Konrad SARZYŃSKI
Uniwersytet Ekonomiczny w Krakowie
Wydział Ekonomii i Stosunków Międzynarodowych

BRING YOUR OWN DEVICE (BYOD) – SZANSA CZY ZAGROŻENIE DLA PRZEDSIĘBIORSTWA?

Streszczenie. Popularyzacja koncepcji Bring Your Own Device (BYOD) w ostatnich latach wynika ze wzrostu mobilności pracowników, zmiany ich zwyczajów oraz dalszego poszukiwania przez firmy możliwości optymalizacji kosztów funkcjonowania biur. Celem artykułu jest systematyka rozwiązań wchodzących w skład BYOD, a także przegląd dotychczasowych doświadczeń w jego wdrażaniu. Wykorzystane zostały zarówno opracowania teoretyczne, jak i praktyczne, na bazie których dokonano analizy szans i zagrożeń płynących z polityki BYOD. Praca na własnym sprzęcie ma liczne zalety, m.in. wzrost kreatywności, efektywności i zadowolenia z pracy pracowników. Jednocześnie wdrożenie BYOD może oznaczać dla przedsiębiorstwa wzrost ryzyka utraty danych, a także wzrost kosztów funkcjonowania i tym samym okazać się nieopłacalne.

Słowa kluczowe: Bring Your Own Device, BYOD, konsumeryzacja IT

BRING YOUR OWN DEVICE (BYOD) – A CHANCE OR THREAT FOR THE COMPANY?

Summary. Popularization of the concept of Bring Your Own Device (BYOD) in recent years resulted from the increase of labour mobility, employee's preferences and further search for the cost optimization possibilities. Aim of this article is to systematize the solutions included in the BYOD concept as well as to review existing literature in this field. Articles presenting both theoretical and practical studies were examined, leading to SWOT analysis of BYOD. Working on own hardware has numerous advantages, including creativity, efficiency and job satisfaction increase. On the other hand, implementing BYOD may lead to increased risk of data loss as well as increased operating costs, and thus may not be unprofitable.

Keywords: Bring Your Own Device, BYOD, IT consumerization

1. Wstęp

Bring Your Own Device (BYOD) oznacza po polsku „przynieś swoje urządzenie". Ta prosta w założeniu koncepcja niesie ze sobą bardzo poważne zmiany w funkcjonowaniu przedsiębiorstw, zmieniając relacje między pracownikiem a miejscem pracy. W tradycyjnym modelu to pracodawca odpowiada za zapewnienie niezbędnych narzędzi pracy, co pozwala pracownikowi skupić się na wykonywaniu swoich obowiązków. BYOD przenosi odpowiedzialność za sprzęt na pracownika, co wymaga od niego większego wysiłku związanego z przygotowaniem stanowiska pracy, a także wiedzy koniecznej do zakupu i konserwacji sprzętu we własnym zakresie.

Najważniejsze pytanie podejmowane przez środowiska akademickie i menedżerów dotyczy jednak bezpieczeństwa danych. Praca na prywatnych urządzeniach zwiększa ryzyko wydostania się informacji poza przedsiębiorstwo i jego pracowników, np. przez dostęp do komputera członków rodziny i znajomych pracownika. Poza ryzykiem kradzieży danych występuje również ryzyko zainstalowania (często nieświadomego) przez osoby trzecie niebezpiecznego oprogramowania, które umożliwi zdalną kradzież cennych danych.

W polskiej literaturze tematyka BYOD jest rzadko poruszana, głównie ze względu na małą popularność tego rozwiązania wśród polskich firm lub też małą świadomość mimowolnego wdrażania pewnych elementów tej koncepcji. Na świecie jest to jednak przedmiot licznych badań, zwłaszcza w USA. Skutkuje to dość dobrym rozpoznaniem problemu i licznymi studiami przypadków w anglojęzycznej literaturze naukowej. Można wyróżnić podejście teoretyczne, starające się usystematyzować problematykę BYOD na podstawie dotychczasowych doświadczeń biznesu i nauki, oraz praktyczne, na które składają się liczne opracowania i wywiady z udziałem kierownictwa wyższego szczebla międzynarodowych korporacji. Istnieje także segment badań nad BYOD w szkolnictwie[1], badający skutki korzystania ze swojego sprzętu zarówno w szkołach, jak i na uczelniach wyższych. Nie będzie to jednak przedmiotem analizy ze względu na całkowicie odmienny charakter.

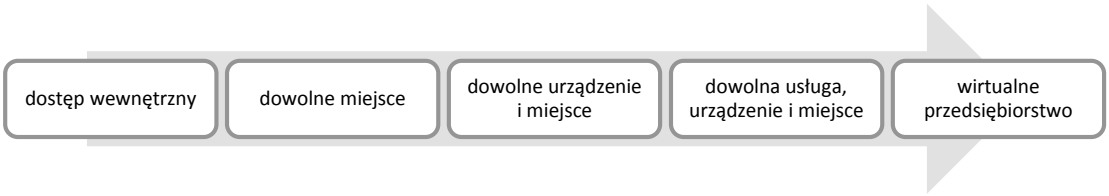
Celem artykułu jest systematyka rozwiązań wchodzących w skład BYOD, a także analiza zalet i wad takiej polityki firmy. Postawiono dwie hipotezy. Pierwsza głosi, że BYOD nie jest tylko tymczasowym trendem, ale wynika z wchodzenia na rynek pracy ludzi przywiązanych do najnowszych technologii, mających odmienne oczekiwania wobec pracy. Druga z kolei wskazuje, że ostateczny bilans wprowadzenia polityki BYOD jest kwestią indywidualną dla każdego przedsiębiorstwa i zależną od specyfiki rynku i istniejącej organizacji pracy, dlatego też nie można jednoznacznie stwierdzić, czy jest to korzystne czy też niekorzystne rozwiązanie.

