

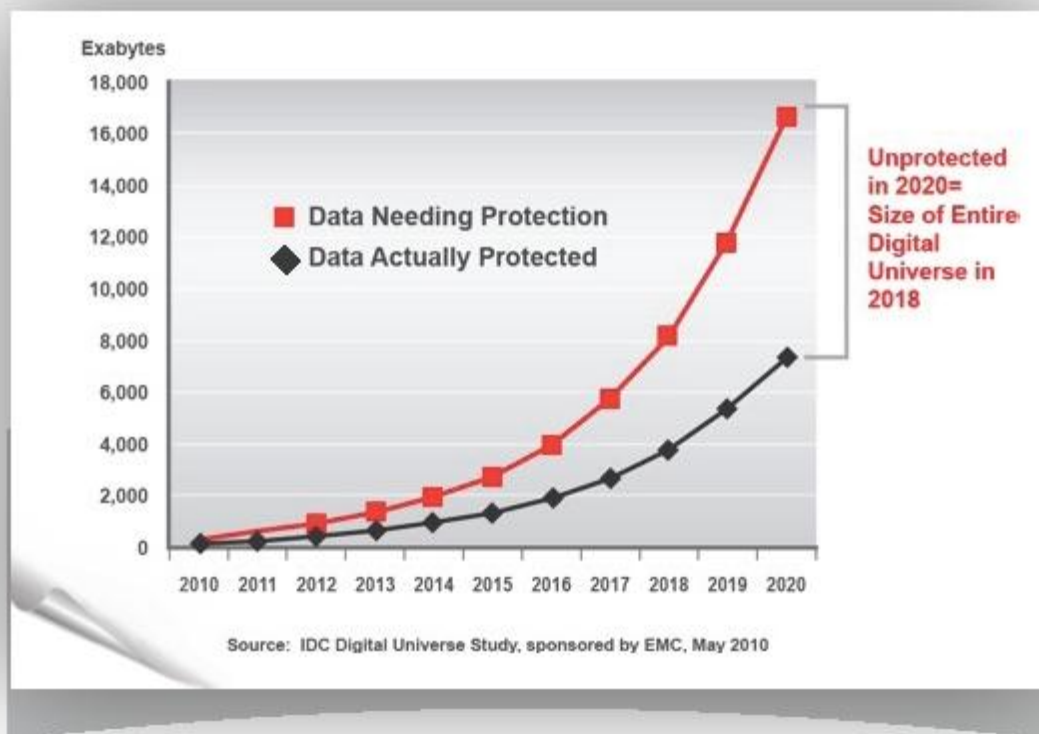


La protezione dei dati nell'era del mobile device: rischi e opportunità nell'uso di tablet e smartphone

