Prethodno priopćenje
Primljeno: 31. listopada 2025.
https://doi.org/10.46672/zsl.10.11.10

Siniša Jovčić*
Magdalena Bednjanec**
Melita Nižetić***

# DIGITALNA TRANSFORMACIJA POSLOVNE SIGURNOSTI

**Sažetak**

Digitalna transformacija posljednjih je godina snažno promijenila poimanje poslovne sigurnosti. Poduzeća više ne štite samo fizičku imovinu i osnovnu IT infrastrukturu, nego i upravljaju čitavim ekosustavom podataka, usluga u oblaku, udaljenih korisnika, dobavljača i javno dostupnih servisa. Takvo okruženje otvara nove prilike za učinkovitije poslovanje, ali istodobno povećava broj i složenost prijetnji: od kibernetičkih napada, preko industrijske špijunaže i curenja podataka, do reputacijskih napada i dezinformacijskih kampanja. Cilj ovoga rada jest prikazati kako se poslovna sigurnost mora mijenjati pod utjecajem digitalne transformacije, koje teorijske modele pritom možemo primijeniti i u kojoj su mjeri hrvatska poduzeća spremna za takvu promjenu. Rad je utemeljen na kombinaciji teorijskog pregleda i rezultata anketnog istraživanja provedenog u listopadu 2025. godine na odabranom uzorku hrvatskih poduzeća različitih veličina, njih ukupno 180. Nalazi pokazuju da je svijest o prijetnjama visoka, ali je provedba sigurnosnih mjera nedovoljno sustavna i često ovisi o pojedincima. Posebno se ističe potreba za razvojem sigurnosne kulture, za snažnijom ulogom uprava u planiranju sigurnosti te za dosljednijom primjenom europskog normativnog okvira (NIS2, CRA, GDPR). Zaključuje se da digitalna transformacija može povećati otpornost i konkurentnost poduzeća, ali samo ako je sigurnost ugradbena, a ne naknadno dodana funkcija.

**Ključne riječi:** digitalna transformacija, poslovna sigurnost, kibernetička otpornost, upravljanje rizicima, sigurnosna kultura, NIS2

## 1. Uvod

Cilj ovoga rada jest analizirati utjecaj digitalne transformacije na poslovnu sigurnost, procijeniti spremnost hrvatskih organizacija te ispitati povezanost percepcije prijetnji, tehnološke pripremljenosti i sigurnosne kulture.

* Siniša Jovčić, mag. ing., predavač, Sveučilište VERN', Zagreb, Hrvatska, sinisa.jovcic@vern.hr
** Magdalena Bednjanec, mag. inf., predavačica, Tehničko veleučilište u Zagrebu, Hrvatska magdalena.bednjanec@tvz.hr
*** Melita Nižetić, Prirodoslovna škola Vladimira Preloga, Zagreb, Hrvatska, melita.nizetic@skole.hr

Uloga sigurnosti u poslovanju u posljednjih se dvadesetak godina bitno promijenila. U vrijeme kada su poslovni procesi bili pretežito analogni, a IT sustavi zatvoreni i unutar organizacije, sigurnost se mogla svesti na kontrolu pristupa, fizičku zaštitu i osnovnu antivirusnu zaštitu. Današnje okruženje potpuno je drukčije: podatci se nalaze u oblaku, zaposlenici rade na daljinu, poduzeća su povezana s partnerima i državnim tijelima putem niza digitalnih servisa, a dio ključnih resursa upotrebljava se u obliku usluge (tzv. *Software as a Service*, *Platform as a Service* i dr.). Svaki od tih elemenata proširuje napadnu površinu i zahtijeva promišljeniji pristup sigurnosti.

Pritom treba naglasiti da digitalna transformacija ne utječe samo na tehničku stranu poslovanja nego i na organizacijsku dinamiku. U uvjetima rada na daljinu i hibridnog rada zaposlenici se često koriste osobnim uređajima, rade iz različitih mrežnih okruženja i pristupaju poslovnim resursima izvan opsega klasične korporativne mreže. Time granice organizacije postaju meke, a sigurnost se iz modela „štitimo opseg" mora preseliti na model „štitimo identitet i podatke", odnosno na koncept „nultog povjerenja" (engl. zero trust). Taj zaokret nije moguće provesti bez jasne politike, bez podrške uprave i bez stalne edukacije zaposlenika.

