

MIGLIORARE LA SODDISFAZIONE DELL'UTENTE FINALE E LA PRODUTTIVITÀ DEL BUSINESS

Considerazioni su COPE
Un'alternativa flessibile e sicura al BYOD

 **BlackBerry**[®]



LE CONSIDERAZIONI SU COPE

Indice

Introduzione	4
COPE: l'alternativa al BYOD	8
COPE: perché ora?	11
Conclusioni	15

La costante adozione delle policy BYOD (Bring Your Own Device) e BYOA (Bring Your Own Application), due dei maggiori catalizzatori del processo di consumerizzazione dell'IT, è fonte sia di ottimismo che di preoccupazione tra migliaia di aziende ed organizzazioni. Dirigenti e manager vedono importanti vantaggi in termini di produttività e redditività. Vantaggi che avranno un impatto sul business con personale completamente mobile e in grado di lavorare da qualunque luogo e in qualunque momento utilizzando i dispositivi e gli strumenti di comunicazione preferiti. CIO e amministratori IT, sebbene condividano i medesimi obiettivi di produttività, nutrono spesso forti perplessità circa la crescente adozione di dispositivi e applicazioni consumer all'interno del flusso di lavoro aziendale che potrebbe comportare potenziali perdite di dati sensibili, rendere i dati aziendali vulnerabili ad attacchi malware ed esporre il business e la dirigenza a costose azioni legali, a scapito anche della reputazione, associate a violazione di privacy o conformità.

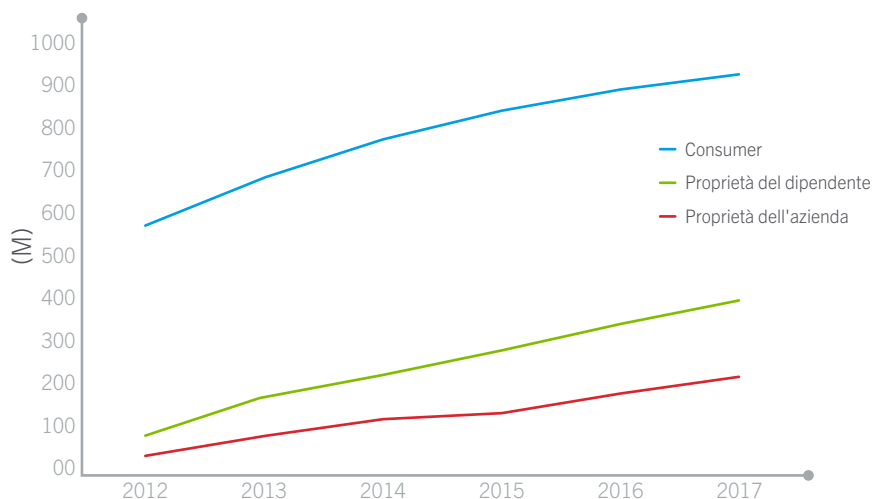
Ma c'è una buona notizia sia per i vertici aziendali che per i CIO: i recenti progressi nel settore EMM (Enterprise Mobility Management) e le emergenti preoccupazioni sulle implicazioni per la sicurezza a lungo termine di BYOD e BYOA, stanno fornendo slancio a un approccio alla mobilità enterprise noto con l'acronimo COPE, o Corporate Owned, Personally Enabled. Andando ad occupare la sfera intermedia tra le opzioni Corporate Owned, Business Only (COBO) e BYOD, COPE offre ai dipartimenti IT un'ampia gamma di strumenti per trovare un equilibrio tra l'esigenza di soddisfare l'utente finale e quella di produttività e sicurezza del business.

Introduzione

La mobilità enterprise è un treno in corsa. Le aziende, testimoni solo di alcune delle positive trasformazioni connesse alla possibilità di lavorare al di fuori dei normali uffici e orari, sono pronte ad accelerare la “mobility” nel prossimo futuro. I manager delle business unit stanno sempre più sperimentando, ad esempio, venditori in grado di fare demo, controllare il livello di scorte e inoltrare ordini sul campo direttamente da un tablet o uno smartphone. Con personale che fa business “al momento”, invece di essere obbligato a finalizzare le transazioni una volta tornato in ufficio per accedere ai sistemi aziendali dall'interno, i vertici aziendali sperano di aumentare sensibilmente produttività e redditività.

Smartphone di proprietà aziendale in aumento

Vendita smartphone nel mondo per tipo di utente, 2012-2017



Il numero di smartphone di proprietà dell'azienda è destinato ad aumentare a una velocità superiore a quella dell'intero mercato. IDC Research ritiene che dei 722,5 milioni di smartphone al mondo nel 2013, 90 milioni di dispositivi (9,4% del mercato totale) siano stati acquistati per uso aziendale. Secondo IDC, nel 2017 gli smartphone corporate saliranno a 234 milioni (15% del mercato complessivo).

Fonte: IDC, Giugno 2013

BYOD *Bring Your Own Device*. Approccio di gestione dei dispositivi mobili aziendali caratterizzato dall'uso di dispositivi personali, in particolare smartphone e tablet, per lo svolgimento di attività lavorative di produttività, elaborazione e comunicazione.

COBO *Corporate-Owned, Business Only*. Approccio di gestione dei dispositivi mobili aziendali in cui un'azienda od organizzazione fornisce ai propri dipendenti un dispositivo mobile dedicato alle attività lavorative di produttività, elaborazione e comunicazione.

COPE *Corporate-Owned, Personally Enabled*. Approccio di gestione dei dispositivi mobili aziendali in cui un'azienda od organizzazione offre ai propri dipendenti la possibilità di scegliere smartphone o tablet di sua proprietà configurati in modo tale da consentire anche attività di elaborazione e comunicazione personali dei dipendenti.