[1] Zob. np. Dawson P.: Five ways to hack and cheat with bring-your-own-device electronic examinations. „British Journal of Educational Technology", 2015; Hao Y.: Exploring undergraduates' perspectives and flipped learning readiness in their flipped classrooms. „Computers in Human Behavior", No. 59, 2016; Song Y.: "Bring Your Own Device (BYOD)" for seamless science inquiry in a primary school. „Computers and Education", 2014.

Przeanalizowane zostały najnowsze opracowania naukowe oraz wywiady i artykuły przygotowane przez osoby odpowiedzialne za wdrażanie BYOD w międzynarodowych korporacjach lub tworzące rozwiązania wspierające takie rozwiązania. Zebrane materiały posłużyły do analizy szans i zagrożeń płynących z polityki BYOD, na podstawie której zweryfikowano postawione hipotezy.

2. W drodze do wirtualnej firmy

BYOD jest ściśle związane z procesem wirtualizacji przedsiębiorstwa – realizuje postulat dostępu z dowolnego urządzenia do sieci bądź plików firmowych. G. Thomson przywołuje pięciostopniowy proces wirtualizacji przedsiębiorstwa (patrz rys. 1), będący jednocześnie efektem postępującej konsumeryzacji[2] sektora IT[3].



Rys. 1. Proces wirtualizacji przedsiębiorstwa
Fig. 1. Process of business virtualization
Źródło: Opracowanie własne na podstawie Thomson G.: BYOD enabling the chaos. „Network Security", February 2012, p. 7.

Pierwszy stopień to sytuacja klasyczna, w której pracownik musi fizycznie przebywać w siedzibie firmy i korzystać ze sprzętu, na którym znajdują się dane lub aplikacje konieczne do wykonania pracy.

Drugi stopień umożliwia dostęp do danych z dowolnego miejsca przez Internet, jednak z wykorzystaniem firmowego sprzętu. Takie rozwiązanie pozwala kontrolować specyfikację techniczną urządzeń, a także zainstalowane na nich aplikacje, rozwiązuje także potencjalny kłopot z licencjami na aplikacje. Pracownik otrzymuje służbowy sprzęt zdolny do pobierania danych z firmowej sieci.

Trzeci stopień pozwala na dostęp do danych przez Internet z dowolnego urządzenia, także prywatnego. Przejście na ten stopień oznacza konsumeryzację urządzeń (*consumerisation of devices*)[4]. Jest to obecnie potencjalnie osiągalny stopień wirtualizacji dla większości przedsiębiorstw.

[2] Instytut Podstaw Informatyki PAN podaje następującą definicję *konsumeryzacji*: „wprowadzenie urządzeń przeznaczonych na rynek konsumencki, np. iPhone do systemu informatycznego firmy oraz całego jej systemu zarządzania.", zob. www.ipi.edu.pl/aktualnosci-ipi/278-konsumeryzacja, 10.12.2016.
[3] Van Leeuwen D.: Bring your own software. „Network Security", March 2014, p. 12.
[4] Thomson G.: BYOD enabling the chaos. „Network Security", February 2012, p. 5-8.

Czwarty stopień umożliwia także wybór oprogramowania, dlatego można tutaj mówić o konsumeryzacji usług (*consumerisation of services*)[5]. Rozwiązanie to wykorzystuje przede wszystkim coraz powszechniejsze aplikacje webowe, znoszące konieczność instalacji oprogramowania na urządzeniu. Innym wariantem takiego etapu może być również BYOS (*Bring Your Own Software* – przynieś swoje oprogramowanie) czy CYOS (*Choose Your Own Software* – wybierz swoje oprogramowanie)[6]. Jest to stosunkowo nowy trend, który skupia uwagę specjalistów jako rozwinięcie czy też zastąpienie BYOD.

Ostatni stopień, wciąż w znacznej mierze utopijny, to pełna wirtualizacja przedsiębiorstwa, czyli całkowita niezależność od lokalizacji oraz stosowanych urządzeń czy oprogramowania. Pracownik teoretycznie nie musiałby fizycznie pojawiać się w przedsiębiorstwie, mógłby mieszkać nie tylko w innym mieście, ale i kraju. Dotyczyłoby to nie tylko wąskiej grupy pracowników, ale całej firmy, której siedziba miałaby raczej symboliczny charakter, np. w postaci niewielkiego lokalu, nawet przy zatrudnianiu tysięcy pracowników.

W procesie przedstawionym przez G. Thomsona rozwiązania zaliczane do BYOD pojawiają się dopiero w trzecim stopniu, kiedy to możliwa staje się praca nie tylko w dowolnym miejscu, ale i na dowolnym urządzeniu. W tym ujęciu przedsiębiorstwo najpierw umożliwia pracę zdalną na sprzęcie należącym do pracodawcy. Możliwa jest jednak również odmienna ścieżka rowoju, w której nawet na pierwszym etapie (dostępie wewnętrznym) pojawia się możliwość pracy na sprzęcie należącym do pracownika. Jest to najprostsza forma polityki BYOD, która nie zmienia formuły pracy w siedzibie firmy ani infrastruktury technicznej, wprowadza jedynie możliwość pracy na własnym urządzeniu.

