


A Review of Bring Your Own Device on Security Issues

SAGE Open
April-June 2015: 1–11
© The Author(s) 2015
DOI: 10.1177/2158244015580372
sgo.sagepub.com


Morufu Olalere^{1,2}, Mohd Taufik Abdullah², Ramlan Mahmud², and Azizol Abdullah²

Abstract

Mobile computing has supplanted internet computing because of the proliferation of cloud-based applications and mobile devices (such as smartphones, palmtops, and tablets). As a result of this, workers bring their mobile devices to the workplace and use them for enterprise work. The policy of allowing the employees to work with their own personal mobile devices is called Bring Your Own Devices (BYOD). In this article, we discuss BYOD's background, prevalence, benefits, challenges, and possible security attacks. We then review contributions of academic researchers on BYOD. The Universiti Putra Malaysia online databases (such as IEEE Xplore digital library, Elsevier, Springer, ACM digital library) were used to search for peer-reviewed academic publications and other relevant publications on BYOD. The Google Scholar search engine was also used. Our thorough review shows that security issues comprise the most significant challenge confronting BYOD policy and that very little has been done to tackle this security challenge. It is our hope that this review will provide a theoretical background for future research and enable researchers to identify researchable areas of BYOD.

Keywords

BYOD policy, security, data leakage, malware, distributed denial of services

Modern computing has undergone several notable transitions since its birth in the 1960s, with progress from mainframe computing to minicomputers and then to client-server-driven personal computing (PC). The PC era led the information technology (IT) world to internet computing. Mobile computing has supplanted internet computing because of the proliferation of cloud-based applications and mobile devices (such as smartphones, laptops, palmtops, and tablets). People are able to experience high-quality computing at their palms through cloud-based applications and mobile devices. Workers bring their personal mobile devices to their workplaces. Mobile devices such as smartphones and tablets combine portability and voice and data services to open up a wide variety of potential mobile applications, “anytime and anywhere” (Disterer & Kleiner, 2013). People have started to bring their mobile devices to their workplaces and connect to their company networks to perform their jobs and connect to various social network platforms such as Facebook and BlackBerry Messenger (BBM).

Using personal mobile devices for work has given rise to a trend called “Bring Your Own Devices” or BYOD (Gheorghe & Neuhaus, 2013; Leavitt, 2013; Scarfo, 2012). BYOD programs and policies empower people to choose the best device to get their work done, including personally owned consumer smartphones, tablets, and laptops (Citrix[®], 2013). BYOD is an enterprise IT policy that encourages

employees to use their own devices to access sensitive corporate data at work through the enterprise IT infrastructure (Li, Peng, Huang, & Zou, 2013). Deloitte (2013) defined BYOD as the use of employee-owned devices to access enterprise content and the enterprise network. A BYOD policy not only allows employees access to enterprise data when at the workplace but also allows them to access enterprise data outside the enterprise environment.

In the next sections, we discuss BYOD prevalence, benefits, challenges, and possible security attacks. We then review existing work on BYOD by academic researchers. Our review searches for peer-reviewed academic research publications, white paper/survey publications, and publications by information security experts by using The Universiti Putra Malaysia online databases published in English language (such as IEEE Xplore digital library, Elsevier, Springer, ACM digital library) in the area of information and communication

¹Federal University of Technology, Minna, Nigeria

²Universiti Putra Malaysia, Malaysia

Corresponding Author:

Mohd Taufik Abdullah, Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400, Serdang, Selangor, Malaysia.
Email: taufik@upm.edu.my



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 3.0 License

(<http://www.creativecommons.org/licenses/by/3.0/>) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (<http://www.uk.sagepub.com/aboutus/openaccess.htm>).

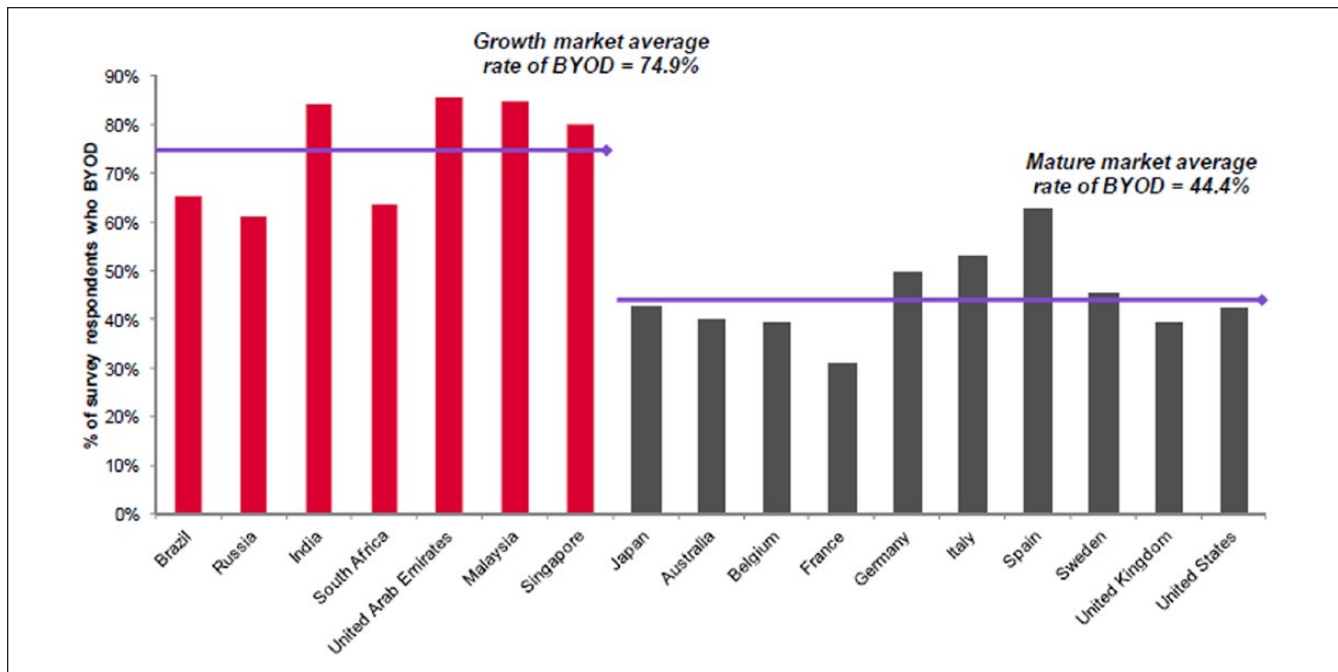


Figure 1. Level of BYOD deployment in both emerging economies and developed economies (Ovum, 2012).

