STRATEGI *"BRING YOUR OWN DEVICES"* PADA PERUSAHAAN SEBAGAI TANTANGAN PENYELARASAN BISNIS DAN TI UNTUK MEMENUHI SASARAN FINANSIAL

Restiadi Bayu Taruno[1)], Wing Wahyu Winarno[2)], Dani Adhipta[3)]

[1), 2), 3)] Jurusan Teknik Elektro dan Teknologi Informasi, Fakultas Teknik, Universitas Gadjah Mada
Jl Grafika 2 Yogyakarta 55281, Telp/Fax:0274 547506
Email : bayu.taruno.cio.8b@mail.ugm.ac.id[1)], wingwahyuwinarno@gmail.com[2)], dani@te.ugm.ac.id[3)]

Abstrak

Konsumerisme dan trivialisme telah merubah wajah TI dalam dunia bisnis. Organisasi dalam perusahaan tengah merancang sebuah kebijakan yang mengizinkan "Bring Your Own Devices" (BYOD) kedalam lingkungan pekerjaan demi peningkatan produktivitas, kolaborasi dan mobilitas pekerja. Dengan menggeser kepemilikan perangkat kepada karyawan, kontraktor dan bahkan departemen, IT meringankan beban secara proses bisnis dan finansial dalam hal pengadaan perangkat, end point procurement dan manajemen. Meskipun memiliki isu besar soal keamanan, kebijakan BYOD bukan lagi tentang kemauan organisasi dalam perusahaan untuk penerapannya, namun tentang kapan kebijak tersebut akan diterapkan.

Kata kunci: *konsumerisme; produktifitas; finansial; keamanan; (key words)*

1. Pengertian *Bring Your Own Devices* (BYOD)

Konsumerisasi adalah sebuah kecenderungan yang berkembang untuk teknologi informasi baru agar muncul pertama di pasar konsumen dan kemudian menyebar ke organisasi bisnis dan pemerintah [1]. Munculnya pasar konsumen sebagai pendorong utama inovasi teknologi informasi dipandang sebagai pergeseran industri TI utama, sebagai organisasi bisnis dan pemerintah besar mendominasi dekade awal penggunaan komputer dan pengembangan.*Bring Your Own devices* (BYOD) (juga disebut membawa teknologi sendiri (*Bring Your Own* Technology : BYOT), membawa telepon Anda sendiri (*Bring Your Own* Phone : BYOP), dan membawa PC Anda sendiri (*Bring Your Own* PC : BYOPC)) adalah sebuah kebijakan yang mengizinkan karyawan untuk membawa perangkat mobile milik pribadi (*laptop*, tablet, dan *smartphone*) ke tempat kerja mereka, dan menggunakan alat-alat tersebut untuk mengakses informasi perusahaan dan aplikasi khusus perusahaan[2][3]. istilah ini juga digunakan untuk menggambarkan praktik serupa yang diterapkan kepada siswa, yaitu menggunakan perangkat pribadi yang dimiliki dalam dunia pendidikan[4].

Saat ini, dengan semakin maraknya penggunaan media sosial dan internet di masyarakat, menimbulkan gejala baru pada trend teknologi yaitu konsumerisme dan trivialisme IT. Tentunya hal ini menimbulkan tantangan baru bagi setiap organisasi baik pemerintah maupun sektor swasta. Di masa kini dengan semakin berkembangnya industri Teknologi Informasi dan Komunikasi sangat jamak ditemui karyawan sebuah perusahaan atau pegawai-pegawai pemerintah yang menggunakan alat komunikasi, laptop dan berbagai piranti lainnya ke dalam lingkungan pekerjaan. Bahkan hasil riset dari sebagian besar bursa di seluruh dunia memberikan nilai 70% pengguna *smartphone* lebih memilih mengakses data-data bisnis dan personalnya melalui piranti-nya sendiri, tanpa dipusingkan dengan kesulitan atau masalah-masalah tentang masih kaburnya batasan diantara keduanya [13].

2. Strategi TI terhadap strategi bisnis

Strategi sangat penting bagi perusahaan untuk dapat memenangkan persaingan pasar. Strategi merupakan arahan dan ruang lingkup dari perusahaan dalam jangka panjang yang akan memberikan keuntungan bagi perusahaan melalui penggunaan sumber daya yang ada dalam lingkungan yang mendukung untuk memenuhi kebutuhan pasar dan memenuhi harapan dari para stakeholder. Strategi yang dilakukan oleh sebuah perusahaan akan membedakannya dengan perusahaan – perusahaan lain. Perusahaan dapat memberikan performa yang lebih baik dari para pesaing hanya jika perusahaan dapat menentukan perbedaan yang dimilikinya dan mempertahankannya. Karena perbedaan ini, maka setiap perusahaan tentunya akan memerlukan penggunaan IT secara berbeda sesuai dengan strategi yang diterapkan. Ada dua kemungkinan yang dapat dilakukan, pertama proses bisnis perlu dilakukan modifikasi agar sesuai dengan IT yang digunakan, atau kedua melakukan penyesuaian atau kustomisasi terhadap IT.

