Владимир Р. Токалић[1]
Амбасада Републике Србије
Абу Даби (Уједињени Арапски Емирати)

Владимир П. Томашевић[2]
Јелена Д. Раут[3]
Универзитет „Унион Никола Тесла“,
Факултет за градитељски менаџмент
Београд (Србија)

005:316.644
007:004.056
Оригинални научни рад
Примљен 12/11/2024
Измењен 24/01/2025
Измењен 03/02/2025
Прихваћен 03/02/2025
doi: 10.5937/socpreg59-54730

СОЦИОЛОШКИ АСПЕКТИ РУКОВОЂЕЊА И УСКЛАЂЕНОСТ ПОНАШАЊА СА БЕЗБЕДНОСНИМ ПОЛИТИКАМА – УЛОГА СВЕСТИ ЗАПОСЛЕНИХ О БЕЗБЕДНОСТИ У НАМЕНСКОЈ ИНДУСТРИЈИ

Сажетак: У дигиталном добу безбедност информација добија већи значај, посебно у наменској индустрији. Ова студија истражује повезаност стилова руковођења и усклађеност понашања запослених са безбедносним политикама. Циљ студије је анализа посредног утицаја трансформационог лидерства на усклађеност понашања запослених са безбедносним политикама, посредством користи од свести запослених о безбедносним противмерама. Коришћен је ХБМ модел, прилагођен наменској индустрији. У истраживању је учествовало 300 испитаника, из четири предузећа. Идентификоване су зависности између мотивације лидера и свести запослених о ефикасности примене безбедносних противмера. Резултати указују на кључне тачке за унапређење, наглашавајући континуирану едукацију и мотивацију лидера у изградњи безбедносне културе, што је од суштинског значаја за успех у међународној трговини прецизном механиком.

Кључне речи: информациона безбедност, наменска индустрија, стилови руковођења, свест о безбедности, безбедносне мере

УВОД

У савременом дигиталном контексту информациона безбедност добија већи значај, нарочито у секторима који се ослањају на електронску обраду података, као што је наменска индустрија. Стилови руковођења у овој индустрији имају значајну

[1] vladimir.tokalic@vs.rs
[2] vladimir.tomasevic@fim.rs; https://orcid.org/0000-0001-9845-2950
[3] jelena.raut@fim.rs; https://orcid.org/0000-0001-5235-5493

улогу у обликовању свести запослених о важности информационе безбедности, што може утицати на усклађеност њиховог понашања са безбедносним политикама (Jevtić & Alhudaidi, 2023). Досадашње студије су недовољно истражиле посреднички утицај стилова руковођења на усклађеност понашања запослених са безбедносним политикама путем свести запослених о информационој безбедности, посебно у наменској индустрији. Истраживање које су спровели Хумаиди и Балакришнан (Humaidi & Balakrishnan, 2015) усмерено је на испитивање посредничког утицаја стилова руковођења на усклађеност понашања запослених са безбедносним политикама, али у здравственом сектору. Њихово истраживање је показало да су свест о озбиљности и корист од свести о безбедносним противмерама, као два од три елемента свести запослених о информационој безбедности (Слика 1), значајни за усклађеност понашања запослених са безбедносним политикама. Структуру ХБМ модела (Слика 1) чине два стила лидерства – трансформациони (инспирише и мотивише запослене кроз визију и промене) и трансакциони (фокус на награђивање и кажњавање за постизање конкретних циљева), три елемента свести запослених о информационој безбедности (свест о озбиљности – запослени разумеју важност информационе безбедности и последице пропуста, свест о осетљивости – запослени разумеју које информације захтевају посебну заштиту, користи од свести запослених о безбедносним противмерама – боља превенција ризика уз очување организационе безбедности) и усклађеност понашања запослених са безбедносним политикама (придржавање безбедносних политика од стране запослених у свакодневним активностима). У студији Рахелија и сарадника (Raheli et al., 2020), истраживачи су настојали да испитају на који начин елементи свести запослених о информационој безбедности утичу на подстицаје за очување воде. Лордо (Lordo, 2018) је дао анализу постојећег стања интердисциплинарности и потребе за развојем интердисциплинарне теорије, где је настојао да користи Модел уверења о здрављу (Health Belief Model – ХБМ) за који сматра да је ограничен у применљивом обиму због својих конструкција. Кроз своје опсежно истраживање и интердисциплинарни приступ, у импликацијама за даља истраживања је предложио истраживачима да кроз ХБМ размењују знања у решавању неких од највећих изазова друштва. ХБМ може у потпуности да објасни сложеност и вишедимензионалност индивидуалног понашања (Yazdanpanah, Komendantova, Shirazu, Linnerooth-Bayer, 2015), стога се изводи закључак да је ХБМ одговарајући модел за истраживање јер може да објасни због чега појединци одлучују да не учествују у превентивном понашању.

Циљ предметног истраживања је анализа индиректног утицаја трансформационог стила руковођења, као једног од два стила руковођења које предвиђа модел истраживања, на усклађеност понашања запослених са безбедносним политикама, посредством користи од свести запослених о безбедносним противмерама, као једног од три чиниоца свести запослених о информационој безбедности, који предвиђа модел истраживања представљен на Слици 1. Настоји се да ови налази буду од користи за колеге истраживаче, менаџмент организација, као и стручњаке за информациону безбедност, омогућавајући им да унапреде стратегије управљања сигурношћу информација и унапреде безбедност у својим организацијама.

УТИЦАЈ СТИЛОВА РУКОВОЂЕЊА НА УСКЛАЂЕНОСТ ПОНАШАЊА ЗАПОСЛЕНИХ СА БЕЗБЕДНОСНИМ ПОЛИТИКАМА

Док су спољашње претње традиционално биле фокус безбедносних напора, истраживања су показала да су унутрашње претње постале најзначајнији извор ризика за организације (Ahmad, Desouza, Maynard, Naseer, Baskerville, 2020; Diesch, Plaff, Krcmar, 2020; Da Veiga, Astakhova, Botha, Herselman, 2020; Hugles-Lartey, Botchey, Qin, 2021). Унутрашње претње проистичу из људских грешака, непажње, друштвених норми или намерних пропуста запослених у организацији (Jevtić & Raut, 2024). Џејмс Мекгрегор Бернз (James MacGregor Burns) је први представио концепт трансформационог лидерства, где разликује трансакционо лидерство које је блиско класичном руковођењу од трансформационог лидерства, које укључује визију, инспирацију и мотивисање следбеника да достигну више нивое посвећености у креативности (Burns, 1978). Бернард Бас (Bernard Bass) је проширио ову теорију и истраживао како трансформациони лидери могу утицати на појединачне перформансе, али и на организационе резултате. Његов рад јасно наглашава да трансформациони лидери комбинују задатке управљања са лидерским особинама, односно да трансформациони стил не одбацује активности руковођења (менаџерске активности), већ их допуњује лидерским елементима, како би постигао дубоке промене у организацији (Bass, 1985). Теорије које су представили Бернз и Бас показују да трансформациони стил интегрише руководилачке задатке са лидерским способностима, чинећи га хибридним приступом који је ефикасан у контексту организационих промена. У овом контексту, стил руковођења у организацији има важну улогу у промовисању свести запослених о информационој безбедности (Humaidi & Balakrishnan, 2015). Социолошке теорије лидерства пружају дубље разумевање начина на који различити стилови руковођења могу утицати на друштвене односе и колективно понашање запослених у наменској индустрији (Bolden, Gosling, Hawkins, 2023; Hirschi, 2015; Cook, Cheshire, Gerbasi, 2018). Социолошки аспекти руковођења, као што су друштвене норме, групни односи, култура и организационе вредности, додатно утичу на усклађеност понашања запослених са безбедносним политикама (Morris, Hong, Chiu, Liu, 2015). Безбедносне политике дефинишу оквир правила, поступака, мера и контрола које организација примењује ради заштите својих информационих система. Усклађеност понашања запослених са безбедносним политикама зависи од њихове свести о информационој безбедности, што је значајно за смањење могућности људских грешака које ту безбедност угрожавају (Von Solms & Von Solms, 2004). Виши ниво свести запослених о информационој безбедности мотивише запослене да усвоје безбедносно одговорна понашања, чиме се подржава усклађеност са безбедносним политикама (Puhakainen & Siponen, 2010). Позитиван групни притисак и улога лидера јачају одговорно понашање, док лидерски приступ у складу са социолошким принципима може допринети колективној одговорности за придржавање безбедносних мера, што је кључно за одржавање културе безбедности у организацији (Bhatti, Irfan, Ozturk, 2023; Mišić & Markov, 2012). Безбедносне мере представљају практичну имплементацију безбедносних политика, обезбеђујући да се смернице и стандарди организације

спроводе кроз техничке, организационе и физичке контроле (Puhakainen & Siponen, 2010). Њихова ефикасност зависи од степена усклађености понашања запослених са безбедносним политикама, које је у великој мери условљено свешћу запослених о значају информационе безбедности. Кључна разлика између безбедносне мере и безбедносне противмере је да безбедносне мере делују превентивно у складу са безбедносним политикама, док безбедносне противмере делују као реактивне акције које долазе након детекције претње или инцидента. Укључивање ових аспеката у истраживачки модел омогућава испитивање постављеног предмета истраживања.