Ma l'elemento propulsivo della mobilità aziendale è il processo di consumerizzazione delle aziende, un fenomeno reso possibile dallo sviluppo di Internet e della banda larga mobile, sinonimo di adozione di policy BYOD da parte di aziende e organizzazioni. Il movimento "Bring Your Own", che si è allargato per includere le applicazioni (BYOA), ha fatto la sua comparsa circa sette anni fa per poi continuare ad acquisire importanza. La società di ricerche di mercato Gartner, infatti, ha previsto che entro il 2017 circa metà dei datori di lavoro richiederanno ai dipendenti di fornire i propri dispositivi.

Il movimento BYOD è ben documentato ed è facile comprendere l'attrattiva esercitata sui vertici delle aziende. Per molti, l'adozione di policy BYOD stimola il personale che utilizza le più recenti innovazioni nei settori Internet ed elettronica di consumo per svolgere il proprio lavoro da qualsiasi luogo e a qualsiasi ora. I dipendenti pagano per dispositivi e abbonamenti voce e connessione dati e molte aziende vedono il BYOD come un meccanismo per ridurre i costi di investimento e di gestione. Dal punto di vista della produttività e del budget, BYOD sembra essere la scelta vincente.

La velocità della "mobilizzazione" dell'azienda, comunque, comporta fluttuazioni continue delle variabili e delle condizioni che definiscono la strategia mobile da parte delle aziende. I recenti progressi nel settore EMM e degli abbonamenti sottoscritti da parte di molte aziende ed organizzazioni per accelerare la mobility dei processi aziendali fondamentali, ad esempio, stanno spingendo alcune aziende a considerare strategie alternative alle policy BYOD.

Alcune società di ricerche di mercato prevedono l'inizio di un progressivo abbandono del BYOD da parte delle aziende. "Il BYOD prevale in molti Paesi ma stiamo andando incontro a un ritorno dell'acquisto direttamente da parte delle aziende che ormai comprendono meglio le difficoltà legate alla sua gestione", suggerisce Strategy Analytics, società internazionale di ricerca, in un rapporto pubblicato alla fine del 2013. "Le preoccupazioni sulla sicurezza indurranno le aziende a rinunciare al BYOD per lasciare che i dipendenti scelgano il proprio dispositivo in alcuni mercati maturi"¹.

Il rovescio della medaglia del BYOD è sempre stato il carico di lavoro inerente le problematiche di risk management a cui va incontro l'IT. Infatti, il BYOD ha dato il via libera a una vera e propria invasione di nuovi dispositivi e applicazioni, che richiedono tutti accesso alle informazioni aziendali strettamente protette. Spesso a corto di personale e oberato di lavoro, l'IT è stato a volte forzato a contenere la miriade di endpoint e applicazioni con rigorose restrizioni od onerosi ostacoli agli occhi degli utenti finali. Queste policy a volte draconiane, insieme alla paura di perdere dati personali o di invasione della privacy, spingono molti utenti finali ad evitare la supervisione dell'IT, ostacolando ulteriormente gli obiettivi di sicurezza dell'azienda.

Se tali condizioni hanno consentito una situazione più "facile" per gli amministratori IT, molti sono comunque stati in grado di gestire i problemi di gestione e sicurezza del BYOD grazie a un equilibrio, possibile se non ottimale, tra sicurezza, soddisfazione dell'utente finale e obiettivi di business. Come è stato accennato prima, comunque, il processo di mobilità del business è stato influenzato da molte variabili e condizioni in evoluzione che probabilmente renderanno sempre più difficile, per l'IT, rendere sicuri gli ambienti corporate senza ostacolare i progressi di produttività che la mobility del personale promette.

¹ Enterprise Mobility Predictions, 2014

Quindi, quali sono i mutamenti imminenti nel panorama della mobilità enterprise che hanno un impatto sull'efficienza del BYOD? Il cambiamento più evidente sarà una notevole espansione ed accelerazione della mobilità dei dipendenti. Se non è già avvenuto, i CIO si dovranno ben presto confrontare con la sfida di rendere sicuri i dati corporate con un numero crescente di dispositivi che si connettono alla rete aziendale. L'accesso mobile sarà allargato a una fetta più ampia del personale e le business unit trasformeranno in senso mobile ulteriori processi lavorativi. Più dispositivi, più utenti e maggiore esposizione dei dati sensibili significano maggiore vulnerabilità a fughe di dati o violazioni della sicurezza mediante i dispositivi mobili.

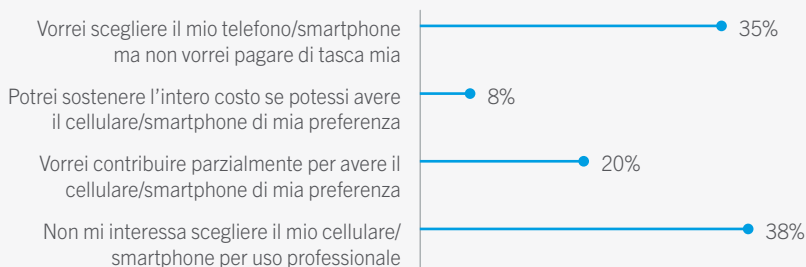
BYOD: creato per il futuro?

La moda del BYOD ha preso vigore negli ultimi anni. Man mano che la mobilità della moderna forza lavoro entra in una nuova fase della sua evoluzione, diventando sempre più parte integrante della competitività e redditività delle aziende, emergono analisi secondo le quali il BYOD, almeno nella sua forma applicativa più libera, pone dei rischi legali e di sicurezza troppo gravi e onerosi perché l'IT possa porvi rimedio senza vanificare il più grande vantaggio del BYOD: la soddisfazione dell'utente che promuove la produttività del dipendente.