IT memegang peranan penting dalam mewujudkan strategi bisnis. Sebuah organisasi yang telah mengadopsi teknologi informasi ke dalam proses bisnis yang dilakukannya, tentunya akan ikut memikirkan peranan yang akan dilakukan oleh IT. Beberapa perusahaan ada yang menggunakan IT untuk menjalankan operasi sehari – hari agar dapat berjalan dengan baik dan efisien. Ada juga perusahaan yang menggunakan IT sebagai *enabler* untuk menciptakan kesempatan – kesempatan baru yang mungkin tidak akan dapat dilakukan tanpa dukungan IT. Serta IT juga digunakan sebagai cara baru untuk

mengatur fungsi – fungsi yang ada dalam organisasi. Peranaan IT dalam organisasi ini juga akan mempengaruhi penyelarasan yang terjadi dalam perusahaan. Menurut Bjorn Cumps Stijn Vieane, dan Guido Dedene (2012), ada tiga peranan IT dalam organisasi yaitu [5]:

1) Memegang peran konservatif sebagai pendukung dalam organisasi. Perusahaan ini memilih menggunakan teknologi IT yang sudah terbukti dan matang.
2) Memegang peran yang kritis dan penting dalam organisasi. Perusahaan ini memilih menggunakan dan menginvestasikan pada teknologi IT terkini.
3) Memegang peran sebagai inovator dalam bisnis.

Perusahaan ini berkompetisi dalam dunia usaha yang sangat tergantung pada teknologi dan menggunakan IT sebagai alat dalam berkompetisi (*competitive weapon*). Namun semakin pesatnya perkembangan teknologi dan semakin cepatnya perubahan dan persebaran teknologi-teknologi baru ini, teknologi informasi mulai kehilangan keunggulan strategis-nya pada management strategis perusahaan. Investasi dan proses penyesuaian teknologi harus melalu pendekatan yang sama sekali berbeda [6].Aplikasi teknologi informasi yang berlebihan dan tidak tepat guna terkadang memberikan sentimen negatif terhadap laba perusahaan.

Kenyataan yang terjadi dalam sebuah proyek penyelarasan teknologi informasi dengan strategi bisnis organisasi adalah terkadang proyek penyelarasan teknologi informasi dengan strategi bisnis terlambat diaplikasikan, atau melebihi anggaran yang telah ditentukan, atau melewati batas penyerahan hasil, atau lebih buruk lagi adalah merupakan kombinasi diantara sebab-sebab diatas [7].

Seperti hal-nya masalah ROI dari sebuah penerapan TI dalam strategi bisnis, tren Bring Your Own Device (BYOD) memiliki kekhawatiran soal dampaknya terhadap kerentanan keamanan data bagi suatu perusahaan. Hal itu terjadi akibat berbagai perangkat bergerak yang dimiliki para karyawan secara bebas mengakses data perusahaan dari mana dan kapan saja tanpa batas-batas yang jelas. Survei *Citrix Workplace of Future* di 19 negara termasuk di Asia Tenggara menyebutkan sebanyak 65 persen responden khawatir tentang masalah keamanan informasi. Apalagi, 52 persen dari responden tidak memahami risiko keamanan dari penggunaan perangkat pribadinya [8]. Dari *State of Mobility Survey* tergambar sebanyak 67 persen responden cemas program jahat masuk jaringan perusahaan dari perangkat bergerak yang dipakai karyawan untuk bekerja. Namun, 55 persen responden telah sadar mencari tahu bagaimana mengatasi potensi ancaman keamanan dan 23 responden telah mengalami kehilangan data bisnis. Ini termuat dalam riset B2B International yang dirilis Kaspersky 2012 [9].

Kejahatan cyber juga terjadi pada perangkat bergerak telah terungkap Norton Cyber Crime (2012) di 24 negara. Ini terjadi akibat 83 responden hanya menggunakan solusi keamanan tingkat dasar pada perangkat bergerak pribadinya atau tidak memakai solusi yang tepat. Apalagi, 67% responden tidak menggunakan solusi keamanan pada perangkat pribadinya. Survei B2B International mengungkapkan 54% data perusahaan hilang akibat kejahatan teknologi informasi (TI). Angka ini nomor dua setelah India yang mencapai 66%, tapi di atas China sebesar 41%.