Предмет истраживања је анализа посредног утицаја стилова руковођења на усклађеност понашања запослених са политикама информационе безбедности путем свести запослених о информационој безбедности. Како модел истраживања разликује три фактора која чине свест о информационој безбедности и два стила лидерства, настојало се да се предмет истраживања додатно конкретизује кроз фокус на посреднички утицај трансформационог лидерства на усклађеност понашања запослених са безбедносним политикама, путем једног фактора свести о информационој безбедности – корист од свести запослених о безбедносним противмерама.

ХБМ модел је иницијално конципиран за анализу понашања у здравству, али се показао као користан алат у истраживањима информационе безбедности (Anuar, Shah, Gafor, Mahmood, Ghazi, 2020). ХБМ модел истиче факторе који обликују понашање појединаца у вези са заштитом информација, чиме се отварају могућности за примену у наменској индустрији. Модел истраживања, приказан на Слици 1, који су развили Хумаиди и Балакришнан (Humaidi & Balakrishnan, 2015), у предметном истраживању прилагођен је наменској индустрији. Омогућава анализу начина на који различити стилови руковођења (трансакциони и трансформациони) утичу на усклађеност понашања запослених са безбедносним политикама путем свести запослених о информационој безбедности (свест о озбиљности – свест запослених о важности информационе безбедности и потенцијалних последица које неадекватно управљање безбедношћу може имати на организацију, свест о осетљивости – разумевање запослених које врсте информација су посебно осетљиве па их је потребно заштити од неовлашћеног приступа, манипулације или откривања, и свест о безбедносним противмерама – у наставку ће бити детаљно објашњено кроз варијабле које је чине) и перципираних баријера. Трансформационо и трансакционо лидерство се посматрају као егзогени конструкти, перципиране баријере и свест запослених о информационој безбедности као посредници, а усклађеност понашања запослених са безбедносним политикама као ендогени конструкт.

Конструкт трансформационо лидерство чине следеће варијабле (Humaidi & Balakrishnan, 2015):

- мој лидер предузима строге мере против оних који не поштују политику информационе безбедности организације,
- мој лидер цени усвајање правилног понашања у вези са информационом безбедношћу,
- мој лидер сматра да ће се мој радни учинак побољшати ако усвојим правилно понашање у вези са информационом безбедношћу.

Варијабле које чине конструкт корист од свести о безбедносним противмерама (Humaidi & Balakrishnan, 2015):

- свестан сам да је примена информационе безбедности ефикасна у смањењу броја безбедносних инцидената у мојој организацији,
- свестан сам да је информациона безбедност ефикасна мера заштите података моје организације,
- свестан сам да је коришћење јаких лозинки ефикасно у спречавању неовлашћеног приступа,
- свестан сам да редовна промена лозинке ефикасно спречава неовлашћени приступ,
- свестан сам да је редовно коришћење антивирусног програма ефикасно у заштити мог рачунара,
- свестан сам да је редовно ажурирање антивирусног програма ефикасно у заштити мог рачунара,
- свестан сам да је скенирање датотека уређаја пре употребе ефикасно у заштити мог рачунара.

Прецизнији резултати истраживања произлазе из прилагођавања модела специфичним захтевима наменске индустрије, што осигурава да резултати истраживања буду применљиви у конкретном контексту, а то доприноси валидности модела.

МЕТОД ИСТРАЖИВАЊА

Ослањајући се на релевантне студије лидерства (Aarons, 2006) и модела уверења о здрављу (Ifinedo, 2012), ово истраживање проширује постојеће знање о факторима који утичу на поштовање безбедносних политика у наменској индустрији. У складу са постављеним предметом и циљем истраживања, дошло се до опште хипотезе:

ОХ: Свест запослених о безбедности информација посредује у односу између стилова руковођења и усклађености понашања запослених са безбедносним политикама у наменској индустрији.

На Слици 1 се може видети да модел предвиђа постављање 16 посебних хипотеза, међутим, претходно је наведен фокус предметног истраживања, који их све не предвиђа. Након наведених техника коришћених у истраживању, биће наведене потврђене посебне хипотезе (од испитаних 16) јер је управо једна посебна хипотеза (ПХ3) циљ истраживања, док га ПХ16 додатно потврђује.

Упитник *Стилови руковођења и понашање усаглашено са безбедношћу информација: посреднички ефекат информационе безбедности (Leadership styles and information security compliance behavior: the mediator effect of information security)* (Humaidi & Balakrishnan, 2015) прилагођен је српском језику са енглеског језика. Упитник је подељен у два одељка. Први одељак чине демографска питања – старост, пол и образовање. Други одељак процењује стилове руковођења, свест запослених о информационој безбедности и усклађеност понашања запослених са безбедносним политикама. Сви индикатори (27) у другом одељку су мерени петостепеном Ликертовом скалом, са распоном од један (уопште се не слажем) до пет (потпуно се слажем).

Узорак су чинили запослени у Југоимпорту – СДПР, Борбеним сложеним системима, Крушику Ваљево и Слободи АД Чачак, док је узорак испитаника детаљно представљен у Табели 1. У истраживању је учествовало 300 испитаника.

Прво је спроведена Уобичајена метода пристрасности (Common-Method Bias – CMB). Затим, спроведен је Харманов једнофакторски тест (Harman's single-factor). У предметном истраживању није идентификован доминантни фактор који објашњава више од 50% варијансе, што указује на то да нема високе концентрације варијабилности која би могла сугерисати присутност CMB у подацима. Недостатак доминантног фактора сугерише да нема јединствене пристрасности која би могла произаћи из методе прикупљања података или других заједничких фактора. Идентификована су два фактора која објашњавају значајан део варијабилности, што указује на сложеније структуре у подацима (Табела 2). Прегледана су факторска оптерећења, композитна поузданост (Composite Reliability – CR) и извучена просечна варијанса (Average Variance Extracted – AVE), како би била процењена конвергентна валидност. Изведен је закључак да су факторска оптерећења за све факторе виша од препоручене вредности од 0,5 – посматране варијабле добро мере латентни фактор. CR за сваки конструкт прелази вредност од 0,7 што указује на високу поузданост мерења латентних фактора. Композитне поузданости за сваки конструкт су се кретале од 0,835 до 0,943. AVE за сваки конструкт је виши од 0,5 – посматране варијабле објашњавају значајан део варијансе латентног фактора. AVE за сваки конструкт је виши од 0,5, што указује на то да посматране варијабле објашњавају значајан део варијансе латентног фактора. AVE конструкт се кретао од 0,559 до 0,797, критичне вредности осигуравају да скуп индикатора објашњава најмање 50% или више варијансе у конструкту. Ови резултати потврђују конвергентну валидност модела, што имплицира да посматране варијабле добро мере латентни фактор и да модел добро описује емпиријске податке, што даље имплицира да је факторска анализа потврдна (модел је добро усклађен са подацима) и да је теоријски модел који тестира веродостојан и ваљан. Спроведена је Кронбахова алфа унутрашње конзистенције, како би се проценило колико су ставке у скали међусобно повезане и конзистентне у мерењу истог конструкта (приказаног на Слици 1). Вредности су се кретале од 0,748 до 0,931, односно трансформационо лидерство носи вредност 0,85, трансакционо лидерство 0,839, свест о осетљивости 0,846, свест о озбиљности 0,862, свест о безбедносним противмерама 0,871, перципиране баријере 0,931 и усклађеност понашања са безбедносним политикама 0,748. Ове вредности су указале да су ставке у скали хомогене и добро усклађене, те да заједно чине поуздану мерну јединицу за циљани конструкт. Висока вредност поузданости пружа поверење у ваљаност резултата истраживања који се темеље на овим скалама. Последњи корак је процена дискриминативне валидности, чији се резултати могу видети у Табели 3. Резултат сугерише да се сваки конструкт јасно разликује од других, што потврђује да мерење није искривљено присуством сувишних варијабли или преклапањем конструката. Овим је осигурано да варијабле адекватно процењују само оно што је намеравано, без конфузије између различитих конструката. Након овога, неопходно је било утврдити линеарну везу између зависне и независне варијабле, где је утврђено да веза јесте линеарна, путем расипања (Scatter plot). Потврђено је да је расподела података нормална, након чега је урађена sqrt трансформација. Тада

су испуњени предуслови за просту линеарну регресију. У Табели 4 могу се видети резултати регресионе анализе, где су потврђене следеће посебне хипотезе, које произлазе из модела на Слици 1:

- ПХ3 – Постоји статистички значајна веза између варијабли трансформационо лидерство и корист од свести о безбедносним противмерама.
- ПХ4 – Постоји статистички значајна веза између варијабли трансакционо лидерство и свест о озбиљности.
- ПХ5 – Постоји статистички значајна веза између варијабли трансакционо лидерство и свест о осетљивости.
- ПХ7 – Постоји статистички значајна веза између варијабли свест о озбиљности и усклађеност са безбедносним политикама.
- ПХ8 – Постоји статистички значајна веза између варијабли свест о осетљивости и усклађеност понашања са безбедносним политикама.
- ПХ14 – Постоји статистички значајна веза између варијабли трансакционо лидерство и усклађеност понашања са безбедносним политикама, посматрајући варијаблу свест о озбиљности као посредничку варијаблу.
- ПХ16 – Постоји статистички значајна веза између варијабле трансформационо лидерство и усклађеност понашања са безбедносним политикама, посматрајући варијаблу корист од свести о безбедносним противмерама, као посредничку варијаблу.

