Security and Privacy Challenge in Bring Your Own Device Environment : A Systematic Literature Review

Tanty Oktavia, Yanti
Doctor of Computer Science
School of Information Systems
Bina Nusantara University
Jakarta, Indonesia
toktavia@binus.edu; yanti@binus.edu

Harjanto Prabowo
Doctor of Computer Science
Bina Nusantara University
Jakarta, Indonesia
harprabowo@binus.edu

Meyliana
School of Information Systems
Bina Nusantara University
Jakarta, Indonesia
meyliana@binus.edu

***Abstract*— BYOD (Bring Your Own Device) has emerged as the fastest growing phenomenon that IT divisions have had to deal. Today there are a variety of tools used to communicate with stakeholder (supplier, customer, distributor, etc) in boundless place, so organizations' data will be kept in the various devices. The changing of this era drives the current trend of employees using their own laptop computers, cellular phones, smart phones, tablet, etc; both for personal and for work. However to successfully implement BYOD, the problems associated with privacy and security in BYOD environment should be identified. According to this circumstance, this study aims to identify some of the legal issues related to security and privacy challenge in BYOD (*Bring Your Own Device)* era, which can be a suggestion for institution to aware with these issues because security and privacy is the most important to any size of organization to run their business process.**

Keywords—component: BYOD, security, privacy challenge

I. INTRODUCTION

The emergence of Web 2.0 and technology of mobile devices offer an integral of every aspect of business process and a free environment to share with users and stakeholders [1]. This terminology comes from IT Consumerization concept [2]. According to this phenomenon, BYOD (*Bring Your Own Device)* is becoming more and more popular in the workplace for official use [3]. The BYOD environment changes the operational processes and methods of organization to operate their business because with BYOD allows employees to bring and use their personal mobile device, whether inside or outside of their working place [4]. In some organizations that have more concern on security, BYOD is not allowed to be adopted. Moreover, the security level of the private network is lower than public networks[5].

However, naturally, people prefer to use their own device because it is often the quickest and most pleasant to monitor their own agendas, reduce personal information overload, optimize the cognitive effort required to be multitasking and customize devices that fit personal work styles[6]. It also along with a number of opportunities for organization itself, one of them is that it cuts costs of organization by shifting the price to buy a device to employee and because people tend to take better care of their own devices, so the organization do not need to replace or maintenance the broken or stolen devices [7].

The dramatic trend of BYOD brings many challenges and concerns. It has forced enterprises to adopt a BYOD vision that is keeping their IT Division on alert for new possible security threats coming from internal and external[8]. The organization data accessed by an employee using its personal device may contain usernames, passwords, confidential emails and documents, text messages, call logs, calendar entries for the meeting, future strategies and employees contact list, etc[9]. Since there are many sensitive and privacy data on the organization are present, the device must be secured from any attack. So the organization needs to identify BYOD policy to secure the device [10].

In BYOD environment, there are many behavioral elements, such as personal devices, access environment, and such characteristics make analysis possible through patterning the access of each use[11]. According to these, there exist different policies followed by different organizations as a security solution for BYOD.

II. THEORETICAL BACKGROUND

A. BYOD

Before 1990s, organizations were used in traditional office settings, through face to face environment. Office equipment consists of telephones, computer, scanner, printer, etc [12]. After over a decade of adoption of internet governance advances in technology and the dramatic change, with increasing use of complementary technologies, such as mobile devices [13]. This phenomenon has shifted organization to be more flexible. One of the concepts is Bring Your Device (BYOD) environment. BYOD sometimes called BYOT (Bring Your Own Technology) or "IT

978-1-5090-3352-2/16/$31.00 ©2016 IEEE 16-18 November 2016, Aston Tropicana Hotel, Bandung, Indonesia
2016 International Conference on Information Management and Technology (ICIMTech)

Consumerization", is the concept to allow employees to bring their own personal devices to a workplace that are capable of Internet connection. The devices can include notebooks, tablets, smartphones, e-readers, etc[14].