Berbagai risiko keamanan yang mungkin timbul akibat penggunaan perangkat bergerak terhadap data-data perusahaan dihadapi divisi TI suatu perusahaan dengan pelarangan penggunaan perangkat cerdas milik karyawan oleh 38 persen responden yang diketahui dari survei B2B International. Bahkan, 19% responden memblokir layanan tersebut bagi karyawan.

3. Strategi penerapan *Bring Your Own Devices* (BYOD)

Sebuah inisiatif penerapan BYOD yang sukses adalah dengan menggabungkan kesederhanaan untuk pengguna secara efektif dengan kontrol keamanan dan manajemen TI. Sementara godaan kuat untuk departemen IT adalah mengembangkan kebijakan spesifik untuk setiap skenario yang mungkin, kenyataannya adalah bahwa pertimbangan yang paling dapat diatasi melalui penerapan beberapa prinsip-prinsip sederhana yang konsisten. Dalam kebanyakan kasus, departemen TI dapat berpikir tentang bagaimana mengelola dan menyediakan akses yang aman ke data dan aplikasi secara perorangan, bukan perangkat yang mereka gunakan.

Perusahaan/organisasi mungkin ingin menetapkan kebijakan lebih rinci mengenai jenis perangkat tertentu, koneksi jaringan, dan lokasi, tetapi ini biasanya akan mewakili satu set skenario yang lebih kecil dan lebih mudah dikelola. Tapi BYOD lebih dari sekedar pergeseran kepemilikan perangkat kepada karyawan. Ini memiliki implikasi yang kompleks dan banyak strategi tersembunyi yang perlu didefinisikan terlebih dahulu dalam pelaksanaannya. Delapan komponen utama untuk strategi BYOD sukses menurut MobileIron [10] :

1) Keberlanjutan
2) Perangkat pilihan
3) Model yang terpercaya
4) Liabilitas
5) Kewajiban Ekonomi
6) Pengalaman dan privasi pengguna
7) Desain Aplikasi dan Kebijakan-kebijakan
8) Pemasaran internal

BYOD adalah merupakan hal baru untuk sebagian besar organisasi dan, sebagai akibatnya, praktek terbaik dari implementasi-nya masih dalam tahap pengembangan. Salah satu perangkap kebijakan dimana departemen IT sebuah perusahaan banyak jatuh ke dalamnya adalah membangun satu set kaku kebijakan BYOD yang tidak berkelanjutan dalam jangka panjang. Agar berkelanjutan, kebijakan BYOD harus memenuhi kebutuhan keduanya;

departemen TI dan karyawan untuk dapat:
1) Mengamankan data perusahaan
2) Meminimalkan biaya implementasi dan penegakan
3) Melestarikan pengalaman pengguna asli
4) Tetap *up-to-date* dengan preferensi pengguna dan inovasi teknologi

Organisasi seringkali memfokuskan sebagian besar waktu dan sumber daya pada dua persyaratan pertama. Tapi dua yang terakhir jauh lebih penting untuk keberlanjutan dalam jangka panjang. Jika implementasi BYOD merusak pengalaman pengguna atau cepat menjadi usang, pegawai akan menemukan cara untuk menghindari kebijakan atau mengakhiri partisipasi mereka dalam program ini. Dalam kedua kasus, tidak satupun baik kebutuhan karyawan maupun perusahaan terpenuhi – baik itu berupa keamanan yang dikompromikan atau nilai bisnis yang hilang. Pengalaman pengguna adalah tes lakmus untuk keberlanjutan kebijakan. Jika kenyamanan pengguna rusak, begitu juga program BYOD yang akan dijalankan.

