

Pelaksanaan BYOD di Organisasi: Pemerhatian ke atas Penguatkuasaan Polisi BYOD

Marziana Abdul Majid¹ & Zulkefli Mansor²

¹*Fakulti Sains dan Teknologi Maklumat
Kolej Universiti Islam Antarabangsa Selangor*

²*Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia*

marziana@kuis.edu.my, kefflee@ukm.edu.my

Abstrak. *Bring Your Own Device (BYOD)* merupakan satu amalan terkini di organisasi yang membenarkan kakitangan membawa peralatan peribadi seperti komputer riba, telefon pintar dan tablet untuk melaksanakan tugas pejabat. BYOD menyeimbangkan keselesaan emosi kakitangan dengan tekanan kerja yang dihadapi. Dari sudut pandang pertama, ia mendatangkan keuntungan kepada organisasi dalam menjimatkan kos operasi. Di sesetengah organisasi, pihak pengurusan tidak dapat menyediakan peralatan yang cukup menyebabkan kakitangan perlu berkongsi dan menunggu giliran untuk menggunakan peralatan tersebut bagi melaksanakan tugas pejabat. Melalui *trend* BYOD, kakitangan berasa lebih selesa menggunakan peralatan sendiri dalam melaksanakan tugas pejabat. Manfaatnya, produktiviti semakin meningkat lantaran kakitangan bekerja dalam suasana yang lebih selesa. Namun, di sebaliknya ia mendatangkan risiko ke atas keselamatan maklumat organisasi. Kajian ini merupakan penelitian terhadap pelaksanaan BYOD di organisasi melalui pembacaan artikel-artikel jurnal yang berkaitan. Ia merangkumi sejauh mana penekanan polisi BYOD di organisasi, limitasi capaian perisian dan maklumat yang dibenarkan ke atas kakitangan, dan isu-isu yang timbul dari amalan BYOD ini. Hasil pemerhatian ini dapat mengenalpasti permasalahan BYOD dalam konteks pengurusan dan keselamatan maklumat terhadap organisasi.

Kata Kunci: BYOD, keselamatan data, polisi BYOD

PENGENALAN

Bring Your Own Device (BYOD) merupakan satu *trend* terkini yang membenarkan kakitangan membawa peralatan peribadi seperti komputer riba, tablet dan telefon pintar ke organisasi bagi melaksanakan tugas harian. *Trend* ini mendapat perhatian di kalangan pekerja organisasi kerana ianya meningkatkan produktiviti di atas keselesaan yang dinikmati oleh mereka dalam melaksanakan tugas pejabat. Maka, pekerja tidak perlu meminjam atau menunggu giliran untuk menggunakan peralatan pejabat khususnya

komputer peribadi memandangkan bilangannya agak terhad di beberapa organisasi. Pihak pengurusan organisasi juga menerima baik kehadiran *trend* BYOD ini oleh kerana ianya dapat menjimatkan kos operasi. Organisasi dapat mengurangkan pembelian peralatan ini selain dapat menjimatkan ruang simpanan.

Namun begitu, organisasi harus menyedari bahawa BYOD juga mendatangkan impak negatif kepada organisasi itu sendiri. Ini kerana data dan maklumat sulit organisasi boleh dicapai melalui peralatan peribadi pekerja. Capaian ke atas maklumat organisasi bukan sahaja dilakukan di dalam organisasi sahaja, malah di mana jua. Lebih membimbangkan sekiranya pekerja tersebut tidak lagi berkhidmat dengan organisasi, namun maklumat organisasi masih berada di dalam peralatan peribadinya seperti komputer riba. Maka, isu popular yang timbul dari BYOD adalah berkaitan keselamatan dan privasi ke atas maklumat organisasi.

Banyak kajian yang dijalankan ke atas BYOD dari aspek yang berbeza seperti polisi keselamatan, rangkakerja BYOD, dan isu-isu berkaitan BYOD. Namun, bilangan kajian ke atas keselamatan maklumat organisasi yang mengamalkan trend BYOD ini agak kurang. Disebabkan itu, kertas kerja ini memfokuskan kepada kajian-kajian yang telah dijalankan berkaitan keselamatan maklumat organisasi yang mengamalkan trend BYOD ini.