Note. BYOD = Bring Your Own Devices.

technology. To conduct general searches, the Google Scholar search engine was also used.

Prevalence of BYOD

Although BYOD began to surface in 2003, it really took off in 2011 (Leavitt, 2013). Growing pressure to enable and support the use of smartphones, tablets, and other personal devices in the workplace means that ignoring the need to put in place some form of BYOD policy is no longer an option for today's businesses (Millard, 2013). According to a Cisco (2012) survey, BYOD is a global phenomenon. Cisco carried out this survey across eight countries in three regions (Latin America, Asia, and Europe) including both enterprises (1,000 or more employees) and midsize companies (500-999 employees). This survey was an expansion of an earlier conducted survey in the United States that included 600 IT leaders from 18 industries. Ovum's (2012) survey of 3,796 consumers in 17 countries in both emerging economies and developed economies (Figure 1) revealed that 75% of users in countries with emerging high-growth economies such as Malaysia, Singapore, Brazil, India, and Russia use their own mobile devices at work, whereas 44% of workers in countries with developed economies such as the United States, United Kingdom, Sweden, Italy, and Japan use their own mobile devices at work. Gartner (2014) predicted that by 2018, 70% of mobile users will conduct all their work on personal smart devices. These reports show that BYOD has become prevalent in both emerging economies and developed countries.

Benefits and Challenges of BYOD

When employees have the flexibility to choose the best device for their office work, they become more mobile and productive. The business benefits by having access to its employees anytime, anyplace, blurring the work-leisure divide, and it may save costs by having employees purchase their preferred device rather than providing devices out of the corporate budget (Mahesh & Hooter, 2013). AirWatch (2012) and Deloitte (2013) identified some valuable benefits of BYOD. These benefits are management flexibility, cost saving, maximized employee contentment, and simplified IT infrastructure. BYOD also provides a high level of convenience to employees. There are published white papers about BYOD from corporate organizations and information security experts that discuss the benefits of BYOD. More details about the benefits of BYOD can be found in Citrix® (2012, 2013), Deloitte (2013), Disterer and Kleiner (2013), Edwards (2013), EY (2013), Hayes (2012), Kerravala (2012), Miller, Voas, and Hurlburt (2012), and Morrow (2012). However, if both the organizations and their employees are to reap the benefits of BYOD, then they must also worry about the challenges of BYOD policy.

Although businesses are mainly concerned with maintaining security, employees are worried about preserving the convenience they need to work from their mobile devices, as well as the privacy they expect regarding the personal information on the device (AirWatch, 2012). One of the biggest challenges for organizations is that corporate data are being delivered to devices that are not managed by the IT department. This has security implications for data leakage, data theft, and