Daniele Gombi – gombi@polaris.it

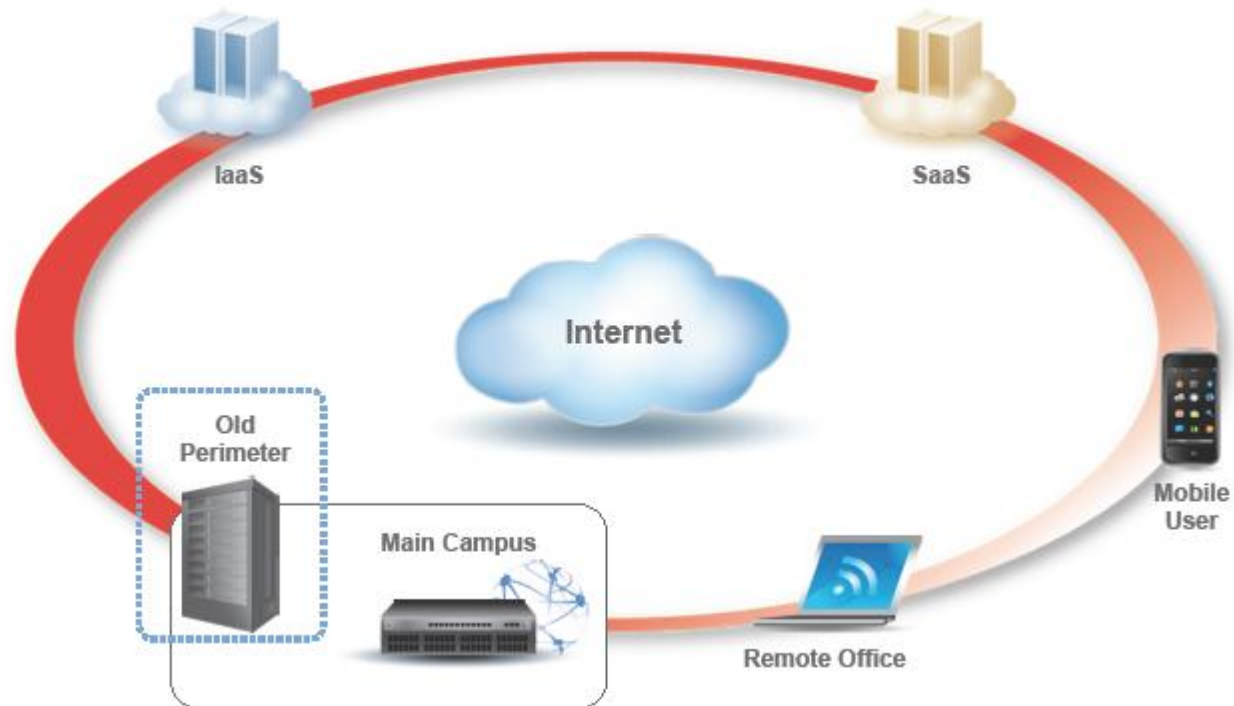


Senza Parole





Il perimetro di riferimento





ALCUNI DATI

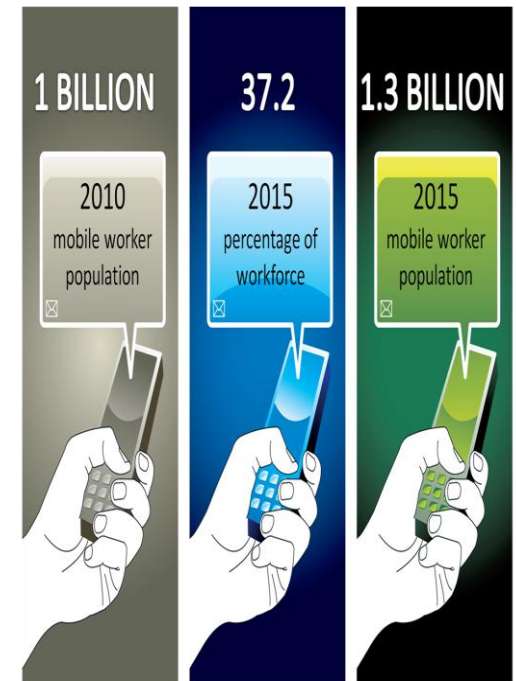
20.000.000 smartphone stimati in Italia
+52% Rispetto al 2010

77% utenti che li usano in ambito aziendale

[Fonte IPSOS Media ICT 2011]

142,7 (4,3%) smartphone persi o rubati
di cui 57% non protetti
di cui 60% contenenti dati critici

