

La sicurezza dei
SOCIAL MEDIA
in ambito **Business**

1 - Chi Siamo

2 - I Social Media

3 - Enterprise & Social Media

4 - Minacce e Rischi di Sicurezza

5 - Le Soluzioni

6 - Conclusioni

1 – CHI SIAMO

Proteggiamo il Patrimonio informativo dei nostri Clienti

Da oltre 10 anni realizziamo per i nostri Clienti **soluzioni di sicurezza d'avanguardia**, ad alto valore aggiunto, con particolare riferimento alle tematiche dell'**Information Governance, Risk Management & Compliance**.

Noi crediamo che la Sicurezza Informatica sia un **driver** e non un costo, e che possa essere implementata in modo **intelligente, efficace e commisurato al contesto**.

Anche nel nuovo campo della sicurezza dei **Social Media** uniamo **competenza, passione, tecnologia e buon senso** per fornire soluzioni semplici, affidabili, scalabili ed economiche, trasformando i **problemi** in **opportunità** di crescita e di miglioramento.



2 – COSA SONO I SOCIAL MEDIA

I Social Media sono un insieme di piattaforme **Web 2.0** tramite le quali gli **utenti** interagiscono **direttamente**, producendo e condividendo **contenuti** propri e/o elaborando contenuti altrui, in **tempo reale**.

“Social media è un termine generico che indica tecnologie e pratiche online che gli utenti adottano per condividere contenuti testuali, immagini, video e audio.”

(Wikipedia)



2 – ELEMENTI CHIAVE DEI SOCIAL MEDIA

I **6 elementi chiave** dei Social Media:

- 1.** Participation
- 2.** Collective dynamics
- 3.** Transparency
- 4.** Independence
- 5.** Persistence
- 6.** Emergence

(Gartner)



“Any user, virtually anywhere in the world, can freely (= liberamente e spesso anche gratuitamente) create content and disseminate this information in real time to a global audience, ranging in size from a handful to literally millions of peers”

(ISACA Social Media White Paper 2010)

2 – QUANTI E QUALI SOCIAL MEDIA?

Secondo **Mashable** i più popolari sono circa **400**;

Secondo **Knowem** i più popolari sono circa **150**;

Wikipedia ne elenca circa **200** (escludendo i siti di Dating ed i Social Networks privati);

I **principali**, tra le varie tipologie, sono circa **20**.



2 – QUANTO SONO DIFFUSI?

30 MILIARDI.

Il numero di **contenuti** (links, news, posts, note, foto, ecc) condivisi ogni **mese** su **Facebook**.

24 ORE.

La durata totale dei **video** caricati ogni **minuto** su **YouTube**.



2 MILIARDI

Il numero di **video** visti ogni **giorno** su **YouTube**.

27 MILIONI.

Il numero medio di **“tweets”** al **giorno** su **Twitter**.

4 MILIARDI.

Il numero di **immagini** ospitate su **Flickr**.

*(What the F**K is social media now?)*

2 – IL FENOMENO FACEBOOK

Oltre **500 MILIONI** di utenti **nel mondo**.

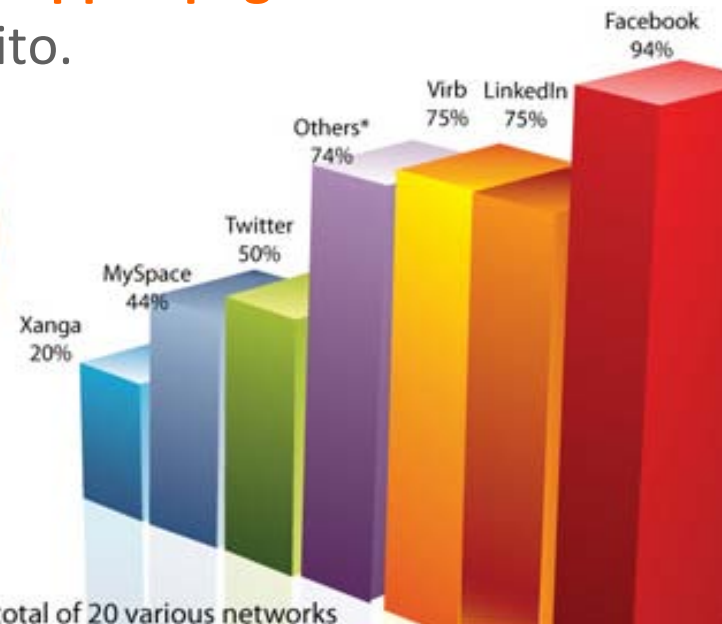
Oltre **17 MILIONI** in **Italia** (+3% nel mese di novembre 2010).

700 MILIARDI i **minuti spesi al mese** su Facebook nel mondo (oltre 1 milione di anni / uomo!).

L'utente medio di FB ha **130 amici**, è connesso a **80 gruppi e pagine di community** e trascorre **oltre 55 minuti al giorno** sul sito.