Jeżeli przedsiębiorstwo zdecydowałoby się na możliwość korzystania z dowolnego urządzenia w dostępie wewnętrznym, wówczas w przypadku umożliwienia również pracy zdalnej ominęłoby drugi etap, przechodząc od razu do trzeciego, czyli dostępu na dowolnym urządzeniu w dowolnym miejscu.

3. Rozwiązania zaliczane do BYOD

BYOD w intuicyjnym rozumieniu oznacza pracę na własnym laptopie bez specjalnego przygotowania, na plikach przechowywanych na niezabezpieczonych nośnikach. Takie rozwiązanie co prawda nie wymaga praktycznie żadnego działania ze strony pracodawcy, jest jednak skrajnie niebezpieczne i może się sprawdzić jedynie w przypadku pracowników niemających dostępu do wrażliwych danych.

[5] Ibidem.
[6] Zob. np. Van Leeuwen D.: op.cit.

W praktyce w ramach BYOD może funkcjonować przynajmniej kilka rozwiązań, różniących się miejscem przechowywania danych i aplikacji oraz skomplikowaniem wdrożenia. Jako skrajne można podać rozwiązania, w których wszystkie dane i operacje na nich odbywają się poza sprzętem pracownika na serwerach firmy oraz takie, gdzie dane, jak i aplikacje znajdują się na dysku urządzenia, które wykonuje również wszystkie operacje. Wybór odpowiedniego wariantu powinien być ściśle uzależniony od wymagań sprzętowych wykonywanych operacji, a także specyfiki miejsca pracy i dostępności urządzeń.

Osadzenie większości zasobów i operacji po stronie firmy w ramach takich rozwiązań, jak wirtualny pulpit, *session virtualization* czy aplikacja internetowa zmniejsza wymagania sprzętowe po stronie pracowników (bardzo istotne w przypadku wykonywania skomplikowanych obliczeń) oraz zmniejsza ryzyko dostępu przez osoby trzecie (żadne pliki z danymi czy aplikacje nie znajdują się fizycznie na sprzęcie pracownika). Istnieje również mniejsze ryzyko niekompatybilności aplikacji z oprogramowaniem pracowników – do pracy wystarczy najczęściej standardowa przeglądarka internetowa. Z drugiej jednak strony takie rozwiązanie wymaga rozbudowania firmowych serwerów oraz wymusza stałe i stabilne połączenie z Internetem[7], co może być w Polsce problemem w przypadku pracy w terenie, poza terenem zabudowanym (praca w obrębie miast w obliczu coraz powszechniejszego zasięgu sieci LTE staje się coraz łatwiejsza).

Najbardziej niezależne rozwiązania, czyli aplikacje natywne i maszyny wirtualne są instalowane bezpośrednio na sprzęcie pracownika, co albo całkowicie eliminuje konieczność połączenia z Internetem, albo ogranicza ją do okresowych niewielkich transferów danych, a także ułatwia konfigurację firmowych serwerów. Dodatkowo użytkownik jest przyzwyczajony do swojego urządzenia i jest w stanie wykorzystać je w efektywniejszy sposób[8]. Zwiększa to jednak wymagania sprzętowe i może uniemożliwiać pracę na starszych lub słabszych (i jednocześnie tańszych) urządzeniach. Rozwiązania te mogą być także potencjalnie bardziej niebezpieczne w przypadku utraty lub kradzieży urządzenia. Z reguły możliwe jest wówczas zdalne zablokowanie dostępu lub usunięcie danych z urządzenia, czego użytkownik musi być świadomy. W niektórych przypadkach (wynikających czy to ze specyfiki pracy czy też z zastosowanego oprogramowania) może okazać się konieczne usunięcie wszystkich danych z urządzenia, co będzie skutkowało również utratą wszystkich prywatnych danych, w tym np. kontaktów, zdjęć z wakacji itp.[9]. Najważniejsze informacje o tym zagadnieniu zostały przedstawione na końcu podrozdzialu.

Opisywane powyżej rozwiązania, jak i większość rozważań na temat BYOD dotyczy przede wszystkim dużych przedsiębiorstw, zwłaszcza korporacji zatrudniających przynajmniej

[7] Disterer G., Kleiner C.: BYOD Bring Your Own Device. „Procedia Technology", No. 9, 2013, p. 51.
[8] Ibidem.
[9] Dhingra M.: Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). „Procedia Computer Science", Vol. 78, 2016, p. 182-183.

kilka tysięcy pracowników, gdzie ze względu na skalę przedsięwzięcia możliwe jest wprowadzenie zaawansowanych systemów informatycznych, a własny dział IT jest w stanie aktywnie zaangażować się w proces zmian. Pozostaje pytanie o dostępność i zasadność wprowadzania polityki BYOD dla małych przedsiębiorstw, zatrudniających kilku-kilkunastu pracowników.

W wielu przypadkach próby wdrażania polityki BYOD mogą być nieuzasadnione ze względu na specyfikę stanowisk pracy – stawiających na fizyczną obecność w siedzibie przedsiębiorstwa oraz brak możliwości odpowiedniego zabezpieczenia danych. Przykładowo, w niewielkich biurach rachunkowych, kancelariach prawnych czy przychodniach medycznych umożliwienie pracy na własnych urządzeniach mogłoby doprowadzić do nieświadomego wycieku bardzo wrażliwych danych.

