Grzegorz Podgórski

Wydział Zarządzania
Uniwersytet Łódzki

Model BYOD w organizacji

1. Wstęp

BYOD (*bring your own device*) to model pracy, w którym pracownicy wykorzystują swoje prywatne urządzenia mobilne w środowisku pracy i w celach służbowych. Jest to jeden z najbardziej dynamicznie rozwijających się trendów ostatnich lat, który wciąż wzbudza wiele emocji. Jest on mylnie kojarzony z instytucjami silnie zinformatyzowanymi i związanymi tylko z sektorem IT. Obecnie można jednak zaobserwować dynamiczny rozwój tego zjawiska we wszystkich sektorach gospodarki, jak również w administracji publicznej. Cyfryzacja oraz wdrażanie modelu BYOD w administracji publicznej i służbie zdrowia zmusza organizacje do reorganizacji infrastruktury IT. Taki model pracy wymusza całkowitą zmianę podejścia do zarządzania: siecią, urządzeniami przenośnymi, bezpieczeństwem danych oraz samymi pracownikami, dla których wyrażenie „być w pracy" nabiera nowego znaczenia. Konsumeryzacja i model pracy BYOD niosą ze sobą ogromne możliwości zarówno dla pracodawców, jak i dla samych pracowników. Jakie korzyści oraz zagrożenia może więc przynieść model BYOD dla administracji publicznej oraz jak należy się przygotować do korzystania z niego?

2. Model BYOD w Polsce i na świecie

Nieformalna tendencja, jaką był jeszcze niedawno model BYOD, rozwinęła się w swego rodzaju fenomen, postrzegany przez niektórych jako przyszłość IT. Zwolennicy tego modelu pracy uważają go za naturalny etap rozwoju przedsiębiorstwa. Dla pracowników korzystających ze swoich prywatnych mobilnych urządzeń wyrażenie „być w pracy" zyskuje nowy sens. Dla pracodawców oznacza całkowitą zmianę podejścia do sposobu zarządzania siecią, urządzeniami przenośnymi, jak również samymi pracownikami. Informatyzacja, której podlega administracja publiczna, służba zdrowia

oraz sektor edukacyjny, w dużej mierze opierała się na tradycyjnym modelu projektowania infrastruktury IT, który zakłada koncentrację bezpieczeństwa na obrzeżach sieci oraz jawne rozgraniczenie sieci od reszty świata. Zresztą taką samą zasadą kierowały się organizacje komercyjne. W związku z tym taka implementacja w żaden sposób nie radzi sobie ze zjawiskiem BYOD, które zaciera wiele granic. W tych sektorach, gdzie wymiana informacji o stanie zdrowia (HIE's), wirtualizacja, *cloud computing*, e-aplikacje, elektroniczne dzienniki, e-nauczanie, e-podręczniki, BYOD oraz sieci bezprzewodowe stają się rzeczywistością, istnieje bardzo duża potrzeba ponownego przemyślenia i przeprojektowania infrastruktury IT, jak również infrastruktury odpowiadającej za bezpieczeństwo IT. Jeśli dodamy do tego zwiększoną liczbę urządzeń prywatnych (zarówno pracowników, jak i pacjentów, petentów, studentów) korzystających z dostępu do informacji oraz usług wewnątrz organizacji, problem staje się jeszcze bardziej naglący. Również na uczelniach wyższych można zaobserwować aktywne wykorzystanie prywatnych urządzeń w głównej mierze przez nauczycieli akademickich. W mniejszym stopniu zjawisko to oddziałuje na jednostki administracji i dziekanaty. Dzieje się tak głównie ze względu na specjalistyczne oprogramowanie, z którego korzystają takie jednostki, jak również na dostęp w dużej mierze do danych osobowych i zamkniętych systemów (dziekanaty). Funkcjonowanie modelu BYOD w sektorze administracji publicznej i na uczelniach wyższych wynika z niedostatku sprzętu lub z faktu, że sprzęt ten jest przestarzały, nie nadaje się do prowadzenia zajęć czy też uniemożliwia wykorzystanie nowoczesnych technologii. Jak pokazują rozwiązania ze świata, wprowadzenie modelu BYOD w takich instytucjach jak szpitale, muzea oraz inne organizacje z sektora publicznego ma wiele zalet. Za przykład może posłużyć holenderskie muzeum Rijksmuseum, które dzięki temu modelowi i mobilnym aplikacjom pozwala na interaktywne zwiedzanie z wirtualnym przewodnikiem na swoim własnym urządzeniu. Innym przykładem z Norwegii jest kompleks leczniczo-badawczo-uniwersytecki w Trondheim. Cały teren, obejmujący 25 hektarów, stanowił wyzwanie w kontekście sprawnego poruszania się nie tylko dla pacjentów czy studentów, ale także dla samych lekarzy. Rozwiązaniem było wprowadzenie modelu BYOD oraz MazeMap, dzięki którym użytkownicy, wykorzystując swoje własne urządzenia mobilne, mogą sprawnie poruszać się po całym kompleksie. W ciągu 3 pierwszych miesięcy skorzystało z tego rozwiązania ponad 10 tys. pacjentów, studentów i pracowników. Jak widać, model ten ma swoje zastosowanie zarówno w firmach komercyjnych, jak i w sektorach publicznych, służbie zdrowia i edukacji.

Funkcjonowanie modelu BYOD w sektorze publicznym oraz w sektorze komercyjnym nie różni się bardzo pod względem działania, zalet, wad i zagrożeń. Firmy komercyjne ze względu na swoją dynamikę rozwoju szybciej reagują na tego typu zmiany, wprowadzając wszelkie udogodnienia szybciej niż sektor publiczny. Nie

oznacza to jednak, iż sam proces wdrożenia czy też zabezpieczenia przed zagrożeniami różni się zasadniczo.

Z modelu BYOD korzystają głównie młodzi ludzie w przedziale wiekowym 20–29 lat, uważani za reprezentantów generacji Y. Jest to pokolenie, które aktywnie wykorzystując nowinki technologiczne, korzysta z mediów i technologii cyfrowych. Cechuje je również podejście do pracy zgoła inne niż to, które reprezentowały poprzednie pokolenia. Dużą wagę przywiązują do życia prywatnego, oczekując od pracodawcy swobody i elastycznego czasu pracy[1].