150 MILIONI di utenti accedono a Facebook da **dispositivi mobili** e sono **due volte più attivi** rispetto agli utenti "tradizionali".

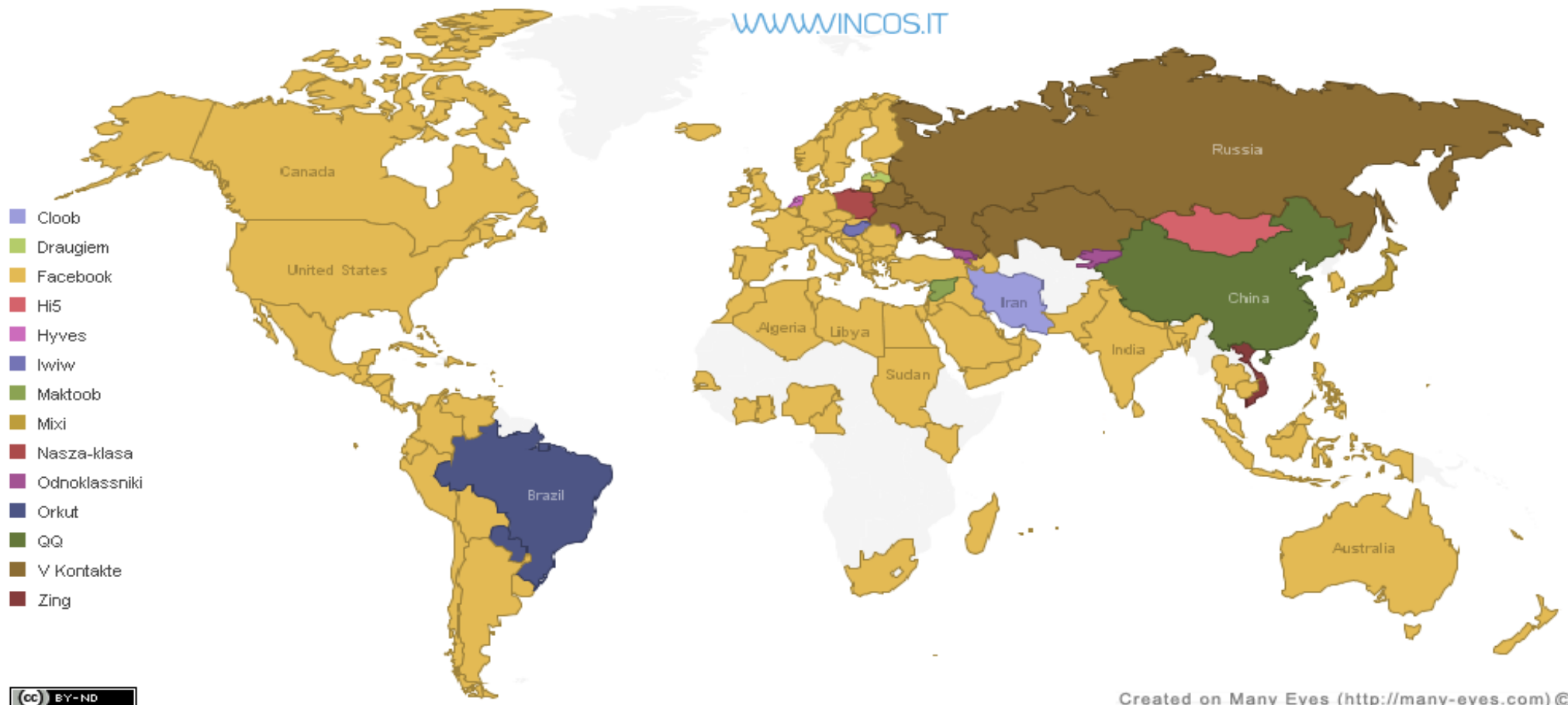
(Facebook Statistics e Vincos Blog - Osservatorio Facebook)



2 – IL FENOMENO FACEBOOK

“Se Facebook fosse una nazione, sarebbe la terza più popolata al mondo, in testa agli Stati Uniti. Solo la Cina e l’India sono più popolate.”