Z drugiej strony nawet bardzo małe przedsiębiorstwa mogą próbować wdrożyć rozwiązania z zakresu BYOD w stosunkowo bezpieczny sposób. Przykładem mogą tu być redakcje lokalnych mediów czy stanowiska grafików komputerowych. Taka praca cechuje się wymogiem dużej kreatywności oraz często nieregularnym trybem pracy, a możliwość pracy na własnym urządzeniu może poprawić efektywność dzięki lepszemu dopasowaniu do potrzeb.

Nieodzownym elementem wdrażania BYOD jest system zarządzania urządzeniami mobilnymi (MDM – *Mobile Device Management*), umożliwiający przynajmniej podstawową kontrolę wszystkich urządzeń, także smartfonów czy tabletów. Jak jednak wskazuje H. Romer, MDM ma dwie poważne wady – skupienie się na całych urządzeniach oraz korzystanie z list dopuszczonych urządzeń[10]. Pierwsza wada jest szczególnie niekorzystna, gdy pliki prywatne są wymieszane z plikami służbowymi, np. na telefonie, gdzie dane o sprzedaży czy baza klientów jest w jednym folderze z listą zakupów, a na urządzeniu są również zdjęcia z wakacji i inne prywatne zasoby. Korzystanie z zamkniętej listy dopuszczonych do sieci/plików urządzeń jest rozwiązaniem anachronicznym ze względu na ilość używanych urządzeń i tempo ich rotacji – dział IT jest wówczas niepotrzebnie obciążony niekończącą się listą próśb o wyrejestrowanie starych i zarejestrowanie nowych urządzeń[11].

Odpowiedzią na zmieniające się warunki pracy jest system zdalnego zarządzania treścią (MCM – *Mobile Content Management*), skupiający się na konkretnych plikach, bez względu na urządzenie, na którym są używane. Ich działanie można obrazowo porównać do szuflady czy skrzyni – przechowywane są w niej firmowe pliki, odizolowane od pozostałych zasobów urządzenia, a przez to zabezpieczone przed infekcją oraz z możliwością łatwego zablokowania dostępu w przypadku utraty urządzenia[12].

Wdrożenie takich systemów może się jednak okazać bardzo drogie, zwłaszcza w przypadku przedsiębiorstw niemających nowoczesnej infrastruktury informatycznej. To z kolei

[10] Romer H.: Best practices for BYOD security. „Computer Fraud and Security", 2014, p. 14.
[11] Ibidem.
[12] Ibidem.

może zaważyć na opłacalności wdrażania BYOD, a w skrajnym przypadku nawet poważnie zagrozić sytuacji finansowej przedsiębiorstwa.

4. Dotychczasowe doświadczenia z BYOD

Wdrożenie BYOD w firmie jest trudne, gdyż według F. Andrusa (specjalista od kontroli sieci i CTO w Bradford Networks) konieczna jest zmiana dotychczasowej filozofii funkcjonowania firmy – urządzenia używane w firmowej sieci i mające dostęp do wrażliwych danych były do tej pory skonfigurowane i sprawdzone przez firmowych informatyków lub wynajętą do tego firmę. W przypadku BYOD informatycy mają bardzo mały wpływ na rodzaj używanych urządzeń, przez co zwiększa się potrzeba kontroli ruchu w firmowej sieci[13]. Wiedza o tym, kto ma dostęp do sieci, staje się niewystarczająca. Potrzebna jest również wiedza, kiedy i gdzie taki dostęp miał miejsce[14].

BYOD to także wyzwanie dla infrastruktury sieciowej – należy zerwać z nieaktualnym już, ale obecnym w świadomości wielu menadżerów założeniem, że jeden pracownik równa się jednemu urządzeniu. Badania wykazują, że studenci są w stanie korzystać jednocześnie nawet z 5 urządzeń podłączonych do sieci[15], jedynie w nieznacznym stopniu ograniczając tę liczbę w pracy – średnio do 3,5[16] (za minimum można uznać co najmniej 2 urządzenia[17]). To rodzi poważne konsekwencje i może wymagać przebudowy firmowej sieci, zwłaszcza zwiększenia przepustowości w przestrzeni wspólnej (sale konferencyjne, kawiarnie, bufety itp.), gdzie może znajdować się naraz duża liczba pracowników. Zmiany w infrastrukturze i zwiększenie obciążenia działu IT mogą zadecydować o opłacalności przedsięwzięcia – szacuje się, że jedynie ok. 14% kosztów wdrażania BYOD dotyczy sprzętu[18].