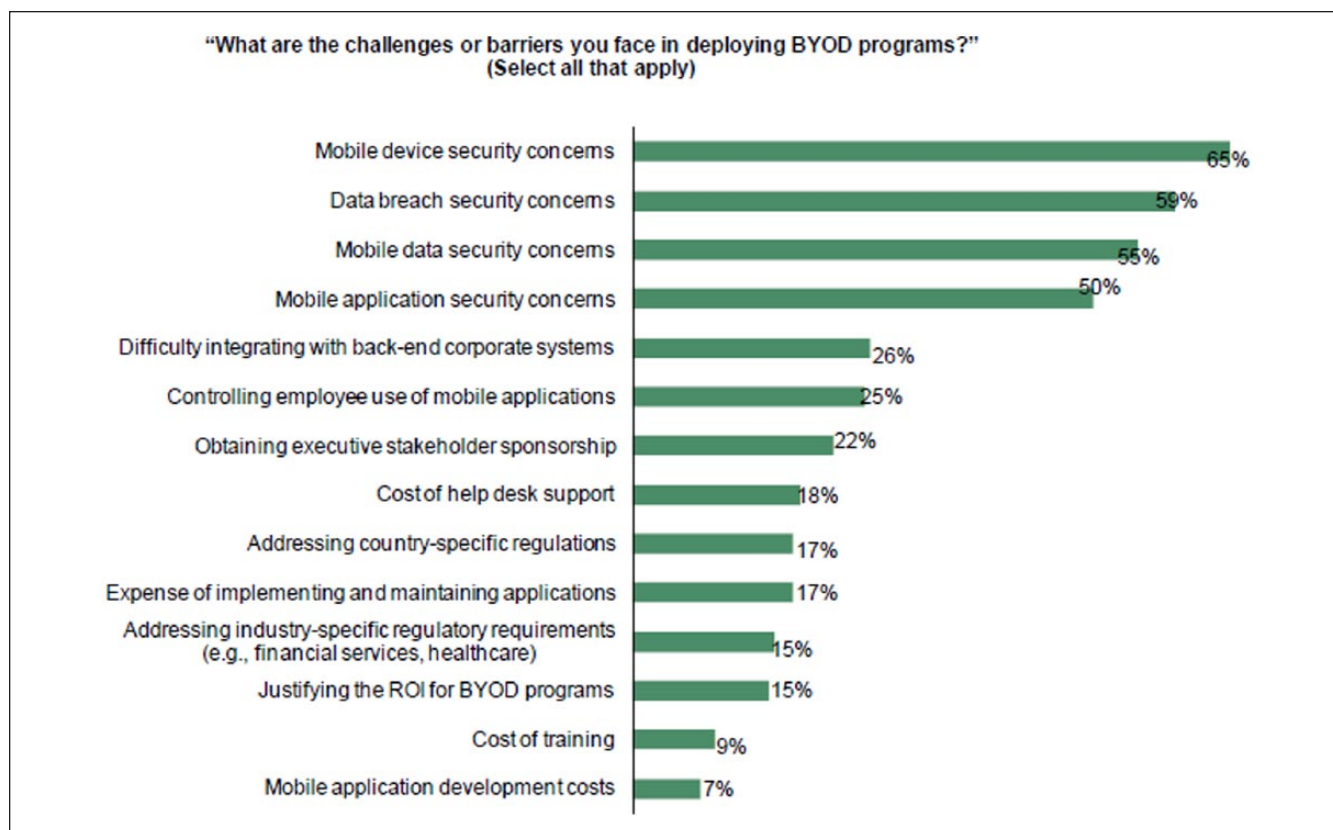


Figure 2. BYOD challenges with security concerns at the top (Forrester, 2012).

Note. BYOD = Bring Your Own Devices.

regulatory compliance (Morrow, 2012). Thielens (2013) noted that the real BYOD challenge is security and that the real security challenge is not actually about the devices, it is about controlling access from the devices to the corporate data. The security challenges associated with BYOD are a point of concern for the captains and information security officers of enterprises. This challenge has also attracted the attention of academic researchers. Alharthy and Shawkat (2013) claimed that loss or theft of mobile devices is the biggest risk that a business could face by implementing BYOD because it leads to loss of data to an unknown user. Thielens (2013) argued that a secure and scalable BYOD strategy is required to manage the risks introduced by employee-owned devices as a result of loss of a mobile device, theft, or employee termination. A Forrester (2012) survey of 202 respondents (Figure 2) with an understanding of the impact of the BYOD program on their business unit or organization revealed that security concerns are among the top challenges to implementing BYOD programs.

BYOD and Mobile Devices Management (MDM) Applications

MDM applications are developed to address some of the challenges associated with mobile devices (such as policy

management, software distribution, and inventory management) that are not related to BYOD security. MDM functionality is similar to that of PC configuration life-cycle management (PCCLM) tools; however, mobile-platform-specific requirements are often also included in MDM suites. More details on how MDM works can be found in MTI Technology (2014). Many enterprises view most of the MDM applications as a solution to the security challenges of BYOD. However, MDM does not completely address the security challenges of BYOD. MDM does not prevent a hacker from attacking an employee's device or a thief from stealing it and accessing sensitive data (Leavitt, 2013). Gartner (2014) predicted that by 2016, 20% of enterprise BYOD programs will fail due to deployment of highly restrictive MDM measures.

Possible Threats of BYOD

A survey carried out by security vendor Trustwave revealed that 90% of vulnerabilities common in desktop computers were also present in mobile devices, regardless of the operating system (Leavitt, 2013). Literature shows that data leakage, distributed denial of service (DDoS), and malware are the most challenging security threats to BYOD (Morrow, 2012).

Table 1. Common Threats of BYOD With Their Causes and Implications for Enterprises.

No.	Attack on BYOD	Causes of attack	Implications on enterprise
1	Data leakage	Malicious user of mobile device Remote access of mobile device by attacker Application vulnerabilities <ul style="list-style-type: none"> • Loss of mobile device • Malicious application • Social engineering 	Enterprise confidential information in the public
2	DDoS	Malicious intention by attacker Exploitable vulnerabilities in enterprise network	Negative impact on the server Deny the availability of the system for legitimate users
3	Malware	Trojan apps: Malicious code can be inserted into the application by an attacker with the intention of attacking devices or enterprise applications Social media, email, and SMS links: Links are embedded in SMS, social media posts, and emails with the intention of redirecting users to a website that hosts malicious files Third-party app stores: Some third-party app stores may host malware that can potentially harm devices, systems, and networks	Theft of enterprise information Enterprise applications malfunctioning Both corporate infrastructure and personal mobile devices of employee are affected by malware

Note. BYOD = Bring Your Own Devices; DDoS = distributed denial of service.

Data Leakage

Data leakage occurs as a result of access to enterprise data anywhere and anytime by employees. An enterprise has little or no control over corporate data because corporate data are now stored and accessed by personal mobile devices of employees. If an employee loses the device, the enterprise data on the device will be available to any person who finds the device. If the data available in the lost personal device are confidential enterprise data, they can be made available publicly by the person in the possession of the device.

DDoSs

A DDoS attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. DDoS can deny regular employees from running machines on computer networks or their own personal devices. Any enterprise that is subjected to a DDoS attack will negatively feel the impact on its server, and this will ultimately deny the availability of the system to legitimate users.

Malware

Malware refers to malicious applications that can affect both mobile devices and corporate applications. Mobile malware include applications with code embedded within them that compromise the security of a mobile device or related data. When a device is compromised by malware, corporate confidential data can be lost and corporate identities can be impersonated by the attacker. In addition to compromising

individual devices, malware can also affect corporate applications, thereby rendering them unusable or non-functional. Malicious applications normally take the form of normal corporate applications that have been injected with malicious code. In addition, malicious applications can be encountered when a user visits a compromised site. More details on how malware affects BYOD can be found in MTI Technology (2014). Table 1 summarizes causes and implications of common threats described above.