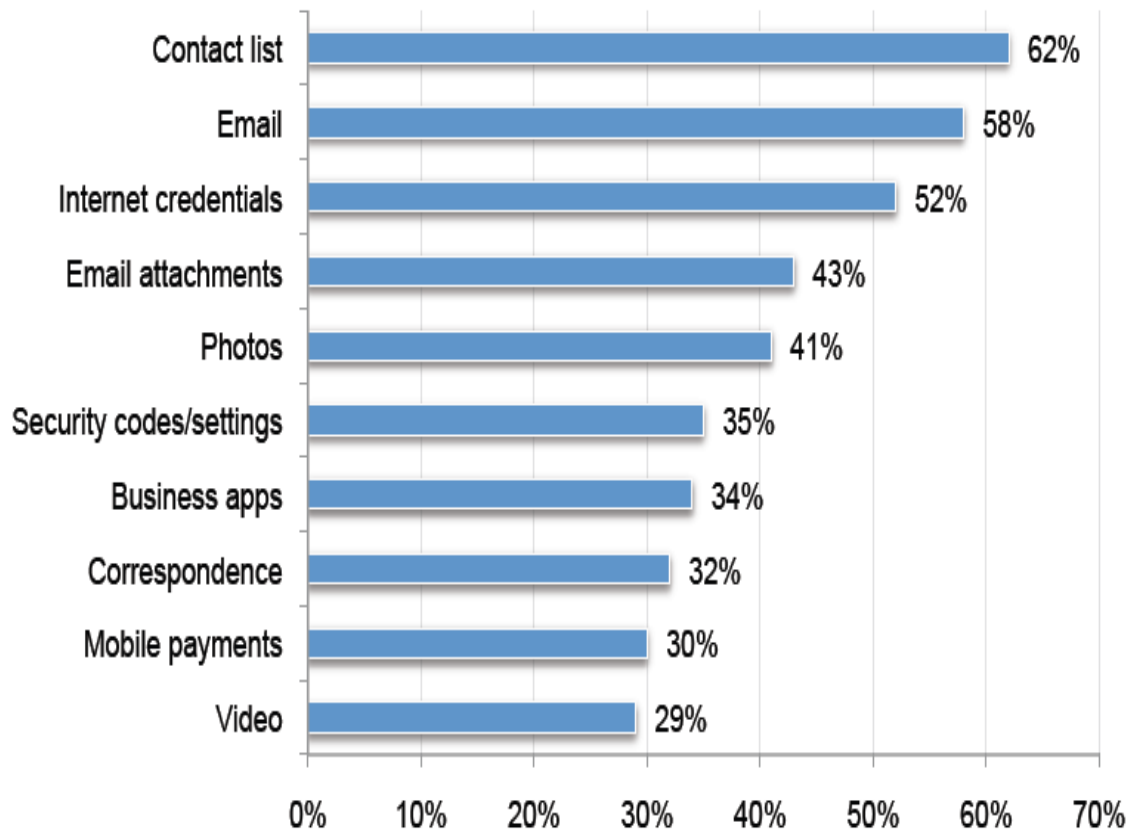
[Fonte Ponemon Institute, 2011 su campione di 439 società U.S.A. in 12 mesi]



The IDC study, [Worldwide Mobile Worker Population 2011-2015 Forecast](#), December 2011 (Doc #232073).



Bar Chart 8. What business information is at risk because of smartphone loss?





INCREASED PRODUCTIVITY



70 PERCENT
of employees with smartphones regularly check their emails outside of normal business hours.

42 PERCENT

of employees log onto their business email accounts while home on sick leave.

43% of employees connect to their emails on their smartphones in order to get ahead and ease their workloads for the following business day.

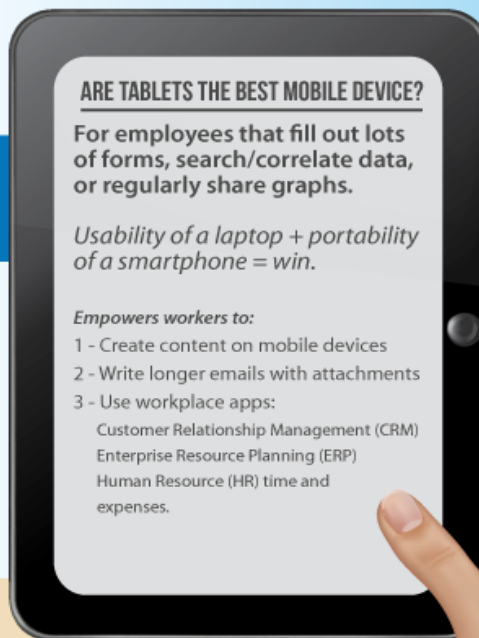
During downtime, 91 percent of employees check their smartphone every six to 12 minutes

91 PERCENT



TABLETS

are the most effective mobile form factor. Tablets by design strike the balance between the usability of a laptop and the portability of a smartphone.