Perusahaan harus berpikir tentang layanan spesifik yang akan tersedia pada perangkat BYO dan perbedaan untuk kelompok pekerjaan tertentu, jenis pengguna, jenis perangkat dan berdasarkan penggunaan jaringan. Selain itu, pekerja BYOD sering membawa solusi kelas konsumen ke perusahaan, dan memungkinkan terjadinya kolaborasi dengan aplikasi dan layanan perusahaan. Ini termasuk versi ringan dari aplikasi enterprise, aplikasi mobile dan mikro, dan terfokus pada layanan konsumen SaaS. Departemen TI harus memutuskan apakah akan mengizinkan solusi seperti ini dapat digunakan untuk kerja, dan jika demikian, apakah mereka bisa diinstal langsung pada *end point* dalam lingkungan yang sama dengan pekerjaan yang berhubungan dengan data.[11]

Membangun kebijakan di sekitar pilihan perangkat memerlukan[10]:
1) Menganalisis preferensi karyawan dan memahami perangkat yang telah mereka beli: Sebuah program BYOD yang tidak mendukung tren saat ini dan pembelian dimaksudkan akan memiliki daya tarik yang terbatas.
2) Mendefinisikan dasar penerimaan dukungan BYOD terhadap keamanan dan fitur dukungan : Tujuannya adalah untuk memasukkan platform ponsel yang diinginkan semua karyawan dalam program ini, tanpa membuat celah keamanan atau dukungan yang menyusahkan. Baseline penerimaan umumnya termasuk manajemen aset, enkripsi, kebijakan password, *remote lock*/*wipe*, dan email/Wi-Fi/konfigurasi VPN. Tanpa hal-hal fundamental tersebut, platform mobile tidak layak untuk perusahaan. Semakin maju/canggih sebuah platform mobile, umumnya harus semakin fokus pada aplikasi yang berhubungan dengan fungsi dan keamanan tingkat tinggi seperti otentikasi berbasis sertifikat. Platform perangkat yang cocok dengan daftar platform maju/canggih mendapatkan akses ke tingkat yang lebih tinggi dari fungsi perusahaan dalam program BYOD.
3) Memahami sistem operasi, hardware, dan variasi menurut wilayah geografis : Pada Android khususnya, perangkat sejenis sebenarnya dapat mendukung kemampuan yang sangat berbeda berdasarkan produsen dan wilayah geografis. Nama merek dari perangkat yang sama juga dapat bervariasi oleh operator nirkabel, yang tentunya berpotensi menambahkan kebingungan.
4) Mengembangkan rencana sertifikasi *light-touch* untuk evaluasi perangkat masa depan: Sebagian besar organisasi berinvestasi dalam program sertifikasi dimuka saat meluncurkan program BYOD mereka. Namun, perangkat baru diperkenalkan ke pasar setiap 3-6 bulan sehingga proses sertifikasi harus berkelanjutan dan terus berkembang. Jika proses ini terlalu berat, tentunya akan menjadi mahal dan akhirnya tertinggal, sehingga kecepatan dan efisiensi sertifikasi sangat penting.
5) Membangun komunikasi yang jelas kepada pengguna tentang perangkat yang diizinkan atau tidak, dan mengapa: Menerapkan BYOD tanpa kejelasan terhadap pengguna tentang perangkat yang didukung, mencegah mereka membeli perangkat yang tidak didukung atau menjadi frustrasi bahwa tingkat layanan yang mereka harapkan dari TI tidak tersedia bagi mereka.
6) Memastikan tim TI memiliki bandwidth untuk tetap up-to-date: Daftar perangkat yang diperbolehkan sangat dipengaruhi oleh permintaan pengguna dan sebagainya dapat berubah dengan cepat, kali seringkali beberapa tahun. Seorang Manager IT dalam perusahaan harus menjadi pakar pada perangkat dan evolusi sistem operasi, jika tidak, program BYOD cepat menjadi usang. Hal ini terutama penting ketika program bergerak melampaui iOS dan BlackBerry menuju variasi system operasi yang lebih beragam.

Perusahaan Kontraktor umumnya calon ideal untuk BYOD. Banyak organisasi sudah mengharapkan kontraktor untuk membawa perangkat mereka sendiri, dan mengharuskan mereka untuk melakukan fungsi jasa kontraktor mandiri[11].

Masalah Keamanan

Lebih dari tiga-perempat dari CIO khawatir bahwa Konsumerisasi lanjut dari produk TI akan menyebabkan resiko bisnis sangat meningkat.[12] Sementara instalasi aplikasi langsung di perangkat-non-perusahaan dapat meningkatkan risiko, program BYOD berdasarkan virtualisasi desktop membuat ini tidak perlu. Semua informasi bisnis tetap aman dalam *data center*, yang berada pada *end point* hanya dalam bentuk terisolasi, terenkripsi, dan hanya jika benar-benar diperlukan. Pada kasus di mana data yang tidak perlu berada pada *end point*, dapat dilindungi melalui isolasi, enkripsi, dan mekanisme *remote wipe*. Untuk mencegah exfiltration, departemen TI dapat menerapkan kebijakan untuk menonaktifkan pencetakan atau akses ke sisi penyimpanan klien seperti drive lokal dan penyimpanan

USB. Pegawai juga harus memastikan bahwa software antivirus / anti-malware terinstal dan diperbarui pada *end point* mereka.

