DOI: 10.19279/TVZ.PD.2016-4-3-10

PRIMJER UVOĐENJA BYOD NAČINA POSLOVANJA

AN EXAMPLE OF INTRODUCING BYOD WAY OF DOING BUSINESS

Dijana Liverić[1], Andrijana Ivančić[2], Ivan Pogarčić[1]

[1]Poslovni odjel, Veleučilište u Rijeci, Rijeka, Hrvatska
[2]Fakultet za ekonomiju i turizam "dr. Mijo Mirković"; Redovni diplomski studij informatike, Sveučilište Jurja Dobrile u Puli

Sažetak

Uvođenje BYOD (Bring Your Own Device) načina poslovanja u tvrtke odnosi se na način poslovanja koji zaposlenicima omogućava korištenje osobnih mobilnih uređaja (mobitel, tablet, laptop) za obavljanje poslova unutar tvrtke u kojoj su zaposleni. U radu će biti prikazani prednosti i nedostaci uvođenja takvog pristupa poslovanju, istražiti će se sigurnosni rizici, financijski pokazatelji kao i metode koje se koriste u IT odjelima. Navedeni pokazatelji rezultat su trenutnog stanja ljudskog potencijala unutar tvrtki u načinu korištenja alata koje trenutna informatička tehnologija pruža, a koja se definira ugovorom izmedju djelatnika i tvrtke.

Ključne riječi: *BYOD, upravljanje mobilnim uređajima, mrežna sigurnost, procjena učinkovitosti*

Abstract

Implementing BYOD business strategy refers to using personal mobile devices (mobile phones, tablets, laptops) for business purposes. Developing a business approach such as BYOD (Bring Your Own Device), requires certain adjustments both for the organization and employees. This paper attempts to present the advantages and disadvantages of introducing such an approach to business, its security risks, financial indicators as well as the methods used in IT departments. These indicators are the result of the current IT technologies and state of human resources within the organizations, defined by the contract between organizations and their employees.

Keywords: *BYOD, mobile device managment, security risks, assessment of efficiency*

1. Uvod

1. *Introduction*

U sve većem porastu razvoja novih tehnologija kao i novih tehnoloških otkrića poput automobila koji se vozi pomoću snage struje, pametnih satova i narukvica, otvaraju se nova područja konkurentnosti u poslovanju. Općeprihvaćena činjenica je da pristup poslovanju koji ne teži što novijem, što boljem razvoju tehnoloških otkrića te zemlje koje ne primjenjuju infomacijsko – komunikacijsku tehnologiju smatraju se zaostalima, slabima, nekonkurentnima.[1]

Informatizacija je uvelike pridonijela razvoju poslovanja, širenju informacija, konkurentnosti poduzeća, odnosno samih država, profitu, ali i razvitku čovjekovog uma tj. ljudskog potencijala kao i samom razvoju poslovanja. U tom smislu, otvaraju se i nove mogućnosti u poslovanju te kao primjer jednog takvog uvođenja novog pristupa razvio se BYOD. Omogućujući zaposlenicima da svoje osobne elektroničke uređaje koriste u poslovne svrhe, stvara se klima koja zapolsenicima na više načina olakšava rad, a poslodavcima prostor za financijsku uštedu u nabavci tehničke opreme. No, da bi takav pristup modernog poslovanja ispunio svoju svrhu, potrebno je jasno definirati, principe kojima će se odrediti kvaliteta rada kao i kvaliteta poslovnih odnosa, uvođenjem BYOD poslovnog modela. Stoga IT odjeli u tvrtkama, stvaraju strategije uvodjenja BYOD-a, na temelju poslovnih procesa koji su u izravnoj vezi s tehnološkom opremom tvrtke i osobnom tehnološkom opremom zaposlenika, mrežnom infrastrukturom, te softverskim rješenjima potrebnim za rad odnosno zaštitu i sigurnost. Prilikom implementacije BYOD strategije

poslovanja predlažu se različita informacijsko-komunikacijska i tehnička rješenja koja su dakako, podložna promjenama u skladu s razvojem tehnologije, ali i razvojem ljudskog potencijala.