Według różnych badań przeprowadzanych na całym świecie, trend BYOD staje się coraz bardziej popularny wśród organizacji, nie tylko tych działających w sferze IT. Jak na razie nie przeprowadzono badań *stricte* odnoszących się do sektora administracji publicznej lub służby zdrowia, jednak i tutaj jesteśmy w stanie zauważyć wzrost wykorzystania urządzeń prywatnych w celach służbowych. W 2012 r. firma Trend Micro przeprowadziła badanie wśród specjalistów z branż IT, z którego wynika, iż prawie 78% firm wprowadziło model BYOD do swoich organizacji[2]. Według badań przeprowadzonych na zlecenie Cisco IBSG Horizon Study także w 2012 r., firm, które akceptują BYOD w formie pozwalającej pracownikom na przyłączanie własnych urządzeń do sieci firmowej, jest 89%[3]. Ciekawe badanie dotyczące również polskiego rynku przeprowadziła w 2013 r. firma Kapsch BusinessCom (wśród m.in. 140 polskich firm w grupie reprezentatywnej znalazło się 23% firm z obszaru ochrona zdrowia i sektor publiczny). Wynika z niego, iż 58% firm oferuje możliwość korzystanie z prywatnych telefonów mobilnych i tabletów do aplikacji IT poza pocztą elektroniczną (w tym tylko 11% wszystkim użytkownikom, a 89% wybranym). Jeśli chodzi o Polskę, dostęp taki zapewniło 37% ankietowanych, co w porównaniu z innymi państwami daje piąty wynik (rysunek 1).

Z badań przeprowadzonych w 2012 r. wśród 3782 osób z 15 krajów świata (w tym Polski) wynika, iż 45% respondentów na świecie oraz 42% w Polsce codziennie korzysta z prywatnych urządzeń mobilnych w celach zawodowych[4]. W przypadku pracowników chęć korzystania z prywatnych urządzeń wiążę się przede wszystkim z możliwością używania własnego urządzenia oraz posiadania stałego dostępu do aplikacji (33%

---

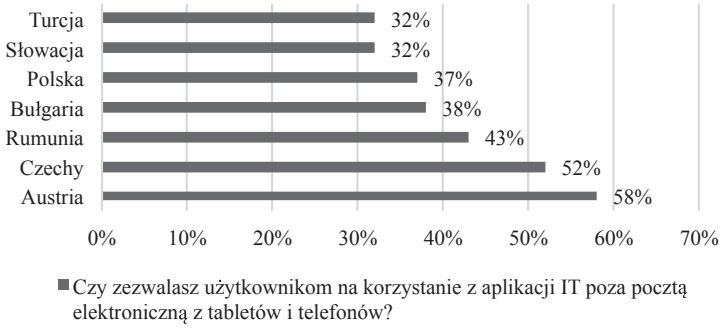
1 J.A. Fazlagić, *Charakterystyka pokolenia Y*, „e-Mentor" 2008, nr 3(25), http://www.e-mentor.edu.pl/artykul/index/numer/25/id/549.

2 *Mobile Consumerization Trends & Perceptions IT Executive and CEO Survey*, Trend Micro, 2012, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf.

3 http://www.cisco.com/web/PL/prasa/news/2012/20120925.html.

4 *2012 IT Security Survey, 'First-Generetion' BYOD Workers Pose Serious Security Challenges*, FortiNet, 2012, http://www.kentconnects.gov.uk/home/Library/byod/2012%20BYOD%20IT%20security%20survey.pdf/at_download/file.

pracowników w Polsce i tyle samo na świecie). Prawie jedna czwarta respondentów uważa, że model BYOD podnosi efektywność ich pracy (24% w Polsce i 26% na świecie).



Rysunek 1. Dostęp do aplikacji IT poza pocztą elektroniczną z prywatnych urządzeń mobilnych typu tablet i telefon

Źródło: opracowanie własne na podstawie: *Branża teleinformatyczna – trendy i wyzwania biznesowe w Austrii, Europie Środkowo-Wschodniej i Turcji*, Kapsch BusinessCom, http://www.outsourcingportal.pl/pl/userfiles/image/raporty/2014/02_lut/25/Branza_Teleinformatyczna_Trendy_i_Wyzwania.pdf.

Wzrost mobilności pracowników i znaczenia mobilnego stylu pracy został także odnotowany w badaniu przeprowadzonym na zlecenie firmy Citrix w 2012 r.[5] Z raportu wynika, że 83% organizacji korzysta z modelu BYOD oraz że w przypadku 73% firm uważa się, że mobilny styl pracy pozwala stworzyć bardziej elastyczne miejsca pracy, a w 53% – że ogranicza to koszty zatrudnienia. Również badania przeprowadzone w drugim kwartale 2014 r. przez firmę FortiNet na polskim rynku dowodzą jednoznacznie, iż firmy jako główną formę korzystania z technologii IT oraz główne wyzwanie związane z bezpieczeństwem IT wskazują mobilność (43%) oraz BYOD (11%)[6]. Firma Cisco w prognozie na lata 2013–2018, zamieszczonej w raporcie *Cisco Mobile Visual Networking Index (VNI)*, przewiduje 4,9 mld użytkowników urządzeń mobilnych (dla porównania – w 2013 r. było ich 4,1 mld). W przypadku Polski zwrot w stronę mobilności i modelu BYOD odnotowano także w raporcie Kapsch BusinessCom, w którym Polska jest w czołówce państw zamierzających wprowadzić model pracy BYOD w ciągu 3 najbliższych lat.

[5] *Workplace of the Future: a global market research report*, Citrix, http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf.

[6] http://www.fortinet.pl/wp-content/uploads/2014/09/Raport-PMR-Fortinet.pdf.

3. Model BYOD – aspekty prawne i licencyjne

W organizacjach stosujących model BYOD szczególnie ważną kwestią są aspekty prawne. W Polsce ustawodawstwo okazuje się nie nadążać za tym dynamicznym zjawiskiem, dlatego trudno w nim szukać konkretnych regulacji prawnych związanych z modelem BYOD. Jedyny przepis odwołujący się do możliwości wykonywania pracy za pomocą własnych narzędzi to art. 67 § 2 kodeksu pracy, odnoszący się do telepracy. Należy także wspomnieć o fakcie, iż to na pracodawcę spada obowiązek dostarczenia narzędzi pracy, o czym wyraźnie mówi art. 94 kodeksu pracy. Dlatego nie może być mowy o narzuceniu takiej formy pracownikom, gdyż stałoby to w sprzeczności z prawem. Można tylko w takim aspekcie mówić o obustronnym porozumieniu, które – jak wskazują wyroki sądów administracyjnych – może być jednak kwestią bardzo kontrowersyjną i kwestionowaną, jako wymuszenie (wyrok NSA z dnia 01.12.2009 r., I OSK 249/09). Należy więc pracownikom stworzyć rzeczywiste warunki, aby mogli dobrowolnie skorzystać z tego modelu pracy, mając jednocześnie alternatywę, z której zawsze mogą skorzystać.