BYOD adoption is broadened and still continues to transform how people and organization operate[15]. Enhancing employee satisfaction and productivity of organization could be key advantages in implementing BYOD in organizations.

B. Security

Organization and individual have constantly facing threats when the rely more on the emerging technologies[16]. The implementation of BYOD gives impact to the organization also give direct impact to the owner or personal devices[17]. In fact, the increasing use of mobile devices and adoption of Bring Your Own Device (BYOD) policy suggest that event security mistakes, such as what if the device is stolen? The fact is not only we lost the device, but the sensitive data from the organization may be lost too. Organization requires secure policy and reliable information because currently, they depend on Information Technology (IT) to organize their business process. Information security itself refers to protection of important asset of the organization[4].

C. Privacy Challenge

The issues about privacy in organizations are always defined to be a significant issue for business. Organizational privacy is the behavior of organization to protect their information assets and their customer personally identifiable information [18]. With organization continuously facing privacy issues, the organization also need to recognize the importance step to keep personal information.

III. RESEARCH METHOD

In this study, we use a Systematic Literature Review (SLR) method to enable us to identify the component of privacy challenge and information security in Bring Your Own Device (BYOD) era. SLR is one of research method to find a state of the art from researcher before. The result from SLR is a summary of the result of research before conduct further research.

A systematic literature review is divided into:

1. Introduction
   In this step, we identify a scope, research question, search process, inclusion and exclusion criteria, and data extraction
2. Analysis of the result
   After we identified the background of study, then we analyze the finding into some categories, which are source of publications, the most prolific authors, the most productive institutions, authors' academic background, authors' background, university in country, year of publications, researched industries and countries, and researched institution size.

The sources of literature gathered from several sources, which are:

- IEEEXplore Digital Library (http:/ieeexplore.ieee.org)
- Science Direct (www.sciencedirect.com)
- Palgrave Macmillan (www.palgrave-journals.com)
- Wiley Online Library (onlinelibrary.wiley.com)
- Inderscience Publishers (www.inderscience.com)
- Emerald Insight (www.emeraldinsight.com)
- Springer Link (link.springer.com)
- Proquest (http://www.proquest.com/)
- TaylorFrancis (http://taylorandfrancisgroup.com/journals/)
- Cambridge University Press (http://www.cambridge.org/)

SEARCH PROCESS

The keywords are used to find a literature based on the research question of this study using a combination of Boolean operators (AND / OR). The following pattern of keyword that is used in this study:

TABLE 1. SEARCHING PROCESS

Research Question	Keyword Search Process
What are the privacy challenges in BYOD environment?	▪ (BYOD OR (Bring AND Your AND Own AND Device)) AND (Security) AND (Privacy AND Challenges) ▪ (BYOD AND (Information AND Security) AND (Privacy AND Challenges)) ▪ (BYOD AND (Information AND Security) OR (Privacy AND Challenges))
What are the criteria of security in BYOD?	

INCLUSION AND EXCLUSION CRITERIA'S

Each keyword was inserted into journal and conference publisher to find a suitable literature according to answer the research question. There are a numerous journal and conference display. So then we try to filter the literature using 3 (three) steps, which are:

1. Studies Found
   The papers related to the specified keyword search process are classified into studies found.
2. Studies Candidate
   The next step is reading the abstract and title of literature. If the abstract and title are sufficient to answer the research question, then this paper will be included for further step. All of the paper that suitable will be classified into studies candidate group.
3. Studies Selected
   After we have studies candidate, the next step is we thoroughly read the introduction and conclusion. The paper that suitable will be used in this study as "studies selected".