2. Karakteristike byod načina poslovanja

2. *Characteristics of byod way of doing business*

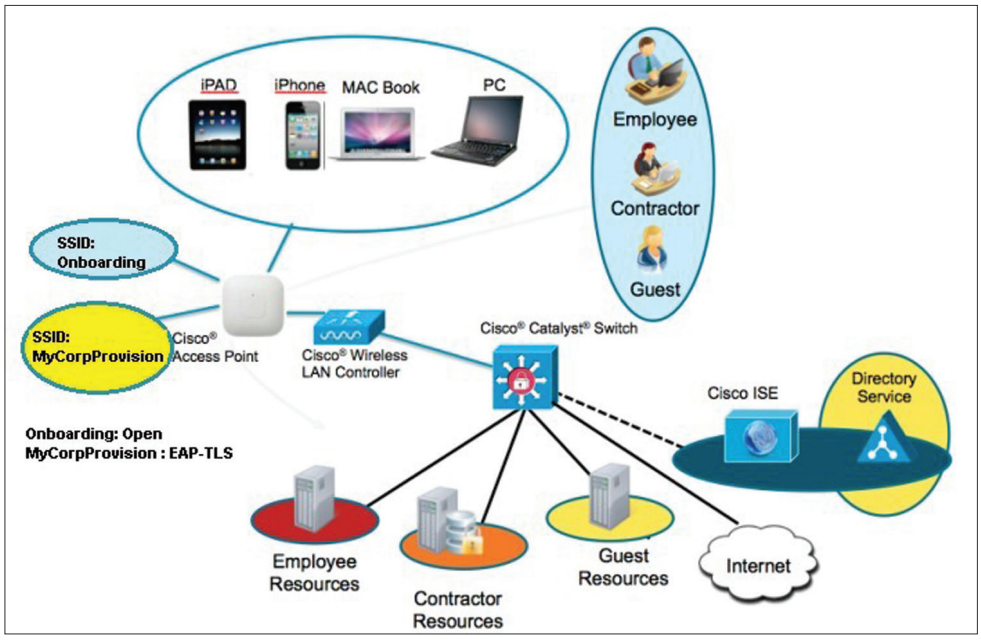
Zaposlenici, u različitim industrijskim granama već duže vrijeme koriste svoje uređaje (mobitele, tablete, prijenosna računala) u poslovanju. Obzirom da se trend proširio na sve veći broj zaposlenika koji korisiti osobne tehnološke uređaje na poslu, organizacije su došle do zaključka kako bi zaposlenici mogli „ponijeti svoj uređaj na posao“ gdje nastaje i sam akronim BYOD (Bring Your Own Device). Prve takve mogućnosti pruža uređaj Blackberry (1984, osnivači: Douglas Fregin, Mike Lazaridis), a nakon njega iPhone (2007, osnivač: Steve Jobs). U početku su organizacije, kontrolirale korištenje mobilnih uređaja koji su bili u vlasništvu tvrtke. No, s vremenom su zaposlenici počeli koristiti i osobne mobitele za spajanje na mrežu tvrtke te se pojavio problem, kako za tvrtku zbog kontrole pristupa, tako i za zaposlenika, koji koristi više uređaja (jedan za posao, a drugi u privatne svrhe).

Osim što je osiguravanje službenih pametnih telefona, tableta, prijenosnih računala za zaposlenike skupo, a samim time mnogim organizacijama nedostižno, uvođenjem BYOD strategije postiže se smanjenje troškova uz povećanje produktivnosti i učinkovitosti.[3]

Istraživanja pokazuju da zaposlenici pokazuju daleko veću učinkovitost zahvaljujući činjenici da se mogu koristiti svojim mobilnim uređajima obavljujući posao izvan ureda.[3] Također, u etičkom smislu, obzirom da poslodavci ne utječu direktno na izbor vrste uređaja, zaposlenike to čini slobodnima u odabiru uređaja kojeg žele koristiti što svakako ide u prilog povećanom zadovoljstvu zaposlenika koje izravno utječe na produktivnost u radu.

Osim pojačane produktivnosti i učinkovitosti zaposlenika te smanjenja financijskih troškova, BYOD strategija poslovanja, otvara pitanja sigurnosti poslovanja. U kontekstu sigurnosti poslovanja unutar BYOD strategije, problematika se odnosi na sigurnost povjerljivih informacija koja je smanjena samim time što se uređaji koriste i izvan ureda, kao i u kontekstu mrežne sigurnosti te upravljanja identitetima.