На основу података из Табеле 4, може се извести закључак о потврђености опште хипотезе. ПХ3 указује на статистички значајну везу између варијабле трансформационо лидерство и користи од свести запослених о безбедносним противмерама, док ПХ16 указује на статистички значајну везу између варијабле трансформационо лидерство и усклађеност понашања запослених са безбедносним политикама, посматрајући варијаблу корист од свести запослених о безбедносним противмерама као медиатинг варијаблу. Овим је испуњен циљ истраживања, односно доказано је да трансформационо лидерство има посреднички утицај на усклађеност понашања запослених са безбедносним политикама посредством користи од свести запослених о безбедносним противмерама. У ПХ3 трансформационо лидерство је посматрано као независна, док је усклађеност понашања запослених са безбедносним политикама посматрана као зависна варијабла, при чему је 94,1% варијације у зависној варијабли објашњено независном, што се може видети на основу Р квадратне (R square) вредности из Табеле 4, која износи 0,941. У ПХ16 је трансформационо лидерство посматрано као независна, усклађеност понашања запослених са безбедносним политикама као зависна, а користи од свести о безбедносним противмерама као посредничка варијабла, при чему је 78,9% варијације у варијабли усклађеност понашања запослених са безбедносним политикама објашњено варијаблом трансформационо лидерство и варијаблом користи од свести запослених о безбедносним противмерама. Тиме су испуњени сви услови за спровођење Crosstab анализе која ће идентификовати варијабле које су испитаници оценили најнижим оценама, што су области које ће бити идентификоване као кључне тачке за унапређење.

РЕЗУЛТАТИ ИСТРАЖИВАЊА

Crosstab анализа је омогућила истраживање повезаности категоричких варијабли и пружила увиде у понашање и карактеристике истраживане популације. У Табели 5 су приказани резултати Crosstab анализе. У Табели 5 су изостављене статистички значајне зависности у којима се највише испитаника у потпуности слажу са оба става, док су истакнуте све остале статистички значајне зависности.

Утврђено је да постоји статистички значајна зависност када је у питању став „мој лидер ме стално мотивише да се придржавам политике информационе безбедности наше организације“ и следећих ставова:

- свестан сам да је коришћење јаких лозинки ефикасно у спречавању неовлашћеног приступа (p – вредност = 0,000) (1),
- свестан сам да је редовно ажурирање антивирусног програма ефикасно у заштити мог рачунара (p – вредност = 0,000) (2),
- свестан сам да је скенирање датотека и уређаја пре употребе ефикасно у заштити мог рачунара (p – вредност = 0,000) (3).

Иако већина испитаника делимично подржава став да их лидери мотивишу да се придржавају безбедносних политика, може се увидети да истовремено постоји висок ниво подршке за придржавање одређених безбедносних противмера. Ово сугерише да би фокус лидера на подстицању поштовања безбедносних политика могао бити од кључног значаја.

Са друге стране, утврђено је да постоји статистички значајна зависност када је у питању став „мој лидер непрестано трага за унапређењима у политици информационе безбедности организација“ и следећег става:

- свестан сам да је скенирање датотека и уређаја пре употребе ефикасно у заштити мог рачунара (p – вредност = 0,000) (4),
- свестан сам да је примена информационе безбедности ефикасна у смањењу броја безбедносних инцидената у мојој организација (p – вредност = 0,000) (5);

као и „мој лидер ме континуирано едукује о значају примене политике информационе безбедности у организацији“ и следећих ставова:

- свестан сам да редовна промена лозинке ефикасно спречава неовлашћен приступ (p – вредност = 0,000) (6),
- свестан сам да је скенирање датотека и уређаја пре употребе ефикасно у заштити мог рачунара (p – вредност = 0,000) (7).

Ови детаљнији увиди осветљавају сложеност повезаности између става лидера, користи од свести запослених о безбедносним противмерама и усклађености понашања запослених са безбедносним политикама. Утврђивање ових веза омогућава организацијама да прецизније идентификују области за побољшање и развију циљане стратегије за унапређење безбедносне културе.

ДИСКУСИЈА

На основу добијених резултата Crosstab анализе за ставове (1), у Табели 5 се може видети да је 62 од 300 испитаника делимично подржало први став, док се у потпуности слаже са другим ставом. Ово чини нешто више од 20% испитаника који показују висок ниво свести о важности јаких лозинки, али осећају делимичну подршку лидера у погледу мотивације за усклађеност понашања са безбедносним политикама. Ово сугерише да запослени имају свест о конкретним безбедносним противмерама, али њихова мотивација од стране лидера остаје на умереном нивоу, што указује на потенцијалну област за унапређење у виду јачања трансформационог лидерства. Већа укљученост лидера би могла подићи ниво мотивације запослених и унапредити усклађеност понашања са безбедносним политикама. Како наводе Хофнајстер и сар. (Hoffneister et al., 2014), лидери који показују идеализоване атрибуте, постижу боље резултате у смислу безбедности на радном месту јер запослени више поштују безбедносне политике када су мотивисани таквим лидерима. Задатак програма развоја лидерства треба да буде унапређење појединачних елемената лидерства, као што су основне вредности, понашања које промовишу безбедност и подстицање усклађености понашања са безбедносним политикама. Надаље, анализа за ставове (2) показује да је највише испитаника (63) изразило делимичну сагласност са првим, а пуну сагласност са другим ставом. Упркос томе што запослени у великој мери препознају ефикасност редовног ажурирања антивирусног софтвера, мотивација од стране лидера да се придржавају ових безбедносних противмера остаје на умереном нивоу. Лидери могу користити стратегије које укључују чешће подсећање на значај ажурирања безбедносних система и обучавање запослених о ризицима који произлазе из неажурираних антивирусних програма (MacMillan, 2021). Следећа анализа (3), где је 45 од 300 испитаника делимично сагласно са оба става, пружа увид у умерену мотивацију од стране лидера и умерену свест запослених о важности ове безбедносне противмере. Запослени разумеју значај скенирања, али не добијају довољно подршке и мотивације од лидера за доследну примену ове безбедносне противмере. Ово се може побољшати кроз подсетнике о важности безбедносне политике (Johnson, 2024). Даља анализа (4) показује да се 50 испитаника у потпуности слаже са првим ставом и делимично са другим. Висока подршка првом ставу показује да запослени препознају напор лидера да ускладе понашања са безбедносним политикама, што је позитиван индикатор посвећености лидерства информационој безбедности. Социолошки аспект лидерства који се огледа у јасној комуникацији и сталној едукацији, треба да буде усмерен на конкретније акције и ефикаснију имплементацију, како би свест запослених о информационој безбедности била додатно повећана (Hu, Dinev, Hart, Cooke, 2012; Kesić, Radojević, Dželetović, 2022; Luknar, 2022). Утврђена статистички значајна веза између ставова (5), при чему је 42 испитаника изразило потпуно слагање са првим ставом и делимично слагање са другим, открива лидерске улоге у подизању свести запослених и указивању на користи од безбедносних противмера. Ипак, чињеница да се 42 испитаника делимично слаже са ефикасношћу примене безбедносних противмера у смањењу инцидената сугерише да иако лидерска подршка постоји, запослени можда нису у потпуности уверени у ефикасност самих

безбедносних противмера у пракси. Анализа ставова (6), где је 42 испитаника изразило потпуно слагање са првим ставом и делимично слагање са другим, указује на специфичне изазове у примени безбедносних противмера међу запосленима. Иако запослени високо вреднују континуирану едукацију коју им пружа лидер, њихова делимична подршка идеји о важности редовне промене лозинки сугерише да можда нису у потпуности свесни потенцијалних ризика повезаних са статичним лозинкама. Анализа ставова (7), 52 испитаника се делимично слажу са оба става, указује на динамику између едукације коју лидери пружају и свести запослених о безбедносним мерама. Иако се велики број испитаника делимично слаже са овим ставовима, ово показује да постоји свест о важности скенирања уређаја пре употребе, али можда и недостатак потпуног поверења или ангажовања у примени ове безбедносне противмере. Резултат може указивати на то да едукација лидера није довољна да би се постигла потпуна сагласност са свим безбедносним противмерама. Лидери треба да прилагоде свој стил руковођења на начин који ће побољшати свест запослених о безбедносним противмерама (Zhu, Feng, Lian, Tsui, 2023). То се односи на активну и континуирану комуникацију која је усмерена на објашњење сваке противмере и њене важности за безбедност организације. Џу и сар. (Zhu et al., 2023) препоручују лидерима да развијају културу која цени информациону безбедност као кључни елемент организацијског успеха, где ће запослени осећати одговорност и учешће у унапређењу безбедносних политика.