Kepentingan BYOD

Komunikasi mobil sudah menjadi amalan pada masa kini dan ia turut mempengaruhi persekitaran korporat. Organisasi kini lebih banyak menggunakan peralatan mobil seperti komputer riba, tablet dan telefon pintar dalam pengurusan mereka. Bukan sahaja di bidang korporat, malah BYOD juga diaplikasikan di dalam Institusi Pengajian Tinggi (Franklin & Mohamed, 2015)(Rahat, 2016). Hasil kajian menunjukkan 84% organisasi menggalakkan BYOD manakala 16% organisasi masih belum bersedia membenarkan BYOD ke dalam organisasi (Dhingra, 2015).

Apabila sesebuah organisasi membenarkan pekerja membawa peralatan sendiri ke pejabat, ia sebenarnya telah mencipta suasana rileks, lebih terbuka dan efisyen. Pekerja dapat menjalankan tugasnya tanpa berasa tertekan. Suasana begini menjadikan pekerja lebih fleksibel, produktif dan dapat menyempurnakan tugasannya dengan lebih cepat dan baik (Olalere, Abdullah, Mahmod, & Abdullah, 2015). Manfaat BYOD ini bukan tertumpu kepada pekerja sahaja malah organisasi juga dapat menjimatkan kos operasi di mana tidak perlu lagi peralatan kepada pekerja (Fani, Solms, Gerber, 2016)(Magruder, Lewis & Smolinski, 2015).

Pelaksanaan BYOD di Organisasi

Kajian yang dijalankan oleh Yu & Computing (2013) mendapati 60% pengguna BYOD lebih berminat melayari aplikasi *free-file sharing* dan 55% daripadanya tidak memaklumkan penggunaan aplikasi tersebut kepada organisasi. Manakala menurut Magruder, Lewis & Smolinski (2015) BYOD tidak sesuai dijadikan amalan di pejabat

memandangkan keadaan ini akan menimbulkan risiko seperti serangan berdasarkan web dan virus serta *denial-of-service* yang akhirnya akan mendatangkan kos di luar jangkaan untuk memperbaiki sistem dan peranti yang terbabit. Keselamatan ke atas maklumat sulit organisasi dan privasi hak pekerja terhadap peralatannya juga merupakan isu yang timbul dalam BYOD (Vorakulpipat, Sirapaisan, Rattanalerdnusorn, & Savangsuk, 2017), (Magruder, Lewis, & Burks, n.d.), (Dhingra, 2016).

Isu dalam BYOD

Tidak dinafikan BYOD merupakan *trend* terkini yang disenangi oleh kedua-dua pihak organisasi dan pekerja namun keperluan organisasi dan keperluan keselamatan maklumat perlulah seimbang (Yu & Computing, 2013), (Zahadat, Blessner, Blackburn, & Olson, 2015). Namun, isu utama dalam *trend* BYOD adalah keselamatan serta kerahsiaan data dan maklumat organisasi (Vorakulpipat et al., 2017), (Magruder et al., n.d.), (Dhingra, 2016). Peralatan yang digunakan adalah milik pekerja namun data yang dicapai dalam melaksanakan tugasannya pejabat adalah milik organisasi. Namun, apabila data organisasi dicapai melalui peralatan peribadi pekerja, maka data tersebut terdedah kepada pelbagai risiko.

Walaupun begitu, kebanyakan organisasi masih tidak mempunyai polisi keselamatan ke atas BYOD (Zahadat, Blessner, Blackburn, & Olson, 2015), (Franklin, n.d.), (Yu & Computing, 2013). Menyedari risiko BYOD itu, empat rangkakerja BYOD telah diperkenalkan iaitu rangkakerja keselamatan, rangkakerja sistem pengurusan BYOD, rangkakerja pengurusan budaya dan privasi, dan rangkakerja enterprise dan keselamatan ruang (Fani, Solms, & Gerber, 2016). Setiap rangkakerja ini mempunyai kelemahan masing-masing seperti yang dilampirkan dalam Jadual 1.