Vodeći se činjenicom da je BYOD strategija koja se prije svega odnosi na poslovanje, ne treba zanemariti činjenicu da je financijski aspekt jedan od preduvjeta koji je potrebno istražiti prije nego li se donese odluka o implementaciji.



Slika 1
prikaz BYOD - komponente uključene u implementaciju [7]

Figure 1
Presentation of BYOD - components involved in the implementation [7]

3. Financijski pokazatelji

3. *Financial indicators*

BYOD strategija poslovanja sadrži troškove koji su uvelike okrenuti prema zaposlenicima, obzirom da zaposlenci sami plaćaju/kupuju svoj uređaj, čime organizacija ostvaruje znatne uštede. No, troškovi se ne odnose isključivo na kupovinu i održavanje uređaja. Naime, korištenje pametnih telefona, osim troškova podatkovnog prijenosa, uključuje i troškove telefonskih razgovora, koji su redovno skuplji, ukoliko se pretplata odnosi na privatne korisnike jer općepoznato je da industrija mobilnih operatera nudi jeftinije tarife za poslovne svrhe. Osim troškova kupovine uređaja i troškova prema mobilnom operateru što ih snose zaposlenici, organizacija svoje troškove ima u održavanju IT infrastrukture, potrebne za poslovanje i zaštitu.

Da bi se identificirale karakteristike koje utječu na profitabilnost implementacije, nove poslovne strategije, korisno je poslužiti se slijedećim metrikama koje nudi najčešće korištena ROI metodologija:

1. Treetop - istražuje utjecaj profitabilnosti na cijelu kompaniju. Profitabilnost može preuzeti ulogu smanjenja troškova zbog potencijala IT da smanji radnu snagu za svaki dani prosjek
2. Pure cost – nekoliko je vrsta čistih troškova u okviru ROI tehnike:
   a. Total Cost of Ownership - (TCO) daje detaljniji uvid oko same podrške i održavanja troškova kroz duže vremensko razdoblje
   b. Gartnerova grupa NOW (Normal Cost of Work Produced) – index koji mjeri troškove vezane za trošak obavljanja jednog zadatka u odnosu na trošak obavljanja sličnih zadataka.
3. Holistic IT - ova metoda jednaka je metodi balansiranog/uravnoteženog prikaza pokazatelja gdje IT odjel pokušava zadržati tradicionalno izbalansirane pokazatelje koji se tiču izvodivosti tj. financija, kupaca, internih operacija, obrazovanja zaposlenika i inovacija. [4],[5]

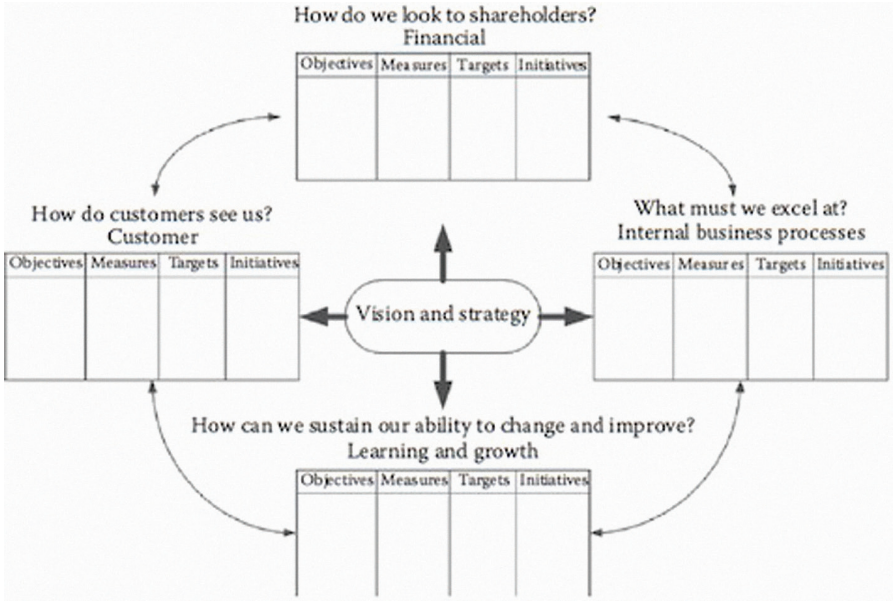
Služeći se ROI(Return on Investment) metodologijom za procjenu učinkovitosti ulaganja moguće je definirati faktore koji su od velike važnosti prilikom uvođenja nove poslovne strategije. Jedan od primjera takvog izračuna nudi rezultate za slijedeće komponente:

a. Produktivnost - mjerenje izlazne jedninice za svaku ulaznu jedinicu
b. Proces - sistem, tijek rada
c. Ljudski resursi - analiza troškova i koristi za određenu inicijativu
d. Faktori zaposlenika - zadržavanje, moral, odgovornost prema obvezama i vještine. [4],[5]

Potrebno je sve navedene rezultate „prevesti“ u financijske izvještaje, kako bi analiza bila potpuna. Ovo uključuje kombinaciju tzv. hard i soft faktora. Hard faktori, sastoje se od tradicionalnih mjera poput izlaznih jedinica, kao što su vrijeme, kvaliteta i troškovi. Soft faktore čini kombinacija onih faktora koje je teško izračunati kao što su: moral, preokret rata, odanost, izbjegavanje konflikta, nove vještine i ideje, uspješno dovršavanje projekata i drugo. Centralna točka svih ovih pokazatelja jest Benchmarking, a njegova svrha je da pripomaže pri učinkovitosti izvedivosti procesa, a uključuje sljedeće:

1. Identificiranje prilika
2. Postavljanje realnih, ali agresivnih ciljeva
3. Postavljanje izazova u smislu što je moguće napraviti
4. Razumijevanje metode poboljšanja procesa
5. Otkrivanje snage u vlastitioj organizaciji
6. Učenje od drugih stručnjaka
7. Priorizacija i alociranje resursa [3]

Nakon što je realizirana financijska analiza, slijedeći korak za pripremu implementacije BYOD načina poslovanja je razvoj strategije za upravljanje mobilnim uređajima te odabir i priprema tehnologije za sigurnosni sustav.



Slika 2
Korištenje Bencmarking-a za BYOD učinkovitost [8]

Figure 2
Using benchmarking for the BYOD efficiency [8]

4. Koraci za realizaciju BYOD

4. *Steps for implementation BYOD*

- PLAN - Provesti analizu troškova / koristi prilikom odlučivanja na koji način će se omogućiti mobilno korištenje, definirati tko će imati pristup, definirati sigurnosnu politiku organizacije, a zatim napraviti procijenu ukupnog IT sustava i podrške
- SIGURNOST I UPRAVLJANJE - Pažljivo izabrati koje tehnologije će se koristiti za upravljanje i osiguranje mobilnih uređaja. Pametni telefon sadrži povjerljive podatke koji mogu biti ukradeni ili izgubljeni stavljanjem osjetljive informacije u pogrešne ruke. Sustav poduzeća koji služi za upravljanje mobilnom tehnologijom mora biti dovoljno fleksibilan za kontrolu veze sa sve većim brojem različitih uređaja
- IZGRADNJA BYOD POLITIKE – Uspostavljanje kvalitetne komunikacije sa zaposlenicima kako bi se razjasnila pravila i rizici takvog načina poslovanja. U tom smislu važno je razjasniti koji uređaji su prikladni, kojim podacima se može pristupati, koji su podaci povjerljivi. Definiranje pravila koja jasno određuju što zaposlenici mogu, a što ne kako bi se dobio maksimum iz novog pristupa poslovanja.
- PODRŠKA – Osigurati pružanje podrške korisnicima sustava u okviru HelpDesk-a.