За успех у примени информационе безбедности неопходно је да лидери не само подстичу већ и активно развијају културу која вреднује информациону безбедност као кључни елемент организацијског успеха, стварајући окружење у којем запослени осећају одговорност и учешће у побољшању безбедносних политика.

ЗАКЉУЧАК

Резултати истраживања указују на значајну везу између трансформационог лидерства и усклађености понашања запослених са безбедносним политикама, посредством користи од свести запослених о безбедносним мерама, уз препоруку за додатне напоре како би се постигла потпуна усклађеност понашања са свим безбедносним политикама. Будућа истраживања могу обухватити факторе који утичу на унапређење комуникације ризика кроз конкретне примере безбедносних инцидената. Лидерима се препоручује да мотивишу запослене континуираним едукативним активностима, као што су радионице, а посебно симулације које приказују реалне ризике и последице неуспеха у примени безбедносних противмера. Овакав приступ може допринети већој свести запослених о користима од безбедносних противмера и повећати доследност у њиховој примени. Ограничења спроведеног истраживања укључују неколико аспеката који треба да буду размотрени у контексту будућих студија. Узорак од 300 испитаника, иако репрезентативан за наменску индустрију, може бити ограничен у смислу опсега различитих индустрија, што може утицати на универзалност резултата. Специфичности различитих сектора или величина организација могу довести до различитих ставова и пракси у вези са информационом безбедношћу. Надаље, препоручује се истраживање начина на који технологије као

што су вештачка интелигенција или блокчејн могу утицати на ефикасност информационе безбедности и лидерске улоге у тим процесима. Коначно, важно је истражити не само мотивацију запослених већ и механизме који омогућавају одржавање и унапређење мотивације на дуге стазе.

На основу анализе резултата истраживања о посредном утицају трансформационог лидерства на усклађеност понашања запослених са безбедносном политиком, посредством користи од свести запослених о безбедносним противмерама, може се извести закључак да анализирани ставови имају значајне социолошке аспекте који се могу применити у контексту индустрије међународне трговине прецизном механиком. Ово истраживање пружа увид у међусобну условљеност кључних варијабли, истичући да важност лидерске мотивације у подстицању усклађености понашања запослених са безбедносним политикама представља социолошки аспект организационе културе. Лидери обликују вредности и приоритете унутар организације, при чему њихов пример и подршка извршавању безбедносних противмера директно утичу на ставове запослених.

Едукација лидера о безбедносним политикама јача њихову способност преношења важности безбедносних мера на запослене, што је од посебног значаја у глобалном окружењу са различитим културама и законодавним оквирима. У прецизној механици, која подразумева осетљиве податке и критичну потребу за очувањем интегритета података, континуирана изградња безбедносне културе постаје кључна за сигурност и одржавање поверења у међународним пословним окружењима.

Vladimir R. Tokalić[1]
Embassy of the Republic of Serbia
Abu Dhabi (United Arab Emirates)

Vladimir P. Tomašević[2]
Jelena D. Raut[3]
University "Union Nikola Tesla", School of Engineering Management
Belgrade (Serbia)

SOCIOLOGICAL ASPECTS OF MANAGEMENT AND BEHAVIOUR COMPLIANCE WITH SECURITY POLICIES – THE ROLE OF EMPLOYEES' SECURITY AWARENESS IN PURPOSE INDUSTRY

(Translation *In Extenso*)

Abstract: In the digital age, information security is gaining greater importance, especially in dedicated industry. This study investigates the relationship between leadership styles and employees' behaviour compliance with security policies. The aim of the study is to analyze the indirect effect of transformational leadership on employee compliance with security policies, through the benefits of employees' security countermeasure awareness. The HBM model, adapted to dedicated industry, was used. The study involved 300 respondents from four companies. Dependencies between leaders' motivation and employees' awareness of security countermeasure effectiveness were identified. The results indicate key points for improvement, emphasizing continuous education and motivation of leaders in building a security culture, which is essential for success in international trade in precision mechanics.

Keywords: information security, dedicated industry, leadership styles, security awareness, security measures

INTRODUCTION

In today's digital context, information security is gaining greater importance, particularly in those sectors relying on electronic data processing, e.g., dedicated industry. Leadership styles in this industry play an important role in shaping employees' awareness of information security importance, which may affect their behaviour compliance with security policies (Jevtić & Alhudaidi, 2023). So far, studies have insufficiently explored the mediator effect of leadership styles on employees' behaviour compliance with security

[1] vladimir.tokalic@vs.rs
[2] vladimir.tomasevic@fim.rs; https://orcid.org/0000-0001-9845-2950
[3] jelena.raut@fim.rs; https://orcid.org/0000-0001-5235-5493

policies through employees' information security awareness, particularly in dedicated industry. The research conducted by Humaidi and Balakrishnan (2015) is directed towards exploring the mediator effect of leadership styles on employees' behaviour compliance with security policies, but in the healthcare sector. Their research shows that severity awareness and benefit of security countermeasure awareness as two of the three elements of employees' information security awareness (Figure 1), are important for employees' behaviour compliance with security policies. The HBM model structure (Figure 1) is made of two leadership styles – transformational (which inspires and motivates employees through vision and changes) and transactional (focused on rewarding and punishing for achieving specific goals), three elements of employees' information security awareness (severity awareness – employees understand the meaning of information security and consequences of omissions; susceptibility awareness – employees understand what information requires special protection; benefits of employees' security countermeasure awareness – better risk prevention with the maintenance of organizational security) and employees' behaviour compliance with security policies (employees adhering to security policies in everyday activities). In the study conducted by Raheli et al. (2020), the researchers tried to explore the manner in which elements of employees' information security awareness affect incentives for water conservation. Lordo (2018) provides the analysis of the existing state of interdisciplinarity and the need for developing an interdisciplinary theory, while trying to use the Health Belief Model (HBM) which he considers limited in the application scope due to its constructs. Through his comprehensive research and his interdisciplinary approach, in the implications for further research, Lordo advised researchers to use HBM in their exchange of knowledge for the purpose of resolving some of the greatest societal challenges. HBM can fully explain the complexity and multidisciplinarity of individual behaviour (Yazdanpanah, Komendantova, Shirazu, Linnerooth-Bayer, 2015), and that is why a conclusion is drawn that HBM is an adequate research model because it can explain why individuals choose not to practise preventive behaviour.

The subject research is aimed at analyzing the indirect effect of the transformational leadership style, as one of the two leadership styles stipulated by the research model, on employees' behaviour compliance with security policies through the benefits of employees' security countermeasure awareness, as one of the three factors of employees' information security awareness stipulated by the research model shown in Figure 1. Efforts are made to make these findings useful to fellow researchers, organization management, as well as information security experts, enabling them to improve information security management strategies and to increase security in their organizations.

THE EFFECT OF LEADERSHIP STYLES ON EMPLOYEES' BEHAVIOUR COMPLIANCE WITH SECURITY POLICIES

While external threats have been the traditional focus of security efforts, research shows that internal threats have become the most important source of risks to organizations (Ahmad, Desouza, Maynard, Naseer, Baskerville, 2020; Diesch, Plaff, Krcmar, 2020; Da Veiga, Astakhova, Botha, Herselman, 2020; Hugles-Lartey, Botchey, Qin, 2021). Internal threats

derive from human errors, negligence, social norms, or deliberate omissions of employees in an organization (Jevtić & Raut, 2024). James MacGregor Burns was the first to introduce the concept of transformational leadership, where he distinguishes transactional leadership, which is close to classical management, and transformational leadership, which involves followers' vision, inspiration and motivation to achieve higher levels of commitment in creativity (Burns, 1978). Bernard Bass expanded this theory and investigated how transformational leaders might affect individual performances, as well as organizational results. His paper clearly emphasizes that transformational leaders combine management tasks with leader characteristics, i.e., that the transformational style does not reject management activities (managerial activities), but complements them with leader elements in order to achieve profound changes in the organization (Bass, 1985). The theories proposed by Burns and Bass show that the transformational style integrates managerial tasks with leader abilities, making it a hybrid approach efficient in the context of organizational changes. In this context, the leadership style in the organization plays an important role in promoting employees' information security awareness (Humaidi & Balakrishnan, 2015). Sociological theories of leadership provide deeper understanding of the manner in which various leadership styles may affect social relations and collective behaviour of employees in in dedicated industry (Bolden, Gosling, Hawkins, 2023; Hirschi, 2015; Cook, Cheshire, Gerbasi, 2018). Sociological aspects of management, such as social norms, group relations, culture and organizational values further affect employees' behaviour compliance with security policies (Morris, Hong, Chiu, Liu, 2015). Security policies define the framework of rules, procedures, measures and controls applied by an organization for the purpose of protecting its information systems. Employees' behaviour compliance with security policies depends on their information security awareness, which is relevant for reducing the possibility of human errors that threaten such security (Von Solms & Von Solms, 2004). A higher level of employees' information security awareness motivates employees to adopt security-responsible behaviours, which supports compliance with security policies (Puhakainen & Siponen, 2010). A positive group pressure and leaders' role strengthen responsible behaviour, while the leaders' approach in line with sociological principles may contribute to collective responsibility for adhering to security measures, which is crucial for maintaining cultural security in an organization (Bhatti, Irfan, Ozturk, 2023; Mišić & Markov, 2012). Security measures are the practical implementation of security policies, ensuring the implementation of guidelines and standards of organization through technical, organizational and physical controls (Puhakainen & Siponen, 2010). Their efficiency depends on the level of employees' behaviour compliance with security policies, which is largely conditioned by employees' awareness of the importance of information security. The key difference between security measures and security countermeasures is that security measures act preventively in compliance with security policies, while security countermeasures are reactive actions following after the detection of threats or incidents. Including these aspects in the research model ensures the examination of the established research subject.