Man mano che le organizzazioni adottano la mobilità e permettono ad ulteriori utenti e partner di accedere a importanti informazioni sempre più sensibili e strategiche da dispositivi mobili, la possibilità di perdere dati o subire attacchi aumentano esponenzialmente. Al crescere delle scommesse sulla sicurezza mobile e la produttività del business, aumentano le probabilità che CIO e responsabili IT, in aziende consapevoli dell'importanza della sicurezza, siano restii ad adottare del tutto il BYOD come base della strategia di mobilità enterprise.

Persino la teoria secondo cui una percentuale consistente dei dipendenti potrebbe sostenere la spesa per l'acquisto del dispositivo personale per attività legate al lavoro può non trovare riscontro nella realtà. Uno studio di Forrester Research del 2013, su più di 3.000 lavoratori in Europa e Nord America, ha messo in evidenza che, se da un lato il 35% delle persone che hanno risposto afferma che vorrebbero scegliere il proprio smartphone per uso professionale, dall'altro non vorrebbe invece contribuire per nulla al suo costo. Solo l'8% afferma che lo pagherebbe interamente, mentre il 20% solo per una parte. Le risposte a una domanda simile sui tablet hanno portato risultati che si discostano di pochi punti percentuali da quelle sugli smartphone. I risultati del sondaggio suggeriscono che un approccio alla gestione della mobilità di tipo COPE, che tipicamente fornisce ai dipendenti la possibilità di scegliere tra dispositivi di proprietà dell'azienda, può potenzialmente attrarre gli utenti finali come BYOD.

"Quanto le interessa poter usare il suo telefono cellulare/ smartphone come cellulare/smartphone professionale?"



Fonte: Forrsights Telecom and Mobility Workforce Survey, Q2 2013, Forrester Research, Inc.

Con l'evolversi della mobilità enterprise e la crescente adozione, in futuro possono presentarsi ulteriori questioni da affrontare per il BYOD.

- **Complessità di gestione.** Il BYOD rende più complessa una soluzione di gestione della mobilità enterprise, tra cui gestione di dispositivi e applicazioni, gestione del ciclo di vita delle applicazioni e dei contratti TLC. Maggiore è la varietà di dispositivi e piattaforme che accedono ai dati aziendali, maggiore è il carico di lavoro per l'IT. Secondo un'indagine condotta da Gartner nel 2013, l'81% delle aziende ha riferito che la mobilità ha fatto aumentare il carico di lavoro per l'assistenza clienti che, con l'ingresso di ulteriori dispositivi utente, sarebbe con ogni probabilità ancor più sottoposta a stress¹.
- **Le minacce alla sicurezza sono in aumento.** I dispositivi mobili sono presi sempre più di mira da hacker e altri malintenzionati come porte d'ingresso agli archivi dei dati aziendali. I cyber criminali vanno dove si trova il denaro e man mano che le aziende estendono i confini mobile delle loro reti, i responsabili IT si possono aspettare che i dispositivi mobile rappresentino un obiettivo sempre più allettante per i cyber criminali.
- **Eredità consumer.** Con aziende che aprono progressivamente i propri canali mobile a dati aziendali più sensibili, un numero sempre crescente di informazioni viene archiviato su dispositivi mobili di tipo consumer non concepiti per ambienti sicuri.
- **Possibili vertenze legali.** Sebbene le normative varino da un Paese all'altro, le società sono in generale meglio protette contro le azioni legali da parte di dipendenti inerenti violazioni della privacy o perdita di informazioni nei casi in cui l'azienda sia proprietaria del dispositivo mobile, rendendo più semplice imporre policy che riducano il rischio di contenziosi.
- **Maggiori spese.** Per le aziende che prevedono un rimborso ai dipendenti per l'utilizzo di servizi voce e dati, una policy BYOD impedisce di usufruire di sconti associati all'acquisto di grandi volumi di trasmissione voce e dati.

¹ "The Impact of Mobility on the IT Service Desk" Gartner Luglio 2013

Oltre a respingere le minacce alla sicurezza in ambienti caratterizzati da elevata mobilità, i CIO dovranno anche vigilare per difendersi da problemi legali inerenti conformità a normative o privacy di dipendenti/clienti, in particolare per quanto riguarda dati e applicazioni che si trovano su dispositivi mobili utilizzati a fini professionali. I CIO si trovano a fronteggiare ulteriori difficoltà, legate al variare delle normative e regole in materia di privacy nel mondo. La maggiore complessità delle richieste che l'IT si trova a fronteggiare spingerà probabilmente i CIO a valutare con attenzione se i vantaggi del BYOD non comportino rischi inaccettabili per l'azienda.

Alla ricerca di una soluzione che faccia da complemento o alternativa al BYOD, le aziende guarderanno probabilmente con occhi nuovi a un modello di mobilità enterprise noto come COPE (Corporate Owned, Personally Enabled), un concetto che trova le sue radici alcuni anni orsono in una sorta di compromesso tra la rigidità del modello COBO (Corporate Owned, Business Only) e l'eccessiva libertà del BYOD.

Nel prosieguo del presente documento si offre un approfondimento del modello COPE, confrontato con gli approcci BYOD e COBO, oltre ad alcune informazioni dettagliate su sviluppi tecnologici e di mercato per sensibilizzare i CIO sul controllo delle policy di gestione dei dispositivi: queste policy sono in grado di soddisfare le necessità degli utenti finali e dei manager e al tempo stesso di consentire la serenità dell'IT?

I costi (nascosti) del BYOD

Il taglio dei costi è spesso indicato come il punto di forza del BYOD. La logica a sostegno di una tale affermazione è che le aziende possono risparmiare se i dipendenti sostengono il costo dei dispositivi mobili. Ma, se da una parte la logica che sottende una simile teoria è comprensibile, può fondarsi in realtà su falsi presupposti e, forse, alcune illusioni.