Prywatne urządzenie pracownika wykorzystywane do wypełniania obowiązków służbowych zostaje objęte firmowym systemem bezpieczeństwa. System taki w mniejszym lub większym stopniu bazuje na sprawowaniu kontroli nad takim urządzeniem, tj. kontroli nad konfiguracją, przechowywanymi danymi, listą dozwolonych lub zakazanych aplikacji itp. Brak uregulowań prawnych w tym zakresie wymusza na pracodawcy porozumienie się w tej delikatnej kwestii z pracownikiem. Porozumienie takie powinno być zawierane w formie pisemnej klauzuli w umowie o pracę lub jako stosowny aneks do tejże umowy. Ochrona prawna jest w tym aspekcie szczególnie istotna, gdyż chodzi o prywatne urządzenie pracownika, na którym znajdują się jego prywatne dane. Monitorowanie przez pracodawcę urządzenia należącego do pracownika bez jego zgody może naruszać prawo i narazić pracodawcę na sankcje prawne. W przypadku dostępu przez pracodawcę do urządzenia prywatnego istnieje możliwość dostępu nie tylko do danych firmowych zgromadzonych na urządzeniu, ale również do danych osobowych lub informacji dotyczących prywatności pracownika. Ma to szczególne znaczenie w świetle ustawy o ochronie danych osobowych. W tej sytuacji także brakuje wyraźnych przepisów prawa regulujących ten aspekt. Dlatego tak ważna jest pisemna obustronna klauzula obejmująca czynności wykonywane po stronie pracownika i pracodawcy. W klauzuli powinny znaleźć się takie prawa pracodawcy, jak możliwość:

- stosowania zabezpieczeń informatycznych na urządzeniu pracownika;
- monitorowania urządzenia;
- usuwania danych firmowych z urządzeń pracownika.

Odpowiednich regulacji dotyczących bezpośrednio BYOD trudno szukać także w polskim systemie podatkowym. Trzeba natomiast pamiętać – co jest niezwykle istotne z punktu widzenia pracodawcy, który zezwala na taki model pracy w swojej instytucji – że odpowiednie organy podatkowe mogą określić, iż pracownik wykonuje tzw. nieodpłatne świadczenie podlegające opodatkowaniu. Jeśli podmiot otrzyma nieodpłatne świadczenie lub świadczenie częściowo odpłatne, jest zobowiązany wykazać z tego tytułu przychód podatkowy – zgodnie z art. 12 ust. 1 pkt 2 ustawy o podatku dochodowym od osób prawnych (PDOP) i odpowiednio art. 14 ust. 2 pkt 8 z uwzględnieniem art. 21 ust. 1 pkt 125 ustawy o podatku dochodowym od osób fizycznych (PDOF). W tym miejscu rozważań rodzi się następny problem związany z brakiem definicji nieodpłatnego świadczenia w ustawach podatkowych. Biorąc pod uwagę wyroki sądów w tej kwestii, można uznać, iż nieodpłatnym świadczeniem są te zdarzenia prawne i gospodarcze w działalności osób prawnych, których skutkiem jest niezwiązane z kosztami lub inną formą ekwiwalentu przysporzenie majątku podatnikowi mające konkretny wymiar finansowy[7]. Aby uchronić się przed ustaleniem, że pracodawca w związku z modelem BYOD otrzymuje nieodpłatne świadczenie, zaleca się wprowadzenie do umowy o pracę klauzuli dotyczącej ekwiwalentu pieniężnego za używanie przez pracownika własnego urządzenia w celach służbowych. Odrębnym problemem jest ustalenie wartości takiego ekwiwalentu[8]. Warto pamiętać natomiast o tym, że po stronie pracownika wypłata takiego ekwiwalentu nie będzie rodziła żadnych skutków podatkowych, ponieważ taki ekwiwalent – zgodnie z art. 21 ustawy o PDOF – jest uznawany za wolny od podatku dochodowego.

Należy również wspomnieć o aspektach licencyjnych systemów operacyjnych oraz oprogramowania, którym będą się posługiwać pracownicy w swoich prywatnych urządzeniach. Systemy operacyjne w prywatnych urządzeniach pracowników mogą być w różnej wersji, a co za tym idzie – mogą być wykorzystane do celów komercyjnych bądź nie. Każde oprogramowanie jest licencjonowane w specyficzny sposób, który w zależności od licencji pozwala na użytkowanie jedynie w firmowych urządzeniach lub określa tylko liczbę urządzeń, w których może być zainstalowane. W przypadku, kiedy licencja oprogramowania zezwala jedynie na instalację w urządzeniach należących do pracodawcy, używanie go na prywatnym urządzeniu jest łamaniem prawa licencyjnego. Pracodawca bierze pełną odpowiedzialność za liczbę urządzeń i wykorzystanie licencji oprogramowania, stąd ważnym aspektem jest kontrola instalowanego firmowego oprogramowania w prywatnym urządzeniu wykorzystywanym przez pracownika do

[7] Definicja sformułowana w wyroku Naczelnego Sądu Administracyjnego z 28.01.2000 r. (I SA/Gd 2285/98), a potem przytoczona w wyroku Sądu Najwyższego z 13.06.2002 r. (III RN 106/01).

[8] Wysokość takiego ekwiwalentu powinna zostać ustalona zgodnie z kryteriami wskazanymi w art. 6711 ust. 3 oraz 2377 ust. 3 kodeksu pracy i obejmować takie elementy jak stopień zużycia sprzętu i aktualne ceny rynkowe.

pracy. Zalecanym rozwiązaniem, które coraz częściej jest stosowane, to model aplikacji w chmurze (*cloud applications*), który nie wymaga instalacji w stacjach końcowych, a ich model licencyjny jest pod tym względem bardzo korzystny dla modelu BYOD.

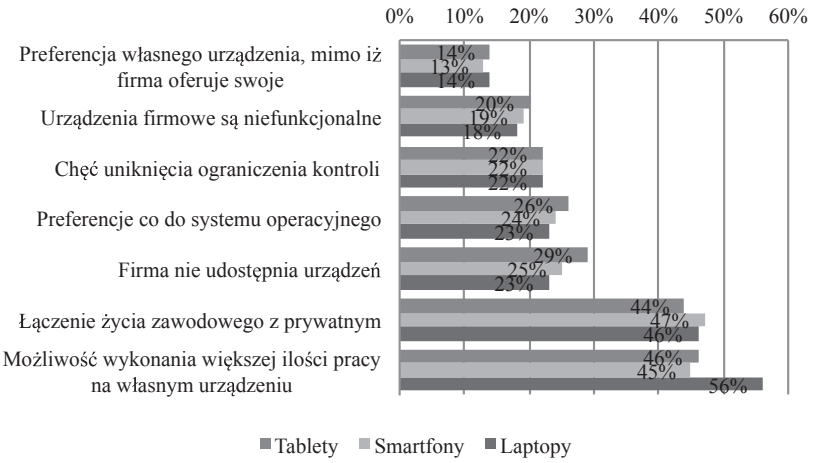
Jak widać, polskie prawo pracy, jak również prawo związane z systemem podatkowym (nie mówiąc już o ochronie danych osobowych) nie jest przygotowane do funkcjonowania tego typu modelu pracy. Dziwi to trochę ze względu na fakt, iż model taki nie jest zupełną nowinką technologiczną, z którą przyszło się nagle zmierzyć ustawodawcom, tylko z roku na rok coraz bardziej rozszerzającym się trendem lub – jak wolą niektórzy – przyszłością wielu organizacji. Takie nieprzygotowanie budzi wiele problemów i powoduje, że w miarę przejrzysty model staje się w wielu miejscach nieczytelny i wrażliwy na wszelkiego rodzaju nadużycia.