Digitalna transformacija nije samo uvođenje novog softvera niti digitalizacija jedne poslovne funkcije. Ona podrazumijeva preoblikovanje načina na koji organizacija stvara vrijednost, kako upravlja informacijama i kako komunicira s korisnicima (Brynjolfsson i McAfee, 2014). Kad se takva promjena dogodi, sigurnost više ne može biti smještena isključivo u IT odjelu. Mora postati dio strateškog upravljanja i biti dio organizacijske kulture. To znači da se o sigurnosti treba raspravljati na razini uprave, uključivati ju u planove ulaganja, mjeriti njezinu učinkovitost i redovito izvještavati o incidentima.

Hrvatska poduzeća u tom se procesu suočavaju s nekoliko specifičnih izazova. Većinu gospodarstva čine mikropoduzeća te mala i srednja poduzeća kojima je teško osigurati stalnog stručnjaka za sigurnost. Dio organizacija i dalje smatra da nisu zanimljiva meta, iako statistike europskih institucija i ENISA pokazuju da su upravo manje i slabije zaštićene organizacije najčešće mete jer su napadačima lakše (ENISA, 2023). Dio menadžmenta sigurnost još uvijek doživljava kao trošak, a ne kao investiciju u povjerenje i reputaciju. U mnogim organizacijama postoje sigurnosni postupci, ali se o tim postupcima ne komunicira dovoljno, pa zaposlenici i ne znaju da postoje. U ovom se radu polazi upravo od te napetosti između svijesti i stvarne prakse.

Polazeći od navedenih izazova i cilja rada, formulirana su četiri istraživačka pitanja:

1. Kako hrvatske organizacije percipiraju ključne digitalne prijetnje?
2. U kojoj su mjeri organizacijski i tehnološki hrvatske organizacije pripremljene za sigurnosne incidente?
3. Kakvu ulogu imaju edukacija i sigurnosna kultura?

4. Koje prepreke organizacije najčešće navode u razvoju sigurnosne zrelosti?

Potom su postavljene hipoteze koje usmjeravaju empirijski dio istraživanja:

H1 (Hipoteza o edukaciji): Organizacije koje provode redovite sigurnosne edukacije imaju višu samoprocijenjenu sigurnosnu spremnost.

H2 (Hipoteza o tehnološkim mjerama): Tehnološke mjere poput MFA, EDR/XDR i DLP nisu jednako rasprostranjene, pri čemu se najčešće primjenjuju osnovne mjere niskog troška.

H3 (Hipoteza o percepciji prijetnji): Percepcija da organizacija nije „zanimljiva meta" pozitivno korelira s nižim stupnjem ulaganja u sigurnosti.

Hipoteze imaju deskriptivan karakter i primarno služe kao okvir za interpretaciju dobivenih obrazaca, a ne za inferencijalno testiranje.

## 2. Teorijski okvir

### 2.1. Pojmovno određenje digitalne transformacije

Digitalna transformacija u literaturi obično se definira kao proces sustavne primjene digitalnih tehnologija s ciljem ostvarivanja novih ili znatno poboljšanih poslovnih procesa, proizvoda i usluga (Davenport, 2020). Bitno je naglasiti da ona uključuje i organizacijsku i kulturološku promjenu. Poduzeće koje samo kupi novi informacijski sustav, ali ne promijeni način rada, zapravo nije prošlo transformaciju. Upravo zato se u novijim radovima naglašava da je digitalna transformacija prije svega pitanje upravljanja promjenom, a tek onda pitanje tehnologije.

Porter i Heppelmann (2015) uvjerljivo pokazuju da digitalizacija proizvode pretvara u pametne i povezane sustave. Ti sustavi stvaraju goleme količine podataka, a podatci su, s gledišta sigurnosti, uvijek i resurs i obveza. Što je više podataka, to je veća vrijednost za napadača. Što je više povezanih sustava, to je veći broj ulaznih točaka. Iz toga proizlazi prva važna teza ovoga rada: sigurnost mora pratiti digitalizaciju brzinom kojom se ona događa. Ako poslovni dio organizacije povuče naprijed, a sigurnost se ne prilagodi, nastaje sigurnosni jaz.