The research subject is the analysis of the indirect effect of leadership styles on employees' behaviour compliance with information security policies through employees' information security awareness. Since the research model distinguishes three factors involving information security awareness and two leadership styles, efforts were made to specify the research subject further through the focus on the mediator effect of transformational leadership on

employees' behaviour compliance with security policies through one factor of information security awareness – benefit of employees' security countermeasure awareness of.

The HBM model was initially devised for analyzing behaviour in healthcare, but it has proved to be a useful tool in the research into information security (Anuar, Shah, Gafor, Mahmood, Ghazi, 2020). The HBM model emphasizes the factors shaping individuals' behaviour in relation to information protection, thus opening possibilities for the application in dedicated industry. The research model, shown in Figure 1 and developed by Humaidi and Balakrishnan (2015), is adapted to dedicated industry in the subject research. It enables analyzing the manners in which various leadership styles (transactional and transformational) affect employees' behaviour compliance with security policies through employees' information security awareness (severity awareness – employees' awareness of the importance of information security and potential consequences of inadequate security management may have on an organization; , susceptibility awareness – employees' understanding of the type of information that is particularly sensitive and needs protection from unauthorized access, manipulation or disclosure, and security countermeasure awareness – below, it will be explained in detail through the variables making it) and perceived barriers. Transformational and transactional leadership are seen as exogenous constructs, while perceived barriers and employees' information security awareness are seen as mediators, and employees' behaviour compliance with security policies is seen as an exogenous construct.

The transformational leadership construct consists of the following variables (Humaidi & Balakrishnan, 2015):

- My leader undertakes firm measures against those who do not adhere to the organization's information security policy,
- My leader appreciates the adoption of proper behaviour in relation to information security,
- My leader believes that my work performance will improve if I adopt proper behaviour in relation to information security.

The variables making the construct of the benefit of security countermeasure awareness (Humaidi & Balakrishnan, 2015):

- I am aware that the application of information security is efficient in reducing the number of security incidents in my organization,
- I am aware that information security is an efficient data protection measure in my organization,
- I am aware that the use of strong passwords efficiently prevents unauthorized access,
- I am aware that changing the password regularly will efficiently prevent unauthorized access,
- I am aware that the regular use of an anti-virus program will efficiently protect my computer,
- I am aware that updating the anti-virus program regularly will efficiently protect my computer,
- I am aware that scanning files and devices before its use will efficiently protect my computer.

More precise research results derive from adapting the model to specific requirements of dedicated industry, which ensures the applicability of the research results in a specific context, thus contributing to the model validity.

RESEARCH METHODOLOGY

Relying on the relevant studies on leadership (Aarons, 2006) and the Health Belief Model (Ifinedo, 2012), this research expands the existing knowledge of the factors affecting the adherence to security policies in dedicated industry. In line with the established research subject and aim, the following general hypothesis has been reached:

GH: Employees' information security awareness mediates in the relationship between leadership styles and employees' behaviour compliance with security policies in dedicated industry.

In Figure 1, it is possible to see that the model envisions the proposal of 16 special hypotheses; however, the focus of the given research is first stated, which does not envision all these hypotheses. After the above-listed techniques used in the research, the special hypotheses that have been confirmed will be given (out of a total of 16 analyzed hypotheses) because one of them (ПХ3) is exactly the research aim, while ПХ16 confirms it further.

The questionnaire *Leadership styles and information security compliance behaviour: the mediator effect of information security effect of information security* (Humaidi & Balakrishnan an, 2015) has been adapted from Serbian into English. It is divided into two sections. The first section contains demographic questions – age, gender and education. The second section assesses leadership styles, employees' information security awareness and employees' behaviour compliance with security policies. All 27 indicators in the second section are measured by the five-point Likert scale, ranging from one (I strongly disagree) to five (I strongly agree).

The sample included the employees of Jugoimport – SDPR, Borbeni složeni sistemi, Krušik Valjevo, and Sloboda AD Čačak, and the detailed sample is shown in Table 1. The research involved 300 respondents.

The Common-Method Bias (CMB) was first applied, and then Harman's single-factor test. In this research, no dominant factor has been identified accounting for more than 50% variance, which indicates that there is no high concentration of variability that could suggest the presence of CMB in the data. The absence of a dominant factor suggests that there is no single bias that might derive from the data collection method or other common factors. Two factors have been identified that account for a substantial part of variability, which indicates more complex structures in the data (Table 2). Factors loadings, Composite Reliability (CR) Average Variance Extracted (AVE) have been examined in order to assess convergent validity. The conclusion has been drawn that factor loadings for all the factors are higher than the recommended value of 0.5 – the analyzed variables measure the latent factor well. CR for each construct exceeds the value of 0.7, which points to high reliability of latent factor measurement. Composite Reliability for each construct ranges from 0.835 to 0.943. AVE for each construct is higher than 0.5 – the analyzed variables account for a substantial part of the latent factor variance. AVE for each construct is higher than 0.5, which indicates that the analyzed variables account for a substantial part of the latent factor variance. AVE construct ranges from 0.559 to 0.797; critical values ensure that the set of indicators accounts for minimum 50% or more of variance in the construct. These results confirm the convergent validity of the model, which implies that the analyzed variables measure the latent factor well, and that the model describes the empirical data well, which

further implies that the factor analysis is affirmative (the model is well harmonized with the data) and that the theoretical model it tests is valid and proper. Cronbach's alpha of internal consistence has been applied to assess how much the items on the scale are interrelated and consistent in the measurement of the same construct (shown in Figure 1). The values ranged from 0.748 to 0.931, where transformational leadership accounts for 0.85, transactional leadership accounts for 0.839, susceptibility awareness accounts for 0.846, severity awareness accounts for 0.862, security countermeasure awareness accounts for 0.871, perceived barriers account for 0.931, and behaviour compliance with security policies accounts for 0.748. These values indicate that the items on the scale are homogeneous and well-coordinated, and together they make a reliable measurement unit for the targeted construct. High reliability value proves trust in the validity of the research results which are founded on these scales. The last step is the assessment of discriminant validity, the results of which may be seen in Table 3. The result suggests that each construct clearly differs from others, which confirms that measurement is not distorted by the presence of superfluous variables or by construct overlapping. This ensures that the variables adequately assess only what has been intended, with no confusion between different constructs. After this, it was necessary to determine a linear relationship between dependent and independent variables, where it was established that the relationship was linear, through the scatter plot. It was confirmed that data distribution was normal, and then square root transformation was performed. In this manner, the prerequisites for simple linear regression were fulfilled. In Table 4 it is possible to see the results of the regression analysis, where the following special hypotheses have been confirmed to derive from the model in Figure 1:

- PH3 – There is a statistically significant relationship between the variables of transformational leadership variable and the benefit of security countermeasure awareness.
- PH4 – There is a statistically significant relationship between the variables of transactional leadership and severity awareness.
- PH5 – There is a statistically significant relationship between the variables of transactional leadership and susceptibility awareness.
- PH7 – There is a statistically significant relationship between the variables of severity awareness and compliance with security policies.
- PH8 – There is a statistically significant relationship between the variables of susceptibility awareness and behaviour compliance with security policies.
- PH14 – There is a statistically significant relationship between the variables of transactional leadership and behaviour compliance with security policies, when looking at the variable of severity awareness as a mediator variable.
- PH16 – There is a statistically significant relationship between the transformational leadership variable and behaviour compliance with security policies, when looking at the variable of the benefit of security countermeasure awareness as a mediator variable.

