University Press, 2009.
[70] E. a. Seemann, W. C. Buboltz, S. M. Jenkins, B. Soper, and K. Woller, "Ethnic and gender differences in psychological reactance: the importance of reactance in multicultural counselling," Couns. Psychol. Q., vol. 17, no. 2, pp. 167–176, 2004.
[71] J. L. Kray, L. Thompson, and A. Galinsky, "Battle of the sexes: gender stereotype confirmation and reactance in negotiations," J. Pers. Soc. Psychol., vol. 80, no. 6, pp. 942–958, 2001.
[72] E. a. Seemann, W. C. Buboltz, A. Thomas, B. Soper, and L. Wilkinson, "Normal Personality Variables and Their relationahip to Psychological Reactance," Individ. Differ. Res., vol. 3, no. 2, pp. 88–98, 2005.
[73] M. E. P. Seligman, Helplessness: On Depression, Development, and Death. San Francisco: W.H. Freeman, 1975.
[74] R. A. Baron, "Counterfactual Thinking and Venture Formation: The Potential Effects of Thinking About 'What Might Have Been,'" J. Bus. Ventur., vol. 15, no. 1, pp. 79–91, 2000.
[75] S. Mueller, T. Volery, and B. von Siemens, "What Do Entrepreneurs Actually Do? An Observational Study of Entrepreneurs' Everyday Behavior in the Start-up and Growth Stages," Entrep. Theory Pract., vol. 36, no. 5, pp. 995–1017, 2012.
[76] J. Dewald and F. Bowen, "Storm Clouds and Silver Linings: Responding to Disruptive Innovations through Cognitive Resilience," Entrep. Theory Pract., vol. 34, no. 1, pp. 197–218, 2010.
[77] P. Westhead, D. Ucbasaran, and M. Wright, "Experience and Cognition - Do Novice, Serial and Portfolio Entrepreneurs Differ?," Int. Small Bus. J., vol. 23, no. 1, pp. 72–98, 2005.

Anže Mihelič je doktorski študent na Pravni fakulteti Univerze v Ljubljani. Njegovi osrednji raziskovalni interesi so usmerjeni predvsem v pravne, psihološke, kriminološke, kriminalnopreventivne in viktimološke probleme v dobi informacijsko-komunikacijskih tehnologij.

Simon Vrhovec je docent na Fakulteti za varnostne vede Univerze v Mariboru. Doktoriral je leta 2015 na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova glavna raziskovalna področja so informacijska varnost, zdravstvena informatika, agilne metode, odpor do sprememb, vodenje projektov razvoja programske opreme, globalni razvoj programske opreme in poslovno-informacijska arhitektura.