Digitalna transformacija također se može promatrati kroz prizmu digitalne otpornosti. Europska komisija (2024) digitalnu otpornost definira kao sposobnost korištenja digitalne tehnologije, a da se pritom zadrži sigurnost, privatnost i kontinuitet poslovanja. Drugim riječima, cilj nije izbjeći rizik (to u digitalnom svijetu nije moguće), nego njime upravljati i učiniti organizaciju dovoljno elastičnom da preživi incident. Takav pogled napušta staru logiku „štitimo sve jednako" i uvodi logiku „štitimo ono što je najvrjednije i najranjivije".

## 2.2. Teorijski modeli korporativne sigurnosti

Korporativna sigurnost razvijala se od prakse fizičke zaštite prema današnjem, znatno širem konceptu koji uključuje i poslovnu tajnu, informacijsku sigurnost, kibernetičku sigurnost, reputacijsku zaštitu i usklađenost s propisima. U teoriji se mogu izdvojiti tri modela koja su za ovaj rad važna:

1. Sustavni model polazi od toga da su ljudi, tehnologija i procesi nerazdvojni. Ako postoji odlična tehnologija, ali zaposlenici ne znaju kako se njome koristiti ili ju zaobilaze, sustav je nesiguran. Ako postoje procedure, ali nema tehničke kontrole, opet je nesiguran. Sigurnost se zato mora dizajnirati unutar čitavog sustava, a ne samo u jednoj točki. Ovaj model posebno je važan u hibridnom i udaljenom radu, gdje se opseg organizacije stalno mijenja.
2. Model životnog ciklusa sigurnosti (NIST, 2023) opisuje sigurnost kao stalno ponavljanje pet faza: identifikacija, zaštita, detekcija, odgovor i oporavak. Taj je model važan jer naglašava oporavak kao jednako važan element sigurnosti. U digitalnom dobu nije realno očekivati da se incident nikad neće dogoditi; realno je imati dobar plan kako ga preživjeti, brzo oporaviti sustave i jasno komunicirati prema korisnicima.
3. Model otpornosti (ENISA, 2023) dodaje dimenziju učenja. Organizacija koja iz svakog incidenta izvuče pouke i promijeni pravila u sljedećem će incidentu biti manje ranjiva. To je ono što Weick i Sutcliffe (2015) zovu menadžmentom neočekivanog.

Za hrvatska poduzeća najkorisniji je upravo ovaj treći, evolucijski pogled na sigurnost jer se njime omogućuje postupna izgradnja sustava i prihvaća činjenica da resursi nisu neograničeni. Umjesto da se traži savršena sigurnost, gradi se dovoljna sigurnost koja odgovara stvarnim rizicima i financijskim mogućnostima.

## 2.3. Ljudski i organizacijski aspekti sigurnosti

U gotovo svim izvješćima o kibernetičkim incidentima ljudski se faktor navodi kao najslabija karika. To ne znači da su ljudi krivci, nego da su upravo ljudi točka na kojoj se sigurnost može najviše poboljšati. NIST (2023) procjenjuje da bi se velik broj incidenata mogao spriječiti samo dosljednom primjenom osnovnih pravila: jakih lozinki, dvofaktorske autentifikacije, provjere izvora poruka i redovitog sigurnosnog kopiranja podataka.

Byram (1997) i Crystal (2012) podsjećaju da je sigurnost i komunikacijski problem. *Phishing* mailovi ne uspijevaju zato što su tehnički savršeni, nego zato što su komunikacijski uvjerljivi. Zaposlenik koji razumije kako funkcioniraju manipulativne poruke u pravilu je otporniji. Zato suvremena sigurnost sve više traži meke vještine: sposobnost uočavanja sumnjivog ponašanja, spremnost na prijavu, kulturu u kojoj

prijava nije „cinkanje", nego profesionalna obveza. Organizacije koje nagrađuju prijavu incidenata imaju bolje izglede da incident uoče u ranoj fazi.