According to the data in Table 4, a conclusion can be drawn about the confirmed general hypothesis. PH3 points to the statistically significant relationship between the variables of transformational leadership and benefit of employees' security countermeasure awareness, while PH16 points to the statistically significant relationship between the variables of transformational leadership and employees' behaviour compliance with security policies, where

benefit of employees' security countermeasure awareness is seen as a mediator variable. In this way, the research aim has been achieved, i.e., it has been proved that transformational leadership has a mediator effect on employees' behaviour compliance with security policies through the benefits from employees' awareness of security policies. У ПХ3, transformational leadership is seen as an independent variable, while employees' behaviour compliance with security policies is seen as a dependent variable, with 94.1% of variation in the dependent variable being explained by the independent variable. This can be seen from R square value in Table 4, which amounts to 0.941. In ПХ16, transformational leadership is seen as an independent variable, employees' behaviour compliance with security policies is seen as a dependent variable, while benefit of security countermeasure awareness is seen as a mediator variable, with 78.9% of variation in the variable of employees' behaviour compliance with security policies being explained by the transformational leadership variable and the benefits of employees' security countermeasure awareness variable. This fulfils all conditions for performing the Crosstab analysis which will identify the variables rated as the lowest by the respondents, namely the areas to be identified as key points for improvement.

RESEARCH RESULTS

The Crosstab analysis enabled research into the relationship between categorical variables and provided insights into the behaviour and characteristics of the analyzed population. Table 5 shows the results of the Crosstab analysis. In Table 5, statistically significant dependencies have been omitted, in which most respondents fully agree with both attitudes, while all other statistically significant dependencies have been emphasized.

A statistically significant relationship has been established between the attitude "My leader constantly motivates me to adhere to our organization's information security policy" and the following attitudes:

- I am aware that using strong passwords is effective in preventing unauthorized access (p – value = 0,000) (1),
- I am aware that regularly updating my antivirus program is effective in protecting my computer (p – value = 0,000) (2),
- I am aware that scanning files and devices before use is effective in protecting my computer (p – value = 0,000) (3).

Although the majority of respondents partially supports the attitude that leaders motivate them to adhere to security policies, it can be seen that, at the same time, there is a high level of support for adhering to certain security countermeasures. This suggests that the leaders' focus on encouraging the adherence to security policies might be of crucial significance.

On the other hand, a statistically significant dependency has been established between the attitude "My leader is constantly looking for improvements in the organization's information security policy" and the following attitude:

- I am aware that scanning files and devices before use is effective in protecting my computer (p – value = 0,000) (4),
- I am aware that the implementation of information security is effective in reducing the number of security incidents in my organization (p – value = 0,000) (5);

The same refers to the dependency between "My leader continuously educates me about the importance of applying the information security policy in the organization" and the following attitudes:

- I am aware that regular password changes effectively prevent unauthorized access (p – value = 0,000) (6),
- I am aware that scanning files and devices before use is effective in protecting my computer (p – value = 0,000) (7).

These detailed insights highlight the complexity of the relationship between the leaders' attitude, the benefits of employees' security countermeasure awareness and employees' behaviour compliance with security policies. Establishing these relationships enables organizations to identify more precisely improvement areas and to develop targeted strategies for security culture improvement.

DISCUSSION

According to the data obtained from the Crosstab analysis for the attitudes (1), in Table 5 it is possible to see that 62 out of 300 respondents partially supported the first attitude, while fully agreeing with the second attitude. This accounts form slightly more than 20% respondents who show a high level of awareness regarding the importance of strong passwords, but who feel leaders' partial support regarding motivation for behaviour compliance with security policies. This suggests that employees are aware of specific security countermeasures, but motivation by their leaders remains at a moderate level, which points to a potential area for improvement in the form of strengthening transformational leadership. Leaders' larger inclusion might raise the level of employees' motivation and improve behaviour compliance with security policies. According to Hoffneister et al. (2014), leaders who show idealized attributes achieve better results in terms of workplace security because employees adhere to security policies more when they are motivated by such leaders. The task of the leadership development program should be the improvement of individual elements of leadership, such as fundamental values, behaviours promoting security and encouraging behaviour compliance with security policies. Furthermore, the analysis for the attitudes (2) shows that most respondents (63) expressed partial agreement with the first attitude and full agreement with the second one. Although employees largely recognize efficiency of regular anti-virus software updating, their being motivated by leaders to adhere to these security countermeasures remains at a moderate level. Leaders may use strategies which include more frequent reminding of the importance of updating security systems and of employees' education about risks deriving from the failure to update anti-virus programs (MacMillan, 2021). The following analysis (3), where 45 out of 300 respondents partially agree with both attitudes, gives an insight into moderate motivation by leaders and employees' moderate awareness of the importance of this security countermeasure. Employees understand the importance of scanning, but they do not receive sufficient support and motivation from their leaders for a consistent application of this security countermeasure. This may also be improved through reminders of the importance of a security policy (Johnson, 2024). The following analysis (4) shows that 50 respondents fully agree with the first attitude and partially with the second one. High support to the

first attitude shows that employees recognize leaders' efforts to harmonize behaviours with security policies, which is a positive indicator of leadership's commitment to information security. The sociological aspect of leadership, reflected in clear communication and permanent education, should be directed towards more specific actions and more efficient implementation in order to additionally raise employees' information security awareness (Hu, Dinev, Hart, Cooke, 2012; Kesić, Radojević, Dželetović, 2022; Luknar, 2022). The statistically significant relationship established between attitudes (5), where 42 respondents fully agree with the first attitude and partially with the second one, reveals leaders' roles in raising employees' awareness and in pointing to the benefit of security countermeasures. However, the fact that 42 respondents partially agree with the efficiency of the security countermeasures application in the reduction of incidents suggests that, although leaders' support exists, employees might not be completely convinced of the efficiency of security countermeasures themselves in practice. The analysis of attitudes (6), where 42 respondents fully agree with the first attitude and partially with the second one, points to specific challenges in the application of security countermeasures among employees. Although employees value highly education provided by their leader, their partial support to the idea of the importance of changing passwords regularly suggests that they might not be fully aware of potential risks related to static passwords. The analysis of attitudes (7), with 52 respondents partially agreeing with both attitudes, points to the dynamics between education provided by leaders and employees' awareness of security measures. Although a large number of respondents partially agrees with these attitudes, this points to the existence of awareness of the importance of scanning devices before their use, and perhaps to the lack of full trust or engagement in the application of this security countermeasure. The result may indicate that leaders' education is not sufficient to achieve full compliance with all security countermeasures. Leaders need to adapt their leadership style in such a way as to raise employees' awareness of security countermeasures (Zhu, Feng, Lian, Tsui, 2023). This refers to active and continued communication directed at explaining each countermeasure and its importance for the organization's security. Zhu et al. (2023) recommend leaders to develop the culture that appreciates information security as a key element of an organization's success, where employees will feel responsible and willingness to participate in the improvement of security policies.

To succeed in the application of information security, leaders need not only to encourage, but also to actively develop a culture which values information security as a key element of an organization's success, thus creating the setting in which employees feel responsibility and willingness to improve security policies.

CONCLUSION

The research results point to an important relationship between transformational leadership and employees' behaviour compliance with security policies, through the benefit of employees' awareness of security measures, with the recommendation for further efforts in order to achieve full behaviour compliance with all security policies. Future research may encompass the factors affecting the improvement of risk communication through specific examples of security incidents. Leaders are recommended to motivate

employees through continuous educational activities such as workshops, and in particular simulations which show real risks and consequences of failure to apply security countermeasures. This approach may contribute to employees' greater awareness of the benefits of security countermeasures, and increase consistency in their application. The limitations of the conducted studies include several aspects which should be considered in the context of future studies. The sample of 300 respondents, although representative for dedicated industry, may be limited in terms of the scope of different industries, which may affect the result universality. Specific features of different sectors or organization size may lead to different attitudes and practices in relation to information security. Furthermore, it is recommended to investigate the manner in which artificial intelligence or blockchain may affect the efficiency of information security and the leaders' role in those processes. Finally, it is important to investigate not only employees' motivation, but also mechanisms enabling the maintenance and improvement of motivation in the long-run.

According to the research results about the indirect effect of transformational leadership on employees' behaviour compliance with the security policy through benefits from employees' security countermeasure awareness, a conclusion may be drawn that the analyzed attitudes have significant sociological aspects which may be applied in the context of international trade in precision mechanics. This research provides an insight into the interdependency of key variables, emphasizing that the importance of leaders' motivation in encouraging employees' behaviour compliance with security policies constitutes the sociological aspect of organizational culture. Leaders set values and priorities within the organization, whereas their personal example and support to the implementation of security countermeasures have a direct effect on employees0 attitudes.

Leaders' education about security policies strengthens their ability to transfer the importance of security measures to employees, which is of particular relevance in the global setting with different cultures and legislative frameworks. In precision mechanics, which implies sensitive data and a critical need for preserving data integrity, a security culture being continuously built becomes crucial for the safety and maintenance of trust in international business settings.