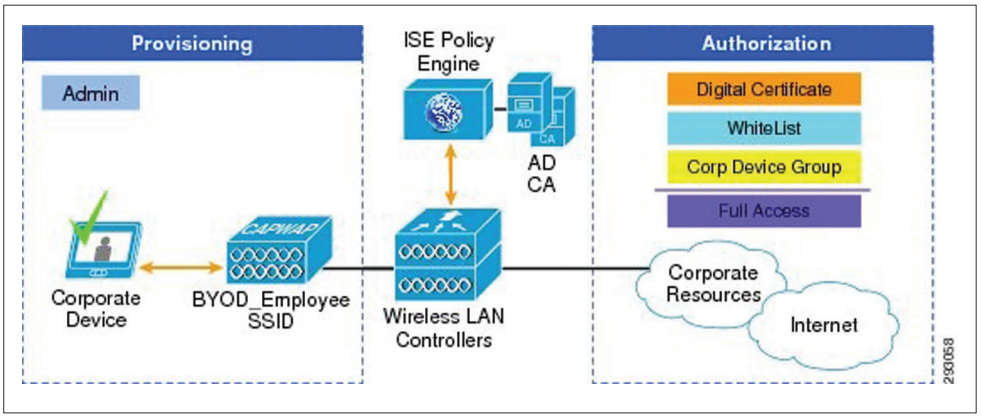
Definiranjem plana, u kojem je provedena analiza troškova i procjena IT sustava, jedan od najvećih zadataka IT sektora, koji nosi i najveću odgovornost u smislu BYOD poslovanja je definiranje upravljanja i uspostava sigurnosnih mjera.

4.1 Upravljanje uređajima i sigurnost

4.1 *device management and security*

Stvaranje uvjeta u okvirima poslovnog okruženja, koja dosad nisu bila korištena, obzirom na stupanj tehnološkog razvoja, zahtjeva razvoj metodologije. Predložena su temeljna 4 koraka, koja se mogu promatrati kao ograničeni pristup, obzirom da su podložna promjeni, a u skladu s razvojem načina implementacije BYOD-a, na koji može utjecati tehnološki napredak kao i ljudski faktor.

Da bi se ostvario sigurniji način pristupa, s računala koje je izvan mreže poduzeća, potrebno je koristiti mehanizme zaštite osiguranja za udaljeni pristup (Secure Remote Access). Takvi mehanizmi zaštite sastoje se od autentikacije korisnika i šifriranja podataka, prilikom prijave. O okviru



Slika 3
Ograničeni BYOD pristup [8]

Figure 3
Limited BYOD approach [8]

sigurnosti to su temeljni aspekti za uspostavu sigurne veze s krajnjim korisnikom (end-point security). Osim toga, tehnologijama za mrežnu sigurnost i upravljanje identitetima potrebno je dodatno povećati sigurnost unutar BYOD načina poslovanja, kroz slijedećih nekoliko aspekata:

- Prijenos povjerljivih informacija preko enkripcijskog kanala osigurati će maksimalnu zaštitu
- Korištenje javnih cloud servisa i backup servisa sa znantnim oprezom
- Pružiti korisnicima vodič za upotrebu Wifi mreža te definirati razinu dosega poslovne mreže. Mnogi uređaji imaju mogućnost lociranja na daljinu te brisanje svih podataka ili to može biti konfigurirano od strane Mobile Device Management-a, no često se uređaji trebaju prvo registrirati
- Mnogi uređaji bi trebali imati omogućen pristup praćenja uređaja u realnom vremenu
- Treba pripaziti na izvor aplikacije koja se instalira na uređaju
- Ako zaposlenik želi nadzirati njegove radnike mora im dati do zanja da ih se nadzire i za koju svrhu te koje su koristi samog nadziranja

Kad se govori o sigurnosti važno je napomenuti da u okviru upravljanja uređajima, također postoje načini za njezino povećanje. Upravljanje uređajima u okviru BYOD-a može se podijeliti na 3 osnovna aspekta:

- upravljanje mobilnim uređajima (mobile device management - MDM),
- upravljanje mobilnim aplikacijama (mobile application management - MAM)
- upravljanje mobilnim sadržajem (mobile content management - MCM)

Objedinjavanjem ovih triju sustava za upravljanjem, također se povećava sigurnosni sustav koji čini glavnu okosnicu korištenja BYOD-a.

Definiranje sigurnosnih mjera kao i struktura upravljanja uređajima kao vanjskim sudionicima BYOD-a, zatvara se strategija poslovanja, za koju je još potrebno napisati zakone i pravila ponašanja za sve sudionike. To se može definirati u okviru politike sigurnosti kompanije.