Researchers' Contributions on BYOD

Although BYOD began to surface in 2003, it really took off in 2011 (Leavitt, 2013), and most of the studies on BYOD were executed by consulting firms that mostly offered descriptions of the phenomenon and normative advice for executives (Björn et al., 2012). There are white papers providing frameworks under which BYOD can be deployed. Some of these white papers identified the risk associated with BYOD and provided non-technical (policy-based solutions) solutions. EY (2013) presented a white paper that divides the BYOD risk landscape into three areas. These areas are securing mobile devices, addressing application risk, and managing mobile environment. The paper offered non-technical solutions to these risks and concluded by presenting eight steps to secure and improve BYOD programs. The Deloitte (2013) research report comprises an effort to formulate an evidence-based commentary on the state of BYOD in the United Kingdom. The report attempts to cut through confusion and offer pragmatic advice incorporating a broad range of management perspectives from IT to risk management, tax, and talent. Another survey of

more than 500 IT professionals aimed to understand and address risk-associated BYOD was carried out by Johnson (2012). The intent of this non-scientific survey was to determine the type of mobile device usage allowed for enterprise applications and what level of policies and controls enterprises have around this type of usage. Denman (2012), Mansfield-Devine (2012), Miller et al. (2012), Morrow (2012), Potts (2012), Thomson (2012), Edwards (2013), Leavitt (2013), Thielens (2013), and Tokuyoshi (2013) presented their expert opinions on BYOD security issues and advice on how organizations can handle this security challenge administratively. They identify data security, malware, and BYOD network security as the main security challenges.

However, the literature shows that security issues in BYOD are a major concern for academic researchers. Niehaves, Koffer, Ortbach, and Katschewitz (2012) claimed that from an information system research perspective, a rigorous application of methods and theory to help practitioners understand the phenomenon of IT consumerization in general, and its implications for employee performance in particular, remain lacking. However, tremendous efforts were made in terms of research on mobile device security, though prior to workers owning mobile devices as tools for the workplace. Different platforms call for different security measures. Moreover, most vendors do not design smartphones primarily for businesses but rather for consumers who will use their phones as personal devices (Grover, 2013). The security mechanisms offered by most popular mobile operating systems offer only limited protection to the threats posed by malicious applications that may be inadvertently installed by the users, and therefore, they do not meet the security standards required in corporate environments (Armando, Costa, & Merlo, 2013). Polla, Martinelli, and Sgandurra (2013) presented a survey on security for mobile devices.

Gheorghe and Neuhaus (2013) aimed to design and evaluate concrete privacy mechanisms called Privacy-Preserving Accountability for personal Devices (PriPARD, pronounced “prepared”) for mobile devices used in a corporate environment. The aim was to protect user privacy within the corporate network and non-disclosure outside this network, and the vision was to gather practical experience with trade-offs between monitoring and privacy need, to help both mobile device users and managers of corporate networks. PriPARD does not examine the overall privacy of existing approaches as perceived by the user of the device, but will look for ways to allow employees to check what private information is emitted and gathered when they work (Gheorghe & Neuhaus, 2013). Werthmann, Hund, and Davi (2013) addressed the open problem of preventing (not only detecting) privacy leaks and simultaneously strengthening security against runtime attacks on iOS. They present the design and implementation of PSiOS, a tool that features a novel policy enforcement framework for iOS.

Li et al. (2013) identified a number of issues using a straightforward approach of checking BYOD smartphones periodically to prevent security breaches. These issues include the following: running constantly scanning anti-malware software on smartphones is power consuming and checking all the smartphones is inconvenient for both the employees and the employer. They propose a carefully planned but otherwise random sampling approach called strategic sampling to address these problems. The contributions of their work are three-fold. They identify threats to enterprise network security based on the unique characteristics of smartphones, introduce a method to measure smartphone security representative in an enterprise network based on the owner’s interests and the co-location logs, and propose to use strategic sampling (probability of use derived from a lottery tree that reflects the smartphones’ representativeness) to address the BYOD smartphone security problem, which balances security responsiveness and cost effectiveness. The work of Jaramillo, Newhook, and Smart (2013) is also related to mobile device security in BYOD. Their work discusses a framework that unifies numerous heterogeneous devices and their software ecosystems into a single flexible platform for enterprise device management and message dissemination. This framework provides a foundation that considers the myriad security, connectivity, and energy implications that are far different from those in a classical enterprise system.

Titze, Stephanow, and Schutte (2013) presented an extensible framework that allows companies to run automated security checks tailored to their specific security requirements independent of application markets. Their framework orchestrates different plug-in security services for checking mobile devices for malware, misbehaving applications, and configurations. In contrast to existing approaches, security services with the framework are exchangeable and can be configured according to user-specific security requirements (Titze et al., 2013). Armando et al. (2013) described a security framework for mobile devices that ensures that only applications that comply with the organization security policy are installed on the registered devices. Their framework consists of a security policy manager that mediates access to the application store and an installer application that tells the user which applications can be safely installed. This is done by inferring behavioral models from applications and by validating them against a security policy. Zhao and Osorio (2012) presented a new mechanism to prevent the use of smartphones for information leaking in corporate networks through the use of static analysis taint tracking. This mechanism is called “TrustDroid™.” TrustDroid™ is a static analyzer based on taint tracking that can be used to prevent leakage of sensitive information by an un-trusted Android smartphone. TrustDroid™ will perform static analysis to determine if there is leakage of sensitive information, and if the possibility of leakage exists, a warning of information leakage is delivered to the user of the device. Kodeswaran,

Chakraborty, Sharma, Mukherjea, and Joshi (2013) described a system that leverages sensors available on the phone as well as on the enterprise infrastructure to identify business data resident on the phone for further secure handling. They proposed a distributed architecture that leverages the context of the user for speculatively distinguishing enterprise data from personal data. The goal is to understand whether a user is engaged in enterprise or personal work by inferring her context from a combination of phone and infrastructure sensors.