The following is searching process of this study:

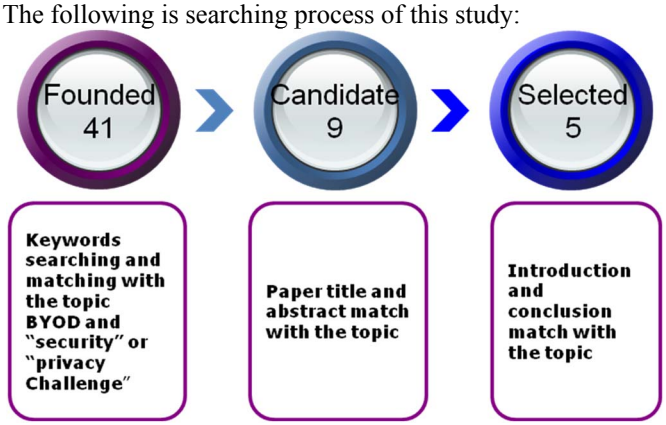

Figure 1. Searching Process

Literature was excluded in this study if the publications date before 2000 and the duplicate paper of the study.

DATA EXTRACTION

This systematic literature review was examined 41 papers from all publishers. From 41 examined papers, there are 9 papers which were selected to be candidate studies based on the title of papers and abstract to answer the research questions of this study. In the last process, we chose 5 papers which can be used in this research, based on the content of those papers which related to the topic. The following is data extraction result to describe the filtering process of this study:

TABLE 2. DATA EXTRACTION IN INCLUSION CRITERIA

Source	Found	Candidate	Selected
Proquest	29	1	0
Taylor Francis	5	2	1
Science Direct	6	5	3
Cambridge	1	1	1
Total	**41**	**9**	**5**

IV. RESULT AND DISCUSSION

Increased Bring Your Own Device (BYOD) adoption must comply with a variety of legal regulations because, in BYOD, all users need to secure the enterprise's confidential resource and data. Moreover, users need to adapt and to realize the critical role they play [19]. Hence, BYOD threat can be approached from multiple perspectives including organizational and technical. According to this fact, we use Systematic Literature Review (SLR) to conceptualize a security and privacy challenge in BYOD organization. So the user will be aware of every factor.

The following is the result of analysis using Systematic Literature Review (SLR) technique:

A. Source of Publications

There are only a few of published papers that describe a component of security and privacy challenge in BYOD. Some of the journals and conferences that are published about this topic, which are journal of legal information management, 2nd International Symposium on Big Data and Cloud Computing, Journal Computers & Security, and Journal of Information Privacy and Security. The following is list of journal for selected paper:

TABLE 3. LIST OF JOURNAL

Title	Journal/Conference		Source	#	%
Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime	Journal		Legal Information Management	1	20%
Modifying security policies towards BYOD	Conference		2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)	1	20%
Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach [1] BYOD Security Engineering: A Framework & its Analysis [2]	Journal		Computers & Security	2	40%
Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments	Journal		Journal of Information Privacy and Security	1	20%
	Total			5	

B. The most prolific authors

As seen from Table 4, there are 13 authors who have written 5 papers in security and privacy challenge for BYOD environment, which are : Brunella Longo, Vignesh U, Asha.S, Duy Dang-Pham, Siddhi Pittayachawan, Nima Zahadat, Paul Blessner, Bill A. Olson, Timothy Blackburn, Abubakar Bello Garbaa, Jocelyn Armaregoa, David Murraya, and William Kenworthya

TABLE 4 LIST OF AUTHORS

Author	#	%
Brunella Longo	1	8%
Vignesh.U	1	8%
Asha.S	1	8%
Duy Dang-Pham	1	8%
Siddhi Pittayachawan	1	8%
Nima Zahadat	1	8%
Paul Blessner	1	8%
Bill A. Olson	1	8%
Timothy Blackburn	1	8%
Abubakar Bello Garbaa	1	8%
Jocelyn Armaregoa	1	8%
David Murraya	1	8%
William Kenworthya	1	8%
Total	**13**	

C. University Affiliation According to Country

The most productive affiliation of security and privacy challenge topic in BYOD come from Australia (6 authors) and United States (4 authors).