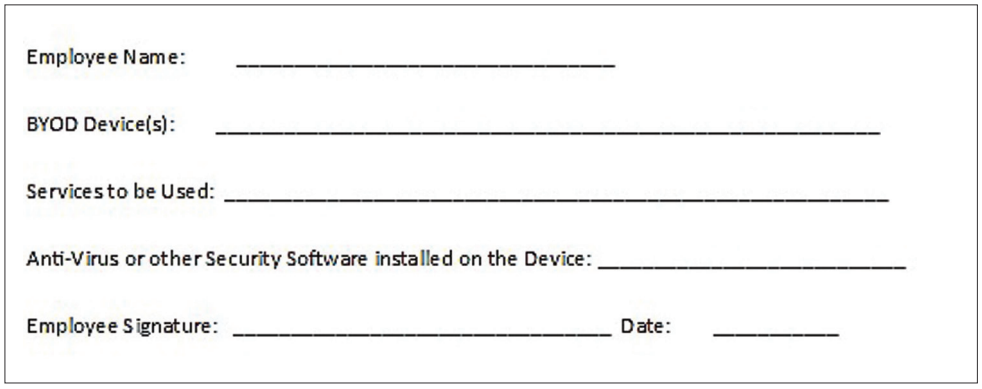
4.2 BYOD politka

4.2 *BYOD policy*

BYOD politka „tjera“ tvrtke da prvo promisle o svim odlukama prije nego uključe i svoje zaposlenike u njih. Pitanja koja se nameću su koje web preglednike smiju zaposlenici koristiti, koji alati pružaju najbolju zaštitu kada je u pitanju veći broj povezanih privatnih uređaja na poslovnu mrežu, koju razinu podrške IT odjel treba pružiti.

Kada organizacija odluči dopustiti korištenje privatnih uređaja (tableta, mobitela, laptopa) zaposlenici se moraju složiti sa uvjetima i pravilima poslovanja koja su namijenjena za spajanje na poslovnu mrežu, a ona uključuje:

a. Korisnik neće spremati ili transformirati osjetljive poslovne informacije na njihove uređaje (osim ako tako nije uređeno)
b. Korisnik će se koristiti lozinkom kako bi zaštitio uređaj
c. Korisnik se slaže da će nastaviti održavanje operativnog sustava i osiguravanje uređaja najnovijim verzijama sigurnosti
d. Korisnik se obvezuje da uređaj neće dijeliti sa drugim članovima obitelji te da će izbrisati informacije koje su se spremile na uređaj prilikom njezina pregledavanja


Employee Name: _____

BYOD Device(s): _____

Services to be Used: _____

Anti-Virus or other Security Software installed on the Device: _____

Employee Signature: _____ Date: _____

Slika 4
Dio ugovora kojeg korisnik BYOD metode potpisuje sa organizacijom [9]

Figure 4
Part of the contract which BYOD employee signed with the company [9]

e. Korisnik se obvezuje imati drugu jaku lozinku za pristup putem PC uređaja
f. Korisnik će imati najnoviji antivirusni program i drugi potreban softver za zašititu.[4]

5. Prednosti i nedostatci BYOD-a

5. *Advantages and disadvantages of BYOD*

BYOD predstavlja zamršenu tanku liniju između posla i igre. Neki od problema koji se javljaju su zloupotrebljavanje (zlonamjerni komentari), prekovremeni rad te problemi privatnosti (rizik od strane korisnika da nešto izbriše) te sigurno poslovno okruženje (primjerice pisanje poruke tijekom vožnje).

Premda se isto može desiti bez obzira na činjenicu tko je vlasnik opreme, veću težinu BYOD oprema dobiva kroz naglasak na vlasništvu. Posebno ako se odnosi vlasnika i kompanije ne definiraju jednoznačno.

5.1 Prednosti

5.1 *Advantages*

Neke od prednosti su poboljšanje zaposlenikovog zadovoljstva, povećana poslovna učinkovitost i povećana fleksibilnost što pokazuju istraživanja. [12] Što se tiče sigurnosti kontrolor uređaja ima mogućnost specificirati koje se točno uređaje smije koristiti, koja vrsta podataka se smije pohraniti na uređajima i koji tip podataka se ne smije pohraniti na uređaj. BYOD politika i implementacija može dovesti do poboljšanja tj. odvajanja svakog procesa zasebno. Primjerice, organizacija može poboljšati/restrukturirati specifični pristup internetskim stranicama sa poslovne mreže kako bi zaustavili protok povjerljivih informacija ili zaustavili nepravilno korištenje poslovne mreže. Postoji i mogućnost za uspostavljanjem Wifi poslovne mreže na koju bi se mogli samo zaposlenici spajati.