Organizacijska kultura sigurnosti gradi se dugoročno. Počinje od vrha ako se uprava ne koristi službenim kanalima, ako ignorira procedure ili traži brža rješenja, šalje jasnu poruku da je sigurnost manje važna od brzine. Suprotno tomu, uprava koja svojim ponašanjem pokazuje da su pravila obvezujuća, stvara okruženje u kojem se i ostali pridržavaju procedura. Rust (2020) ide i korak dalje pa tvrdi da je sigurnost zapravo ulaganje u reputaciju: poduzeće koje se odgovorno odnosi prema podatcima partnera i kupaca jača svoje tržišno povjerenje.

### 2.4. Normativni i regulatorni okvir Europske unije

Europska unija u posljednjih je nekoliko godina uvela niz akata koji sigurnost čine obveznim, a ne samo poželjnim elementom poslovanja. NIS2 Direktiva (European Union, 2022) traži od ključnih i važnih subjekata da uvedu mjere upravljanja rizicima, da imaju planove kontinuiteta poslovanja i da incidente prijave u vrlo kratkim rokovima. Bitno je da se odgovornost penje do razine uprave, odnosno više nije dovoljno da IT nešto radi nego i uprava mora dokazati da nadzire sigurnost.

„Akt o kibernetičkoj otpornosti" („Cyber Resilience Act") (European Union, 2022) usmjeren je prema proizvođačima i dobavljačima softvera i hardvera te traži da sigurnost bude ugrađena već u dizajnu. To je važno za poduzeća jer smanjuje rizik koji dolazi izvana, iz lanca dobave.

Naravno, GDPR (European Union, 2016) i dalje postavlja vrlo visoke zahtjeve za zaštitu osobnih podataka i za transparentnost prema korisnicima. Kombinacija ovih propisa čini jasnu poruku: u prostoru Europske unije sigurnost i privatnost nisu opcija, nego obveza.

Za hrvatska poduzeća ovo znači dvostruku obvezu: prema nacionalnom zakonodavstvu i prema europskim pravilima. Manja poduzeća u pravilu nemaju dovoljno ljudi da sama prate sve promjene, pa je rješenje u zajedničkim rješenjima (zajedničke platforme, sektorski SOC-ovi, zajedničke edukacije), ali i u korištenju usluga stručnih institucija i komora.

## 3. Metodologija istraživanja

Istraživanje na kojem je utemeljen empirijski dio rada provedeno je u listopadu 2025. putem mrežnog upitnika. Upitnik je bio anoniman, a sudjelovanje dobrovoljno. Ciljna skupina bili su zaposlenici i menadžeri u hrvatskim poduzećima koji se u svom radu susreću s IT-em, sigurnošću ili upravljanjem procesima. Iako je riječ o namjernom uzorku, cilj je bio dobiti uvid u stvarno stanje, a ne statističku reprezentativnost.

Prikupljeno je 180 valjanih odgovora. S obzirom na to da je riječ o relativno malom uzorku, rezultati su ponderirani kako bi se dobila slika koja bolje oponaša strukturu hrvatskog gospodarstva (dominacija malih i srednjih poduzeća, ali i prisutnost većih). Takav je postupak čest u istraživanjima sigurnosti jer upravo subjekti koji su najosjetljiviji na sigurnost najčešće i odgovaraju na ankete.

Polazeći od cilja rada, istraživanje je operacionalizirano putem četiriju istraživačkih pitanja: (1) kako hrvatske organizacije percipiraju ključne digitalne prijetnje, (2) u kojoj su mjeri organizacijski i tehnološki pripremljene za sigurnosne incidente, (3) kakvu ulogu imaju edukacija i sigurnosna kultura te (4) koje prepreke organizacije najčešće navode u razvoju sigurnosne zrelosti. Ova se istraživačka pitanja formuliraju deskriptivno, u skladu s eksplorativnim karakterom rada i veličinom uzorka.

Upitnik je imao četiri dijela:

1. opći podatci (veličina, djelatnost, pozicija ispitanika)
2. percepcija prijetnji (koliko su ozbiljni kibernetički napadi, reputacijske prijetnje, curenje podataka)
3. organizacijska i tehnološka pripremljenost (postojanje strategije, plana odgovora, MFA, EDR/XDR, DLP)
4. edukacija i kultura (učestalost obuka, uloga uprave, spremnost na prijavu incidenata).