TABLE 5. RESEARCHERS' COUNTRY AND INSTITUTION

Country	#Inst	%Inst	#Author	%Author
United Kingdom	1	8%	1	8%
India	2	15%	2	15%
Australia	6	46%	6	46%
United States	4	31%	4	31%
Total Country : 4	13		13	

D. Authors' academic background

From Table 6, we can conclude the most authors' academic background for this research topic come from an information system, which are 46%.

TABLE 6. DISCIPLINE OF AUTHOR

Discipline of Author	#	%
Computer Science	3	23%
Information System	6	46%
Engineering	3	23%
Health	1	8%
Total	13	

E. Authors' Background

Table 7 shows the researchers' background of expertise. The 13 researcher are categorized into 3 fields, which are lecturer (46%), professional (31%) and student (23%).

TABLE 7. RESEARCHERS' BACKGROUND

Background Author	#	%
Lecturer	6	46%
Professional	4	31%
Student	3	23%
Total	13	

F. The Most Productive Institutions

The most productive institutions come from Murdoch University (4 authors) and The George Washington University (4 authors).

TABLE 8. UNIVERSITY OF AUTHOR

Institution	#Authors	%
Murdoch University	4	31 %
The George Washington University	4	31 %
RMIT University	2	15 %
VIT University	2	15 %
University of Cambridge	1	8%
Total	**13**	

G. Year of Publications

This topic of research is still new, we can check from the year of publication. As seen from Table 9, this topic begins to research from 2013. So it means this topic still new, then we can explore about this topic for further research.

TABLE 9. PUBLICATION YEAR

Year	#	%
2015	3	60%
2014	1	20%
2013	1	20%
Total	5	

H. Researched Industries and Countries

This topic comes from specific industry, but it can be implemented from various sectors. From the description in Table 10, we can see the industry/sector that is possible to implement.

TABLE 10. RESEARCHED INDUSTRIES AND COUNTRIES

Industry/sector	In Country	#Papers	%
Education Industry	Australia	1	20%
Information Technology Industry	Cambridge	1	20%
Security Industry	United State	1	20%
General	India, Australia	2	40%
Total		5	

I. Researched Institution Size

Table 11 shows that research institution falling in the small company, which haven't a procedure to manage BYOD circumstances.

TABLE 11. RESEARCHED INSTITUTION SIZE

Company Size	#Paper	%
Small	3	60%
Large	2	40%
Total	5	

J. Security and Privacy Challenge Mapping

BYOD is subject to various threats as the devices involved are controlled by personal. As employee are working for the organization on their personal device, there are many risks of leakage or directly access to personal data [20]. The pace of BYOD environment is increasingly complicating the method to identify security and privacy challenge. The security policy to be followed is different for an enterprise-owned device and an employee owned device[21]. Many organizations suffer great losses because of missing implementing standards for information security with the goal of better dealing with security and privacy vulnerabilities [22].

From this study, we classified security and privacy challenge into 13 components (Table 12), which are data, device, network, malware, bandwidth, inconsistent security policy, leakage in shared media, readable data, inter-application data leakage, ownership, password, modify and damage records, and vandalize technical equipment.

TABLE 12. SECURITY AND PRIVACY CHALLENGE

Security Challenge	Brunella Longo, 2013	Vignesh.U, Asha.S, 2015	Duy Dang-Pham , Siddhi Pittayachawan, 2014	Nima Zahadat, Paul Blessner, Timothy Blackburn, Bill A. Olson, 2015	Abubakar Bello Garbaa, Jocelyn Armaregoa, David Murraya & William Kenworthy, 2015
Data	√				√
Device	√	√	√	√	√
Network					√
Malware (viruses)			√		√
Bandwidth Issues					√
Inconsistent Security Policies				√	
Leakage in Shared Media				√	
Readable Data Stays in Disposed Devices				√	
Inter-application Data Leakage				√	
Ownership		√			
Password		√			
Modify and damage records	√				
vandalize technical equipment	√				