Może się jednak okazać, że przyjęcie polityki BYOD będzie nieuniknione – badania ESET wykazują, że 80% zatrudnionych w amerykańskich firmach pracowników używa prywatnego sprzętu do wykonywania czynności związanych z pracą[19], według Harris przede wszystkim komputerów stacjonarnych (47%) i laptopów (41%), z czego mniej niż połowa jest odpowiednio zabezpieczona[20]. Badania wykazują również, że granica między pracą a sferą prywatną coraz bardziej się zaciera – blisko 2/3 dzisiejszych amerykańskich studentów

[13] Mansfield-Devine S.: Interview: BYOD and the enterprise network. „Computer Fraud and Security", April 2012, p. 15.
[14] Ibidem, p. 16.
[15] Ibidem.
[16] Romer H.: op.cit., p. 13.
[17] Mansfield-Devine S.: op.cit., p. 16.
[18] Podgórski G.: BYOD w organizacji. „Studia Ekonomiczne Regionu Łódzkiego", nr XI, 2013, s. 238.
[19] Morrow B.: BYOD security challenges: Control and protect your most sensitive data. „Network Security", December 2012, p. 5.
[20] Ibidem.

oczekuje od przyszłego pracodawcy dostępu do firmowych danych także z domu czy innego dowolnego miejsca, a 29% z nich byłoby w stanie nawet odrzucić ofertę pracy, jeżeli firma zabraniałaby dostępu do portali społecznościowych w czasie pracy[21]. Korzystanie z własnych urządzeń i wedle własnego upodobania zaczyna być postrzegane przez pracowników nie jako przywilej, ale jako ich prawo[22], zwłaszcza w przedziale wiekowym 20-29 lat, którego przedstawiciele najczęściej pracują w systemie BYOD[23]. Dane te dobitnie pokazują, że BYOD nie jest tylko tymczasowym trendem, ale wynika ze zmieniających się oczekiwań i zwyczajów pracowników, co tym samym potwierdza pierwszą z postawionych hipotez.

Owe przenikanie się sfery prywatnej z zawodową ma także swój wyraz w strukturze plików na urządzeniach, zwłaszcza telefonach i tabletach, gdzie prywatne dane (np. zdjęcia z wakacji czy imprez) są wymieszane z danymi firmowymi, także tymi wrażliwymi czy poufnymi. To z kolei rodzi ryzyko, że przy nieumiejętnie skonfigurowanych ustawieniach kopii zapasowych, dane firmowe mogą być automatycznie przekazywane na serwery takich usług, jak OneDrive, Dropbox czy Dysk Google, wydostając się całkowicie poza kontrolę pracodawcy. Istnieje również ryzyko zainfekowania służbowych plików przez wirusy z prywatnych plików, a następnie przedostanie się złośliwego oprogramowania do sieci firmowej, narażając firmę na straty finansowe i wizerunkowe[24]. W takiej sytuacji kluczem staje się kontrola danych pobieranych, z firmowej sieci i sposobu ich przetwarzania, aby zminimalizować ryzyko utraty danych lub ich wycieku[25]. Zagadnienia związane z zachowaniem przez pracowników bezpieczeństwa w Internecie, zwłaszcza zaś umiejętności wybierania bezpiecznych sieci bezprzewodowych oraz zachowywania ostrożności przy wykonywaniu pracy w miejscach publicznych doczekały się analiz z psychologicznego punktu widzenia. Starają się one wykryć potencjalne zagrożenia, na które najbardziej narażeni są mobilni pracownicy, ale także cechy osobowości, które predysponują do zachowań niebezpiecznych z punktu widzenia pracodawcy[26].

Istotną kwestią jest również współpraca pracowników z działem IT. Ze względu na zaangażowanie pracowników w zakup sprzętu, może się okazać, że wiedzą o nim więcej niż firmowy dział IT[27]. Powinni wówczas być włączani do procesu opracowywania zasad korzystania z firmowej sieci, tak aby nie ograniczała ona ich produktywności. Należy także

[21] Thomson G.: op.cit., p. 6-8.
[22] Leclercq-Vandelannoitte A.: Leaving employees to their own devices: new practices in the workplace. „Journal of Business Strategy", Vol. 36, No. 5, 2015, s. 19.
[23] Podgórski G.: op.cit., s. 234.
[24] Romer H.: op.cit., p. 13.
[25] Morrow B.: op.cit., p. 5.
[26] Zob. np. Jeske D., Briggs P., Coventry L.: Exploring the relationship between impulsivity and decision-making on mobile devices. „Personal and Ubiquitous Computing", Vol. 20, No. 4, 2016, p. 545-557; Grant C.A., Wallace L.M., Spurgeon P.C.: An exploration of the psychological factors affecting remote e-worker's job effectiveness, well-being and work-life balance. „Employee Relations", Vol. 36, No. 5, 2013, p. 527-546.
[27] Mansfield-Devine S.: op.cit., p. 16.

rozróżnić dwie grupy pracowników – chcących używać prywatnych urządzeń *w* pracy oraz *do* pracy[28]. O ile pierwsza grupa szuka raczej rozrywki w czasie pracy pod pozorem wykonywania obowiązków na swoim urządzeniu, o tyle druga grupa powinna zostać w szczególny sposób włączona w proces tworzenia polityki BYOD. Dzięki temu możliwe będzie zwiększenie efektywności pracy na swoim urządzeniu.

Nie ulega wątpliwości, że wszyscy pracownicy powinni zostać przeszkoleni z zakresu bezpieczeństwa danych i podstawowych zasad konfiguracji prywatnego sprzętu[29]. Konieczne jest, by pracownicy nie tylko znali, ale także rozumieli procedury bezpieczeństwa, a także byli świadomi, że nawet jeżeli przynoszą swój sprzęt, to dział IT wciąż jest odpowiedzialny za jego bezpieczeństwo[30]. O skali zagrożenia bezpieczeństwa może świadczyć badanie Elitetele.com, wedle którego aż 21% Brytyjczyków pracujących w formule BYOD używało jednocześnie komputerów do pracy i do oglądania materiałów pornograficznych[31] (w rzeczywistości odsetek ten prawdopodobnie jest większy). Podejmowanie działań potencjalnie niebezpiecznych na sprzęcie, na którym znajdują się firmowe dane, naraża nie tylko pracownika, ale również jego pracodawcę na utratę lub kradzież danych.