Podatci su obrađeni deskriptivno, a rezultati prikazani narativno, u skladu s uputama časopisa i pravilima citiranja (APA). U odnosu na ograničenja uzorka, rezultati se tumače kao indikativni jer se ne mogu potpuno primijeniti na sve hrvatske organizacije.

## 4. Rezultati istraživanja

Analiza odgovora pokazala je nekoliko jasnih obrazaca koji se ovdje navode taksativno:

1. visoka svijest, ali neujednačena praksa – više od 70 % ispitanika navodi da su *ransomware* i *phishing* vrlo ozbiljne prijetnje, ali samo 41 % organizacija ima formalno zapisan i poznat plan odgovora na incidente; prijetnje se prepoznaju, ali se ne pretvaraju uvijek u procedure
2. edukacija je ključna točka – čak 47 % poduzeća provodi barem jednu obuku godišnje, 30 % to radi povremeno, a 23 % uopće ne; upravo tih 23 % iskazuje i najmanju sigurnost u vlastitu spremnost; pritom su najbolji rezultati u organizacijama koje kombiniraju kratke *online* edukacije sa simuliranim *phishing* kampanjama
3. tehnologija se uvodi postupno – MFA-om se koristi većina, EDR/XDR-om oko 40 %, a DLP-om tek petina ispitanika, što je razumljivo jer su MFA i osnovne za-

štite najdostupnije i ne traže velike promjene u procesima, dok napredna rješenja često traže dodatno osoblje i prilagodbu infrastrukture

4. prepreke su ponovljive – glavne su prepreke nedostatak novca (33 %), nedostatak stručnih ljudi (28 %) i nedovoljna podrška uprave (20 %); ovo se poklapa s europskim izvješćima za mala i srednja poduzeća.

Zanimljiv je i nalaz da dio ispitanika smatra da njihova organizacija nije zanimljiva meta. To je tipičan primjer kognitivne pristranosti: napadači vrlo često ciljaju upravo manje i slabije zaštićene subjekte jer je šansa za uspjeh veća, a rizik od otkrivanja manji.

## 5. Rasprava

Hrvatske organizacije digitalne prijetnje percipiraju kao vrlo ozbiljne, osobito *ransomware* i *phishing* napade. Preko 70 % ispitanika ocjenjuje ih visoko rizičnima, dok reputacijske prijetnje i curenje podataka slijede odmah nakon njih. Međutim, unatoč visokoj razini svijesti, percepcija se ne prenosi uvijek u formalizirane procedure – samo 41 % organizacija posjeduje jasno definiran plan odgovora na incidente. Uočena je i pristranost dijela ispitanika koji smatraju da „nisu zanimljiva meta", što je u suprotnosti s europskim trendovima napada na manje organizacije.

Tehnološka i organizacijska pripremljenost organizacija jest srednjeg stupnja: osnovne mjere poput MFA-a široko su implementirane, dok napredniji sustavi (EDR/XDR, DLP) značajno zaostaju. Organizacijski elementi, poput strategije i formalnog plana odgovora na incidente, prisutni su kod dijela organizacija, ali ne sustavno. Samo se manji dio organizacija nalazi na „proaktivnoj razini", dok većina ostaje između reaktivne i funkcionalne zrelosti. Najveće prepreke identificirane su kao nedostatak financijskih sredstava, stručnog osoblja i podrške uprave.

Edukacija i kultura sigurnosti ključni su čimbenici sigurnosne spremnosti hrvatskih organizacija. Rezultati istraživanja pokazuju jasnu vezu između učestalih edukacija i višeg stupnja samoprocijenjene sigurnosne zrelosti. Organizacije koje provode barem jednu edukaciju godišnje značajno rjeđe izražavaju nesigurnost i imaju veći stupanj primjene tehnoloških mjera. Kultura sigurnosti, posebno jasna komunikacija uprave, prijavljivanje incidenata i dosljedno poštivanje procedura, pokazuje se jednako važnom kao i tehnološke mjere. Nedostatak edukacije i slaba kultura sigurnosti povezani su s nižim ulaganjima, slabijim tehnološkim kapacitetima i percepcijom da organizacija „nije meta". Time se potvrđuje da ljudski i organizacijski faktori imaju presudan utjecaj na digitalnu otpornost.