ARE TABLETS THE BEST MOBILE DEVICE?

For employees that fill out lots of forms, search/correlate data, or regularly share graphs.

Usability of a laptop + portability of a smartphone = win.

Empowers workers to:

- 1 - Create content on mobile devices
- 2 - Write longer emails with attachments
- 3 - Use workplace apps:
 - Customer Relationship Management (CRM)
 - Enterprise Resource Planning (ERP)
 - Human Resource (HR) time and expenses.

BENEFITS FROM MOBILITY

- Reduced labor expenses
- Higher job completion rates
- Reduced paperwork
- Improved customer service and response times
- Productivity improvements
- Reduced liability
- More accurate billing & record keeping
- Increased customer satisfaction
- Reduced sales cycles
- Streamlined workflow with added visibility
- Increased productivity and efficiencies
- Reduced operational costs
- Improved data collection and accuracy

WHO BENEFITS FROM MOBILITY?

Used for applications in vertical processes: work order tasks, data capture, spare parts ordered, inspection check offs. Particularly in the public sector and utilities industries, the conversion to paperless mobile workflows has a high return on investment (ROI) from reduced administrative expense increased data accuracy and reduced cycle time.

Deploying & Managing Mobile Apps in the Field

FIVE KEY QUESTIONS



CONSIDERAZIONI

(Nonostante l'elevato tasso di introduzione sul mercato dei device mobili, solo **una minima parte delle aziende ne sta supportando ufficialmente l'uso < 20%**)

1. Eterogeneità delle caratteristiche tecnologiche
2. Vulnerabilità tecniche
3. Comportamenti non idonei e non consapevolezza
4. BYOD – promiscuità dei dati personali e aziendali
5. Difficoltà di controllo su utilizzo e raccolta dati (fotocamera)
6. Elevata probabilità di furto o perdita
7. Mancanza di preliminare analisi dei rischi
8. Mancanza di procedure di incident handling
9. Non analisi dei trattamenti effettuati
10. Non applicazione delle misure minime di sicurezza



CONSIDERAZIONI

Ma anche
11. Potenziale geolocalizzazione



The screenshot displays the 'www.cellphone-phonebeagle.info' interface. On the left, a table lists tracking events for a device named 'My Demo Kid' on 09/20/2011. The table includes columns for Device Time, Type, Accuracy, and Information. Below the table are controls for filtering (Auto-select, Clear, All, Smart, GPS/Network), navigation (Previous Day, Next Day), and a 'Download New' button. On the right, a map of Washington, D.C. shows several colored markers (red, blue, green) connected by lines, indicating movement paths. Map controls like 'Zoom To Markers', 'Close Bubbles', 'Toggle Accuracy', and 'Toggle Directions' are visible at the top of the map area.

Device Time	Type	Accuracy	Information
<input type="checkbox"/> 09/20/2011 5:05:06 PM	GSM-Tower	578m	T-Mobile
<input checked="" type="checkbox"/> 09/20/2011 5:05:06 PM	GPS	20m	
<input type="checkbox"/> 09/20/2011 4:35:06 PM	GSM-Tower	578m	T-Mobile
<input checked="" type="checkbox"/> 09/20/2011 4:35:06 PM	GPS	20m	
<input checked="" type="checkbox"/> 09/20/2011 4:05:06 PM	GSM-Tower	577m	T-Mobile
<input type="checkbox"/> 09/20/2011 4:05:06 PM	GPS	40m	No Fix
<input type="checkbox"/> 09/20/2011 3:35:06 PM	GSM-Tower	577m	T-Mobile
<input checked="" type="checkbox"/> 09/20/2011 3:35:06 PM	GPS	40m	
<input type="checkbox"/> 09/20/2011 3:05:06 PM	GSM-Tower	850m	T-Mobile
<input checked="" type="checkbox"/> 09/20/2011 3:05:06 PM	GPS	10m	
<input type="checkbox"/> 09/20/2011 2:35:06 PM	GSM-Tower	850m	T-Mobile
<input checked="" type="checkbox"/> 09/20/2011 2:35:06 PM	GPS	10m	
<input type="checkbox"/> 09/20/2011 2:05:06 PM	GSM-Tower	850m	T-Mobile
<input checked="" type="checkbox"/> 09/20/2011 2:05:06 PM	GPS	10m	
<input checked="" type="checkbox"/> 09/20/2011 1:35:06 PM	GSM-Tower	680m	T-Mobile
<input type="checkbox"/> 09/20/2011 1:35:06 PM	GPS	45m	No Fix