U cilju postizanja kvalitetnijeg upravljanja BYOD pristupa poslovanju, pitanjima poput: koje informacije bi smjele biti transferirane putem privatnih uređaja, a koje bi trebale imati ograničen pristup, stvaraju se temeljni preduvjeti za cjelokupni sustav. Također treba razmatrati i sam utjecaj BYOD-a na cijelu organizaciju. Osim toga, jasno definirana BYOD politika, podrazumijeva i to da zaposlenici razumiju svoju odgovornost, prilikom spajanja na poslovnu mrežu, putem privatnih uređaja.

5.2 Nedostaci

5.2 *Disadvantages*

Premda je BYOD općenitog karaktera, najčešće se veže uz IT. Ključna stavka BYOD načina poslovanja je ta da zaposlenici sami održavaju i nadziru rad uređaja. Stoga, briga o organizacijskim podacima dolazi na prvo mjesto. Onaj koji nadzire rad uređaja mora voditi brigu o tome koju vrstu informacije sadrži, gdje bi one mogle biti pohranjene, kako se transformiraju, otkriti potencijalno „curenje“ informacija, povezanost između poslovnog i osobnog korištenja, doseg sigurnosti pojedinog uređaja te o načinima kako se odnositi u pojedinim situacijama, primjerice, što napraviti ako zaposlenik napusti svoj trenutni posao te kako se nositi sa gubitkom, krađom, padom uređaja.

6. Zaključak

6. Conclusion

Projektni (pa čak i IT) menadžment, u smislu upravljanja uređajima zahtjeva veliku brigu unutar BYOD-a. Sigurnosni rizici su veliki, obzirom da se neki od njih ne mogu zatvoriti tehnologijama za mrežnu sigurnost te je ljudski faktor itekako važan čimbenik u očuvanju sigurnosti.

Pretjerana kompleksnost i nedostatak skalabilnosti veliki su izazovi za organizacije. No svi navedeni čimbenici, stvaraju izazov IT profesionalcima, koji već sada, većim stupnjem automatizacije omogućavaju lakši prelazak na BYOD.

BYOD(BYOA/BYOT/BYOS) način poslovanja, očekivano otvara mnoge nove mogućnosti vezane za upotrebu vlastitih resursa u poslovnom okruženju. U tom smislu, BYOS (Bring Your Own Software) koji također donosi financijske uštede za organizacije i veću slobodu zaposlenicima, otvoriti će mnogo više pitanja i stvoriti jednu potpuno novu paradigmu u IT sektoru. Navedeni poslovni pristupi svakako utječu na ljudski potencijal koji raste u skladu s razvojem tehnologije, a u kojem smjeru će se kretati, ostaje nam za promatranje.

7. Reference

7. *References*

[1] http://www.crowdresearchpartners.com/wpcontent/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf, preuzeto 7.11.2016

[2] https://www.whitehouse.gov/digitalgov/bring-your-own-device#key-considerations, preuzeto. 7.11.2016

[3] http://www.bitglass.com/press-releases/byod-trends-report, preuzeto. 7.11.2016

[4] Keyes,J. Bring Your Own Devices (BYOD) - Survival Guide, Auerbach Publications, ISBN 9781466565036 - CAT# K16077, 2013

[5] Keyes,J., BYOD for Healthcare, Auerbach Publications, ISBN 9781482219814 - CAT# K22173, 2014

[6] Juran,J.M., A. Blanton Godfrey,A. B., Juran's Quality Handbook, McGraw Hill, ISBN-13: 978-0070340039, 1998

[7] Siedel,G.J., Siedel,J.V., Employers and the Law: 2013-14 Anthology of Best Articles, Van Rye Publishing, 2014

[8] Provisioning Corporate Devices http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html, 7.11.2016., Cisco Systems, Inc.