Rezultati potvrđuju ono što teorija već dugo govori: sigurnosni problem u organizacijama najčešće nije tehnološki, nego organizacijski i kulturni. Većina alata dostupna je, dio je čak i besplatan ili ugrađen u postojeće sustave, ali se organizacije

njima ne koriste ili se njima koriste djelomično. Razlog je što sigurnost još nije u potpunosti ušla u redoviti menadžerski ciklus – planiranje, provođenje, praćenje i izvještavanje.

Dobiveni nalazi ujedno omogućuju provjeru triju postavljenih hipoteza. Prvo, H1 je potvrđena: organizacije koje provode redovite edukacije pokazuju višu razinu samoprocijenjene spremnosti i rjeđe izražavaju nesigurnost u vlastite sigurnosne kapacitete. Drugo, H2 je potvrđena jer se uočava jasna razlika u rasprostranjenosti tehnoloških mjera – MFA je široko implementiran, dok se EDR/XDR rješenjima koristi oko 40 % organizacija, a DLP-om tek manji dio, što je u skladu s očekivanom hijerarhijom troškova i složenosti. Treće, H3 je potvrđena jer ispitanici koji smatraju da njihova organizacija „nije zanimljiva meta" istodobno navode nižu razinu ulaganja, slabiju tehničku zaštitu i manju formaliziranost procedura. Ovi obrasci potvrđuju da perceptivni čimbenici mogu značajno utjecati na zrelost sigurnosnog sustava.

Možemo izdvojiti tri razine zrelosti:

1. reaktivna razina: sigurnost se spominje samo kad se nešto dogodi; procedure su često nepoznate; zaposlenici ne znaju kome prijaviti incident; uprava se uključuje naknadno
2. funkcionalna razina: postoje osnovne politike, MFA, *backup*, antivirusni programi, možda i plan odgovora; edukacija se povremeno provodi; uprava zna za rizike, ali ih ne mjeri redovito
3. proaktivna/integrirana razina: sigurnost je dio strategije, mjeri se (npr. broj incidenata, vrijeme oporavka, postotak obučenih), redovito se testira (simulacije *phishinga*), upotrebljava se više izvora (ENISA, NIST), a dio je postupaka automatiziran.

Hrvatska poduzeća, prema dobivenim odgovorima, većinom su između prve i druge razine. To nije dramatično loše, ali znači da se bez svjesne odluke uprave teško prelazi na treću razinu. Upravo tu se vidi važnost NIS2 kojim se aktivno potiču uprave da preuzmu nadzor.

Drugo važno pitanje iz rasprave jest odgovornost uprave. NIS2 vrlo jasno kaže da je uprava odgovorna za nadzor nad mjerama sigurnosti. To je za hrvatsku praksu važna promjena jer sigurnost više nije stvar informacijske tehnologije. Kada je uprava odgovorna, onda se sigurnost planira u budžetu, mjeri se učinak, uvodi se red u dokumentaciju i prate se promjene propisa.

Treće, važno je uočiti da se dio poduzeća oslanja na dobavljače i oblak („to nam rješava *provider*"). To može biti prihvatljivo rješenje, ali samo ako je odnos uređen ugovorima, ako postoji provjera i ako organizacija ipak zadržava nadzor nad podatcima. Inače se sigurnost samo udalji, ali se rizik ne smanjuje.

## 6. Limiti istraživanja i prijedlozi za buduća istraživanja

Iako provedeno istraživanje daje koristan uvid u stanje poslovne sigurnosti u hrvatskim poduzećima u kontekstu digitalne transformacije, potrebno je jasno istaknuti njegova ograničenja. Prvo i najočitije ograničenje jest veličina i struktura uzorka. U istraživanju je sudjelovalo 180 ispitanika, a rezultati su ponderirani da bi se dobila reprezentativnija slika. Takav pristup dopušta opis trendova, ali ne omogućuje izvođenje statistički snažnih zaključaka niti generalizaciju na cjelokupno hrvatsko gospodarstvo. U budućim bi istraživanjima bilo korisno provesti anketu na većem uzorku, uz jasnu stratifikaciju prema djelatnosti (npr. financije, turizam, javni sektor, IT) i prema veličini poduzeća.