196/2003

PRIVACY
On Cloud & mobile

I principali adempimenti formali correlati all'utilizzo dei dispositivi in ambito aziendale





MISURE MINIME? IDONEE?

- Presenza di una password di accesso “forte”
- Autenticazione e gestione credenziali
- Blocco dopo un periodo di inattività
- Remote Wipe (corporate content wipe o total wipe)
- Cifratura della memoria (interna ed esterna)
- Aggiornamento periodico strumenti
- Monitoraggio della manipolazioni dei dati sul dispositivo
- Firewall ed Antivirus
- VPN di accesso alle risorse aziendali
- Archiviazione e backup dei dati
- Separazione dei dati aziendali dai dati personali



ALTRI RIFERIMENTI NORMATIVI

Dismissione dispositivi mobili (sim, schede di memoria interne e removibili) – Provvedimento 13 ottobre 2008

Accesso promiscuo alla e-mail aziendale e personale – Linee Guida 01 marzo 2007

Piattaforme centralizzate di gestione dei dispositivi mobili – Provvedimento AdS 27 novembre 2008

Geolocalizzazione, utilizzo ibrido – Statuto dei lavoratori

Modello di organizzazione idoneo e rischi connessi ai dispositivi mobili, reati informatici in ambito “mobile” – D.Lgs 231/2001



Consigli per l'uso dei dispositivi personali in azienda

1. STABILIRE UNA POLICY

Essere chiari su quando e come i dispositivi personali sono autorizzati a collegarsi alla rete aziendale. Esplicitare i livelli di accesso consentiti

2. VALUTARE STRUMENTO di MANAGEMENT

Verificare attentamente la possibilità di utilizzare un software MDM (Mobile Device Management) per gestire dati a diversa classificazione, implementare policy di sicurezza e stabilire controlli di monitoraggio



Consigli per l'uso dei dispositivi personali in azienda

3. IDENTIFICARE RISCHI E RESPONSABILITA'

Quali dati sono presenti nei dispositivi personali? costituisce la minaccia principale anche in relazione alla conformità normativa.

Chi è responsabile dei dati contenuti nel device?

4. MEASURE TWICE, CUT ONCE

Definire il modello di Governance e le linee guida per l'uso dei dispositivi mobili e dei relativi software prima di iniziare i trattamenti



Consigli per l'utilizzo dei dispositivi personali in azienda

5. INCIDENT HANDLING

Implementare una policy per i dispositivi persi o rubati

Possono essere bloccati da remoto?

Possono essere ripuliti da remoto?

6. DIFFERENZIARE I DISPOSITIVI

Differenziare i devices permette di frazionare il rischio di attacchi maligni.



Consigli per l'utilizzo dei dispositivi personali in azienda

7. FISSARE LIMITAZIONI

Le persone sono abituate ad utilizzare a piacimento il proprio dispositivo mobile, devono accettare consapevolmente l'utilizzo conforme alla policy aziendale

8. FORMARE, EDUCARE, FARE RISPETTARE

Formare

Educare

Fare Rispettare

... mantenere un contatto continuo con gli utilizzatori



<https://privacycloudmobile.clusit.it>





Grazie dell'attenzione !!

Daniele Gombi – gombi@polaris.it