Untuk melindungi jaringan perusahaan, beberapa organisasi menerapkan teknologi kontrol akses jaringan (NAC) untuk memberikan otentifikasi, menghubungkan ke jaringan dan memeriksa apakah perangkat yang terhubung memiliki perangkat lunak antivirus dan patch keamanan yang up-to-date. Access Gateway juga dapat digunakan untuk menyediakan granular, berbasis kebijakan akses browser ke aplikasi dan data. Password sign-on tunggal dan kuat memungkinkan baik kenyamanan dan keamanan. Di luar firewall, virtualisasi dan enkripsi dapat menghilangkan sebagian besar kerentanan keamanan Wi-Fi, enkripsi WEP, nirkabel terbuka, 3G/4G dan konsumen kelas metode akses.

BYOD menambahkan lapisan lain untuk model kepercayaan, karena tingkat kepercayaan untuk perangkat pribadi mungkin berbeda dari perangkat yang disediakan perusahaan. Kebijakan privasi akan bervariasi, sesuai dengan kehendak dan harapan pengguna. Sebagai contoh, pengguna dapat menerima jika tidak dapat menggunakan aplikasi jaringan sosial pada perangkat perusahaan, namun jenis kebijakan ini tidak dapat diterima untuk perangkat pribadi. Membangun model kepercayaan BYOD membutuhkan:

1) Proses identifikasi dan penilaian risiko untuk masalah sifat keamanan yang umum pada perangkat pribadi : Karyawan yang menggunakan perangkat pribadi berbeda dari perangkat perusahaan, misalnya, mereka menunduh aplikasi lebih banyak. Jadi dengan BYOD, perangkat mungkin lebih sering tidak patuh terhadap kebijakan perusahaan lebih, dan sebagainya.
2) Mendefinisikan pilihan remediasi (notifikasi, kontrol akses, karantina, *selective wipe*): Opsi ini mungkin berbeda dalam keberagaman dari BYOD ke perangkat perusahaan. Sebagai contoh, pada perangkat perusahaan dengan tingkat keamanan risiko sedang, remediasi yang mungkin terjadi adalah proses penghapusan penuh. Tetapi pada perangkat pribadi, tindakan remediasi yang mungkin terjadi lebih ringan, seperti blokir terhadap akses perusahaan, diikuti dengan penghapusan selektif sebatas data-data perusahaan saja.
3) Menetapkan kebijakan berjenjang: "Kepemilikan" menjadi dimensi penting sebagai dasar mengatur kebijakan. Akibatnya, perangkat pribadi dan perusahaan masing-masing akan memiliki kebijakan yang berbeda untuk keamanan, privasi, dan distribusi aplikasi.
4) Menetapkan identitas pengguna dan perangkat: Karena pilihan perangkat menjadi beragam, konfirmasi identitas pengguna dan perangkat, yang biasanya melalui sertifikat, menjadi lebih penting.
5) Memandang secara kritis dan lebih serius untuk keberlanjutan dari kebijakan keamanan yang diberlakukan: Dampak yang mungkin terjadi terhadap pengalaman pengguna, kemampuan pengguna menerima imbal-balik pengalaman pengguna dan fitur aplikasi perusahaan dalam jangka panjang. Jika tingkat kepercayaan dari perangkat pribadi sangat rendah sehingga keamanan membutuhkan pembatasan penggunaan yang luas, pengalaman pengguna perangkat karyawan akan rusak, dan baik kebijakan maupun program BYOD tidak akan berkelanjutan.

Pada kasus seperti pegawai yang menggunakan BYOD meninggalkan organisasi, kebijakan BYOD dilanggar atau perangkat BYO hilang atau dicuri, departemen TI harus memiliki mekanisme untuk menghentikan akses langsung ke data dan aplikasi.

Implementasi Kebijakan BYOD

Setelah inisiatif BYOD perusahaan telah dirancang, komunikasi sangat penting untuk implementasi yang sukses. Pegawai harus menerima bimbingan dan pelatihan untuk membantu mereka memutuskan apakah akan berpartisipasi dan bagaimana memilih perangkat yang tepat untuk kebutuhan mereka. Mereka juga harus memahami tanggung jawab yang datang dengan membawa perangkat mereka sendiri, termasuk bagaimana data dapat diakses, digunakan dan disimpan. Data yang menyangkut pekerjaan dan bisnis perusahaan harus dijaga dan dipisahkan pada perangkat BYOD untuk mendukung persyaratan e-discovery dan kebijakan retensi data, kebijakan yang serupa berlaku pada email yang menyangkut pekerjaan tidak boleh dikirim dari rekening pribadi. Kebijakan penggunaan pada perangkat BYO yang diterima harus menerapkan cara yang sama seperti yang mereka lakukan pada perangkat perusahaan.