4. Wady i zalety modelu BYOD

Jak już wspomniano wcześniej, model BYOD rozwija się bardzo dynamicznie nie tylko w firmach zajmujących się głównie IT, ale w należących do różnych sektorów wszelkich organizacjach – zarówno tych prywatnych, jak i państwowych. Model ten przynosi ze sobą wymierne korzyści dla pracodawcy i samych pracowników. Niestety budzi on także duży niepokój, zwłaszcza jeśli chodzi o ochronę danych, dostęp do infrastruktury IT organizacji, a także obsługę nowych urządzeń, spoczywającą na działach IT.

We wczesnej fazie rozwoju modelu BYOD na świecie główna obawa odnosiła się do spadku produktywności pracowników korzystających z prywatnych urządzeń. Jednak jak na razie badania przeprowadzane na zlecenie takich firm jak Cisco, Trend Micro, Fortinet nie potwierdzają jej zasadności. Wynika to głównie z faktu, iż z takiego modelu pracy korzystają młodzi ludzie (z pokolenia Y), którzy łączą w dużej mierze swoje życie zawodowe z prywatnym. Z badań wynika, iż 80% firm, które wykorzystują model BYOD, odnotowało korzyści finansowe wynikające bezpośrednio z tej decyzji. Aż 65% pracowników biorących udział w badaniu twierdzi, iż taki styl pracy zwiększa ich elastyczność, a 62% z nich wskazuje na wzrost produktywności. Jak pokazują badania firmy Cisco[9], to właśnie możliwość korzystania z własnego urządzenia i wykonywania na nim większej części pracy oraz przenikanie się życia zawodowego i prywatnego jest odnotowywane jako wzrost produktywności (rysunek 2).

[9] J. Loucks, R. Medcalf, L. Buckalew, F. Faria, *Wpływ trendu BYOD na finanse. Korzyści z modelu BYOD dla firm o zasięgu światowym*, http://www.cisco.com/web/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Whitepaper-PL.pdf.



Rysunek 2. Główne powody używanie własnych urządzeń w pracy

Źródło: opracowanie własne na podstawie: J. Loucks, R. Medcalf, L. Buckalew, F. Faria, *Wpływ trendu BYOD na finanse. Korzyści z modelu BYOD dla firm o zasięgu światowym*, http://www.cisco.com/web/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Whitepaper-PL.pdf.

Zastosowanie modelu BYOD w organizacji jest powodem różnych problemów i kwestii formalnych, które muszą być rozwiązane. Najważniejszy jest oczywiście problem zapewnienia bezpieczeństwa. Nie mniej istotne jest zapewnienie pracownikom odpowiedniej pomocy technicznej ze strony działu IT organizacji. W przypadku standardowego modelu pracy to dział IT miał decydujący wpływ na decyzje co do kupowanego sprzętu, systemów operacyjnych i aplikacji na nim się znajdujących. W przypadku modelu BYOD dział IT staje przed nowym wyzwaniem, jakim jest wsparcie wielu systemów operacyjnych, aplikacji, jak również różnorakich modeli i typów urządzeń. Jedynie 22% firm zgadza się na korzystanie ze wszystkich urządzeń, które ma pracownik. Większość (71%) organizacji wprowadzających model BYOD zapewnia wsparcie tylko dla wybranych urządzeń posiadanych przez pracowników[10]. Należy pamiętać o tym, iż decyzja ta przekłada się bezpośrednio nie tylko na koszty związane z obsługą przez dział IT większej liczby urządzeń (szkolenia działu IT, odpowiednie oprogramowanie itp.), ale także na bezpieczeństwo całej organizacji. Na uwagę zasługuje również fakt, iż jedynie 14% kosztów związanych z modelem BYOD ma związek ze sprzętem, co podkreśla wagę wyboru właściwych modeli nadzoru i pomocy technicznej, aby móc zachować kontrolę nad kosztami. Organizacje, które wdrożyły rozwiązania typu BYOD, w większości (58%) zapowiadają wzrost wydatków związanych z IT, a aż 37% nie jest pewnych co do przyszłych kosztów.

[10] http://www.cisco.com/web/PL/prasa/news/2012/20120925.html.

Jeśli zaś chodzi o zalety wykorzystania modelu BYOD w sektorach publicznych, takich jak np. edukacja, to – jak już wspomniano wcześniej – pozwala on na dostęp do najnowszych technologii tam, gdzie odnotowano brak takiego dostępu lub był on bardzo ograniczony. Brak sprzętu to w dalszym ciągu duży problem wielu placówek edukacyjnych (i nie tylko edukacyjnych), zarówno tych na niższym, jak i wyższym poziomie. Pomimo dostępu do wielu form finansowania zakupu sprzętu, oprogramowania itp. tempo zmian w IT wymusza ciągłą modernizację tej infrastruktury, na co wiele instytucji nie może sobie pozwolić. Praca w tym modelu pozwala nauczycielom na wprowadzenie bardziej indywidualnego podejścia do nauczania oraz nowych, bardziej kreatywnych i zinformatyzowanych technik nauczania, które mogą się opierać na dostarczaniu informacji studentom przez różne formy komunikacji, realizowaniu zadań i prowadzeniu laboratoriów oraz mogą być pomocne w przypadku studentów obcojęzycznych. Główny problem dotyczący wykorzystania także prywatnych urządzeń uczniów/studentów w przypadku nowoczesnych technik nauczania polega na dostępności odpowiednich aplikacji oraz utrzymaniu odpowiedniego poziomu bezpieczeństwa po jednej i drugiej stronie.

Nie tylko sektor edukacyjny znajduje zastosowanie dla modelu BYOD. Informatyzacja, wkraczając do sektora ochrony zdrowia i sektora publicznego, wymusza także tu stosowanie nowych technologii. Lekarz pracujący w kilku placówkach zdrowia wyposażony w stosowne aplikacje potrzebuje jedynie połączenia sieciowego, aby w pełni móc korzystać z modelu BYOD. Dynamicznie rozwijająca się telemedycyna także pozwala na wykorzystanie tego modelu przez lekarza w kontakcie z pacjentem, do stawiania diagnozy, przeprowadzania konsultacji czy też omawiania otrzymanych wyników. Przykłady zalet użycia tego modelu w sektorze publicznym można by mnożyć: począwszy od korzystania z poczty elektronicznej we własnym urządzeniu, na szerokim zastosowaniu, wykorzystującym aplikacje, chmury obliczeniowe oraz aplikacje mobilne skończywszy.