REFERENCES/ЛИТЕРАТУРА

Aarons, G. A. (2006). Transformational and transactional leadership: Association with attitudes toward evidence-based practice. *Psychiatric services*, 57 (8). Available at: Transformational and Transactional Leadership: Association With Attitudes Toward Evidence-Based Practice | Psychiatric Services (psychiatryonline.org)

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71 (8), 939–953. https://doi.org/10.1002/asi.24311

Anuar, H., Shah, S. A., Gafor, H., Mahmood, M. I., Ghazi, H. F. (2020). Usage of health belief model (HBM) in health behavior: A systematic review. *Malaysian journal of medicine and health sciences*, 16 (11), 2636–9346. Available at: 2021010809001826_2020_0366_.pdf (upm.edu.my)

Bhatti, O. K., Irfan, M., Öztürk, A. O. (2023). Influence of responsible leadership on inclusive organizations: A mixed-method study. *International Journal of Organizational Leadership.* Available at: https://acikerisim.medipol.edu.tr/xmlui/handle/20.500.12511/11006

Bolden, R., Gosling, J., Hawkins, B. (2023). *Exploring leadership: Individual, organizational, and societal perspectives.* Oxford University Press

Bulgurcu, H., Cavusoglu, H., Benbasat, I. (2009). Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors, presented at 2009 International Conference on Computational Science and Engineering CSE '09.

Cook, K. S., Cheshire, C. & Gerbasi, A. (2018). "Power, dependence, and social exchange theory". *Contemporary social psychological theories*, 166–193. Available at: https://ieeexplore.ieee.org/abstract/document/5283116

Bass, B. M. (1960). *Leadership, Psychology and Organizational Behavior.* New York: Harper

Burns, J. M. G. (1978). *Leadership.* New York: Harper & Row

Da Veiga, A., Astakhova, L. V., Botha A., Herselman, M. (2020). Defining organizational information security culture – Perspectives from academia and industry. *Computers and Security*, 92, 191713. https://doi.org/10.1016/j.cose.2020.101713

Diesch, R., Plaff, M., Krcmar, H. (2020). "A comprehensive model of information security factor for decision-makers". *Computers and Security,* 92, 101747. https://doi.org/10.1016/j.cose.2020.101747

Hagen, J. M., Albrechtsen, E., Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16 (4), 377–397. https://doi.org/10.1108/09685220810908796

Hirschi, T. (2015). Social control theory: A control theory of delinquency. In: *Criminology theory* 289–305.

Hoffmeister, K., Gibbons, A. M., Johnson, S. K., Cigularov, K. P., Chen, P. Y., Rosecrance, J. C. (2014). The differential effects of transformational leadership facets on employee safety. *Safety science*, 62, 68–78. https://doi.org/10.1016/j.ssci.2013.07.004

Hovav, A., D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 49 (2), 99–110. https://doi.org/10.1016/j.im.2011.12.005

Hu, Q., Dinev, T., Hart, P., Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43 (4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Hugles-Lartey, J., Li, M., Botchey, F. E., Qin, Z. (2021). Human factor, a critical weak point in the information security of an organizations Internet of things. *Heliyon*, 7 (3). Available at: Human factor, a critical weak point in the information security of an organization's Internet of things (cell.com)

Humaidi, N., Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: mediator effect of information security awareness. *International journal of information and education technology*. Available at: Leadership-Styles-and-Information-Security-Compliance-Behavior-The-Mediator-Effect-of-Information-Security-Awareness.pdf (researchgate.net)

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31 (1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Jevtić, N., Alhudaidi, I. (2023). The importance of Information Security for Organizations. *Serbian Journal of Engineering Management*, 8 (2), 48–53. DOI: 10.5937/SJEM2302048J

Jevtić, N., Raut, D. (2024). Analysis of sociological aspects of information security using the HAIS-Q model. *Sociološki pregled*, 58 (1), 231–252. DOI: 10.5937/socpreg58-47480

Johnson, D. (2024). *Leadership Fundamentals for Cybersecurity in Public Policy and Administration: Lessons for the Global South*. Taylor & Francis. DOI: 10.4324/9781003496250

Kesić, D. B., Radojević, K. Z., Dželetović, M. U. (2022). The impact of the national security system on the prevention of security threats in the Republic of Serbia: attitudes of secondary school students, *Sociološki pregled*, 56 (1), 354–382. https://doi.org/10.5937/socpreg56-35763

Lordo, R. F. (2018). The importance of interdisciplinarity. Redefining the health belief model. Senior Theses, 220. Available at: https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1221&context=senior_theses;

Luknar, I. (2022). Abuse of information and communication technologies: Concept and organization in the Republic of Serbia. *Politika nacionalne bezbednosti*, 22 (1), 171–188. 171–188. DOI: 10.22182/pnb.2212022.8. [In Serbian]

MacMillan, J. (2021). *Infosec strategies and best practices: Gain proficiency in information security using expert-level strategies and best practices*. Packt Publishing Ltd. ISBN 978-1-80056-635-4

Mišić, A. M., Markov, S. (2012). Feminist critical discourse of leadership with emphasis on transformational leadership theory. *Sociološki pregled*, 46 (3), 341–365. DOI: 10.5937/socpreg1203341M

Morris, M. W., Hong, Y. Y., Chiu, C. Y., Liu, Z. (2015). Normology: Integrating insights about social norms to understand cultural dynamics. *Organizational behavior and human decision processes*, 129, 1–13. https://doi.org/10.1016/j.obhdp.2015.03.001

Puhakainen, P., Siponen, M. (2010). Improving employees' compliance through information security training: An action research study. *MIS Quarterly*, 34 (4), 757–778. https://doi.org/10.2307/25750704

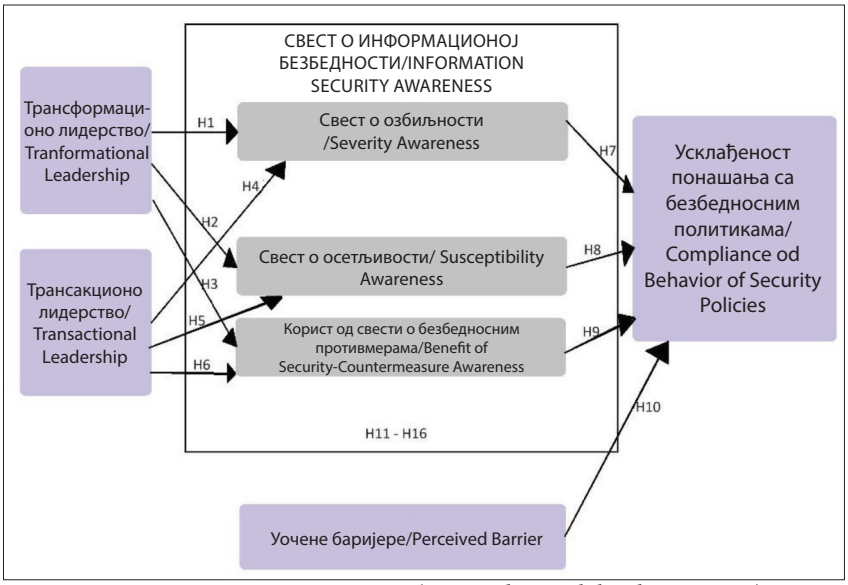
Raheli, H., Zarifian, S., Yazdanpanah, M. (2020). The power of the health belief model (HBM) to predict water demand management: A case study of farmers' water conservation in Iran. *Journal of Environmental Management*, https://doi.org/10.1016/j.jenvman.2020.110388

Von Solms, R., Von Solms, B. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23 (5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Yazdanpanah, M., Komendantova, N., Shirazu, Z. N., Linnerooth-Bayer, J. (2015). Green or in between? Examining youth perceptions of renewable energy in Iran. *Energy Research & Social Science*, 8, 78–85. https://doi.org/10.1016/j.erss.2015.04.011

Zhu, J., Feng, G., Liang, H., Tsui, K. L. (2023). How do paternalistic leaders motivate employees' information security compliance? Building a climate and applying sanctions. *Journal of the Association for Information Systems*, 24 (3), 782–817. DOI: 10.17705/1jais.00794

НАЗАД
BACK



Слика 1: *Модел истраживања* (Humaidi & Balakrishnan, 2015) /
Figure 1: *Research model* (Humaidi & Balakrishnan, 2015)

Табела 1: *Узорак испитаника (резултат аутора)* /
Table 1. *Sample of respondents (the authors' result)*

НАЗАД
BACK

	Приближан број запослених / Approximate number of employees	Број прихваћених упитника из предузећа (број који пропорционално одговара броју запослених у односу на узорак који је формиран – 300 испитаника) / The number of accepted questionnaires from the company (the number that corresponds proportionally to the number of employees in relation to the sample that was formed – 300 respondents)
Југоимпорт – СДПР / Jugoimport – SDPR	3.500	129
Борбени сложени системи / Borbeni složeni sistemi	130	5
Крушик Ваљево / Krušik Valjevo	2.500	92
Слобода АД / Sloboda AD	2.000	74
ПОЛ ИСПИТАНИКА / GENDER OF RESPONDENTS		
Мушки / Male	231	
Женски / Female	69	
СТАРОСТ ИСПИТАНИКА / AGE OF RESPONDENTS		
До 30 година / Up to 30 years	48	
Од 31 до 40 / From 31 to 40	65	