Kim, Gong, Park, and Park (2013) in their work selected major domestic and external websites that provide cloud, VoIP, messenger, and email services and examined whether data are encrypted or not for constructing a safe smart work infrastructure. Wire shark was used as the inspection tool in both wired/wireless environment, and they verified that both wired and wireless environments had a very high encryption rate of identity or passwords (average encryption rate = 85.5%), but that the encryption rate of data was relatively low (average encryption rate = 27.8%). To mitigate the problem of security in the BYOD environment, Chung, Chung, Escrig, Bai, and Endicott-Popovsky (2012) proposed a novel distributed access control architecture called 2-Tier Access Control (2TAC), which uses a double-layer access control along with device security profiles, anti-virus or malware scanners, and social networking. 2TAC architecture consists of two individual and contained layers of security. A device control tier is located on the device, and a cloud control tier is located in the cloud. Peng, Li, Han, Zou, and Wu (2013) believed that many existing BYOD security practices are costly to implement and intrusive to employees, which to some degree negates BYOD's perceived benefits. To address this problem, they proposed prioritized defense deployment. A concept and a distributed algorithm both named T-dominance were proposed to capture the temporal-spatial pattern in an enterprise environment. They identified a few desirable properties of prioritized defense deployment and analytically showed that T-dominance satisfied such properties.

Kerravala (2012) claimed that BYOD requires new network strategies. In this article, technical reasons why new network strategies should be the way forward for BYOD were identified. The challenges with current network architecture were mentioned vis-à-vis proposed changes to network architecture. Scarfo (2012) presented a brief survey about the emerging methods and models to approach the BYOD phenomenon from the security point of view. The security models around BYOD summarized in the brief survey come from two opposite approaches: hand-off devices versus hand-on devices (Scarfo, 2012). Copeland and Crespi (2012) proposed a method of translating enterprise business objectives into service delivery policy rules in mobile broadband networks. This proposition enables the enterprise to control their own session policies for BYOD user and apply selective funding with prioritized service delivery. The

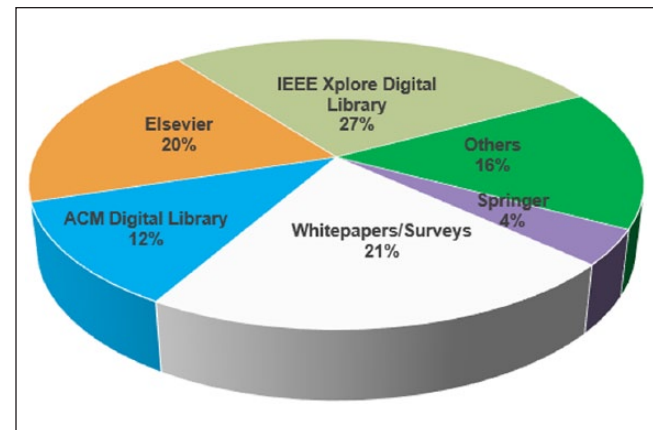


Figure 3. Percentage of article obtained from different domains of literature.

proposed Enterprise Business Context (eBC) policy process uses internal corporate data to define session context attributes, which are evaluated against business policies to produce an eBC profile.

The appendix presents the summary of contributions in research, research area addressed, and author(s) of the research. It is important to note that this summary is a result of our search for only BYOD-related publications using different academic and professional journals such as the IEEE Xplore digital library, Elsevier, Springer, ACM digital library databases, and Google Scholar index journals.

Review Analysis and Discussion

With the prevalence of BYOD in both the developed and emerging economies, there is no denying that BYOD is here to stay. Gartner Inc. predicts that half of employers worldwide will stop providing devices by 2017 and require employees to bring their own (Leavitt, 2013). However, as both the employees and employers enjoy the benefits of BYOD, they must also worry about the security challenges of BYOD policy. To address this challenge, there is a need for both academic researchers and information security professional to have a better understanding of both the theoretical and security challenges facing BYOD. This article however presents theoretical background on and security challenges of BYOD by reviewing different publications from different domains of literature.

However, in searching for publications related to BYOD, we used BYOD, Bring Your Own Device, BYOD Challenges, BYOD threats, BYOD challenges, and BYOD security threats as keywords and phrases for our search. After thorough searching with these keywords and phrases, we were able to gather 51 publications related to BYOD. Figure 3 presents the percentage of publications obtained from different domains of literature including ACM digital library, Elsevier, IEEE Xplore digital library, Springer, white paper/

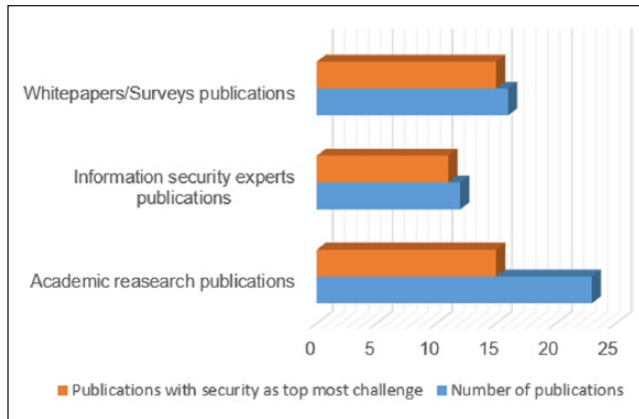


Figure 4. Security as the top-most challenge for all categories of publications.

surveys from different IT vendors, and other Google Scholar index journals.

Meanwhile, for the purpose of analysis, we divided all papers into three categories. The first category is publications from academic researchers, the second category is publications from information security experts, and the third category is white papers/surveys publications from different IT industries. It is important to note that in all three categories, security has been identified as the most significant challenge facing BYOD, as seen in Figure 4. Meanwhile, not much has been done by academic researchers to address this security challenge. Out of 15 publications that address security issues, 9 publications address the data leakage problem, 3 publications address security policy, 3 address malware, and none address DDoSs. Considering the benefits and prevalence of

BYOD in both the developed and emerging economies, it is expected that many academic researchers will be interested in providing solutions to the security challenge.