Drugo ograničenje odnosi se na samonavođenje i percepcijske odgovore. Ispitanici su sami procjenjivali razinu sigurnosti u svojim organizacijama, učestalost edukacija i postojanje sigurnosnih politika. Takvi podatci mogu biti pod utjecajem subjektivnih procjena, društveno poželjnih odgovora ili jednostavno nedovoljne informiranosti zaposlenika o internim aktima. Dio ispitanika je, primjerice, naveo da nije siguran postoji li plan odgovora na incidente, što znači da plan možda postoji, ali da se o planu nije dovoljno komuniciralo. Zato bi u budućim istraživanjima trebalo kombinirati anketne podatke s dokumentarnom analizom (uvid u pravilnike, planove, zapisnike o vježbama) ili barem s polustrukturiranim intervjuima s odgovornim osobama za sigurnost.

Treće ograničenje odnosi se na vremenski okvir. Istraživanje je provedeno u listopadu 2025., u razdoblju kada su organizacije u Hrvatskoj još uvijek usklađivale svoje procese s europskim direktivama nove generacije (posebno NIS2 i CRA). To znači da su današnji rezultati vjerojatno nešto bolji, pogotovo u sektorima koji su izravno regulirani (energetika, zdravstvo, financije). Stoga bi bilo korisno provoditi longitudinalna istraživanja i ponavljati istu anketu u razmacima od 12 ili 24 mjeseca da bi se pratio rast sigurnosne zrelosti.

U istraživanju je težište usmjereno pretežito na organizacijsku i tehnološku dimenziju sigurnosti, dok su ekonomske i pravne posljedice incidenata samo marginalno dotaknute. Buduća istraživanja trebala bi uključiti i troškovnu analizu (npr. prosječan trošak incidenta za malo poduzeće, trošak edukacije u odnosu na smanjenje incidenata, usporedba internog i *outsourcing* modela sigurnosti) te analizu usklađenosti s nacionalnim i europskim propisima. Time bi se dobila potpunija slika koristi i prepreka pri ulaganjima u sigurnost.

U istraživanju je korišten kvantitativni upitnik koji je dobar za prepoznavanje obrazaca, ali slabiji za razumijevanje dubinskih razloga. Bilo bi iznimno korisno provesti kvalitativne studije slučaja u hrvatskim poduzećima koja su uspješno provela sigurnosnu transformaciju  primjerice u bankarskom sektoru, u velikim IT-tvrtkama

ili u javnim institucijama koje pružaju e-usluge. Takve bi studije mogle pokazati koje su točno organizacijske odluke, obrasci vodstva i modeli edukacije doveli do vidljivog povećanja otpornosti.

Iako ovo istraživanje potvrđuje da u hrvatskim poduzećima postoji svijest o digitalnim rizicima, za dublje razumijevanje odnosa među digitalnom zrelosti, sigurnosnom kulturom i organizacijskim upravljanjem potrebna su šira, metodološki raznolika i sektorski specifična istraživanja. Kombinacija kvantitativnih i kvalitativnih metoda, uz izravno uključivanje menadžmenta i državnih tijela, mogla bi dati temelje za nacionalne smjernice o digitalnoj sigurnosti poslovnih subjekata.

## 7. Zaključak

Za digitalnu transformaciju poslovne sigurnosti nije pitanje hoćemo li ju provesti, nego koliko ćemo ju brzo i koliko zrelo provesti. Organizacije koje digitaliziraju poslovanje, a ne jačaju istodobno sigurnost, zapravo povećavaju izloženost i dugoročne troškove. Organizacije koje sigurnost uključe u strategiju dobivaju suprotno: otpornije su na incidente, brže se oporavljaju i uživaju veće povjerenje korisnika, partnera i regulatora.

Rezultati ovoga istraživanja dodatno potvrđuju da zrelost sigurnosnih praksi ovisi o kontinuiranoj edukaciji, dosljednoj primjeni tehnoloških mjera i ispravnoj percepciji rizika, što je u skladu s postavljenim hipotezama.