Jadual 1. Pelaksanaan rangkakerja BYOD (Fani et al., 2016)

Rangkakerja	Kekuatan	Kelemahan
Rangkakerja keselamatan BYOD	<ul style="list-style-type: none">- Mesra persekitaran organisasi- Peralatan BYOD adalah berdaftar- Organisasi menilai peralatan dan keselamatan maklumat- Organisasi pemantauan berterusan.	<ul style="list-style-type: none">- Rangkakerja menekankan aspek teknikal dalam pengurusan peralatan BYOD- Persekutuan industry kecil dan sederhana tidak dinyatakan kesesuainnya.
Rangkakerja pengurusan system	<ul style="list-style-type: none">- Mengenalpasti ancaman terhadap penilaian risiko	<ul style="list-style-type: none">- Tidak begitu menitikberatkan keselesaan pekerja.

	<ul style="list-style-type: none"> - Membangunkan polisi /strategi bagi pengurusan BYOD - Merancang sebelum polisi dilaksanakan. 	<ul style="list-style-type: none"> - Tidak menekankan kepada persekitaran industri kecil dan sederhana (IKS).
Rangkakerja kawalan budaya dan keselamatan BYOD	<ul style="list-style-type: none"> - Mengenalpasti budaya organisasi - Membangunkan polisi - Jelas terhadap elemen dan data yang memerlukan keselamatan. 	<ul style="list-style-type: none"> - Fungsi pekerja tidak diberi pertimbangan yang wajar - Tidak menitikberatkan persekitaran industri kecil dan sederhana. -
Rangkakerja ruang dan keselamatan BYOD	<ul style="list-style-type: none"> - Terdapat analisis peralatan BYOD dan pentadbiran teknologi maklumat. - Terdapat BYOD polisi di organisasi. - Keselesaan adalah dititiberatkan. 	<ul style="list-style-type: none"> - Terdapat kekangan dalam pengurusan risiko. - Tidak menitikberatkan persekitaran industri kecil dan sederhana.

KESIMPULAN

Secara keseluruhannya, organisasi menerima baik *trend* BYOD kerana ia memberi banyak manfaat kepada produktiviti organisasi itu sendiri. Namun, isu utama yang timbul apabila organisasi membenarkan BYOD adalah keselamatan data organisasi dan privasi terhadap peralatan pekerja. Pemerhatian terhadap beberapa artikel jurnal mendapati ketiadaan polisi BYOD di organisasi merupakan antara faktor yang menyumbang kepada isu-isu tersebut. Polisi BYOD perlulah merangkumi keselamatan peralatan, *encryption* dan kata laluan pekerja, pengkategorian data antara organisasi dan pekerja, perisian penyahvirus, capaian tanpa wayar, capaian secara mobil dan privasi ke atas hak milik peralatan tersebut (Dhingra, 2016). Selain saranan menguatkuasakan polisi BYOD dalam organisasi, rangkakerja keselamatan BYOD juga difikirkan perlu sebagai penyelesaian bagi mengenalpasti teknologi, polisi dari pihak pengurusan dan integrasi pekerja dalam organisasi (Zahadat et al., 2015).

RUJUKAN

- Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device. *Procedia - Procedia Computer Science*, 78(December 2015), 179–184.
<http://doi.org/10.1016/j.procs.2016.02.030>
- Fani, N., Solms, R. von, & Gerber, M. (2016). A framework towards governing Bring Your Own Device in SMMEs; *2016 Information Security for South Africa (ISSA)*, 1–8. <http://doi.org/10.1109/ISSA.2016.7802922>
- Franklin, O. U. (n.d.). The Future of BYOD in Organizations and Higher Institution of Learning.
- Magruder, J. S., Lewis, S. X., & Burks, E. J. (n.d.). Bring Your Own Device (BYOD) -- Who Is Running Organizations ? Carl Smolinski, 15(1), 55–61.
- Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 5(2), 2158244015580372-.
<http://doi.org/10.1177/2158244015580372>
- Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Security and Communication Networks*, 2017. <http://doi.org/10.1155/2017/2057260>
- Yu, W. E., & Computing, T. C. (2013). Feature BYOD Security Considerations of Full Mobility, 1, 1–4.
- Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. a. (2015). BYOD security engineering: a framework & its analysis. *Computers & Security*, 55, 81–99.
<http://doi.org/10.1016/j.cose.2015.06.011>