Model kepercayaan dan pertimbangan perangkat pilihan yang dijelaskan dalam bagian sebelumnya keduanya memiliki dampak yang mendasar pada strategi aplikasi untuk BYOD. Pada awalnya, organisasi berasumsi BYOD hanyalah sebuah keputusan kepemilikan perangkat dengan dampak minimal pada aplikasi. Tetapi aplikasi tentunya melibatkan data perusahaan, dan jika tingkat kepercayaan dari perangkat BYOD berbeda dibandingkan dengan perangkat tradisional, maka akan mempengaruhi desain aplikasi dan distribusi. Disamping itu, karyawan akan mengharapkan aplikasi internal harus mendukung semua perangkat BYOD yang disetujui, tidak hanya sebuah subset. Hal ini berarti bahwa perlu investasi yang lebih dalam pengembangan aplikasi dan pengujian oleh perusahaan, atau pendidikan yang jelas dan komunikasi bagi karyawan pada aplikasi apa saja yang didukung pada perangkat apa, dan mengapa.
Beberapa pertimbangan desain aplikasi dan tata kelola meliputi:

1) Merancang aplikasi mobile untuk mencocokkan tingkat kepercayaan dari perangkat pribadi: Tim pengembangan aplikasi harus memutuskan apakah desain aplikasi mereka berbeda untuk perangkat pribadi dengan perangkat korporasi. Perbedaan ini umumnya berpusat pada bagaimana aplikasi menangani data lokal dan didorong oleh tingkat kepercayaan perangkat target. Sebuah strategi

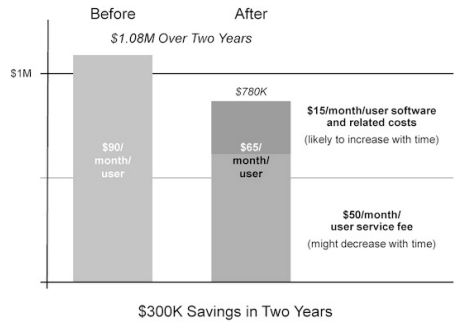
bersama tentu lebih hemat biaya, sementara strategi yang terpisah dapat mengoptimalkan pengalaman pengguna.

2) Memodifikasi ketersediaan katalog aplikasi berdasarkan jenis perangkat: aplikasi internal tertentu mungkin tidak sesuai pada perangkat pribadi untuk alasan keamanan. Sebagai contoh, kasus ponsel; semua perangkat mungkin memiliki akses ke aplikasi manajemen, tetapi hanya perangkat perusahaan tertentu yang dapat mengakses aplikasi proyeksi keuangan.
3) Berkomitmen untuk investasi sumber daya: Akan ada investasi tambahan untuk mendukung aplikasi inti perusahaan pada perangkat pribadi - misalnya, aplikasi sekarang mungkin perlu mendukung sistem operasi dan jenis perangkat yang lebih beragam. Maka tim pengembang aplikasi yang baik harus mendukung serangkaian luas, atau dukungan terbatas yang jelas bagaimana dan mengapa berkomunikasi dengan basis karyawan.
4) Memperbarui kebijakan penggunaan yang dapat diterima: Karyawan akan menuntut kebebasan untuk menggunakan berbagai aplikasi pada perangkat pribadi BYOD mereka. Dalam pikiran mereka, fakta bahwa perangkat ini juga digunakan untuk aplikasi perusahaan tidak membenarkan pembatasan aplikasi pribadi mereka. Oleh karena itu, pembatasan yang jelas diperlukan, seperti untuk tujuan keamanan perusahaan harus dijelaskan kepada karyawan, misalnya, "Aplikasi “A” dikenal dapat mengakses dan mengirimkan daftar kontak pribadi kepada pihak ketiga yang tidak diketahui."
5) Menentukan tingkat penegakan pelanggaran app (notifikasi, kontrol akses, karantina, atau *Selective Wipe*): Sekali lagi, komunikasi yang jelas sama pentingnya dengan kebijakan aktual dan hasil yang ingin dicapai.