Zagrożenia dotyczące modelu pracy BYOD są głównie związane z brakiem pełnej kontroli nad tymi urządzeniami oraz ochroną danych. W prawie każdej organizacji istnieje większa lub mniejsza liczba pracowników mobilnych, którzy posługują się odpowiednimi metodami dostępu do danych i procedurami ochrony samych urządzeń. Problemem jest jednak odpowiednie zarządzanie uwzględniające bezpieczeństwo urządzeń prywatnych. Po pierwsze, ich identyfikacja, po drugie, odpowiednia weryfikacja i – po trzecie – wdrożenie odpowiednich procedur ochrony i dostępu do danych. Nie może także dochodzić do ograniczania praw użytkownika korzystającego z danego urządzenia, co również znacznie utrudnia całą sprawę. Niezwykle istotnym elementem jest tutaj także świadomość samych użytkowników dotycząca bezpieczeństwa pracy i korzystania z takich urządzeń. Poważną kwestią, która szczególnie napawa strachem

pracowników działów IT, jest stworzenie bardzo heterogenicznego środowiska pracy, nad którym bardzo szybko można stracić kontrolę. Konieczne jest wyspecjalizowane oprogramowanie do zarządzania i sprawowania kontroli nad mobilnym środowiskiem. Wprowadzenie takiego oprogramowania powoduje oczywiście powstanie kosztów, które instytucja będzie musiała ponieść w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.

Istnieje wiele zagrożeń zarówno wynikających z wykorzystania samych urządzeń mobilnych w organizacji, jak i związanych z tym, iż są to urządzenia prywatne. Do głównych zagrożeń wynikających z modelu BYOD można zaliczyć:

- utratę danych;
- nieautoryzowany dostęp do infrastruktury IT organizacji;
- kradzież urządzenia mobilnego;
- ryzyko infekcji szkodliwym oprogramowaniem;
- wyciek firmowych danych;
- brak pełnej kontroli nad prywatnymi urządzeniami;
- niezabezpieczone systemy operacyjne;
- brak dostatecznych metod zabezpieczenia mobilnego urządzenia;
- niezaakceptowane aplikacje w urządzeniach prywatnych;
- brak lub niedostateczna ochrona antywirusowa i antyphishingowa.

Nie bez znaczenia jest sam system operacyjny, który obsługuje mobilne urządzenie. W raporcie firmy Trend Micro, która poddała analizie pod względem bezpieczeństwa najważniejsze platformy mobilne, stwierdzono, iż zdecydowanym liderem okazał się system BlackBerry, za nim uplasował się system IOS5, następnie Windows Phone i wreszcie Android. Według danych zawartych w raporcie *BYOD & Mobile Security*, pod względem wsparcia systemów operacyjnych w modelu BYOD system IOS wspierało 76% ankietowanych firm w 2014 r. i 72% w 2013 r. Następnie uplasowały się takie systemy jak Android (69% i 61% odpowiednio w latach 2014 i 2013), Windows (66% i 51% w latach 2014 i 2013) oraz RIM – Blackberry (40% i 48% odpowiednio w latach 2014 i 2013). To ukazuje skalę problemu, z jakim każda organizacja musi się zmierzyć, planując wdrożenie BYOD. Wiele urządzeń, systemów operacyjnych i aplikacji może stać się potencjalną luką w szczelnym systemie ochrony danych w organizacji. Wsparcie dla wielu systemów operacyjnych przekłada się na zwiększenie kosztów związanych z utrzymaniem, wyszkoleniem i wyposażeniem działów IT w organizacji. Wpływa to także nie tylko na koszty, ale także na czas, jaki poświęcają pracownicy działu *helpdesk* na rozwiązywanie problemów użytkowników (co deklaruje aż 14% respondentów, wskazując to jako negatywny skutek wdrożenia narzędzi służących zapewnieniu bezpieczeństwa w przypadku urządzeń mobilnych). Wprowadzenie modelu BYOD w organizacji to wyzwanie szczególnie dla działów IT, które poniosą

największe koszty z tym związane – zarówno finansowe, które pozwolą utrzymać odpowiedni poziom bezpieczeństwa, jak i te związane z pracą własną, szkoleniami i zakupem oprogramowania. Wykorzystanie modelu BYOD w sektorze administracji publicznej, służbie zdrowia i edukacji jest obciążone takimi samymi wadami, zaletami i zagrożeniami jak w przypadku organizacji komercyjnych.

5. Wpływ funkcjonowania modelu BYOD na finanse

Poparcie dla BYOD – jak pokazują statystyki – jest coraz większe. Podstawowe pytanie, jakie zadają sobie przedstawiciele organizacji (oprócz tego odnoszącego się do bezpieczeństwa), dotyczy aspektu finansów. Czy rzeczywiście taki model może przynieść organizacji wymierne korzyści finansowe? Z tym pytaniem spróbowano się zmierzyć m.in. w firmie Cisco, która przeprowadziła wiele badań związanych z utworzeniem modelu finansowego dla organizacji z 18 branż z sześciu krajów. Model ten uwzględnia koszty oraz korzyści wynikające ze stosowania trendu BYOD w ramach dwóch scenariuszy[11]:

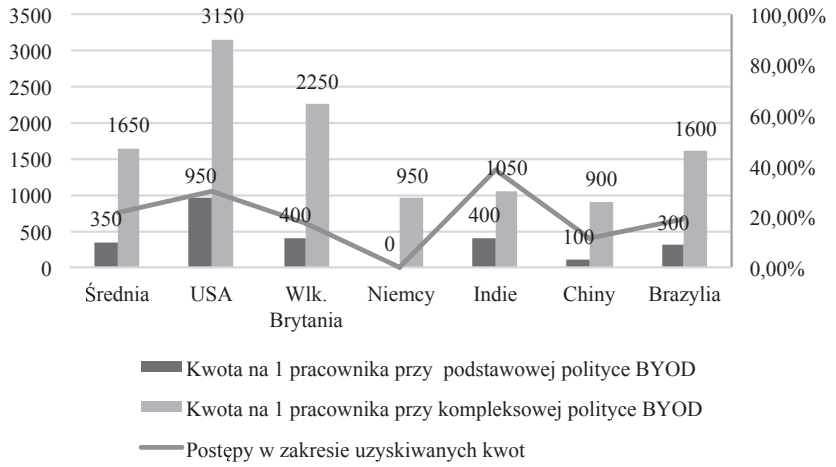
- podstawowe rozwiązanie w zakresie trendu BYOD – stanowi sposób, w jaki rozwiązanie to jest obecnie wdrażane w organizacjach, i obejmuje niekompletną mozaikę funkcji i zasad postępowania;
- pełne rozwiązanie w zakresie trendu BYOD – jest związane z bardziej strategicznym podejściem do trendu BYOD i obejmuje osiem centralnych funkcji wymaganych przez firmy do skutecznego zarządzania trendem BYOD.