Na temelju teorijskog pregleda i provedenog istraživanja mogu se dati sljedeće preporuke, odnosno potrebno je:

1. sigurnost ugraditi u strateške dokumente – ona mora biti vidljiva u misiji, ciljevima, planu ulaganja i izvještavanju upravi
2. uspostaviti stalne programe edukacije – jednokratne radionice nisu dovoljne; sigurnosna svijest pada ako se ne obnavlja
3. primijeniti međunarodne okvire (NIST, ISO/IEC 27001) i uskladiti se s europskim propisima (NIS2, CRA, GDPR)
4. razvijati kulturu prijavljivanja – incident koji nije prijavljen ne može se analizirati i iz njega se ne može učiti
5. poticati suradnju i zajednička rješenja, posebno za mala i srednja poduzeća isplativo je dijeliti usluge, alate i edukacije
6. mjeriti sigurnost – ako se ne prate pokazatelji (broj incidenata, vrijeme oporavka, broj obučenih zaposlenika), sigurnost će uvijek biti nevidljiva i zato potisnuta.

Digitalna sigurnost jest alat za izgradnju povjerenja. Organizacije koje to razumiju brže će se prilagoditi europskim zahtjevima i imati jasnu komunikacijsku pred-

nost na tržištu. Upravo zato sigurnost treba promatrati kao integrirani dio digitalne transformacije, a ne kao njezin dodatak.

Sustavni pristup, potkrijepljen jasnim hipotezama i analitičkim uvidom, pokazuje da otpornost nije rezultat pojedinačne mjere, već kombinacije kulture, tehnologije i upravljačkog angažmana.

## Literatura


1. Brynjolfsson, E. i McAfee, A. (2014). *The Second Machine Age.* New York: W. W. Norton & Company.
2. Byram, M. (1997). *Teaching and Assessing Intercultural Communicative Competence.* Multilingual Matters.
3. Crystal, D. (2012). *English as a Global Language.* Cambridge University Press.
4. Davenport, T. (2020). *The AI Advantage.* MIT Press.
5. ENISA (2023). *Threat Landscape Report 2023.* European Union Agency for Cybersecurity.
6. European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (31. listopada 2025.)
7. European Union (2022). *Directive (EU) 2022/2555 (NIS2).* Official Journal of the EU. (31. listopada 2025.)
8. Europska komisija (2024). *Digital Decade Policy Programme 2030.* Brussels: European Commission.
9. NIST (2023). *Cybersecurity Framework 2.0 Draft.* National Institute of Standards and Technology.
10. Porter, M. i Heppelmann, J. (2015). How smart, connected products are transforming companies. *Harvard Business Review,* 93(10), 96–114.
11. Rust, R. (2020). *The future of marketing.* International Journal of Research in Marketing, 37(1), 15–26.
12. Weick, K. E. i Sutcliffe, K. M. (2015). *Managing the Unexpected: Sustained Performance in a Complex World.* Jossey-Bass.

# DIGITAL TRANSFORMATION OF CORPORATE SECURITY


## Abstract

In recent years, digital transformation has fundamentally reshaped the conceptual framework of corporate security. Organizations no longer focus solely on protecting physical assets and core IT infrastructure; instead, they manage an extensive ecosystem of data, cloud services, remote users, vendors, and publicly accessible services. While this environment fosters opportunities for increased operational efficiency, it simultaneously expands the attack surface and enhances the complexity of threats — ranging from cyberattacks and industrial espionage to data breaches, reputational attacks, and disinformation campaigns. The objective of this paper is to examine the evolution of corporate security under the influence of digital transformation, identify applicable theoretical models, and assess the readiness of Croatian enterprises for such transitions. The research methodology integrates a theoretical overview with the results of a survey conducted in October 2025 among a sample of Croatian organizations of varying sizes. The findings indicate that while threat awareness is high, the implementation of security measures remains insufficiently systematic and often contingent upon individual efforts. The study highlights a critical need for developing a robust security culture, strengthening the role of management boards in security planning, and ensuring more consistent compliance with the European regulatory framework (NIS2, CRA, GDPR). The conclusion is that digital transformation can enhance organizational resilience and competitiveness, provided that security is treated as an embedded, rather than a retroactive, function.


**Keywords:** digital transformation, corporate security, cyber resilience, risk management, security culture, NIS2, Croatia