Nie jest oczywiste, czy wdrożenie koncepcji BYOD obniży koszty funkcjonowania przedsiębiorstwa. Możliwe, że w niektórych sektorach gospodarki lub przy niektórych rozwiązaniach organizacyjnych koszty związane z przygotowaniem infrastruktury sieciowej i obsługą zróżnicowanych prywatnych urządzeń mogą zniwelować oszczędności płynące z rezygnacji z organizacji stanowisk pracy[32].

W Polsce tematyka BYOD wciąż jest słabo rozpoznana. Polscy pracownicy zostali jednak objęci m.in. badaniem FortiNet w 2012 roku, z którego wynika, że z prywatnych urządzeń w pracy korzysta codziennie 42% z nich (średnia światowa 45%), zaś nigdy ze swoich urządzeń nie korzystało w pracy 15% (średnia światowa 8%)[33]. Zwłaszcza niemal dwukrotnie większy odsetek pracowników niekorzystających z prywatnego sprzętu może świadczyć o pewnym opóźnieniu w rozprzestrzenianiu się najnowszych trendów w polskiej gospodarce, a także o bardziej tradycyjnym modelu pracy, zakładającym wykorzystanie jedynie sprzętu dostarczanego przez pracodawcę. Z kolei według badania Ipsos MORI dla Microsoft „Nowoczesne IT w MŚP" z 2015 roku, aż 54% polskich pracowników otwiera firmowe pliki poza biurem[34].

[28] Ibidem, p. 17.
[29] Morrow B.: op.cit., p. 8.
[30] Thomson G.: op.cit., p. 5.
[31] Zob. Horton R.: Not safe for work. „Computer Fraud and Security", March 2015, p. 18-20.
[32] Leclercq-Vandelannoitte A.: op.cit., p. 20.
[33] Podgórski G.: op.cit., s. 235.
[34] https://news.microsoft.com/pl-pl/2015/01/26/byod-po-polsku/#sm.00007t752617pcz1pmh2bzt14uklx, 17.12.2016.

Nastawienie polskich pracowników do BYOD wydaje się podejrzliwe i raczej negatywne, o czym świadczą wypowiedzi Internautów w dyskusjach na temat BYOD. W skrajnym wypadku na jednym z portali anonimowe wypowiedzi w dość ostry i wulgarny sposób określają takie rozwiązania mianem wyzysku, a także ironicznie proponują wprowadzenie polityki BYOC (*Bring Your Own Chair* – przynieś swoje krzesło) i BYOS (*Bring Your Own Salary* – przynieś swoją wypłatę)[35].

5. Analiza SWOT BYOD

Na podstawie dotychczasowych doświadczeń przedsiębiorstw, a także opracowań teoretycznych można podjąć próbę zestawienia najważniejszych szans i zagrożeń płynących z wdrożenia polityki BYOD w przedsiębiorstwie (patrz tabela 1).

Tabela 1

Analiza szans i zagrożeń związanych z BYOD

szanse	**zagrożenia**
• wzrost kreatywności pracowników • wzrost produktywności pracowników (dopasowanie sprzętu do ich potrzeb) • wzrost mobilności pracowników • szybsza reakcja pracowników na zmienność otoczenia • wzrost zadowolenia pracowników i szansa na zatrudnienie lepszych kandydatów • obniżenie kosztów działalności przedsiębiorstwa (zakup sprzętu, potrzebna przestrzeń biurowa)	• wzrost kosztów działalności przedsiębiorstwa • wzrost obciążenia działu IT • wzrost kosztów oprogramowania (konieczność zapewnienia kompatybilności z wieloma platformami) • spadek kontroli nad pracownikiem • ryzyko dostępu do firmowych danych osób trzecich • ryzyko wycieku wrażliwych danych np. do sieci społecznościowych

Źródło: Opracowanie własne.

Głównym zadaniem kierownictwa firmy jest odpowiedź na pytanie, czy korzyści płynące z wdrożenia BYOD w przedsiębiorstwie będą przewyższały koszty. Jest to zadanie trudne, gdyż części korzyści nie da się łatwo sprowadzić do wartości pieniężnych. Jak na efektywność firmy wpłynie wzrost komfortu pracy pracownika? Czy umożliwienie zakupu sprzętu zgodnego z preferencjami (także w zakresie nieistotnym dla pracodawcy – np. koloru obudowy) wpłynie pozytywnie na produktywność pracownika?

Nie jest też oczywiste, czy kupno sprzętu przez pracowników faktycznie przyczyni się do obniżenia kosztów działalności ze względu na potencjalnie wysokie koszty wdrożenia systemu zarządzania urządzeniami i/lub oprogramowaniem. Jest to kwestia zindywidualizowana i powinna być rozpatrywana oddzielnie dla każdego przedsiębiorstwa, dlatego też w ogólnej analizie koszty działalności zostały wpisane zarówno po stronie szans (możliwe oszczędności wynikające z utrzymania jedynie kluczowej infrastruktury technicznej), jak i zagrożeń (koszty

[35] http://www.chip.pl/news/wydarzenia/statystyka/2015/01/byod-po-polsku, 16.12.2016.

systemu zarządzania i kontroli mogą okazać się wyższe od oszczędności). Może się jednak okazać, że potencjalne korzyści występują w strategicznym dla przedsiębiorstwa obszarze lub wpłyną tak znacznąco na ulepszenie funkcjonowania przedsiębiorstwa, że ryzyko wystąpienia dodatkowych kosztów będzie akceptowalne.