Conclusion

We present a broad view of BYOD policy by providing a theoretical foundation, deployment level, benefits, challenges, possible security attacks, and work done by researchers on BYOD. We conduct an exhaustive review of the literature to identify publications and their methodological approaches and to identify topic areas of BYOD research. Our review shows that security-related challenges are the most significant challenges facing BYOD. We believe this state-of-the-art review on BYOD contributes to practice and research by providing researchers with theoretical foundations and open issues in BYOD research. Our future work will focus on the design of a BYOD network access control system. We aim to design a two-layer access control system. The first layer will use a two-factor authentication technique to address the problem of unauthorized access to enterprise resources. This layer will serve as the authentication layer for mobile devices in BYOD environment. The proposed two-factor authentication technique will use knowledge-based and biometrics-based authentication techniques. The second layer will serve as a monitor for mobile devices when connected to enterprise resources. This layer will monitor behavior of mobile devices while connected to the enterprise network. The layer will be based on a trust model and Fuzzy logic concepts. Our overall future network access control system will enable enterprise network administrators to remotely control and monitor mobile devices before and after connection to the enterprise network.

Appendix

Summary of Researchers' Contributions on BYOD.

No.	Author(s)	Research area addressed	Contribution to knowledge
1	Alharthy and Shawkat (2013)	Security	They designed and implemented a BYOD solution, which builds a security strategy. The strategy focuses on providing almost all details about the latest BYOD threats affecting the network and security requirements to prevent these threats.
2	Armando, Costa, and Merlo (2013)	Security	Their study proposed a security framework for mobile devices that ensures that only applications complying with the organization's security policy can be installed. A prototype implementation of the proposed security framework for Android OS was presented.
3	Ballagas, Rohs, Sheridan, and Borchers (2013)	Deployment issues	Their work examined the different types of user interactions and deployment issues surrounding large public displays. They selected and developed a usage paradigm in which people use personal devices to interact with large public displays.
4	Disterer and Kleiner (2013)	Organizational issues	They described and discussed organizational issues, technical approaches, and solutions.
5	Gajar, Ghosh, and Rai (2013)	Security	Their work provided various mobility strategies, defense measures, control aspects, management and governance aspects to look for when implementing a BYOD strategy in an organization.

(continued)

Appendix (continued)

No.	Author(s)	Research area addressed	Contribution to knowledge
6	Gessner, Girao, Karame, and Li (2013)	Security	They proposed a solution that enhances the security in the BYOD scenario without compromising the usability and flexibility of the system. Their proposed solution does not require modifications to the underlying operating system of the device and enables IT officials to remotely manage their desired security policies.
7	Jaramillo, Newhook, and Smart (2013)	Security	They came up with a framework that unifies numerous heterogeneous devices and their software ecosystems into a single flexible platform for enterprise device management and message dissemination. The framework provides a foundation that considers the myriad security, connectivity, and energy implications that are far different from "classical" enterprise system.
8	Kim, Gong, Park, and Park (2013)	Security	Their study selected major domestic and external websites that provide cloud, VoIP, messenger, and email services and examined whether data were encrypted or not for constructing a safe smart work infrastructure. Their results verified that both wired and wireless environment had a very high encryption rate of identity or passwords (average encryption rate = 85.5%), but a relatively low encryption rate of data (average encryption rate = 27.8%).
9	Kodeswaran, Chakraborty, Sharma, Mukherjea, and Joshi (2013)	Security	They proposed a distributed architecture that leverages the context of the user for speculatively identifying enterprise data from personal data.
10	Lee, Lee, and Kim (2013)	Security	They suggested WLSA (White-List Based Security Architecture) for better mobile office security and presented required procedures and the analysis of the expected security enhancement.
11	Li, Peng, Huang, and Zou (2013)	Security	They came up with a method called strategic sampling. This method addresses the problem of periodic security checking for all BYOD smartphones. The study proposed a carefully planned but otherwise random sampling approach.
12	Mahesh and Hooter (2013)	Security	Their study developed and presented an integrated user-owned mobile device policy that will address the security of a business network.
13	Peng, Li, Han, Zou, and Wu (2013)	Security	The authors believed many current BYOD security practices are costly to implement and intrusive to employees, which to some degree, negates BYOD's perceived benefits. Their study proposed a concept and a distributed algorithm both named T-dominance, to capture the temporal-spatial pattern in an enterprise environment.
14	Titze, Stephanow, and Schutte (2013)	Security	They proposed a framework that allows companies to run automated security checks, tailored to their specific security requirements and independent of app markets. According to the authors, the framework operates on a virtual replica, which is created from a physical device, thereby allowing deeper inspection than the current state-of-the-art solution.
15	Werthmann, Hund, and Davi (2013)	Security	Their study addressed the open problem of preventing (not only detecting) privacy leaks and simultaneously strengthening security against runtime attacks on iOS. Design and implementation of PSiOS, a tool that features a novel policy enforcement framework for iOS, was presented.
16	Yang, Vlas, Yang, and Vlas (2013)	Deployment issues	Their study proposed the Risk Management Quintet as a model for understanding the BYOD practice. The relationships between the components of the Quintet, that is, technology adoption, control, liabilities, user perception, and user behavior, were also examined in the context of control mechanisms.