Gran parte del costo reale del BYOD dipende, naturalmente, dalla natura della policy BYOD. Anche se le aziende non pagano i telefoni cellulari dei dipendenti, è altamente probabile che debbano farsi carico degli abbonamenti voce e connessione dati tramite un sistema di rimborso spese, potenzialmente molto più costoso del dispositivo in sé per sé. Talvolta è possibile realizzare risparmi consistenti acquistando grandi quantità di connessione dati e minuti di conversazione. Si tratta di risparmi non consentiti alle aziende che pagano sotto forma di rimborso spese mensile.

Inoltre, una policy BYOD aperta, che deve supportare potenzialmente dozzine di diversi tipi di dispositivi, sistemi operativi e relative versioni,

può introdurre una complessità di gestione di gran lunga superiore ai costi associati alla gestione di un numero di dispositivi e applicazioni più controllato. Tenere traccia di più dispositivi e piattaforme può richiedere un più numeroso staff di assistenza tecnica o la spesa aggiuntiva per l'installazione di prodotti MDM o EMM per coprire l'intero spettro di smartphone e tablet.

Ma sono i costi imprevisi legati a potenziali falle nella sicurezza del BYOD a potersi rivelare i più onerosi. Sebbene nessuna azienda sia mai completamente protetta dalla perdita o dal furto di dati aziendali o della proprietà intellettuale, il livello di protezione offerto da una policy sui dispositivi mobili più conservativa è spesso superiore a quello che ragionevolmente ci si può aspettare in un ambiente BYOD. Mentre da una parte è quasi impossibile attribuire un prezzo alla perdita di proprietà intellettuale, la divulgazione di informazioni altamente riservate a un concorrente può avere conseguenze disastrose.

Un altro costo BYOD inatteso può essere associato a spese legali. La gravità varia da paese a paese, e le sanzioni finanziarie connesse a

violazioni della conformità e delle normative spesso raggiungono cifre a sei zeri. E, se nessuna policy sui dispositivi mobili enterprise è infallibile, maggiore è il loro numero, minore è il controllo che l'IT può avere su di essi e maggiore la probabilità che i contenuti vadano persi o siano sottratti. Stessa cosa vale per le vertenze legali sulla privacy dei dipendenti. In alcune nazioni d'Europa, ad esempio, le sanzioni per il controllo o l'eliminazione delle informazioni personali del dipendente possono essere pesanti. Il numero di azioni legali associate ad invasione della privacy e la probabilità che tali azioni portino come risultato il pagamento di indennità tendono a diminuire se il dispositivo è di proprietà dell'azienda, invece che del dipendente.

Non si tratta solo di una questione di denaro, in ogni caso. Un'infrazione della sicurezza può danneggiare in modo grave la reputazione di un'azienda, soprattutto se gestisce informazioni sensibili dei clienti, come nel caso di servizi finanziari o del settore salute. Le azioni legali indette da dipendenti possono rappresentare anche un grosso problema in fase di ricerca di personale.

COPE: The BYOD Alternative

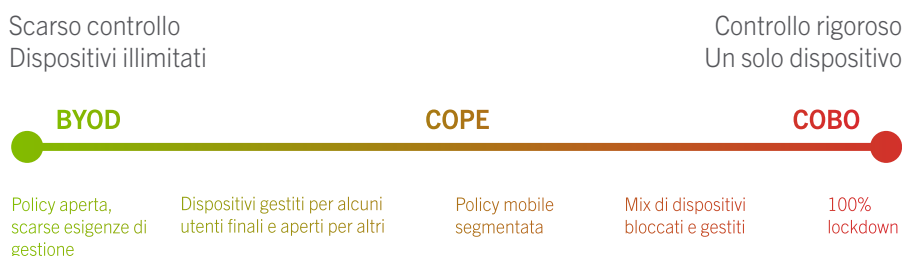
L'approccio COPE alla mobilità enterprise è l'opposto del BYOD, che, nella sua forma primitiva, rappresenta un vero e proprio incubo per i dipartimenti IT. Spesso indicato come il "Far West" della mobilità enterprise, uno scenario BYOD libero è caratterizzato da personale motivato che accede ai dati attraverso una gamma di smartphone e tablet su cui sono installate numerose versioni di un gruppo ristretto di piattaforme mobile, la maggior parte delle quali concepite per ambienti consumer. Mancando le risorse per stare al passo della varietà di dispositivi e la rapida introduzione di upgrade dei sistemi operativi, gli amministratori IT sono alla perenne rincorsa per il controllo dei mobile agent che accedono alla rete aziendale e per mitigare il rischio che dati sensibili escano al di fuori dell'azienda o che hacker malintenzionati vi possano accedere.

COPE rappresenta anche un'alternativa all'approccio COBO, spesso caratterizzato da policy utente ultra-conservative. L'azienda è proprietaria del dispositivo e stabilisce in modo rigoroso come questo possa essere utilizzato dai dipendenti. Il divieto assoluto di fare uso personale dello smartphone, del tablet o di un dispositivo più robusto è la clausola più diffusa nella maggior parte delle policy utente di tipo COBO. È stato solo con l'avvento della banda larga mobile (che ha creato un canale diretto tra dispositivi mobili e Internet), che si è messo in evidenza il più importante rovescio della medaglia dell'approccio COBO. Con il divieto di utilizzare i dispositivi forniti dall'azienda come canali per comunicazioni commerciali, social media e altri siti Web, i dipendenti hanno iniziato presto a portare sul posto di lavoro i propri dispositivi, con l'idea di utilizzare un unico dispositivo per comunicazioni e attività di elaborazione informatica professionali e personali.

E COPE è nato proprio a metà strada tra la rigidità di COBO e l'anarchia del BYOD. Gran parte dell'interesse di COPE sta proprio nel supportare un'ampia gamma di possibili usi. In generale, comunque, un piano di mobilità enterprise di tipo COPE offre agli utenti finali la possibilità di scegliere tra una gamma di dispositivi di proprietà aziendale approvati e preventivamente configurati con ambienti lavorativi e personali separati. Molti manager IT lo vedono come la pretesa di avere tutto e il suo contrario. Combina essenzialmente il controllo di COBO con le attrattive di BYOD. Ad esempio, può offrire libera produttività e una superiore soddisfazione dell'utente, senza la noiosa complessità e le vulnerabilità associate alle policy BYOD poco regolate.

Anche se COPE viene descritto sempre come l'opposto del BYOD, in realtà una tale definizione non coglie il fatto che entrambi gli approcci inseguano lo stesso obiettivo: migliorare l'esperienza d'uso del personale con un dispositivo mobile che possa essere utilizzato in modo sicuro e allo stesso tempo per lavoro e attività di elaborazione informatica e comunicazione personale. I due approcci mirano allo stesso risultato procedendo in direzioni opposte. Con BYOD viene esteso all'ambiente lavorativo l'uso di un dispositivo consumer. Al contrario, COPE parte da una prospettiva professionale, in cui l'IT preconfigura una parte del dispositivo per uso personale. Dal punto di vista della gestione e della sicurezza, è facile comprendere la ragione per cui COPE viene visto sempre più dai CIO come un'interessante alternativa a BYOD.

Per i dispositivi mobili corporate gli approcci coprono un ampio spettro, dai più conservativi ai più tolleranti, dove COBO, che forza il blocco di smartphone, tablet e altri dispositivi per restringerne l'uso esclusivamente ad applicazioni e contenuti corporate, si colloca al primo estremo. Le policy BYOD che, in casi limite possono anche non porre alcuna limitazione al numero e tipo di dispositivi che i dipendenti utilizzano per portare avanti il business, ricade invece all'estremo opposto. Si può quindi pensare a COPE come a una policy in grado di ridurre la rigidità di certi approcci COBO o rafforzare i controlli un po' troppo lassi del BYOD, prospettiva che si pone al centro dello spettro.



Pur costituendo quest'idea un eccesso di semplificazione, COPE può anche essere visto come un set di policy flessibili e adattabili intermedie tra il blocco corporate e il BYOD. Consentendo la fusione di policy conservative e più aperte, COPE rappresenta un modo per raggiungere il principale obiettivo del dipartimento IT: proteggere le informazioni dell'azienda da accessi non autorizzati, malware e fuga di dati, senza porre eccessive restrizioni sui tipi di dispositivi e applicazioni a disposizione delle persone che lavorano che potrebbero rallentare il business.

Da un punto di vista pratico, COPE offre all'IT l'opportunità di imporre un significativo livello di gestione e uniformità di policy nell'intera azienda, solitamente caratterizzata da dozzine di diversi profili di rischio e casi di impiego. Anche i singoli dipendenti, forniti di molteplici dispositivi (controllati da un piccolo gruppo di sistemi operativi) possono usufruire della produttività e della protezione della privacy di COPE senza sovraccaricare l'IT con una gestione complessa o esporre l'azienda a rischi in materia di sicurezza.

Come accade con quasi ogni aspetto della mobilità enterprise, anche l'adozione di COPE ha un punto critico: tarare adeguatamente l'approccio. Se l'IT, ad esempio, non riesce a stilare un elenco di dispositivi approvati sufficientemente ampio da soddisfare le aspettative di una buona fetta di utenti finali e offre applicazioni corporate la cui usabilità e produttività sono scarse rispetto a quella delle app disponibili su Internet, gli utenti si rivolgeranno al download di applicazioni dai siti commerciali e utilizzeranno i propri dispositivi per il lavoro.

Implementazione corretta di COPE

Data la sua adattabilità, il successo o il fallimento dell'adozione di COPE dipende fortemente dalla sua implementazione. Ecco alcuni esempi di best practice e linee guida:

- Fornire un elenco di dispositivi approvati al tempo stesso sufficientemente ampio da soddisfare i dipendenti e ristretto da non sottoporre a stress eccessivo il personale IT per ciò che riguarda la gestione di dispositivi e applicazioni né introdurre elementi di rischio
- Ricorrere al concetto di "container", consentendo la completa separazione degli ambienti lavorativi e personali e offrendo ai dipendenti un libero controllo della parte di dispositivo riservata ad uso personale.
- Creare un documento che descriva la policy sui dispositivi mobili con una chiara definizione di responsabilità degli utenti e restrizioni concernenti la sicurezza in entrambi gli ambienti, professionale e personale.
- Lasciare che il core business detti la policy mobile. Quale approccio (COBO, BYOD o COPE) porterà il maggior equilibrio tra sicurezza, produttività e soddisfazione dell'utente? Quale favorirà le iniziative di mobilitazione del personale?
- Non partire dal presupposto che la proprietà del dispositivo costituisca una protezione assoluta dalle accuse di invasione della privacy da parte del personale. Le normative continuano ad essere infatti poco chiare al riguardo; e mentre la proprietà consente alcune misure di protezione in caso di eliminazione di dati personali, l'IT deve continuare ad operare col guanto di velluto quando gestisce dati personali.
- Indipendentemente dal livello di flessibilità della policy COPE adottata, bisogna attendersi che un certo numero di utenti estranei continui ad accedere ai dati aziendali con i propri dispositivi. Estendere le policy per gestire questo fatto e minimizzare il rischio.
- Decisione lasciata agli utenti finali. L'erroneo assunto sulle preferenze degli utenti finali ha rovinato centinaia di startup. Ciò che l'IT ipotizza essere accettabile e adottabile da parte dei dipendenti può anche rivelarsi del tutto fuori strada.
- Considerare attentamente COPE per l'implementazione in ambienti multinazionali. La gravità delle implicazioni legali connesse all'eliminazione di informazioni personali dei dipendenti sugli end point utilizzati per lavoro, varia molto da un Paese all'altro. E l'adozione di una policy COPE in tutta l'azienda consente la migliore protezione contro i procedimenti legali in un ambiente così poco omogeneo.
- Per ambienti caratterizzati da un ampio spettro di casi di impiego e profili di rischio, oltre che di dispositivi e tipi di sistema operativo, un approccio COPE offre la flessibilità necessaria a coprire tutte le sfaccettature di un ambiente di mobilità enterprise altamente stratificato senza sacrifici in termini di sicurezza.

Il più importante obiettivo di qualsiasi policy COPE è assicurare che la maggioranza degli utenti sia soddisfatta dai dispositivi messi a disposizione dall'azienda sia dal punto di vista professionale che personale.

COPE: perché ora?

L'evoluzione della mobilità enterprise sta portando a una convergenza di condizioni verso un ambiente positivo per la potenziale adozione su larga scala delle policy COPE. I tre principali elementi sono le preoccupazioni per la praticabilità del BYOD nel lungo periodo di fronte all'impetuosa accelerazione prevista del processo di mobilità del personale; la maturità delle tecnologie di gestione di applicazioni e dispositivi che consente a un singolo dispositivo di "mescolare" informazioni personali e inerenti il lavoro; la capacità di COPE di permettere agli amministratori IT di imporre policy di mobilità enterprise flessibili e dettagliate che soddisfino le esigenze di usabilità e produttività senza lasciare l'azienda in balia di attacchi, fughe di dati o costose azioni legali.

BYOD: le questioni di lungo termine

BYOD rappresenta l'estremità più "libera" dello spettro di policy per i dispositivi corporate. Etichettato come il "Far West" della gestione della mobilità enterprise, il BYOD è popolare tra utenti e responsabili IT perché promuove l'uso di dispositivi personali e applicazioni consumer per lo svolgimento di attività correlate al lavoro. I dipendenti sono presumibilmente più produttivi quando utilizzano strumenti a loro familiari, e probabilmente disponibili a lavorare per orari più prolungati. Il BYOD è stato anche definito da molti "IT friendly" per la sua capacità di ridurre i costi di investimento e di gestione, alleggerendo lo staff IT dell'ingrato lavoro di gestione di parte o tutti i dispositivi mobili.

In ogni caso, al maturare e al diffondersi del BYOD, emergono informazioni secondo le quali, almeno nella sua forma meno controllata, pone importanti difficoltà di gestione, rischi per la sicurezza e legali e può essere meno economico di quanto si creda, spingendo così molte aziende a cercare un'alternativa più controllata.

Divisione lavoro/vita privata

L'introduzione e la separazione in compartimenti stagni, che consente al business di isolare i dati corporate da quelli personali sui dispositivi mobili, è uno dei punti di forza di COPE. Essendo maturata la tecnologia di "containerizzazione", (il che fornisce all'IT meccanismi più efficienti e sofisticati di separazione degli ambienti per profili d'uso professionale e personale sui dispositivi mobili), COPE sta diventando sempre più interessante agli occhi del CIO. La containerizzazione rende probabilmente più accettabili le policy COPE per i dipendenti che preferiscono il BYOD superando la loro riluttanza ad esporre informazioni personali sui loro dispositivi al dipartimento IT. Se gli utenti possono essere rassicurati sul fatto che le loro informazioni siano separate dai dati corporate e che le attività di gestione, come l'eliminazione dei dati, possano limitarsi alla porzione del dispositivo dedicata al lavoro, i dipendenti possono essere più inclini ad utilizzare un dispositivo di proprietà dell'azienda per comunicazioni ed attività di elaborazione informatica personali.

Al tempo stesso, la containerizzazione è vista da alcuni responsabili IT come strumento per fare chiarezza nel caos gestionale associato all'approccio BYOD. L'offerta di containerizzazione che consente la gestione comune di sistemi operativi diversi potrebbe semplificare molto la gestione dei dispositivi e delle applicazioni per gli specialisti IT

Nuova flessibilità

COPE introduce nuova flessibilità ed adattabilità nella battaglia senza fine dei responsabili IT per trovare l'equilibrio perfetto tra mitigazione del rischio, esigenze di business e soddisfazione dell'utente. Anche se gli approcci alla mobilità enterprise di COBO e BYOD possono presentare sfumature diverse, COPE offre un più ampio spettro di diverse implementazioni, mettendo così a disposizione dell'IT soluzioni più duttili. Le aziende soggette a rigorosi requisiti di audit e conformità, ad esempio, possono richiedere di imporre regole più rigide per l'accesso alla rete o la condivisione dei dati. Ed è possibile inoltre che vogliano ridurre le possibilità di scelta dei dispositivi per gli utenti che gestiscono dati sensibili. Altri possono voler far avvicinare la loro policy di mobilità enterprise al tradizionale ambiente BYOD, caratterizzato da dispositivi e piattaforme eterogenei e minore sicurezza.

Ulteriori vantaggi

Da un lato, la capacità di far sì che un dispositivo sia utilizzato a scopi sia professionali che personali e la maggiore sicurezza dei dati corporate da fughe o compromissioni attraverso backdoor dei dispositivi mobili sono i principali punti di forza di un modello di gestione della mobilità di tipo COPE. I CIO adottano questo approccio per trovarsi nella posizione di introdurre ulteriore sicurezza, vantaggi gestionali e di risparmio non disponibili in un ambiente BYOD, tra cui:

- Riduzione del caos di dispositivi: COPE fornisce all'IT la capacità di limitare la varietà di dispositivi e piattaforme che accedono alle informazioni dell'azienda e di ridurli a un numero gestibile. Offrendo agli utenti una gamma di popolari dispositivi tra cui scegliere modesta ma significativa, l'IT può riuscire a raggiungere il duplice obiettivo di soddisfare la base di utenti e ridurre fortemente la complessità di gestione di dispositivi e applicazioni.

Mobility, alcuni esempi di vertenze legali

Banda larga mobile e proliferazione dei dispositivi hanno promosso ambienti in cui è possibile lavorare in ogni momento e ovunque ci si trovi. Ma i sostenitori stanno cominciando a fare un passo indietro, spinti dalla presentazione di reclami o dalla ricerca di indennizzi attraverso vertenze per potenziali violazioni della privacy o delle leggi sul lavoro. La tecnologia rende indistinto il confine tra vita privata e professionale mentre le vertenze sulla definizione dei limiti sono destinate probabilmente ad aumentare. E un tale panorama in continua evoluzione per le aziende viene complicato dalle differenze di normative, cultura e morale tra i diversi paesi.

In generale le aziende sono più protette contro azioni legali da parte dei dipendenti per violazione della privacy o perdita di informazioni se hanno fornito dispositivi mobili di proprietà aziendale, facilitando così l'imposizione di policy che riducano il rischio di azioni legali. Anche se le normative sulla mobilità enterprise sono relativamente recenti, gli inizi di BYOD e il processo di mobilità del personale hanno già prodotto alcune importanti cause legali che possono mettere in guardia.

Sarebbe stato opportuno, ad esempio, che il Dipartimento di polizia della città di Chicago avesse applicato una policy sull'uso degli

smartphone in dotazione ai funzionari di polizia. Nel 2010, i poliziotti che sostenevano che messaggi e chiamate sugli smartphone al di fuori dell'orario di lavoro prestabilito costituissero ore di straordinario, hanno fatto causa all'amministrazione cittadina chiedendo di pagarle a titolo retroattivo secondo le prescrizioni del Fair Labor Standards Act. Mentre i funzionari hanno affermato pubblicamente che l'attività sugli smartphone rientrava tra le normali responsabilità degli agenti, sarebbe stato possibile evitare il procedimento legale adottando una policy formulata con attenzione o configurando gli smartphone in modo tale che non fossero disponibili per attività inerenti il lavoro al di fuori dell'orario di servizio.

Un aumento delle azioni legali connesse all'impiego degli smartphone al di fuori dei normali orari di lavoro ha suggerito a uno studio legale californiano che si sta specializzando in diritto del lavoro e delle relazioni sindacali di dedicare un blog all'argomento. Il post pubblicato il 2 maggio 2013 sul California Public Agency Labor & Employment Blog riguardante l'uso degli smartphone nelle ore di straordinario suggerisce alle aziende di prendere diverse precauzioni per evitare processi. Nell'elenco anche il consiglio di ridurre il rischio controllando l'accesso dei dipendenti alla rete

e alla posta elettronica. E al di fuori degli Stati Uniti le potenziali cause legali sulla gestione dei dispositivi mobili sono ancora di più. In molti paesi europei, infatti, i diritti dei lavoratori e la privacy dei cittadini sono particolarmente protetti.

Alcuni agenti di polizia, questa volta in Svezia, sono finiti nei guai con la legge dopo aver inavvertitamente incluso un civile in una chat riguardante delle indagini in corso. L'incidente, riferito in numerosi rapporti pubblicati nel febbraio 2014, ha coinvolto diversi ufficiali di polizia che utilizzavano una comune applicazione di messaggistica di tipo consumer per scambiare comunicazioni e condividere immagini relative ad indagini in corso. Anche se, apparentemente, nessuna informazione sensibile sembra sia stata divulgata al di là del professore universitario che era stato inavvertitamente incluso nella chat di gruppo, fughe di informazioni di questo tipo da parte di agenzie governative possono facilmente comportare cause legali e danno alla reputazione dell'agenzia oltre che andare ad intaccare la fiducia dei cittadini. Un approccio COPE alla gestione della mobilità enterprise offre diverse opzioni per ridurre o eliminare il rischio che informazioni sensibili sfuggano attraverso canali pubblici

- **Ridurre i costi:** acquistando grandi lotti di dispositivi e piani di traffico voce e dati, le aziende possono usufruire di sconti sulla base del volume. Si tratta di una prospettiva interessante soprattutto per quelle aziende che rimborsano i dipendenti per l'acquisto dei dispositivi e degli abbonamenti di traffico voce e dati.
- **Inasprire il controllo dei contenuti:** una policy COPE, che implica solitamente la preconfigurazione da parte dell'IT dei dispositivi mobili con partizioni sicure per separare dati lavorativi e personali, consente alle aziende di controllare i contenuti corporate. Oltre alle preoccupazioni per la sicurezza associate allo scarso controllo dei dati e delle comunicazioni inerenti il lavoro, è fondamentale anche una rigorosa tutela dei contenuti enterprise per il rispetto della conformità ai requisiti regolatori, come eDiscovery o regolamenti di settore, incluso l'Health Insurance Portability and Accountability Act (HIPAA) o requisiti di sorveglianza recentemente imposti alla comunità finanziaria USA sulla scia della crisi economica del 2008.
- **Centralizzare il controllo:** una policy COPE consente un ambiente di gestione efficiente che porta all'imposizione di policy valide nell'intera azienda più di quanto faccia BYOD, che spesso richiede policy separate per ogni business unit. COPE permette l'applicazione di policy e regole di governance standard per tutta l'organizzazione, contribuendo in tal modo alla riduzione dei costi connessi alla complessità di gestione.

COPE: non si tratta di una panacea

Nonostante le sue interessanti caratteristiche in termini di efficiente equilibrio tra interesse del business, usabilità ed obiettivi di gestione del rischio in aziende di ogni dimensione, COPE non risolve i problemi di tutte le aziende. È possibile che alcune organizzazioni, a seconda delle dimensioni e dell'importanza del livello di sicurezza, preferiscano l'apertura del BYOD e che altre inciampino nella flessibilità di COPE, trovando difficile mettere a punto le policy per raggiungere un equilibrio soddisfacente tra esigenze di IT, vertici aziendali e dipendenti.