Wyniki badań oraz dane wewnętrzne firmy Cisco pozwoliły na przeprowadzenie oceny wpływu prezentowanych zmian na produktywność. Badanie wykazało, iż o wiele większe zyski związane z modelem BYOD odnotowały firmy, które realizowały scenariusz pełny (kompleksowy), a nie podstawowy. Roczne korzyści wynikające z wdrożenia scenariusza podstawowego i pełnego w przeliczeniu na pracownika mobilnego przedstawia rysunek 3.

Dla instytucji nie bez znaczenia są także koszty związane z zakupem urządzeń dla pracowników, a przy modelu BYOD pracownicy sami ponoszą koszty urządzeń, na których pracują. Zazwyczaj takie urządzenia, które są docelowo urządzeniami prywatnymi, mają o wiele lepsze parametry techniczne niż te, jakimi dysponują pracodawcy. Z badań przeprowadzonych wśród pracowników w USA wynika, iż pracownicy decydujący się na model BYOD wydają rocznie prawie 810 USD na prywatne

[11] J. Loucks, R. Medcalf, L. Buckalew, F. Faria, op.cit.

urządzenia mobilne, w przypadku krajów europejskich takich jak Niemcy czy Wielka Brytania wydatki są jeszcze większe i sięgają prawie 970 USD. Część firm decyduje się partycypować w kosztach poniesionych przez pracowników, ale nie jest to regułą. Co najważniejsze, pracownicy nie oczekują tego typu zachowania od pracodawców. Ważnym aspektem korzystania z całkowicie prywatnych urządzeń jest również to, iż pracownicy będą skłonni bardziej dbać o te urządzenia, za które zapłacili swoimi, z wysiłkiem zarobionymi pieniędzmi.



Rysunek 3. Roczne korzyści w przeliczeniu na jednego pracownika mobilnego generowane w przypadku scenariusza podstawowego i pełnego modelu BYOD

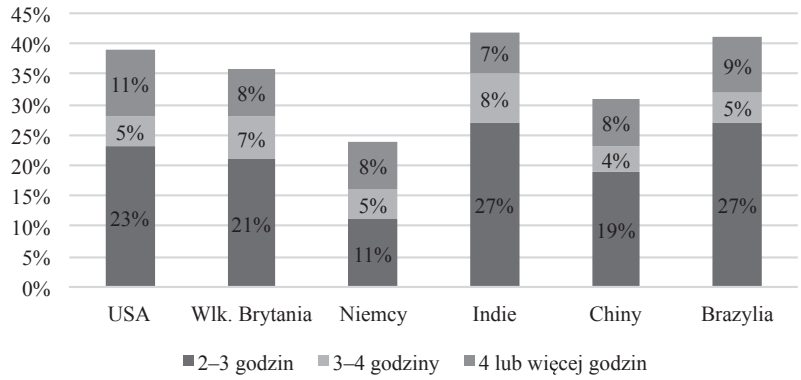
Źródło: opracowanie własne na podstawie: J. Loucks, R. Medcalf, L. Buckalew, F. Faria, *Wpływ trendu BYOD na finanse. Korzyści z modelu BYOD dla firm o zasięgu światowym*, http://www.cisco.com/web/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Whitepaper-PL.pdf.

Z raportów firmy Cisco wynika również, iż odpowiednio wdrożona polityka BYOD w organizacji pozwala pracownikom zaoszczędzić nawet do 81 minut tygodniowo, co może przynieść organizacji oszczędności sięgające nawet 1,6 tys. USD na jednego pracownika. Duża część użytkowników BYOD (aż 36%) staje się „hiperproduktywna", oszczędzając dzięki używaniu do pracy własnych urządzeń co najmniej 2 godziny tygodniowo[12] (rysunek 4).

Wprowadzenie modelu BYOD wiąże się, jak już wcześniej wspomniano, nie tylko z korzyściami finansowymi, ale także z kosztami. Wynikają one z konieczności modernizacji infrastruktury IT, przeprowadzania szkoleń dla pracowników i pracowników

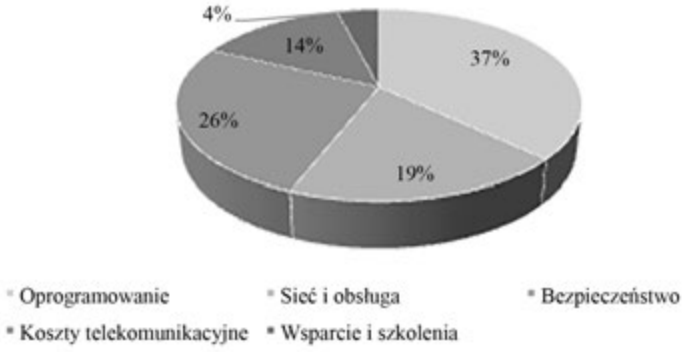
[12] Ibidem.

działów IT oraz zakupu odpowiedniego oprogramowania potrzebnego do wsparcia użytkowników. Szczegółowy rozkład kosztów przedstawia rysunek 5.



Rysunek 4. Odsetek pracowników oszczędzających godziny w tygodniu dzięki wykorzystywaniu własnych urządzań w modelu pracy BYOD

Źródło: opracowanie własne na podstawie: J. Loucks, R. Medcalf, L. Buckalew, F. Faria, *Wpływ trendu BYOD na finanse. Korzyści z modelu BYOD dla firm o zasięgu światowym*, http://www.cisco.com/web/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Whitepaper-PL.pdf.



Rysunek 5. Typowy rozkład kosztów związanych z modelem BYOD

Źródło: opracowanie własne na podstawie: J. Loucks, R. Medcalf, L. Buckalew, F. Faria, *Wpływ trendu BYOD na finanse. Korzyści z modelu BYOD dla firm o zasięgu światowym*, http://www.cisco.com/web/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Whitepaper-PL.pdf.

Wysokie przychody osiągane dzięki wprowadzeniu modelu BYOD dają organizacjom ogromne możliwości. Nie należy jednak zapominać o ścisłej kontroli wydatków przeznaczanych na tego typu rozwiązanie. Jak wykazują badania, tylko w przypadku strategicznego, pełnego wdrożenia BYOD korzyści przewyższają koszty. Dlatego

tak ważne jest świadome zaplanowanie i kompleksowe podejście do problemu. Zagwarantowanie właściwej obsługi rozwiązania BYOD będzie korzystne zarówno dla organizacji, jak i dla pracowników.