(continued)

Appendix (continued)

No.	Author(s)	Research area addressed	Contribution to knowledge
17	Björn et al. (2012)	Theoretical framework	Their work presented a well-grounded theoretical perspective and also answers the following research questions: What areas of information systems are specifically affected by IT consumerization? What are the advantages and disadvantages of IT consumerization from both employee and organization perspectives? Which theories in the IS context can increase our understanding of the relationship between IT consumerization and employee (work) performance?
18	Chung, Chung, Escrig, Bai, and Endicott-Popovsky (2012)	Access control	A novel architecture called 2TAC that uses double-layer access control along with device security profile, anti-virus or malware scanners, and social networking was proposed.
19	Copeland and Crespi (2012)	Policy control	They proposed a method of translating enterprise business objectives into a service delivery policy rule in a mobile broadband network. The proposed method enables enterprises to control their own session policies for BYOD users and apply selective funding with prioritized service delivery.
20	Kerravala (2012)	BYOD network	This work explained why BYOD requires new network strategies. The author recommended the following for next-generation Wireless Local Area Network (WLAN) strategy: IT leaders need to have a laser focus on user experience, embrace consumer technologies and BYOD, and be willing to accept change and develop new strategic relationships.
21	Scarfo' (2012)	Security	The work presented a brief survey about the emerging methods and models to approach the BYOD phenomenon from the security point of view.
22	Singh (2012)	Survey on deployment level	The study involved a survey that determined the level of deployment of BYOD in different sectors and industries. The study also depicted the different threats that affected BYOD policy. The survey showed that the application of BYOD policy would be lucrative for different types of organizations.
23	Zhao and Osorio (2012)	Security	The paper presented a mechanism called "TrustDroid™," which is a static analyzer that utilizes taint tracking to prevent leakage of sensitive information by an un-trusted Android Smartphone.

Note. BYOD = Bring Your Own Devices; 2TAC = 2-Tier Access Control; IT = information technology.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research and/or authorship of this article.

References

- AirWatch. (2012). *Enabling bring your own devices (BYOD) in the enterprise*. Retrieved from http://www.ciosummits.com/media/solution_spotlight/byod-whitepaper.pdf
- AlHarthy, K., & Shawkat, W. (2013, November-December). *Implement network security control solution in BYOD environment*. IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia.
- Armando, A., Costa, G., & Merlo, A. (2013, March). *Bring your own device, securely*. Proceedings of the 28th annual ACM Symposium on Applied Computing, Coimbra, Portugal.
- Ballagas, R., Rohs, M., Sheridan, J. G., & Borchers, J. (2013). *BYOD: Bring your own device*. Retrieved from <http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf>
- Björn, N., Sebastian, K., Kevin, O., & Stefan, K. (2012). Towards an IT consumerization theory: A theory and practice review. Working papers, ERCIS – European research center for information systems, no 13. Retrieved February 10, 2014 from <http://hdl.handle.net/10419/60246>
- Chung, S., Chung, S., Escrig, T., Bai, Y., & Endicott-Popovsky, B. (2012, December). *2TAC: Distributed access control architecture for "bring your own device" security*. ASE/IEEE International Conference on Biomedical Computing, Washington, DC.
- Cisco. (2012). *BYOD: A global perspective* (Survey report). Retrieved from http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf
- Citrix®. (2013, April). *Best practices to make BYOD simple and secure* (White paper). Retrieved from http://www.citrix.com/content/dam/citrix/en_us/documents/oth/byod-best-practices.pdf
- Citrix®. (2012, March). *Bring your own devices* (Solution brief). Retrieved from <http://www.prosysis.com/wp-content/uploads/2013/06/Citrix-BYOD-Solution-Brief.pdf>