4. Pengaruh finansial penerapan *Bring Your Own Devices* (BYOD)

Efisiensi biaya virtualisasi desktop memungkinkan untuk merancang kebijakan pengganti *laptop* yang menghasilkan penghematan yang signifikan untuk IT disamping membantu membiayai biaya perangkat untuk pegawai atau departemen agar dapat berpartisipasi. Dalam sebuah survei terbaru, 40% perusahaan yang berencana untuk memperkenalkan program ini, berniat untuk membayar subsidi kira-kira sama dengan jumlah biaya yang diperlukan departemen IT untuk mendapatkan dan mengelola perangkat yang sebanding. Sedang 31% perusahaan lainnya berencana untuk menawarkan beberapa tingkat kontribusi terhadap biaya keseluruhan yang dikeluarkan oleh Pekerja.[13]

Ada kasus di mana biaya negara saat mobilitas dapat dipotong, seperti dalam kasus umum menggantikan perangkat BlackBerry yang sudah ada yang menyediakan mobile email dan kalender. Sebagai contoh, memindahkan tenaga kerja 500 orang bergerak berjalan perusahaan-disediakan perangkat BlackBerry dengan biaya sebesar $ 90 per bulan untuk hasil perangkat pribadi milik pengurangan 29% dalam biaya keras, menggunakan standar $ 50-per-bulan tingkat penggantian, sementara investasi sekitar US $ 360 per pengguna dalam infrastruktur baru, software dan dukungan (lihat Gambar 1).



Sumber: Gartner (Agustus 2012)

Gambar 1. Sebuah contoh situasi dimana BYO mampu menghemat biaya : Penggantian Blackberry

Dampak ekonomi jangka panjang mungkin berasal dari sumber yang tidak terduga lainnya. Strategi BYOD belum berada di organisasi perusahaan cukup lama untuk dapat secara definitif menilai dampak ekonomi mereka, tapi di sini ada beberapa dimensi penting yang perlu dipertimbangkan:

1) Perangkat keras: Yang paling menarik adalah tidak perlu membeli hardware. Namun, banyak perusahaan besar secara tradisional memberikan subsidi atas pembelian *smartphone* pegawai-nya, sehingga penghematan besar yang sebenarnya bisa diperoleh, menjadi kurang dari yang diharapkan.
2) Biaya yang berlebihan: Ketika karyawan memiliki visibilitas pribadi ke penggunaannya, terutama penggunaan berlebih, perilaku mereka cenderung menjadi lebih bertanggung jawab. Mereka menggunakan perangkat yang lebih hemat saat roaming, dan mereka cenderung waspada akan penggunaannya. BYOD menimbulkan tanggung jawab pribadi.
3) Rencana Layanan: Beberapa organisasi terus memilih untuk membayar layanan penuh, sementara beberapa perusahaan lain pindah ke pemberian peningkatan gaji bulanan tetap untuk pengguna sebagai kompensasi atas biaya layanan yang digunakan, seringkali didasarkan pada tingkat senioritas dan fungsi dalam organisasi. Namun, keunggulan negosiasi dengan operator nirkabel dapat hilang jika model penagihan tidak menyediakan konsolidasi apapun.
4) Produktivitas: Ini lebih sulit untuk dihitung, tetapi akses ke fungsi perusahaan pada perangkat pilihan karyawan, dan bukan dengan perangkat pilihan perusahaan, tidak hanya dapat meningkatkan kepuasan tetapi juga peningkatan produktivitas kerja. Karyawan sekarang memiliki alat yang ingin mereka gunakan untuk pekerjaan yang harus mereka lakukan.
5) Helpdesk: Kebijakan kuno menyatakan bahwa

BYOD akan meningkatkan biaya helpdesk karena fragmentasi penambahan pilihan perangkat. Menerapkan kebijakan helpdesk baru pada program dukungan penuh dan "upaya terbaik" yang sedang berjalan menciptakan kompleksitas tambahan.

6) Implikasi Pajak : Beberapa daerah memiliki implikasi pajak yang berbeda untuk perangkat yang dibiayai perusahaan versus perangkat yang dibiayai secara pribadi. Biaya program BYOD akan dipengaruhi oleh apakah perusahaan memiliki kewajiban untuk mengikat penggantian ke perkiraan persentase penggunaan bisnis, dan bagaimana rinci bahwa audit perlu.

ROI program BYOD adalah kombinasi dari variabel di atas dibandingkan dengan nilai kepuasan karyawan dan produktivitas. Faktor pengaruh eknomi BYOD terpusat pada peningkatan produktifitas, mengelola biaya kompleksitas, dan menyadari nilai penggunaan perangkat pribadi yang lebih bertanggung jawab.