Szansą z punktu widzenia przedsiębiorstwa, ale jednocześnie potencjalnym zagrożeniem dla pracowników jest szybsza reakcja na zachodzące zmiany – od pracownika mającego na prywatnym komputerze lub telefonie dostęp do firmowych danych przełożony może oczekiwać pracy także późnym wieczorem, w czasie weekendów czy urlopu, aby np. jak najszybciej odpowiadać kluczowym klientom, stale monitorować wyniki kampanii marketingowych itp. Kwestie zacierania się różnic między czasem pracy a czasem wolnym i pracą przez całą dobę budzą obawy nie tylko pracowników, ale również naukowców, zwracających na to uwagę przy podnoszeniu tematyki pracy zdalnej[36]. Z drugiej strony mniejsze możliwości kontroli pracowników mogą nie przypaść do gustu właścicielom i menedżerom o tradycyjnych metodach zarządzania, zakładającym konieczność stałego fizycznego nadzoru w czasie pracy.

W mniejszych firmach, w których nie ma działu IT, opracowanie i wdrożenie instrukcji bezpieczeństwa może okazać się niemożliwe ze względu na niedostateczną wiedzę pracowników oraz właścicieli. Niezrozumienie zagrożeń wiążących się z wprowadzanymi zmianami może prowadzić do podejmowania działań zagrażających bezpieczeństwu przedsiębiorstwa.

Ciekawą kwestią jest zapotrzebowanie na przestrzeń biurową – choć znacznie słabiej akcentowane, może to być źródło znacznych oszczędności wraz z wdrożeniem polityki BYOD. Możliwy jest wzrost zatrudnienia przy niezmienionej powierzchni przedsiębiorstwa, a tym samym obniżenie udziału najmu w kosztach działalności. Należy jednak podkreślić, że będzie to miało miejsce jedynie w sytuacji, gdy dzięki polityce BYOD i zwiększonej dzięki temu mobilności pracowników część z nich zacznie wykonywać swoje obowiązki poza miejscem pracy.

Kontrowersyjne mogą być również rozwiązania z zakresu dostępu do danych o aktywności na prywatnych urządzeniach. W jakim stopniu pracodawca ma prawo kontrolować aktywność na prywatnym urządzeniu? Czy powinien mieć prawo do zdalnego usunięcia danych bądź zablokowania urządzenia w przypadku jego utraty, lub podejrzenia o dostęp osób trzecich? Co z utraconymi w ten sposób prywatnymi danymi? Pytania te wciąż są pozostawione bez

[36] Zob. np. Cousins K., Robey D.: Managing work-life boundaries with mobile technologies. „Information Technology & People", Vol. 28, No. 1, 2015, p. 34-71; Hovav A., Putri F.F.: This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. „Pervasive and Mobile Computing", Vol. 32, 2016, p. 35-49; Wright K.B. et al.: Work-Related Communication Technology Use Outside of Regular Work Hours and Work Life Conflict: The Influence of Communication Technologies on Perceived Work Life Conflict, Burnout, Job Satisfaction and Turnover Intentions. „Management Communication Quarterly", Vol. 28, No. 4, 2014, p. 507-530.

jasnej odpowiedzi, a rozwiązanie tych dylematów będzie indywidualne dla każdej firmy, w zależności od wrażliwości jej danych oraz formy pracy pracowników.

W kontekście Polski należy zwrócić uwagę na nieuregulowany stan prawny rozwiązań z zakresu BYOD i możliwe tego konsekwencje. Brakuje przystosowania np. zapisów licencyjnych do sytuacji, w której kupującym jest firma, natomiast licencja zostaje wykorzystana na sprzęcie należącym do osoby prywatnej[37].

Z zaprezentowanej analizy szans i zagrożeń jasno wynika, że ostateczny bilans wprowadzenia polityki BYOD jest kwestią indywidualną dla każdego przedsiębiorstwa i zależną od specyfiki rynku i istniejącej organizacji pracy, dlatego też nie można jednoznacznie stwierdzić, czy jest to korzystne czy też niekorzystne rozwiązanie. Postawiona we wstępie hipoteza została tym samym zweryfikowana pozytywnie.

6. Podsumowanie

Celem artykułu było usystematyzowanie rozwiązań wchodzących w skład BYOD, a także analiza zalet i wad takiej polityki firmy. Postawione zostały dwie hipotezy – o zmianach oczekiwań pracowników jako przyczynie popularyzacji polityki BYOD oraz o trudnościach z jednoznacznym określeniem, czy trend ten jest korzystny czy niekorzystny dla przedsiębiorstw, a ostateczna ocena zależy od indywidualnych uwarunkowań. Obie hipotezy zostały zweryfikowane pozytywnie w wyniku przeglądu literatury oraz wykonanej analizy SWOT.