- Copeland, R., & Crespi, N. (2012, October). *Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules*. IEEE 16th International Conference on Intelligent in Next Generation Networks, Berlin, Germany.
- Deloitte. (2013). *Understanding the bring-your-own-device landscape* (A Deloitte research report). Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-understanding-the-bring-your-own-device%20landscape.pdf>
- Denman, S. (2012). Why multi-layered security is still the best defence. *Network Security*, 2012, 5-7. doi:10.1016/S1353-4858(12)70043-0
- Disterer, G., & Kleiner, C. (2013). BYOD bring your own device. *Procedia Technology*, 9, 43-53. doi:10.1016/j.protcy.2013.12.005
- Edwards, C. (2013). Identity: The new security perimeter. *Computer Fraud & Security*, 2013, 18-19. doi:10.1016/S1361-3723(13)70082-4
- EY. (2013). *Bring your own device: Security and risk considerations for your mobile device program* (Insights on governance, risk and compliance). Retrieved from [http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/\\$FILE/Bring_your_own_device.pdf](http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf)
- Forrester. (2012). *Key strategies to capture and measure the value of consumerization of IT*. Cambridge, MA: Forrester Consulting. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_forrester_measure-value-of-consumerization.pdf
- Gajar, P. K., Ghosh, A., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4, 62-70.
- Gartner. (2014, January). Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018. *Gartner Newsroom*. Retrieved from <http://www.gartner.com/newsroom/id/2648515>
- Gessner, D., Girao, J., Karame, G., & Li, W. (2013). Towards a user-friendly security-enhancing BYOD solution. *NEC Technical Journal*, 7, 113-116.
- Gheorghe, G., & Neuhaus, S. (2013, November). *Poster: Preserving privacy and accountability for personal devices*. Presented at the Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS' 13), Berlin, Germany.
- Grover, J. (2013). Android forensics: Automated data collection and reporting from a mobile device. Rochester Institute of Technology, RIT Scholar Works. Retrieved from <http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=5389&context=theses>
- Hayes, J. (2012). The device divided. *Engineering and Technology*, 7, 76-78. doi:10.1049/et.2012.0909
- Jaramillo, D., Newhook, R., & Smart, R. (2013, April). *Cross-platform, secure message delivery for mobile devices*. Proceedings of IEEE, Southeastcon, Jacksonville, FL.
- Johnson, K. (2012, March). *BYOD security survey* (A SANS white paper). Retrieved from <http://www.sans.org/reading-room/analysts-program/mobility-sec-survey>
- Kerravala, Z. (2012). *Bring-your-own-device requires new network strategies* (ZK Research). Retrieved from http://www.xirrus.com/cdn/pdf/zeusk_byod_requires_new_network_strategies
- Kim, D. H., Gong, J. H., Park, W. H., & Park, N. (2013, June). *Vulnerability of information disclosure in data transfer section for safe smartwork infrastructure*. International Conference on Information Science and Applications (ICISA), Suwon, South Korea.
- Kodeswaran, P., Chakraborty, D., Sharma, P., Mukherjee, S., & Joshi, A. (2013, September). *Combining smart phone and infrastructure sensors to improve security in enterprise settings*. 1st International Workshop on Pervasive Urban Crowdsensing Architecture and Applications, Zurich, Switzerland.
- Leavitt, N. (2013). Today's mobile security requires a new approach. *IEEE Computer Society*, 46, 16-19.
- Lee, J., Lee, Y., & Kim, S. (2013). A white-list based security architecture (WLSA) for the safe mobile office in the BYOD era. In James J. (Jong Hyuk) Park, Hamid R. Arabnia, Cheonshik Kim, Weisong Shi, & Joon-Min Gil (eds) *Grid and pervasive computing* (Vol. 7861, pp. 860-865). Berlin, Germany: Springer.
- Li, F., Peng, W., Huang, C., & Zou, X. (2013, June). *Smartphone strategic sampling in defending enterprise network security*. IEEE International Conference on Communications, Budapest, Hungary.
- Mahesh, S., & Hooter, A. (2013). *Managing and securing business networks in the smartphone era* (Management Faculty Publications, Paper 5). Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5
- Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security*, 2012, 14-17. doi:10.1016/S1361-3723(12)70031-3
- Millard, A. (2013). Ensuring mobility is not at the expense of security. *Computer Fraud & Security*, 2013, 11-13. doi:10.1016/S1361-3723(13)70080-0
- Miller, K. W., Voas, J., & Hurlburt, G. F. (2012). BYOD: Security and privacy considerations. *IT Professional*, 14, 53-55. doi:10.1109/MITP.2012.93
- Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, 2012, 5-8. doi:10.1016/S1353-4858(12)70111-3
- MTI Technology. (2014). *Bring your own device: The future of corporate computing* (MTI white paper). Retrieved from https://mti.com/Portals/0/Documents/White%20Paper/MTI_BYOD_WP_UK.pdf
- Niehaves, B., Koffer, S., Ortbach, K., & Katschewitz, S. (2012, July). *Towards an IT consumerization theory: A theory and practice review* (Working papers, European Research Center for Information Systems, No. 13). Retrieved from <http://hdl.handle.net/10419/60246>
- Ovum. (2012). *An emerging market trend in more ways than one* (Consumer impact technology). Retrieved from <http://www.us.logicalis.com/global/united%20states/whitepapers/logicalisbyodwhitepaperovum.pdf>
- Peng, W., Li, F., Han, K. J., Zou, X., & Wu, J. (2013, October). *T-dominance: Prioritized defense deployment for BYOD security*. IEEE Conference on Communication and Network Security (CNS), National Harbor, MD.
- Polla, M. L., Martinelli, F., & Sgandurra (2013). A survey on security for mobile devices. *IEEE Communications Surveys & Tutorials*, 15, 446-470.
- Potts, M. (2012). The state of information security. *Network Security*, 2012, 9-11. doi:10.1016/S1353-4858(12)70064-8

- Scarfo, A. (2012, November). *New security perspectives around BYOD*. Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, Victoria, British Columbia, Canada.
- Singh, N. (2012). BYOD genie is out of the bottle—"Devil or angel." *Journal of Business Management & Social Sciences Research*, 1, 1-12.
- Thielens, J. (2013). Why API are central to a BYOD security strategy. *Network Security*, 2013, 5-6. doi:10.1016/S1353-4858(13)70091-6
- Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, 2012, 5-8. doi:10.1016/S1353-4858(12)70013-2
- Titze, D., Stephanow, P., & Schutte, J. (2013, March). *A configurable and extensible security service architecture for smart-phones*. 27th International Conference on Advance Information Networking and Applications Workshops, Barcelona, Spain.
- Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security*, 2013, 12-13. doi:10.1016/S1353-4858(13)70050-3
- Werthmann, T., Hund, R., & Davi, L. (2013). *PSiOS: Bring your own privacy & security to iOS devices*. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China.
- Yang, A. T., Vlas, R., Yang, A., & Vlas, C. (2013, September). *Risk management in the era of BYOD*. 2013 International Conference on Social Computing, Alexandria, VA.
- Zhao, Z., & Osorio, F. C. (2012, October). TrustDroid™: Preventing the use of smartphones for information leaking in corporate networks through the use of static analysis taint tracking. In *Proceeding of the 7th International Conference on Malicious*

and Unwanted Software (MALWARE) 2012(Fajardo, Puerto Rico), IEEE Explore, 135 - 143. Available online at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6461017>.

Author Biographies

Morufu Olalere is a lecturer from Department of Cybersecurity Science, Federal University of Technology, Minna, Nigeria. He is a PhD student at the Information Security Research Group, Faculty of Computer Science and Information Technology, Uputra Malaysia.

Mohd Taufik Abdullah obtained a PhD from University Putra Malaysia, Malaysia. He is a senior lecturer from Department of Computer Science and also member of Information Security Research Group, Universiti Putra Malaysia, Malaysia. His research interest is security in computing and digital forensics.

Ramlan Mahmod holds a PhD from University of Bradford, United Kingdom. He is currently a professor at Department of Computer Science and also head of Information Security Research Group, Universiti Putra Malaysia, Malaysia. His research interest is artificial intelligence and security in computing.

Azizol Abdullah obtained his PhD in Distributed System from University Putra Malaysia, Malaysia. He is a senior lecturer at Department Communication Technology and Network and currently, he is deputy dean (Academic and Student Affair), faculty of Computer Science and Information Technology, Universiti Putra Malaysia. His main research areas include cloud and grid computing, network security, wireless and mobile computing and computer networks.