Trovare il giusto numero e mix di dispositivi approvati, ad esempio, può non essere cosa semplice. Gli amministratori IT che non riescono ad offrire agli utenti una sufficiente varietà di dispositivi facilmente vanno incontro a reazioni negative da parte del personale che ricorre sempre più ai propri. Anche l'incapacità di supportare alcuni sistemi operativi può creare ulteriori problemi. Mentre Blackberry, iOS e Android dominano lo spettro di piattaforme mobile nella maggior parte delle aziende, altre piattaforme godono di popolarità in alcuni mercati ed aree geografiche. Le aziende che non supportano tali piattaforme non saranno in grado di attirare gli utenti finali verso un modello di mobilità enterprise di tipo COPE.

In un certo senso, COPE potrebbe non essere visto come strategia di policy per i dispositivi mobili ma semplicemente come una variazione di policy BYOD o a più stretto controllo dell'azienda. Una strategia di livello intermedio, caratterizzata soprattutto da un alto numero di variabili e combinazioni, potrebbe invece rivelarsi troppo complessa e costosa.

Conclusioni

È finito il tempo in cui l'assegnazione di un dispositivo mobile significava solo lavoro e niente tempo libero. La gestione della mobilità enterprise è evoluta al punto in cui anche i settori altamente "regolati" hanno la possibilità di consentire ai dipendenti di utilizzare i dispositivi dell'azienda in dotazione per attività di elaborazione informatica e comunicazione, come social media, giochi e altre forme di intrattenimento digitale. Simili progressi nella gestione dei dispositivi mobili e delle applicazioni, insieme alla rapida accelerazione del processo di mobilitazione del personale e il loro impatto sulla capacità di un'azienda di rendere sicuri i dati archiviati su una varietà sempre maggiore di dispositivi di proprietà dei dipendenti sta generando un impulso di interesse per complementi e alternative a BYOD.

COPE sta conoscendo un nuovo slancio come modello di gestione dei dispositivi mobili enterprise grazie alla sua capacità di combinare la libertà e la flessibilità di BYOD con il controllo e la sorveglianza di COBO. Elemento fondamentale del richiamo di COPE è l'offerta di una potenziale soluzione al rompicapo che le aziende si trovano ad affrontare quando si avventurano in ambiziose iniziative di mobilitazione del personale: come fornire la giusta misura di protezione delle informazioni sensibili dell'azienda senza provocare un deterioramento dell'esperienza utente o interferire con la capacità di massimizzare la produttività.

Mentre il BYOD è stato e continua ad essere adottato dalle aziende per la sua capacità di migliorare la produttività del personale, pone anche di fronte a rischi per la sicurezza e di gestione che talvolta hanno creato tensione tra l'IT, i vertici aziendali e gli utenti finali. I responsabili IT di settori come quello degli enti pubblici, dell'education, dei servizi sanitari, finanziari e legali, sono stati sommersi dal BYOD per via della loro incapacità di sanzionare in modo sicuro l'uso personale dei dispositivi aziendali. COPE, con la sua capacità di consentire la configurazione di smartphone, tablet e altri dispositivi mobili aziendali per comunicazioni e attività informatiche personali, offre una via per allineare in modo del tutto nuovo i vari clienti a un interesse per la mobilitazione dell'azienda.

Le soluzioni di enterprise mobility management di BlackBerry, leader mondiale nel settore delle comunicazioni mobile, supportano un ampio spettro di policy con un equilibrio ottimale tra gestione del rischio, produttività del business e soddisfazione dell'utente finale su piattaforme BlackBerry, iOS e Android.

La capacità di BlackBerry di supportare un ambiente COPE è stata documentata in un rapporto del 2014 di Gartner Inc. dal titolo "Protecting Enterprise Information on Mobile Devices, Using Managed Information Containers". Nel documento si afferma che "BlackBerry si avvicina ad offrire un prodotto per supportare COPE. I dispositivi BlackBerry 10 con BlackBerry Enterprise Service 10, Service Pack 2, includono uno spazio personale separato da quello lavorativo sul dispositivo; possono inoltre essere definite policy su ciò che l'utente è autorizzato a fare all'interno dello spazio personale. Altri prodotti di mobile management non supportano un tale modello"

BlackBerry Enterprise Service 10

BES10 è una piattaforma unificata multi sistema di gestione dei dispositivi, delle applicazioni e dei contenuti con sicurezza e connettività integrate che consentono di gestire efficacemente gli ambienti di mobilità enterprise complessi. Concepito pensando alla sicurezza, BES10 facilita la gestione di dispositivi BlackBerry, iOS e Android corporate e BYOD da un'unica console di gestione. La perfetta divisione fra contenuti professionali e personali tiene conto, senza alcun compromesso, delle esigenze dell'utente finale e dell'azienda.

BlackBerry Balance

La tecnologia BlackBerry® Balance™ offre ai dipendenti la libertà e la privacy che desiderano per il loro uso personale e consente al tempo stesso la sicurezza e la gestione necessarie per l'uso professionale. È il meglio per entrambi i mondi, già disponibili senza soluzione di continuità in ogni smartphone BlackBerry® 10 e gestiti attraverso BlackBerry Enterprise Service 10. Le app e le informazioni personali e professionali sono mantenute separate e

l'utente può semplicemente passare dallo spazio personale a quello professionale.

Secure Work Space per iOS & Android

Secure Work Space è un'opzione di connettività sicura che offre un livello superiore di controllo e di sicurezza ai dispositivi iOS e Android™, tutti gestiti tramite la console di amministrazione BES10. Le applicazioni gestite sono sicure e separate dalle applicazioni e dai dati personali, fornendo app e-mail, calendario e contatti integrati, un browser sicuro di livello enterprise e assicurano la visualizzazione e la modifica degli allegati con Documents To Go™.