Wprowadzenie przez firmę polityki BYOD może przynieść korzyści zarówno w postaci wzrostu efektywności i kreatywności pracowników, jak i obniżenia kosztów funkcjonowania przedsiębiorstwa. Może się jednak okazać, że w przypadku firm posiadających wrażliwe dane, określoną specyfikę pracy lub zatrudniających niewielką ilość pracowników, wdrożenie polityki BYOD przyniosłoby straty w wyniku czy to utraty kontroli nad ważnymi danymi czy też wzrostu kosztów przy jednoczesnym braku wzrostu efektywności pracowników. Dlatego też decyzja powinna być w każdym przypadku poprzedzona analizą zarówno istniejącej struktury przedsiębiorstwa, jak i otoczenia, w jakim działa.

Popularność BYOD nie wynika z wykreowanej mody, ale z wchodzenia na rynek pracy młodych ludzi, przywiązanych do najnowszych technologii, a jednocześnie zupełnie nieprzywiązanych do jednego miejsca. Obserwowane już na uczelniach wyższych przyzwyczajenia do korzystania z kilku urządzeń oraz ciągła praca *online* przenoszone są do miejsca pracy.

Najwięcej obaw w przypadku BYOD związanych jest z bezpieczeństwem danych, w tym zwłaszcza ryzykiem dostępu do nich osób trzecich poza siedzibą przedsiębiorstwa. Istnieje jednak wiele sposobów ograniczania takiego ryzyka, od podstawowych w postaci

[37] Podgórski G.: op.cit., p. 241.

przeszkolenia pracowników z zasad bezpiecznego korzystania z Internetu czy stworzenia bezpiecznych procedur dostępu do danych aż po wdrożenie skomplikowanych (i często kosztownych) systemów kontroli urządzeń lub danych.

Zagadnienia z zakresu wirtualizacji przedsiębiorstw (czego szczególną formą jest wprowadzenie polityki BYOD) są tematem niezwykle perspektywicznym ze względu na rosnącą rolę Internetu i coraz większą dostępność zaawansowanych usług sieciowych. Procesy te wciąż są słabo rozpoznane w warunkach polskiej gospodarki, dlatego też konieczne jest podjęcie badań diagnozujacych przemiany polskich przedsiębiorstw w tym zakresie. Przyniesie to również korzyści samym przedsiębiorcom przez zwiększenie wiedzy na temat innowacyjnych metod zarządzania z wykorzystaniem nowoczesnych technologii. Uwaga badaczy nie powinna się jednak skupiać jedynie na największych przedsiębiorstwach, ale również obejmować te małe i mikro, które także mogą zyskać na wprowadzeniu innowacyjnych rozwiązań z zakresu zarządzania.

Bibliografia

1. Cousins K., Robey D.: Managing work-life boundaries with mobile technologies. „Information Technology & People", Vol. 28, No. 1, 2015.
2. Dawson P.: Five ways to hack and cheat with bring-your-own-device electronic examinations. „British Journal of Educational Technology", 2015.
3. Dhingra M.: Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). „Procedia Computer Science", Vol. 78, 2016.
4. Disterer G., Kleiner C.: BYOD Bring Your Own Device. „Procedia Technology", No. 9, 2013.
5. Grant C., Wallace L.M., Spurgeon P.C.: An exploration of the psychological factors affecting remote e-worker's job effectiveness, well-being and work-life balance. „Employee Relations", Vol. 36, No. 5, 2013.
6. Hao Y.: Exploring undergraduates' perspectives and flipped learning readiness in their flipped classrooms. „Computers in Human Behavior", No. 59, 2016.
7. Horton R.: Not safe for work, „Computer Fraud and Security", March, 2015.
8. Hovav A., Putri F.F.: This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, „Pervasive and Mobile Computing", Vol. 32, 2016.
9. Jeske D., Briggs P., Coventry L.: Exploring the relationship between impulsivity and decision-making on mobile devices, „Personal and Ubiquitous Computing", Vol. 20, No. 4, 2016.
10. Leclercq-Vandelannoitte A.: Leaving employees to their own devices: new practices in the workplace. „Journal of Business Strategy", Vol. 36, No. 5, 2015.

11. Van Leeuwen D.: Bring your own software. „Network Security", March 2014.
12. Mansfield-Devine S.: Interview: BYOD and the enterprise network. „Computer Fraud and Security", April 2012.
13. Morrow B.: BYOD security challenges: Control and protect your most sensitive data. „Network Security", December 2012.
14. Podgórski G.: BYOD w organizacji. „Studia Ekonomiczne Regionu Łódzkiego", nr XI, 2013.
15. Romer H.: Best practices for BYOD security. „Computer Fraud and Security", 2014.
16. Song Y.: "Bring Your Own Device (BYOD)" for seamless science inquiry in a primary school. „Computers and Education", No. 74, 2014.
17. Thomson G.: BYOD enabling the chaos. „Network Security", February 2012.
18. Wright K.B., Abendschein B., Wombacher K. et. al.: Work-Related Communication Technology Use Outside of Regular Work Hours and Work Life Conflict: The Influence of Communication Technologies on Perceived Work Life Conflict, Burnout, Job Satisfaction and Turnover Intentions. „Management Communication Quarterly", Vol. 28, No. 4, 2014.
19. http://www.chip.pl/news/wydarzenia/statystyka/2015/01/byod-po-polsku, 16.12.2016.
20. www.ipi.edu.pl/aktualnosci-ipi/278-konsumeryzacja, 10.12.2016.
21. https://news.microsoft.com/pl-pl/2015/01/26/byod-po-polsku/#sm.00007t7526l7pcz1pmh2bzt14uklx, 17.12.2016.