V. CONCLUSION

These days the distribution and the use of personal device have expanded. This phenomenon brings to the Bring Your Own Device (BYOD) era where an employee uses their personal device [23]. For those organizations that have implemented the Bring Your Own Device (BYOD) paradigm, both their employees and their business can get benefit from this concept. In fact, employees gain flexibility by being able to work boundless and they also feel comfortable when using personal devices. On the other side, an organization can increase employee productivity[24]. But, there are some security issues. In this study, we investigate a

critical component according to security and privacy challenges in BYOD era. For privacy challenge, it consists 4 (four) components which are data, device, network, and bandwidths. Then, for security, it also consists 9 (nine) components, which are: malware, inconsistent security policy, leakage in shared media, readable data, inter-application data leakage, ownership, password, modify and damage records, and vandalize technical equipment. The organization should change their security policies and adopt the enhanced security policies to aware with the identified threat from this study. However, an ideal solution must be able to separate corporate space from personal data and protect corporate data [25].

VI. FUTURE RESEARCH

This study only defines components of privacy challenges and information security based on the study literature review process. It will need some statistic validation to verify all the component can be applied in all organization. Our future work will focus on the proposed design of a BYOD policy because there are a lot of BYOD policies available for organizations [26] so we need to identify the appropriate BYOD policies into the organization.

REFERENCES

[1] M. Eslahi, M.V. Naseri, H. Hashim, N.M. Tahir, E.H.M. Saad, BYOD: Current state and security challenges, in: ISCAIE 2014 - 2014 IEEE Symp. Comput. Appl. Ind. Electron., 2015: pp. 189–192. doi:10.1109/ISCAIE.2014.7010235.

[2] A. Scarfo, New security perspectives around BYOD, Proc. - 2012 7th Int. Conf. Broadband, Wirel. Comput. Commun. Appl. BWCCA 2012. (2012) 446–451. doi:10.1109/BWCCA.2012.79.

[3] I. Woodring, M. El-Said, An economical cluster based system for detecting data leakage from BYOD, ITNG 2014 - Proc. 11th Int. Conf. Inf. Technol. New Gener. (2014) 610–611. doi:10.1109/ITNG.2014.98.

[4] A.B. Garba, J. Armarego, D. Murray, W. Kenworthy, Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments, J. Inf. Priv. Secur. 11 (2015) 38–54. doi:10.1080/15536548.2015.1010985.

[5] M. Uehara, Proposal for BYOD based virtual PC classroom, Proc. - 16th Int. Conf. Network-Based Inf. Syst. NBiS 2013. (2013) 377–382. doi:10.1109/NBiS.2013.60.

[6] B. Longo, Learning on the Wires: BYOD, Embedded Systems, Wireless Technologies and Cybercrime., Leg. Inf. Manag. 13 (2013) 119. doi:10.1017/S1472669613000285.

[7] M.R. Waterfill, C.A. Dilworth, BYOD: Where the Employee and the Enterprise Intersect, Employee Relat. Law J. 40 (2014) 26–36. http://search.proquest.com.library.capella.edu/docview/1546570100?accountid=27965\nhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ:abiglobal&rft_val_fmt=info:ofi/fmt:

[8] T.A. Yang, R. Vlas, A. Yang, C. Vlas, Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior, Proc. - Soc. 2013. (2013) 411–416. doi:10.1109/SocialCom.2013.64.

[9] S. Ali, M.N. Qureshi, A.G. Abbasi, Analysis of BYOD Security Frameworks, (2015) 56–61. doi:10.1109/CIACS.2015.7395567.