6. Bezpieczeństwo informacji związane z modelem BYOD

Utrzymanie odpowiedniego poziomu bezpieczeństwa w przypadku mobilnych użytkowników nie jest zadaniem łatwym, a jeśli chodzi o mobilnych użytkowników pracujących w modelu BYOD, jest to jeszcze bardziej skomplikowane. Szczególnie trudne zadanie czeka organizacje w sektorze publicznym, który w dużej mierze operuje danymi osobowymi. Te organizacje, które już wprowadziły mechanizmy ochrony użytkowników mobilnych, mają ułatwione rozpoczęcie procesu zapewnienia bezpieczeństwa w modelu BYOD. Wdrażanie takiej ochrony powinno być dobrze zaplanowane i stosownie wdrożone oraz – co najważniejsze – powinno być kompleksowe. Bardzo ważnymi elementami takiego wdrożenia dotyczącego ochrony danych i informacji są: aktualizacja firmowej polityki bezpieczeństwa informacji (PBI), szkolenia pracowników i członków działów IT oraz zakup odpowiedniej infrastruktury. Infrastruktura ta jest niezbędnym elementem, który gwarantuje sprawowanie kontroli nad mobilnym i prywatnym środowiskiem pracy funkcjonującym w organizacji. Pozwala ona na identyfikację urządzeń, monitorowanie ich zabezpieczeń, zarządzanie nimi, blokowanie dostępu z danych urządzeń, zdalną modyfikację ustawień dotyczących bezpieczeństwa, wycofywanie urządzenia z użycia, zarządzanie zasobami, zarządzanie aplikacjami oraz wdrażanie korporacyjnej polityki bezpieczeństwa. W związku z tym elementami składowymi, bez których model BYOD nie może funkcjonować, są aplikacje typu MDM (ang. *mobile device management*). Oprogramowanie typu MDM umożliwia kompleksowe zarządzanie oraz monitorowanie mobilnych urządzeń, które mają dostęp do poufnych danych i usług. Coraz częściej aplikacje tego typu są rozszerzane o aplikacje typu MAM (ang. *mobile application management*) oraz MCM (ang. *mobile content management*) lub są częścią pakietu MDM. Zazwyczaj oprogramowanie takie składa się z wielu modułów odpowiadających za poszczególne funkcje, takie jak: identyfikacja urządzenia, przydzielanie przywilejów, zdalne blokowanie skradzionych lub zgubionych urządzeń, aktualizujące, a także alarmujące użytkownika o niebezpieczeństwie lub niedozwolonej aktywności. Zasady działania tego typu oprogramowania są w zależności od producenta oprogramowania różne, natomiast efekt jest taki sam – poprawa bezpieczeństwa i kontrola nad urządzeniami mobilnymi. Oczywiście, to, czy wszystkie moduły tego typu oprogramowania – łącznie z agentowymi instalowanymi

w prywatnych urządzeniach – zostaną zaimplementowane, zależy wyłącznie od firmy. Na pewno żadna firma nie może myśleć o pomyślnym wdrożeniu modelu BYOD bez wcześniejszego zainstalowania aplikacji typu MDM – „nie ma BYOD bez MDM".

Jaki jest więc najważniejszy element procesu zapewnienia bezpiecznego środowiska pracy dla modelu BYOD? Odpowiednio opracowana i wdrożona polityka BYOD wchodząca w skład PBI oraz infrastruktura typu MDM. Odpowiednie procedury, regulaminy i strategię działania wchodzące w skład PBI powinny określać:

- to, jakiego typu urządzenia mogą pojawiać się w sieci organizacji (smartfon, tablet, laptop) oraz na jakich zasadach (czy potrzebna jest zgoda przełożonego itp.);
- to, jakie systemy operacyjne oraz w jakiej wersji są dopuszczane i wspierane przez dział IT;
- to, jakie warunki musi spełniać używane urządzenie (np. możliwość szyfrowania danych, dostępność form łączności, zabezpieczenie dostępu do urządzenia);
- to, jakie oprogramowanie musi się koniecznie w nim znajdować – chodzi głównie o oprogramowanie antywirusowe, antyphishingowe, antyspyware'owe itp., może to być również dedykowane oprogramowanie agentowe;
- listę dozwolonych aplikacji na prywatnych urządzeniach lub ewentualnie listę zakazanych aplikacji na prywatnych urządzeniach;
- procedury opisujące konfigurację, aktualizację oraz konserwację takich elementów urządzenia, jak system operacyjny, system antywirusowy, zapora systemowa, inne aplikacje i mechanizmy zabezpieczające;
- zabezpieczenia fizyczne bądź sprzętowe, które będą chronić dane w przypadku kradzieży urządzenia;
- procedurę permanentnego kasowania danych z urządzenia w przypadku zwolnienia pracownika czy też sprzedaży przez niego urządzenia;
- określenie zasobów, do których będzie konfigurowany dostęp z tychże urządzeń;
- sankcje dyscyplinarne i karne w przypadku naruszenia procedur i/lub zaniedbań ze strony użytkownika.

Nie należy również zapominać o tym, iż większość organizacji ma w swoich zasobach dane osobowe, które powinny podlegać innym kryteriom ochrony. Wiąże się to także z innym podejściem do wprowadzanych zabezpieczeń w przypadku, kiedy użytkownicy w modelu BYOD mają mieć do takich danych dostęp. Wówczas należy ustalić to:

- czy dane osobowe mogą być przetwarzane w urządzeniach mobilnych;
- gdzie dane osobowe mogą być przechowywane i przetwarzane;
- czy dane mogą być przenoszone lub przetwarzane w prywatnych urządzeniach, a jeśli tak, to w jaki sposób oraz ewentualnie jakie warunki muszą być ku temu spełnione;

- jakie jest ryzyko wycieku takich danych z urządzeń prywatnych;
- czy dane osobowe mogą się mieszać z prywatnymi danymi w urządzeniu pracownika;
- jakie powinny być mechanizmy zabezpieczające urządzenie mobilne, jeśli takie dane będzie przechowywać bądź przetwarzać;
- jaka procedura została wdrożona, by pracownik nie mógł przetwarzać danych, gdy nie będzie pracował w organizacji.

W raporcie *BYOD & Mobile Security Report*[13] w odniesieniu do modelu BYOD i bezpieczeństwa znajdują się następujące stwierdzenia:

- głównym aspektem jest utrzymanie mobilności użytkowników (57%), ich satysfakcja (56%) i produktywność (54%);
- główną bolączka instytucji jest utrata danych firmowych lub danych należących do klientów firmy (67%) oraz nieautoryzowany dostęp do danych i systemów w organizacji (57%);
- wymagane jest wprowadzenie dodatkowych nakładów IT na zwiększenie bezpieczeństwa (30%);
- jako jedno z głównych problemów z bezpieczeństwem wyróżnia się ryzyko ochrony haseł (67%), zdalny dostęp do danych (52%) oraz użycie szyfrowania (43%).

Jak widać, ze względu na aspekty bezpieczeństwa wdrożenie BYOD nie jest zadaniem łatwym. Jednak, gdy jest ono odpowiednio zaplanowane, to wraz z dobrze opracowaną polityką bezpieczeństwa informacji pozwalają zapanować nad nowym wyzwaniem. Na pewno wymaga to stworzenia lub zmodyfikowania już istniejących strategii dotyczących infrastruktury IT, jak również całej organizacji. Dużym wyzwaniem może być kontrola przepływu danych w urządzeniach mobilnych. Natomiast dzięki takim rozwiązaniom jak konteneryzacja, zapewniająca oddzielenie danych firmowych od prywatnych, szyfrowanie, podnoszenie poziomu świadomości użytkowników dzięki odbywanym przez nich szkoleniom oraz infrastruktura MDM prawie każda organizacja może wdrożyć model pracy BYOD – choć na pewno nie będzie to proces łatwy ani tani. Jednak zyski wynikające ze zwiększonej produktywności użytkowników, ich zadowolenia oraz korzyści finansowe powinny zrównoważyć lub nawet przewyższyć koszty.