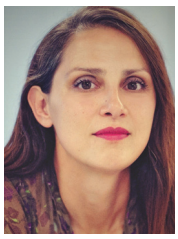
[9] Mobile Information Technology Device Policy https://www.whitehouse.gov/digitalgov/bring-your-own-device#sample2, 7.11.2016., Digital Goverment, the White House President Barack Obama,

[10] Components involved in the deployment https://supportforums.cisco.com/blog/12276831/tech-talk-deploying-cisco-secure-bring-your-own-device-byod-solution, preuzeto 7.11.2016

[11] Using Balanced Scorecard To Measure BYOD Effectivenesshttp://www.ittoday.info/ITPerformance Improvement/ Articles/2 014-07Keyes1.html, 7.11.2016., Taylor & Francis LLC,

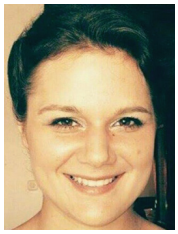
[12] http://tyntec.com/sites/default/files/uploads/tyntec-byod-summary-20150709.pdf, preuzeto 7.11.2016.

AUTORI · *AUTHORS*



Dijana Liverić

Dijana Liverić - asistent na Poslovnom odjelu za Informatiku te na odjelu Telematike, na Veleučilištu u Rijeci, u posljednje 3 godine. Magistra pedagogije i magistra edukacije informatike. U dvanaestogodišnjoj praksi radila je na izradi aplikativnih rješenja u području gospodarstva u raznim industrijskim vertikalama. Autor je mnogih modularnih rješenja u ERP sustavima, a pretežno u području financija i ljudskih resursa. Takodjer, autor je i koautor nekolicine znanstvenih i stručnih članaka, prezentiranih na međunarodnim i domaćim skupovima. Područje interesa: izgradnja informacijskih sustava, upravljanje poslovnim procesima putem IT-a



Andrijana Ivančić

Andrijana Ivančić je rođena 22.11.1992. godine u Bjelovaru. Nakon završetka Turističko-ugostiteljske škole u Bjelovaru upisuje preddiplomski studij Informatike na Sveučilištu Jurja Dobrile u Puli, Fakultet ekonomije i turizma „dr. Mijo Mirković“. Tijekom svog boravka u Puli počinje se baviti volontiranjem u udrugama točnije u Centru za mlade Pula u kojem objavljuje svoj prvi članak u časopisu za mlade „3ska“, Volonterskom centru Istre te već 2 godine aktivno volontira u udruzi Start-Up Udruga iz Pule u kojoj sudjeluje na organizaciji različitih konferencija poput „Inspire Me konferencija“, konferencija koja se održava u 5 različitih gradova unutar RH, i projekata poput Regional Case Study, Istrian Tourism Competition i dr. Sudjelovanjem na projektu „Career Booster“ osvojila je i nekoliko prvih mjesta u timskom riješavanju poslovnih slučajeva od strane poduzeća. Uz svoje fakultetske obaveze preostalo vrijeme ispunjava pomaganjem obitelji oko vođenja O.P.G Ivančić u Bjelovaru u sklopu kojeg proizvode i prodaju raznovrsne sadnice cvijeća.

Ivan Pogarčić

Doc.dr.sc. Ivan Pogarčić, profesor visoke škole, radi na Veleučilištu u Rijeci u nastavnom zvanju profesora visoke škole, za kolegije Modeliranje i simulacije, Objektno orijentirane tehnologije, Ekonomika informacijskih sustava i Informacijski sustav računovodstva u okviru stručnog studija informatike. 2005. godine radi na izradi programa Specijalističkog studija informatike kao nastavka postojećeg stručnog studija. Za taj program je Veleučilište u Rijeci dobilo dopusnicu nadležnog Ministarstva za izvođenje. 2006. godine polazi Carnetovu eLearning akademiju, smjer eLearning management uz certifikaciju. Iste godine stječe, nakon položenih ispita, certifikat ispitivača za osnovne i napredne module ECDL programa. Od svibnja 2012. do danas radi na Veleučilište u Rijeci kao profesor više škole te kao docent na Sveučilištu Jurja Dobrile u Puli.
Autor je i koautor stotinjak radova objavljenih i prezentiranih na domaćim i međunarodnim skupovima, te kao poglavlja u knjigama. Područja interesa: eAktivnosti, teorija odlučivanja, objektno orijentirane tehnologije, izgradnja informacijskih sustava, geografski informacijski sustavi, inteligentni transportni sustavi

Korespodencija
pogarcic@veleri.hr