Од 41 до 50 / From 41 to 50	110
Од 51 до 60 / From 51 to 60	58
Преко 61 / Over 60	19
ОБРАЗОВАЊЕ ИСПИТАНИКА / EDUCATION OF RESPONDENTS	
Четврти степен образовања / Fourth level of education	238
Седми степен образовања / Seventh level education	58
Осми степен образовања / Eight level of education	8

Табела 2: *Резиме факторске анализе за CMB тест (резултат аутора)* / Table 2: *Summary of the factor analysis for CMB test (the authors' result)*

Компоненте / Components	Почетне сопствене вредности / Initial Eigenvalues			Екстракције суме оптерећења на квадрат / Extraction Sums of Squared Loadings		
	Укупно / Total	% варијансе / % of Variance	Кумулативно % / Cumulative %	Укупно / Total	% варијансе / % of Variance	Кумулативно % / Cumulative %
1	9.761	36.151	36.151	9.761	36.151	36.151
2	7.218	26.734	62.884	7.218	26.734	62.884
3	1.857	6.879	69.764	1.857	6.879	69.764
4	1.518	5.622	75.386	1.518	5.622	75.386
5	1.463	5.418	80.804	1.463	5.418	80.804
6	1.172	4.342	85.146	1.172	4.342	85.146
7	1.150	4.261	89.406	1.150	4.261	89.406

Табела 3: *Дискриминативна валидност (резултат аутора)* / Tabela 3: *Discriminant validity (the authors' result)*

	Трансформационо лидерство / Transformational Leadership	Трансакционо лидерство / Transactional Leadership	Свест о осетљивости / Susceptibility Awareness	Свест о озбиљности / Severity Awareness	Уочене баријере / Perceived Barries	Корист од свести о безбедносним противмерама / Benefit of Security Countermeasure Awareness	Усклађеност понашања са безбедносним политикама / Behaviour compliance with security policies
Трансформационо лидерство / Transformational Leadership	**.865**						
Трансакционо лидерство / Transactional Leadership	.009	**.842**					
Свест о осетљивости / Susceptibility Awareness	.007	.812	**.824**				

Свест о озбиљности / Severity Awareness	.013	.815	.810	**.829**			
Уочене баријере / Perceived Barrier	.032	-.039	-.078	-.051	**.893**		
Корист од свести о безбедносним противмерама / Benefit of Security Countermeasure Awareness	.790	.017	.015	.026	.048	**.839**	
Усклађеност понашања са безбедносним политикама / Behaviour compliance with security policies	.023	.729	.713	.719**	-.054	.034	**.748**

Табела 4: *Резултати тестирања хипотеза (резултат аутора)* / Table 4: *Results of hypothesis testing results (the authors' result)*

X / H	Хипотезе – компоненте / Hypotheses – components	R квадрат / R square	β	p – вредност за β / p – value for β	Резултати / Results
X3 / H3	**Трансформационо лидерство --> Корист од свести о безбедносним противмерама / Transformational Leadership --> Benefit of Security Countermeasure**	0.941	0.941	0.000	Подржано / Supported
X4 / H4	Трансакционо лидерство --> Свест о озбиљности / Transactional Leadership --> Severity Awareness	0.836	0.848	0.000	Подржано / Supported
X5 / H5	Трансакционо лидерство --> Свест о осетљивости / Transactional Leadership --> Susceptibily Awareness	0.868	0.868	0.000	Подржано / Supported
X7 / H7	Свест о озбиљности --> Усклађеност понашања са безбедносним политикама / Severity Awareness --> Behaviour compliance with security policies	0.843	0.843	0.000	Подржано / Supported
X8 / H8	Свест о осетљивости --> Усклађеност понашања са безбедносним политикама / Susceptibily Awareness --> Behaviour compliance with security policies	0.908	0.873	0.000	Подржано / Supported
X14 / H14	Трансакционо лидерство --> Свест о озбиљности --> Усклађеност понашања са безбедносним политикама / Transactional Leadership --> Security Awareness --> Behaviour compliance with security policies	0.857	0.253	0.000	Подржано / Supported
X16 / H16	Трансформационо лидерство --> Корист од свести о безбедносним противмерама --> Усклађеност понашања са безбедносним политикама / Transformational Leadership --> Benefit of Security Countermeasure Awareness --> Behaviour compliance with security policies	0.789	0.756	0.000	Подржано / Supported

НАЗАД
ВАСК

Табела 5: *Crosstab анализа (резултати аутора)*
/ Table 5: *Crosstab analysis (the authors' result)*

	19. Свестан сам да је коришћење јаких лозинки ефикасно у спречавању неовлашћеног приступа. / 19. I am aware that using strong passwords is effective in preventing unauthorized access.					Укупно / Total
1. Мој лидер ме стално мотивише да се придржавам политике информационе безбедности наше организације. / 1. My leader constantly motivates me to adhere to our organization's information security policy.	1	2	3	4	5	
	2	8	15	0	0	25
	3	4	22	11	0	40
	5	14	41	19	0	80
	0	0	0	22	**62**	84
	0	1	9	33	28	71
Укупно / Total	11	27	87	85	90	300
	22. Свестан сам да је редовно ажурирање антивирусног програма ефикасно у заштити мог рачунара. / 22. I am aware that regularly updating my antivirus program is effective in protecting my computer.					Укупно / Total
1. Мој лидер ме стално мотивише да се придржавам политике информационе безбедности наше организације. / 1. My leader constantly motivates me to adhere to our organization's information security policy.	1	2	3	4	5	
	2	9	14	0	0	25
	3	7	19	11	0	40
	7	13	39	21	0	80
	0	1	0	20	**63**	84
	0	2	8	32	29	71
Укупно / Total	12	32	80	84	92	300
	23. Свестан сам да је скенирање датотека и уређаја пре употребе ефикасно у заштити мог рачунара. / 23. I am aware that scanning files and devices before use is effective in protecting my computer.					Укупно / Total
1. Мој лидер ме стално мотивише да се придржавам политике информационе безбедности наше организације. / 1. My leader constantly motivates me to adhere to our organization's information security policy.	1	2	3	4	5	
	6	4	10	4	1	25
	6	12	22	0	0	40
	9	19	24	28	0	80
	2	1	17	**45**	19	84
	0	1	15	33	22	71
Укупно / Total	23	37	86	119	42	300
	23. Свестан сам да је скенирање датотека и уређаја пре употребе ефикасно у заштити мог рачунара. / 23. I am aware that scanning files and devices before use is effective in protecting my computer.					Укупно / Total
2. Мој лидер непрестано трага за унапређењима у политици информационе безбедности организације. / 2. My leader is constantly looking for improvements in the organization's information security policy.	1	2	3	4	5	
	5	3	4	0	0	12
	4	6	14	3	1	28
	11	23	3	13	0	70
	3	5	23	44	19	94
	0	0	24	**50**	22	96
Укупно / Total	23	37	88	110	42	300

НАЗАД
BACK

	17. Свестан сам да је примена информационе безбедности ефикасна у смањењу броја безбедносних инцидената у мојој организацији./ 17. I am aware that the implementation of information security is effective in reducing the number of security incidents in my organization.					Укупно / Total
3. Мој лидер ме континуирано едукује о значају примене политике информационе безбедности у организацији. / 3. My leader continuously educates me about the importance of applying the information security policy in the organization.	1	2	3	4	5	
	3	3	5	0	0	11
	9	6	11	0	1	27
	18	22	31	7	4	82
	0	16	15	21	38	90
	0	0	20	**42**	28	90
Укупно / Total	30	47	82	70	71	300
	20. Свестан сам да редовна промена лозинке ефикасно спречава неовлашћен приступ. / 20. I am aware that regular password changes effectively prevent unauthorized access.					Укупно / Total
3. Мој лидер ме континуирано едукује о значају примене политике информационе безбедности у организацији. / 3. My leader continuously educates me about the importance of applying the information security policy in the organization.	1	2	3	4	5	
	3	3	5	0	0	11
	9	6	11	0	1	27
	18	22	31	7	4	82
	0	16	15	21	38	90
	0	0	20	**42**	28	90
Укупно / Total	30	47	82	70	71	300
	23. Свестан сам да је скенирање датотека и уређаја пре употребе ефикасно у заштити мог рачунара. / 23. I am aware that scanning files and devices before use is effective in protecting my computer.					Укупно / Total
3. Мој лидер ме континуирано едукује о значају примене политике информационе безбедности у организацији. / 3. My leader continuously educates me about the importance of applying the information security policy in the organization.	1	2	3	4	5	
	2	1	5	3	0	11
	5	6	12	4	0	27
	12	17	34	16	3	82
	3	12	24	35	16	90
	1	1	13	**52**	23	90
Укупно / Total	23	37	88	110	42	300