[13] http://scadahacker.com/library/Documents/Threat_Intelligence/InfoSec%20-%20BYOD%20and%20Mobile%20Security%202014.pdf.

7. Podsumowanie

Model pracy BYOD staje się coraz bardziej popularny. Początkowy trend, jakim był model BYOD, staje się nieodzownym krokiem, dzięki któremu organizacje zatrudniają bardziej zadowolonych pracowników, wykazujących się większą produktywnością, a organizacje takie są zdecydowanie bardziej atrakcyjne dla przyszłych pracowników. Model ten stanowi też przyszłość, jeśli chodzi o administrację publiczną, służbę zdrowia i sektor edukacyjny, w których jego zastosowania stają się coraz częstsze. Krok w stronę BYOD należy zrobić świadomie i kompleksowo, wdrażając odpowiednie procedury, mechanizmy, aneksując umowy pracowników oraz wprowadzając oprogramowanie do zarządzania taką infrastrukturą. Przedstawiciele części organizacji – świadomie bądź nie – przybliżyli się do modelu BYOD, przymykając oko na korzystanie z prywatnych urządzeń w pracy, ale nie wiedzieli wówczas, z jakimi zagrożeniami przyjdzie im się zmierzyć i na jakie niebezpieczeństwa się narażają. Jak wykazują badania, odpowiednio wdrożony model BYOD może przynieść organizacji wiele korzyści zarówno finansowych, jak i personalnych. Nie należy jednak zapominać o zagrożeniach z nim związanych, które w przypadku nieodpowiedniego wdrożenia mogą przysporzyć organizacji wiele problemów.

Model BYOD staje się zjawiskiem, które wkracza także do administracji publicznej, służby zdrowia i edukacji. Brak szczegółowych danych nie pozwala określić, w jakim stopniu zjawisko to zagościło w tych sektorach. Jednak patrząc na rozwój i wykorzystanie urządzeń mobilnych, można śmiało stwierdzić, że są one tam stosowane. Jak wspomniano wcześniej, sam proces wdrożenia tego modelu w tych sektorach czy też zagrożenia z nim związane są tożsame z tymi z sektora prywatnego.

Mając na uwadze statystyki i prognozy dotyczące modelu BYOD, można stwierdzić, że wydaje się on naturalnym etapem rozwoju organizacji i przyszłością, na jaką każda organizacja musi się przygotować. Szkoda tylko, że – jak na razie – za szybko rozwijającym się trendem nie nadążają regulacje prawne oraz że ciągle istnieje duża potrzeba pracy nad narzędziami zapewniającymi bezpieczeństwo w tego typu rozwiązaniach.

Bibliografia

2012 IT Security Survey, 'First-Generetion' BYOD Workers Pose Serious Security Challenges, FortiNet, 2012, http://www.kentconnects.gov.uk/home/Library/byod/2012%20BYOD%20IT%20security%20survey.pdf/at_download/file.

Branża teleinformatyczna – trendy i wyzwania biznesowe w Austrii, Europie Środkowo-Wschodniej i Turcji, Kapsch BusinessCom, http://www.outsourcingportal.pl/pl/userfiles/image/raporty/2014/02_lut/25/Branza_Teleinformatyczna_Trendy_i_Wyzwania.pdf.

BYOD&Mobile Security Report, http://scadahacker.com/library/Documents/Threat_Intelligence/InfoSec%20-%20BYOD%20and%20Mobile%20Security%202014.pdf.

Check Point 2013 Security Report, Check Point, http://www.checkpoint.com/campaigns/security-report.

Duże przedsiębiorstwa w Polsce a bezpieczeństwo IT, Fortinet, 2014, http://www.fortinet.pl/wp-content/uploads/2014/09/Raport-PMR-Fortinet.pdf.

Fazlagić J. A., *Charakterystyka pokolenia Y*, „e-Mentor" 2008, nr 3 (25), http://www.e-mentor.edu.pl/artykul/index/numer/25/id/549.

http://www.cisco.com/web/PL/prasa/news/2012/20120925.html.

Karp G., *Bring Your Own Device – jak zorganizować pracę w firmie*, http://www.eversheds.pl/articlesFiles/1171_2013-07_proseed_byod_jak_zorganizowac_prace_w_firmie_gkarp_anierzwicki.pdf.

Loucks J., Medcalf R., Buckalew L., Faria F., *Wpływ trendu BYOD na finanse. Korzyści z modelu BYOD dla firm o zasięgu światowym*, http://www.cisco.com/web/about/ac79/docs/BYOD/Financial-Impact-of-BYOD-Whitepaper-PL.pdf.

Mobile Consumerization Trends & Perceptions IT Executive and CEO Survey, Trend Micro, 2012, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf.

Mobilność, IT-Manager, http://it-manager.pl/wp-content/uploads/Mobilno%C5%9B%C4%87–1.pdf.

Największe zagrożenia dla bezpieczeństwa w Internecie w roku 2014 – głos polskich ekspertów, Raport Fundacji Bezpieczna Cyberprzestrzeń, https://www.cybsecurity.org/wp-content/uploads/2014/01/Raport_FBC_Najwieksze_zagrozenia20141.pdf.

Yoshida H., *Top 10 IT Industry Trends for 2013*, http://www.hds.com/in/news-resource-center/press-releases/2012/in121212.html.

Workplace of the Future: a global market research report, Citrix, http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/workplace-of-the-future-a-global-market-research-report.pdf.

* * *

BYOD model in the organization

Summary

BYOD (Bring Your Own Device) was one of the top ten IT trends in 2013 which have had a significant impact on IT departments in companies and public organizations. The impact of this trend is not limited only to IT departments, as it also spread to other areas of organizations. Like all the new trends it brings with it many benefits for both the organization and its employees, but many hazards and problems, too. The aim of the paper is to discuss the BYOD

phenomenon in Poland and abroad and to indicate the origins of its development, which are due to the needs of the 'Y generation' workers. The article shows the changes in the approach to the management of the institutional network, mobile devices, as well as to employees themselves, for whom the phrase 'be at work' takes on a new meaning. Moreover, the issues related to the threats and challenges associated with the implementation of the BYOD in an institution are discussed. Not without importance are the legal conditions and the elements of the Information Security Policy for organizations that need to be changed. BYOD gives the IT staff, administrators of personal data, and the owners of the organization a headache. Is it just a trend that forces a completely different approach to many areas of the organization or the future reality that is developing very dynamically and for which we have to prepare?

Keywords: BYOD, generation Y, mobile security, mobile work, security, data protection