5. Kesimpulan

Sebuah program BYOD sering mengurangi perawatan total yang diperlukan untuk setiap perangkat karena pengguna juga merupakan pemilik. Kebijakan BYOD harus menguraikan secara eksplisit bagaimana berbagai dukungan dan tugas pemeliharaan akan ditangani dan dibayar perusahaan.

Sebagai strategi atas hubungan yang kuat antara tren IT seperti *consumerization, workshifting*, mobilitas dan komputasi awan, BYOD akan terus mengubah cara orang dan organisasi melakukan pekerjaan. Dengan strategi yang tepat, mengaktifkan pengiriman data on-demand, aplikasi dan desktop ke perangkat lain, akan:

1) Memberdayakan pegawai untuk memilih perangkat mereka sendiri sehingga dapat meningkatkan produktivitas, kolaborasi dan mobilitas
2) Melindungi informasi sensitif dari kehilangan dan pencurian selain menanggapi mandat privasi, kepatuhan dan manajemen risiko
3) Mengurangi biaya dan menyederhanakan manajemen melalui self-service provisioning dan manajemen dan pemantauan otomatis
4) Menyederhanakan IT dengan memungkinkan aplikasi yang akan dibangun sekali dan berjalan pada perangkat apapun

Pegawai-pegawai dan departemen-departemen mendapatkan kebebasan untuk memilih perangkat mereka sendiri, termasuk Windows dan Mac ® desktop dan laptop, iOS, Android dan perangkat berbasis Windows mobile, Google Chromebooks dan perangkat mobile RIM ®. Seamless roaming dan pengalaman definisi tinggi di seluruh perangkat, lokasi dan jaringan memastikan kenyamanan optimal dan produktivitas. Keamanan, perlindungan data, dan tata kelola TI yang melekat dalam lingkungan virtual berlaku untuk perangkat BYO sama efektifnya dengan perangkat perusahaan.

Daftar Pustaka

[1] http://en.wikipedia.org/wiki/Consumerization
[2] BYOD on pcworld.com
[3] http://en.wikipedia.org/wiki/Bring_your_own_device
[4] Bring Your Own Technology (BYOT) on maleehome.com
[5] Bjorn Cumps, Stijn Vieane, and Guido Dedene., (2012) "Linking The Strategic Importance of ICT with Investment in Business-ICT Alignment:An Explorative Framework", IGI Global.com DOI: 10.4018/978-1-4666-1779-7.ch003
[6] Nicholas G. Carr, "IT doesn't matter," in Harvard Business review, May, 2003, pp. 41-49.
[7] "IT Strategy Considerations", Hitachi Consulting Strategy Business Forum, September 20th 2006.
[8] Citrix, Workplace of the future; a global market research report, 2012.
[9] Symantec Corporation, 2012 Norton Cybercrime report, 2012.
[10] BYOD Strategies : MobileIron BYOD Withepaper
[11] Best Practices to Make BYOD Simple and Secure : Citrix BYOD Withepaper, 2012.
[12] Ann Bednarz, January 6, 2012, Network World, "Consumerization creates IT management blind spots, increases business risk: survey".
[13] Citrix, Global BYO Index: IT Organizations Embrace Bring-Your-Own Devices, 2011.

Biodata Penulis

Restiadi Bayu Taruno, memperoleh gelar Sarjana Teknik (S.T.), Jurusan Teknik Informatika Universitas Gadjah Mada, Yogyakarta, lulus tahun 2012. Saat ini penulis sedang menempuh pendidikan S2 di Magister Teknologi Informasi Universitas Gadjah Mada dengan minat konsentrasi *Chief Information Officer*.

Wing Wahyu Winarno (edit), memperoleh gelar Sarjana Ekonomi (S.E), Jurusan Akuntansi Universitas Gadjah Mada Yogyakarta, lulus tahun 1987. Memperoleh gelar Master of Accountancy and Financial Information Technology (MAFIS) College of Business, Cleveland State University, Ohio U.S.A., lulus tahun 1994. Memperoleh gelar Doktor pada Pasca Sarjana Ilmu Akuntansi Universitas Indonesia, Jakarta. Saat ini menjadi dosen tetap di STIE (Sekolah Tinggi Ilmu Ekonomi) YKPN, Yogyakarta.

Dani Adhipta (edit), memperoleh gelar Sarjana sains di Jurusan Fisika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Gadjah Mada (1998). Memperoleh gelar Magister Teknik Di Teknik Elektro, Universitas Gadjah Mada (2004). Saat ini menjadi dosen di Jurusan Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada.