Indice

Consumerization

Contesto

Diffusione crescente di smartphone, tablet e più in generale di dispositivi portatili tra la popolazione

Sempre maggiore **disponibilità** di dati e servizi in mobilità, soprattutto per il business

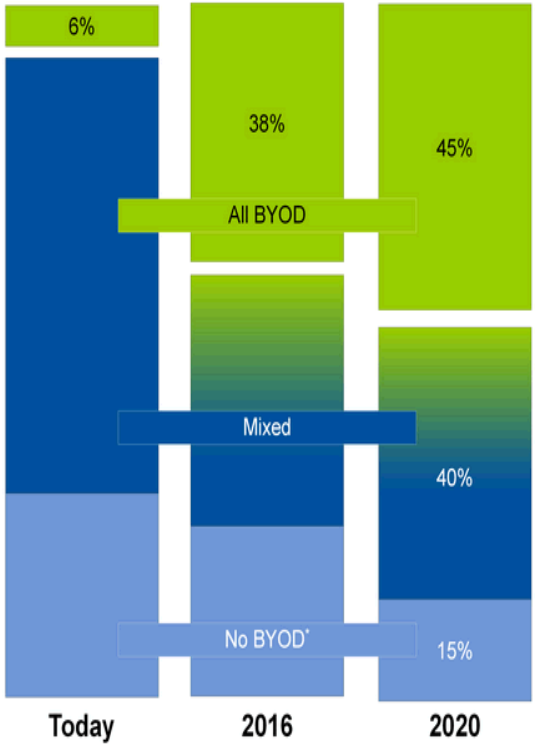
Modello BYOD

- I dipendenti richiedono di poter utilizzare i dispositivi personali anche per **finalità di business**
- L'azienda vuole fornire dati e servizi in mobilità mantenendo un **livello di rischio accettabile**

Consumerization

I trend del mercato

Secondo **Gartner**(*) il **38%** delle imprese entro il **2016** non fornirà più dispositivi mobile corporate ai propri dipendenti

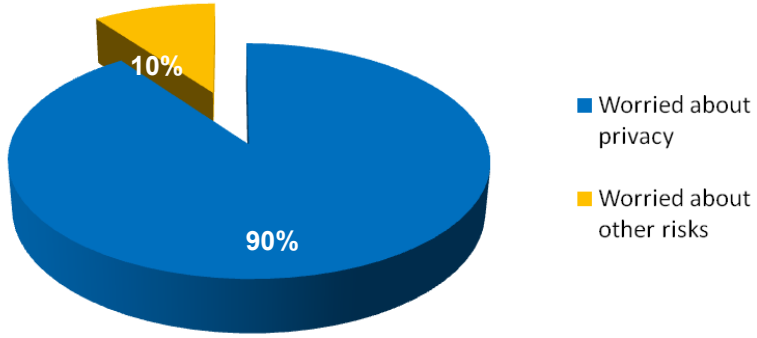


(*) Source: Gartner – “Bring Your Own Device: The Facts and the Future” (11 April 2013)

Consumerization

Le limitazioni del fenomeno

Secondo una survey effettuata da **KPMG**(*), la **fiducia** e la **privacy** rappresentano i principali elementi di criticità rispetto all'adozione delle nuove tecnologie 'mobile' anche da parte degli utenti: infatti ben il **90%** degli intervistati ha espresso un elevato livello di preoccupazione per la **sicurezza dei propri dati personali**

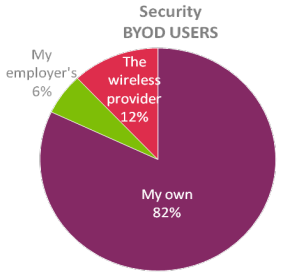


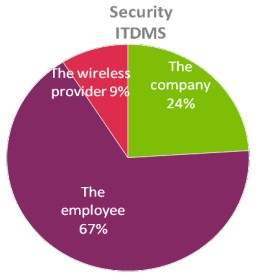
(*) Source: KPMG Consumers and Convergence 5, conducted in the 2011 and included 9,600 consumers across 31 countries

Consumerization

I responsabili della messa in sicurezza

Secondo una survey condotta da **CTIA**(*) , la maggior parte degli **utenti** e dei professionisti dei dipartimenti **IT** (ITDMs) pensano che sia **responsabilità del dipendente, non dell'azienda**, mettere in sicurezza i device, nonostante questi siano utilizzati per accedere a dati aziendali





(*) The survey was conducted by CTIA – The Wireless Association, an international nonprofit trade association that has represented the wireless communications industry since 1984,in February 2013 with 250 Information Technology Decision Makers and more than 1,000 full-time employed mobile device users

Consumerization

Le policy

Sempre secondo la stessa survey, emerge come il **47%** degli **utenti** e il **42%** dei professionisti dei dipartimenti **IT** intervistati sostengono che le aziende presso cui operano **non si sono dotate di una policy** ben definita per regolare l'uso dei devices secondo il modello **BYOD**

(*) The survey was conducted by CTIA – The Wireless Association, an international nonprofit trade association that has represented the wireless communications industry since 1984,in February 2013 with 250 Information Technology Decision Makers and more than 1,000 full-time employed mobile device users

Consumerization

Le applicazioni

Infine dalla stessa indagine emerge come le **cinque applicazioni più usate** dai dipendenti sui device personali per motivi di lavoro siano l'email, l'agenda, la programmazione degli impegni, i database, le applicazioni aziendali e i servizi di directory

Company information or applications	Users	ITDMs
Email	89%	92%
Calendaring and Scheduling	57%	75%
Databases	28%	32%
Company Applications	28%	39%
Directories	25%	31%
Financial information	19%	16%
File servers	19%	33%
Other	6%	4%

(*) The survey was conducted by CTIA – The Wireless Association, an international nonprofit trade association that has represented the wireless communications industry since 1984,in February 2013 with 250 Information Technology Decision Makers and more than 1,000 full-time employed mobile device users

Vantaggi del modello BYOD

Punti di forza

Maggior soddisfazione e **produttività** dei propri dipendenti

Maggiore utilizzo di **servizi e dati di business in mobilità** con relativo aumento della qualità dei servizi offerti dall'azienda

Riduzione dei **costi** per l'acquisto dei dispositivi

Rischi per la sicurezza del modello BYOD

Rischi per la sicurezza

L'utilizzo di dati di business su dispositivi personali **aumenta il rischio** a cui sono esposte le informazioni aziendali

Le principali minacce a cui si espone l'azienda sono legate a:

- **componente umana**
- **vulnerabilità di sistemi e servizi**
- **compliance**

Rischi per la sicurezza del modello BYOD

Rischi
Componente umana

Il **comportamento dell'utente** rappresenta la minaccia principale per la sicurezza delle informazioni

Alcune **minacce** che espongono a rischi per la sicurezza:

- furto o smarrimento del dispositivo
- divulgazione non autorizzata di informazioni riservate
- utilizzo di servizi non sicuri
- gestione impropria delle credenziali di accesso

Rischi per la sicurezza del modello BYOD

Rischi
Vulnerabilità di sistemi e servizi

Il software e i dispositivi utilizzati sono tipicamente indirizzati al **mercato consumer** e non sono ottimizzati per esigenze di business

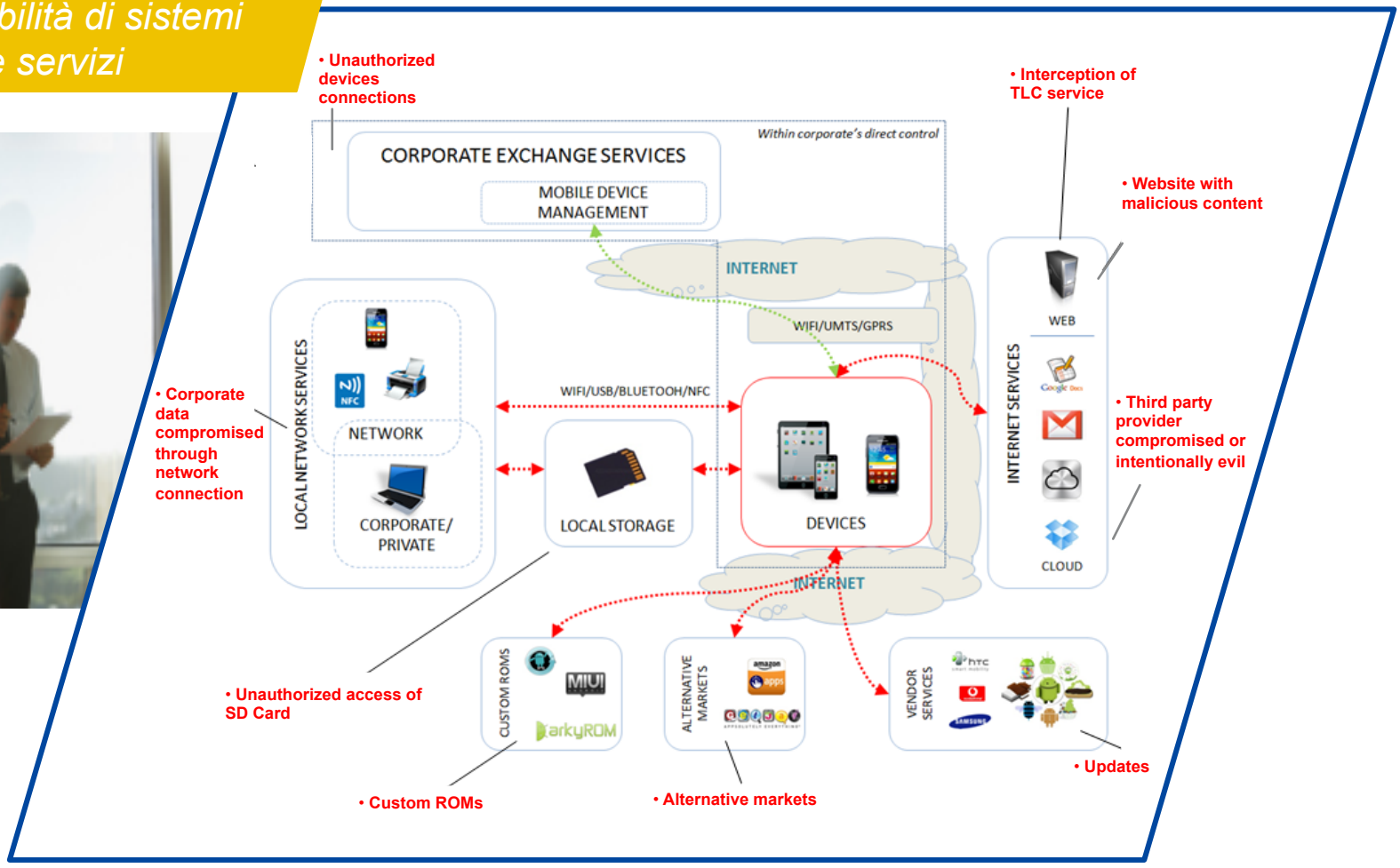
Per tali dispositivi non sempre è garantito il rispetto di specifici **standard di sicurezza delle informazioni**

Alcune **minacce** che espongono a rischi per la sicurezza:

- malware e virus
- connessione a reti non sicure/non protette
- utilizzo di servizi cloud non sicuri

Rischi per la sicurezza del modello BYOD

Rischi
Vulnerabilità di sistemi e servizi



Rischi per la sicurezza del modello BYOD

Rischi
Compliance

L'azienda nel gestire la **commistione tra dati aziendali e dati personali e riservati** del dipendente deve ripensare alla definizione **di nuove policy**

I dati personali e riservati dell'utente devono essere trattati secondo nuovi paradigmi che tengano però presenti le linea guide aziendali e gli obiettivi di business

Le procedure di utilizzo e gestione devono essere chiare al dipendente **(formazione/training)** e devono individuare le responsabilità tra le parti

Rischi per la sicurezza del modello BYOD

Rischi
Compliance

I dispositivi personali e i dati riservati dell'utente devono essere trattati mantenendo un equilibrio tra le esigenze lavorative e i diritti degli incaricati

L'azienda deve valutare attentamente i rischi legati alle normative applicabili relativamente all'utilizzo dei dispositivi mobili

Gli ambiti di compliance da considerare sono molteplici e possono riguardare, ad esempio:

- **Legge 231** (reati informatici)
- **Statuto dei lavoratori** (controllo a distanza)
- **Codice Privacy** (misure di sicurezza, trasferimento dei dati, utilizzo di internet e della posta elettronica, ecc.)

Rischi per la sicurezza del modello BYOD

Rischi
Codice Privacy

La normativa Privacy richiede una serie di adempimenti formali di **misure minime ed idonee** da implementare che vanno ripensate in ottica mobile, quali ad esempio:

- gestione delle informative e dei consensi
- individuazione della titolarità/co-titolarità nei trattamenti
- gestione delle credenziali di accesso
- modalità di autenticazione informatica
- protezione dei dati da accessi non consentiti
- ripristino della disponibilità dei dati e dei sistemi
- cifratura per trattamenti di dati sensibili

Processo di gestione strutturato del BYOD

Mobile Device Management

L'implementazione di un modello efficace di BYOD necessita di strumenti che consentano un'adeguata gestione centralizzata (**Mobile Device Management**)

Una soluzione MDM fornisce:

- un set di **controlli di sicurezza minimi**
- **monitoraggio** e controllo dei dispositivi mobile

Le soluzioni MDM e i dispositivi mobili devono essere selezionati secondo i requisiti individuati dall'azienda per il proprio modello BYOD

Processo di gestione strutturato del BYOD

Governance e Compliance

Per garantire un adeguato livello di governance del modello BYOD è necessario inoltre adottare:

- Policy e linee guida per i dipendenti
- Policy implementate a livello software sull'MDM

Inoltre è opportuno garantire un efficace **gestione dell'infrastruttura tecnologica** e in particolare dell'MDM

Particolare attenzione dev'essere posta anche agli aspetti di **formazione e sensibilizzazione** degli utenti

Approccio metodologico KPMG

Le quattro fasi

Fase 1 – Analisi dei rischi e definizione modello target

- Effettuare un'analisi dei rischi aziendali legati alla soluzione e definire un modello strutturato sulla base delle esigenze di business

Fase 2 – Analisi requisiti e scelta soluzione tecnologica

- Analizzare e definire i requisiti tecnologici e funzionali ed organizzativi al fine di identificare la soluzione tecnologicapiù adatta al modello prescelto ed individuare policy e procedure da indirizzare

Fase 3 – Implementazione

- Gestire e coordinare in maniera integrata il piano degli interventi necessarie per implementare il modello target; implementazione tecnologica, definizione delle policy e dei processi di gestione, attività di formazione, ecc.

Fase 4 – Governance dei dispositivi

- Definizione ed attuazione di un approccio operativo per la gestione della soluzione implementata

Grazie

Presentation by **Luca Boselli**

Luca Boselli
Associate Partner
KPMG Advisory S.p.A.
T: +39 02 6763 2942
M: +39 348 3056864
E: lboselli@kpmg.it
www.kpmg.it

cutting through complexity