Tendenze e percezioni della consumerizzazione mobile

Sondaggio dei dirigenti IT e dei CEO

RAPPORTO FINALE

CONFRONTI: BATTERIE 1 E 2

REDATTO PER:

TREND MICRO, INC.

DA:

DECISIVE ANALYTICS, LLC

Cheryl Harris, Ph.D.

Responsabile della ricerca

Decisive Analytics, LLC

575 Madison Ave, 10th Floor

New York, NY 10022

917.628.6167

SOMMARIO

SINTESI

Panoramica e obiettivi

L'obiettivo complessivo del presente progetto consiste nel valutare la consapevolezza dei problemi legati alla consumerizzazione delle IT/dell'informatica all'interno dell'azienda e nell'approfondire le conoscenze su**:**

- **Atteggiamenti**
- **Percezioni**
- **Sviluppo delle politiche interne legate alla consumerizzazione**
- **Altre preoccupazioni emergenti**

L'***"IT consumer"*** è stata definita come una significativa tendenza economica trasversale in base a uno studio recente (DELL/KACE, *CIO Magazine*, 15 settembre 2011) che ha dimostrato che per l'87% dei dirigenti, i dipendenti utilizzano i dispositivi personali per fini di lavoro, con attività che vanno dalle funzioni e-mail al calendario, da ERP a CRM. Ciò ha esercitato una certa pressione sulla direzione ai fini dell'elaborazione di politiche efficaci ai fini dell'integrazione dei dispositivi personali, dei servizi in-the-cloud e delle altre manifestazioni di "IT consumer" sul posto di lavoro.

Per meglio comprendere l'impatto di questa trasformazione sull'ambiente IT di lavoro, e per scoprire come i dirigenti stanno scendendo a patti con questa realtà, lo studio si è focalizzato sui dirigenti che sono stati coinvolti in modo diretto e in tempi recenti nella valutazione dell'impatto della consumerizzazione presso la loro azienda e/o nell'assunzione di decisioni sulle politiche relativamente alla stessa.

Metodologia

È stato condotto un sondaggio online che ha coinvolto dirigenti IT e CEO di grandi aziende (almeno 500 dipendenti) situati negli Stati Uniti, nel Regno Unito e in Germania. La prima batteria di interviste è stata condotta tra il 3 e l'11 gennaio 2012 e la seconda tra il 10 e il 20 aprile 2012. Questa seconda batteria ha interessato un nuovo campione che non aveva preso parte alla prima. Il sondaggio originario è stato in gran parte conservato per la seconda batteria, insieme ad alcune nuove domande selezionate.

Confronto di batterie per gruppi intervistati

	Batteria 1 *N=*	*Batteria 2* *N=*
CEO	**26**	**21**
Dirigente IT senior	**410**	**415**
Totale	**436**	**436**

Batteria 1 *(gennaio 2012)*
In totale sono stati intervistati 436 dirigenti senior. Sono state condotte 410 interviste con dirigenti IT (50% degli Stati Uniti, 25% del Regno Unito e 25% della Germania). Altre 26 interviste sono state rivolte esclusivamente a CEO di aziende più grandi negli stessi tre paesi.

Batteria 2 *(aprile 2012)*
In totale sono stati intervistati 436 dirigenti senior. Sono state condotte 415 interviste con dirigenti IT (50% degli Stati Uniti, 25% del Regno Unito e 25% della Germania). Altre 21 interviste sono state rivolte esclusivamente a CEO di aziende più grandi negli stessi tre paesi.

Profilo: batterie combinate

Gli intervistati comprendevano dipendenti di aziende da un minimo di 500 a più di 20.000 dipendenti negli Stati Uniti, nel Regno Unito e in Germania. L'attività primaria delle aziende presso cui erano impiegati comprendeva contabilità, servizi commerciali, progettazione, governo, trasporti e aziende municipali; il 15,5% complessivo dichiarava di far parte del settore manifatturiero mentre un altro 15,9% descriveva l'attività principale della propria azienda come consulenze informatiche o integrazione di sistemi.

825 intervistati erano amministratori IT senior e 47 erano i CEO della rispettiva azienda. I ruoli più comuni nell'ambito IT erano quelli di responsabile/ amministratore (30,6%), CIO/CSO/CTO (20,9%) e vicepresidente/direttore della sicurezza IS/IT (20,3%).

Gli intervistati dovevano avere una certa influenza sulle decisioni relative ai dispositivi che i dipendenti dell'azienda potevano o meno utilizzare per accedere alla rete aziendale. La maggior parte dei dirigenti IT (62,3%) ha dichiarato di essere il principale responsabile di tali decisioni. Ovviamente, quasi tutti i CEO (93,6%) hanno affermato di essere i principali responsabili di queste decisioni.

Prassi BYOD e motivi che guidano la scelta

Quasi tutte le aziende (76,7%) dello studio consentono ai dipendenti di utilizzare i propri dispositivi personali, quali laptop, netbook, smartphone e tablet, per le attività lavorative.

La percentuale di dirigenti che ha affermato con più frequenza di adottare l'approccio BYOD è stata quella degli statunitensi (80%), seguiti dagli omologhi britannici (70,8%) e dai tedeschi (75,4%). È interessante notare che i dirigenti con meno di 45 anni hanno dichiarato più spesso che le loro aziende consentono ai dipendenti di utilizzare i propri dispositivi al lavoro.

Quasi tutte le aziende intervistate adottano una politica di sicurezza IT per i dispositivi di proprietà dei dipendenti che accedono alla rete aziendale (89,7%) e impongono l'uso di dispositivi presenti in elenchi preapprovati e/o che sono preapprovati e con software di protezione installato (53,7%). Programmano inoltre di isolare le applicazioni aziendali e/o i dati quando vengono utilizzati dispositivi personali in ambito di lavoro (71,2%). Inoltre, più dell'80% impone ai dipendenti di installare software di protezione sui dispositivi personali.

I CEO sono utenti entusiasti di molti dispositivi mobili: l'84,8% di loro afferma di avere utilizzato gli smartphone al lavoro e il 73,7% dei dirigenti IT dichiara di aver fatto altrettanto. Il secondo dispositivo citato più di frequente è il laptop (78% per i CEO, 68% per i dirigenti IT), seguito da iPad o tablet (82,6% per i CEO, 45,2% per i dirigenti IT). Circa un terzo ha affermato di utilizzare software o app dei dispositivi mobili e circa la stessa percentuale ha dichiarato di utilizzare soluzioni di archiviazione dati online o in-the-cloud. Quasi la medesima proporzione ha riferito di utilizzare Facebook (32,4%), LinkedIn (20,4%), Twitter (18,8%) o YouTube (13,1%). Tuttavia sono stati circa il doppio i CEO che hanno dichiarato di usare YouTube rispetto ai dirigenti IT.

Esistono più ambienti operativi associati ai dispositivi mobili di fascia consumer e molte aziende limitano fortemente quelli a cui consentono l'uso nell'ambito della rete aziendale. I dispositivi personali consentiti più diffusi sono risultati essere Android (69,3%), BlackBerry (69,2%), quindi iOS (53,6%), Windows (50%) e Symbian (24%).

Alla richiesta di classificare i sistemi operativi succitati in base a sicurezza e gestibilità, BlackBerry è risultato al primo posto seguito da iOS al secondo e Android in terza posizione. Windows è finito al quarto posto e Symbian in coda.

Molte poche aziende hanno dichiarato che tutti i dispositivi utilizzati in azienda sono di proprietà dei dipendenti, stimando tuttavia che un terzo o meno dei dispositivi in

uso siano proprietà personale dei dipendenti. Secondo gli intervistati, software e app per laptop, tablet, netbook e spazio di archiviazione sono più spesso di proprietà aziendale che dei dipendenti. Gli smartphone, invece, sono risultati essere più spesso di proprietà dei dipendenti, anche se di poco.

Quasi l'80% delle aziende ha implementato un'infrastruttura desktop virtuale o VDI in modalità di hosting client o di sincronizzazione remota. Solo il 15% non ha ancora implementato una VDI.

Il sistema operativo più utilizzato dalle aziende sui dispositivi informatici non mobili (server e desktop) è risultato essere di gran lunga Windows (77,7%), anche se alcuni utilizzano Mac OS come sistema operativo principale (13,5%) e altri Linux (7,6%) o Unix (1%).

Tra i **principali motivi** che spingono i dipendenti ad utilizzare i dispositivi mobili sul lavoro troviamo:

- Mobilità migliorata (capacità di lavorare fuori sede o in movimento, 43,1%).
- Evitare di portare o aggiornare più dispositivi (13,6%).
- L'idea che l'approccio BYOD è un vantaggio per il dipendente (10,5%).

Esperienza di violazione della sicurezza

Quasi tutte le aziende che adottano l'approccio BYOD hanno segnalato di avere subito violazioni dei dati o della sicurezza a seguito dell'accesso alla rete aziendale da parte del dispositivo personale di un dipendente (46,5%).

Le risposte alle violazioni della sicurezza legate ai dispositivi di proprietà degli utenti sono state diverse ma quella più comunque è stata limitare i privilegi di accesso ai dati (45%), richiedere l'installazione immediata di software di protezione (42,9%) o semplicemente revocare i privilegi BYOD (11,6%). Per le aziende tedesche, la cosa più importante era insistere sull'installazione di software di protezione in risposta a una violazione, mentre per le aziende statunitensi è stato più frequente l'eliminazione dell'accesso BYOD.

Le aziende hanno dichiarato di disporre di criteri per la cancellazione remota di un dispositivo mobile smarrito o di un dipendente che se ne va (35,5%), mentre alcuni adottano questa prassi solo nel caso di dispositivo smarrito (23,3%). Alcune imprese hanno affermato di cancellare selettivamente le applicazioni dati aziendali quando necessario (10,1%).

Software di protezione

La maggior parte delle aziende (83%) impone ai dipendenti di installare software per proteggere e gestire i dispositivi mobili se utilizzati per il lavoro. Abbiamo chiesto alle aziende che *non* impongono il software di protezione perché lo facessero. Sorprendentemente, la risposta più comune è stata "consentiamo soltanto agli utenti fidati di collegarsi alla rete" (25,7%) e "non eravamo preoccupati della sicurezza su questi dispositivi" (15,6%). Alcuni affermano di non avere mai avuto una soluzione software (13,8%) o di essere ancora alla ricerca di una soluzione software (12,8%.) Meno citati il rifiuto degli utenti (11%), la percezione di un costo elevato (10%) e la percezione di complessità (3,7%).

Considerando esclusivamente la sicurezza degli smartphone, quasi tutti (89,5%) hanno espresso perplessità sulla sicurezza dei dati su questi dispositivi.

Criteri d'uso accettabili (CUA)

Moltissime aziende (79,7%) hanno dichiarato di avere fornito criteri d'uso accettabili (CUA) ai dipendenti in merito alla responsabilità di azienda e dipendenti rispetto all'uso, alla sicurezza e alla responsabilità civile per i dispositivi di proprietà dei dipendenti.

Alla domanda su quali fossero gli elementi che includevano nei documenti CUA, le aziende:

- per il 12,2% hanno dichiarato che in caso di smarrimento dei dispositivi, l'azienda era in grado di cancellare il dispositivo in remoto;
- per il 10% hanno fatto dichiarazioni che indicavano che il reparto IT aziendale avrebbe monitorato regolarmente dati, download e altre attività sul dispositivo mobile e/o che, nei casi di controversie aziendali, i dati sul dispositivo avrebbero potuto essere rivelati o il dispositivo stesso avrebbe potuto essere confiscato;
- per il 9,7% hanno affermato che i tentativi di accesso errati avrebbero potuto causare l'eliminazione dei dati, che la posizione geografica del dispositivo avrebbe potuto essere rilevata o che la responsabilità dei dati sul dispositivo ricade sull'azienda stessa.

Impatto BYOD sui costi

L'introduzione dei dispositivi di proprietà dei dipendenti può avere un impatto sui costi associati al supporto dell'approccio BYOD, mentre alcune aziende scoprono

che i costi complessivi possono aumentare o effettivamente scendere con l'avvento dell'approccio BYOD, e per molte ragioni.

È interessante notare che circa il 40% delle aziende ha dichiarato che i **costi sono diminuiti** dopo l'introduzione dell'approccio BYOD (39,3%). Insieme alle imprese che hanno dichiarato che i costi sono rimasti invariati (23,3%), la maggioranza delle aziende ha concordato sul fatto che l'approccio BYOD o ha ridotto i costi complessivi o li ha lasciati invariati.

È interessante osservare che gli intervistati della seconda batteria (aprile 2012) hanno riferito con molta meno frequenza che l'approccio BYOD aveva incrementato i costi complessivi, dichiarando più spesso che i costi erano rimasti invariati o erano scesi, rispetto agli intervistati del primo sondaggio di gennaio 2012. È possibile che le valutazioni sull'impatto dei costi siamo migliorate con la maggiore esperienza BYOD acquisita o che i costi complessivi associati all'approccio BYOD siano semplicemente scesi nei mesi successivi.

I motivi per cui i costi sono stati visti scendere erano suddivisi quasi equamente tra minori spese in conto capitale per le IT (per l'acquisto dei dispositivi da parte dei dipendenti stessi) (37,9%), minori costi di assistenza tecnica desktop (31,3%) e maggiore produttività dei dipendenti (29,6%).

Tra coloro per cui i costi erano diminuiti a seguito dell'adozione dell'approccio BYOD, il primo motivo era l'incremento dei costi del supporto tecnico (41,2%) o l'incremento delle spese in conto capitale per le VDI (31,5%). Meno citati i maggiori costi per il software o per la virtualizzazione software (27%).

Alla domanda diretta che chiedeva di valutare l'impatto complessivo dei dispositivi mobili dei dipendenti in azienda, appare evidente che l'approccio BYOD introduce dei costi di transizione oltre ai vantaggi che possono annullare tali costi, come la maggiore produttività e soddisfazione dei dipendenti e la maggiore soddisfazione dei clienti.

Ulteriore impatto dell'approccio BYOD

L'impatto effettivo dell'approccio BYOD, quindi, potrebbe benissimo coinvolgere la cultura e la filosofia aziendale. Quando abbiamo cercato di sondare in che misura i dirigenti senior fossero d'accordo con le affermazioni che descrivevano l'impatto delle BYOD, sono emersi alcuni dati interessanti.

I dirigenti concordavano sul fatto che adottare l'approccio BYOD garantisse un vantaggio sulla concorrenza, fosse un vantaggio per i dipendenti, fosse un utile strumento per il reclutamento e la conservazione del personale e che i dipendenti,

di fatto, avessero “il diritto di utilizzare i propri dispositivi informatici sul lavoro.” L’uso fatto dai dipendenti dei propri dispositivi viene visto come un metodo per incrementare significativamente la creatività e l’innovazione e per migliorare l’equilibrio tra vita professionale e vita privata.

I CEO si sono dimostrati più positivi verso l’impatto dell’approccio BYOD rispetto ai dirigenti IT. Emerge un divario tra il punto di vista dei CEO e il modo in cui i dirigenti IT ritenevano che l’azienda avrebbe valutato le varie affermazioni; ciò porta a pensare che i dirigenti IT potrebbero non essere tanto in armonia con le opinioni dei CEO quanto ci si aspetterebbe.

La maggior parte degli intervistati (62,9%) ha concordato che permettere l’uso dei dispositivi di proprietà dei dipendenti sul lavoro influenza positivamente l’opinione che i dipendenti hanno dell’azienda e circa la metà (47,5%) ha dichiarato che influenza anche positivamente l’opinione dell’azienda che hanno i clienti.

Il futuro dell’approccio BYOD

L’espansione dell’approccio BYOD viene generalmente considerata inevitabile dalle aziende intervistate. Molte ritengono infatti che sarà prevalente in futuro per tutti gli utenti aziendali. Circa un quinto pensa che sostituirà i PC per la maggior parte degli utenti (17%) anche se qualcuno ritiene che verrà usata principalmente per le operazioni di comunicazione e di messaggistica (14,7%).

Le aziende sono attivamente impegnate nella pianificazione di come continueranno a integrare l’approccio BYOD al loro interno. Tra le modifiche considerate: acquisizione di nuovo software o tecnologia per gestire i problemi della sicurezza (21,4%), riorganizzazione del reparto IT (20,3%, ma molto più diffusa tra i CEO, che per due terzi sarebbero favorevoli alla riorganizzazione del reparto IT), spostamento a una piattaforma dall’architettura sottile o ridefinizione del supporto generale dei dispositivi informatici (rispettivamente 14,6% e 16,2%).

Più di un quarto ha previsto una riallocazione del budget che non prevede l’acquisto di dispositivi informatici e alcuni riassegnerebbero i budget per il software (8%).

Abbiamo anche chiesto a tutti gli intervistati di sintetizzare la loro opinione su quali siano le sfide future per l’approccio BYOD nelle rispettive aziende. Anche se alcuni interpellati hanno respinto con forza l’approccio BYOD in quanto impraticabile nel loro settore o nella loro azienda (ad es. il personale amministrativo governativo)**, i più hanno affermato che l’approccio “BYOD è il futuro”.**

CONCLUSIONI

1. **L'approccio BYOD è già diffuso**, con più di 3/4 (76,7%) di aziende che consentono ai propri dipendenti di utilizzare i propri dispositivi personali come laptop, smartphone e tablet sul lavoro. La frequenza è maggiore per le aziende statunitense rispetto a quelle britanniche o tedesche.

2. **Quasi tutte le aziende che adottano l'approccio BYOD impongono l'installazione di software di protezione** sui dispositivi personali. Molti fornitori diversi si occupano di questo mercato, e il 4,3% ha affermato che il fornitore di soluzioni di sicurezza dell'azienda è Trend Micro. I leader del mercato per questo campione sono McAfee (16%), Kaspersky (12,6%) e Symantec Norton (14,9%). I motivi per non installare il software di protezione erano diversi, ma vi sono perplessità diffuse sulla sicurezza dei dati degli smartphone (85,9%).

3. **Violazioni della sicurezza hanno colpito quasi la metà delle aziende** che adottano l'approccio BYOD e le risposte più comuni a tali violazioni sono state modifiche ai protocolli di sicurezza, con limitazione dei privilegi di accesso ai dati (45%) o installazione di software di protezione (42,9%). Alcune aziende interrompono del tutto l'approccio BYOD dopo una violazione.

4. **I CEO sono generalmente più entusiasti dell'approccio BYOD rispetto ai dirigenti IT**, poiché questi ultimi conoscono fin troppo bene i problemi della sicurezza e dell'assistenza che l'approccio BYOD comporta. I CEO stessi utilizzano vari dispositivi mobili e spesso affermano che incrementano la loro produttività oltre a quella dei dipendenti.

5. **L'approccio BYOD dà alle aziende un vantaggio sulla concorrenza.** Quasi la metà dei CEO ha dichiarato che l'approccio BYOD conferisce un vantaggio sulla concorrenza, mentre la stessa affermazione l'ha fatta un numero minore di dirigenti IT.

6. **L'approccio BYOD viene visto come uno strumento per trattenere e reclutare dipendenti.** Quasi la metà dei CEO (46%) e dei dirigenti IT (42,5%) ha concordato sul fatto che l'approccio BYOD è un vantaggio per il personale e viene utilizzato per attirare o trattenere i dipendenti.

7. **L'approccio BYOD migliora l'innovazione e la creatività e incrementa la produttività.** È opinione diffusa che l'approccio BYOD migliori la produttività dei dipendenti (secondo il 47% dei CEO e il 46% dei dirigenti IT) oltre all'innovazione e alla creatività (50,7% per i CEO, 48% per i dirigenti IT).

8. **I dipendenti preferiscono le aziende che adottano l'approccio BYOD, e lo stesso i clienti.** La maggior parte degli intervistati (62,9%) ha concordato che permettere l'uso dei dispositivi di proprietà dei dipendenti sul lavoro influenza positivamente l'opinione che i dipendenti hanno dell'azienda e circa la metà (47,5%) ha dichiarato che influenza positivamente anche l'opinione dell'azienda che hanno i clienti.

9. **L'approccio BYOD *riduce* o lascia invariati i costi.** Anche se l'approccio BYOD impone di spendere in software di protezione e assistenza, come insiste la maggior parte delle aziende che lo adotta, l'impatto di tale approccio rappresenta un calo nei costi complessivi o un'assenza di variazione. È un dato importante che deve venire condiviso con le aziende interessate all'introduzione di politiche sui dispositivi di proprietà dei dipendenti, poiché più della metà della aziende intervistate ha dichiarato che i costi sono calati (36%) o sono rimasti invariati (20,1%).

10. **L'approccio BYOD è un diritto dei dipendenti?** Quasi la metà dei CEO è di questa opinione. È una domanda provocatoria che richiede ulteriori approfondimenti.

11. **Sono attivi criteri d'uso accettabili (CUA) in quasi tutte le aziende** che adottano l'approccio BYOD. Alla domanda relativa ai componenti dei documenti CUA, la disposizione più diffusa è la capacità del reparto IT aziendale di cancellare in remoto i dispositivi, seguita dal diritto di monitorare l'attività, dalla possibilità di rivelare i dati in caso di controversia e dal fatto che i tentativi di accesso errati possono causare l'eliminazione dei dati.

12. **L'espansione dell'approccio BYOD sul posto di lavoro è considerata inevitabile.** Tuttavia, i dirigenti senior conoscono bene i rischi possibili e sono pronti a investire secondo esigenza per facilitare al massimo le implementazioni.