[10] U. Vignesh, S. Asha, Modifying security policies towards BYOD, Procedia Comput. Sci. 50 (2015) 511–516. doi:10.1016/j.procs.2015.04.023.

[11] T. Kim, H. Kim, A system for detection of abnormal behavior in BYOD based on web usage patterns, 2015 Int. Conf. Inf. Commun. Technol. Converg. (2015) 1288–1293. doi:10.1109/ICTC.2015.7354798.

[12] F. Mamaghani, Impact of Information Technology on the Workforce of the Future : An Analysis, Int. J. Manag. 23 (2006) 845.

[13] C. Cromer, Understanding Web 2.0's influences on public e-services: A protection motivation perspective, Innov. Manag. Policy Pract. 12 (2010) 192–205. doi:10.5172/impp.12.2.192.

[14] K. Madzima, M. Moyo, H. Abdullah, Is bring your own device an institutional information security risk for small-scale business organisations?, 2014 Inf. Secur. South Africa - Proc. ISSA 2014 Conf. (2014). doi:10.1109/ISSA.2014.6950497.

[15] T. Shumate, M. Ketel, Bring Your Own Device: Benefits, risks and control techniques, Ieee Southeastcon 2014. (2014) 1–6. doi:10.1109/SECON.2014.6950718.

[16] D. Dang-Pham, S. Pittayachawan, Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach, Comput. Secur. 48 (2015) 281–297. doi:10.1016/j.cose.2014.11.002.

[17] N. Selviandro, G. Wisudiawan, S. Puspitasari, M. Adrian, Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control, 2015 3rd Int. Conf. Inf. Commun. Technol. ICoICT 2015. (2015) 113–118. doi:10.1109/ICoICT.2015.7231407.

[18] S.F. Clouse, R.T. Wright, R.E. Pike, Employee Information Privacy Concerns with Employer Held Data : A Comparison of two prevalent privacy models, J. Inf. Priv. Secur. 6 (2010) 47–71. doi:10.1080/15536548.2010.10855893.

[19] N. Zahadat, P. Blessner, T. Blackburn, B. a. Olson, BYOD security engineering: a framework & its analysis, Comput. Secur. 55 (2015) 81–99. doi:10.1016/j.cose.2015.06.011.

[20] G. Kulkarni, R. Shelke, R. Palwe, V. Solanke, S. Belsare, S. Mohite, Mobile Cloud Computing - Bring Your Own Device, Commun. Syst. Netw. Technol. (CSNT), 2014 Fourth Int. Conf. (2014) 565–568. doi:10.1109/CSNT.2014.119.

[21] M. Dhingra, Legal Issues in Secure Implementation of Bring Your Own Device (BYOD), Procedia Comput. Sci. 78 (2016) 179–184. doi:10.1016/j.procs.2016.02.030.

[22] K. Hajdarevic, V. Dzaltur, Internal penetration testing of Bring Your Own Device (BYOD) for preventing vulnerabilities exploitation, in: Information, Commun. Autom. Technol. (ICAT), 2015 XXV Int. Conf., 2015.

[23] E.B. Koh, J. Oh, C. Im, A Study on Security Threats and Dynamic Access Control Technology for BYOD , Smart-work Environment, Int. Multiconference Eng. Comput. Sci. II (2014) 6.

[24] G. Costantino, F. Martinelli, A. Saracino, D. Sgandurra, Towards enforcing on-the-fly policies in BYOD environments, 2013 9th Int. Conf. Inf. Assur. Secur. IAS 2013. (2014) 61–65. doi:10.1109/ISIAS.2013.6947734.

[25] Y. Wang, J. Wei, K. Vangury, Bring your own device security issues and challenges, 2014 IEEE 11th Consum. Commun. Netw. Conf. (2014) 80–85. doi:10.1109/CCNC.2014.6866552.

[26] R. Afreen, Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges, Int. J. Emerg. Trends Technol. Comput. Sci. 3 (2014) 233–236.