*(What the F**K is social media now?)*



(cc) BY-ND

Created on Many Eyes (<http://many-eyes.com>) ©

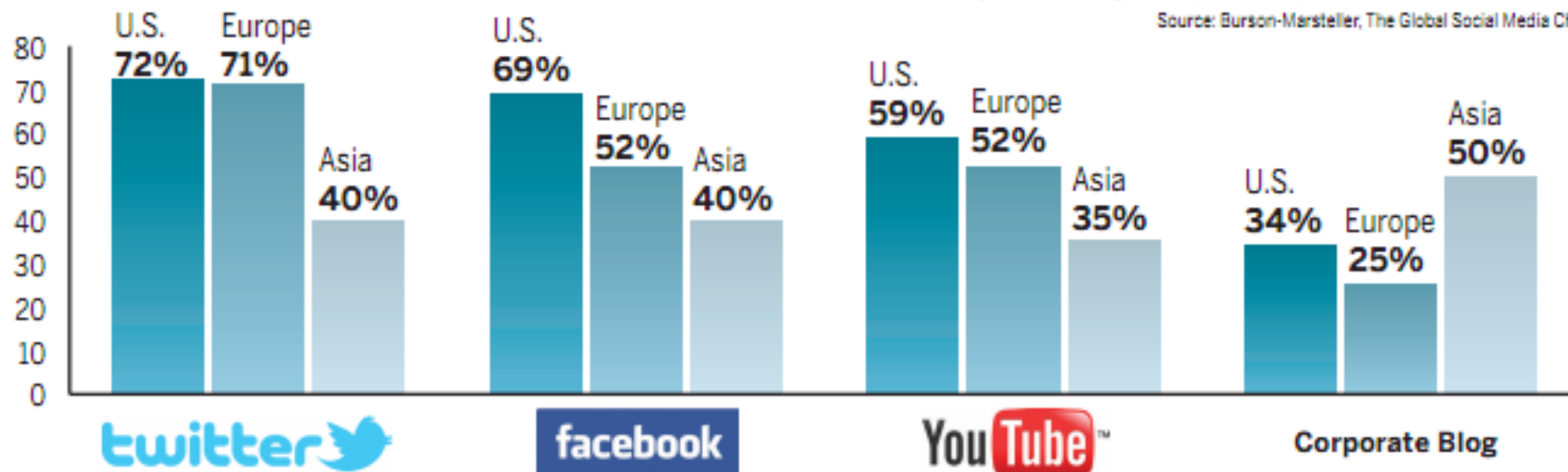
3 – LA DIFFUSIONE NEL MONDO ENTERPRISE

The number of Facebook users in the United States grew 3.43 percent last month.

Fortune Global 100 companies

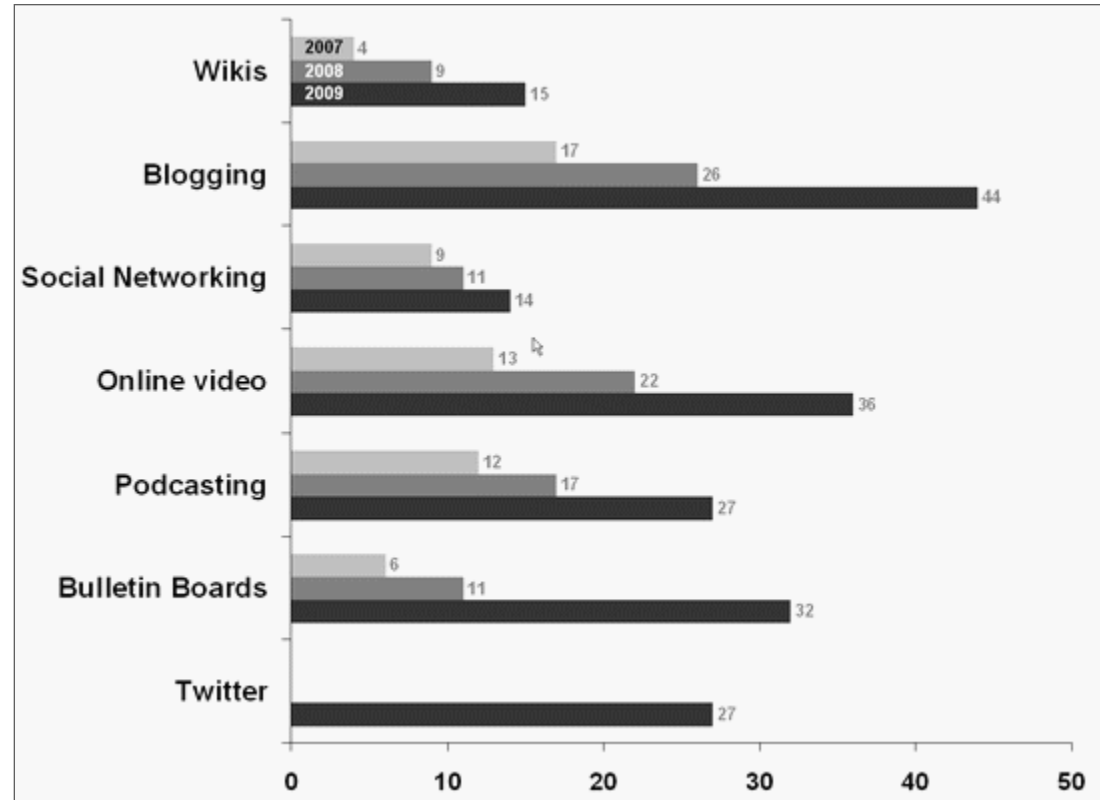
The proliferation of corporate engagement in social media. Data was collected between November 2009 and January 2010 among the top 100 companies of *Fortune's* Global 500.

Source: Burson-Marsteller, The Global Social Media Check-up



(*SC Magazine* – Shining the spotlight on Social Media - 2010)

3 – IL TREND DI ADOZIONE NEL MONDO ENTERPRISE

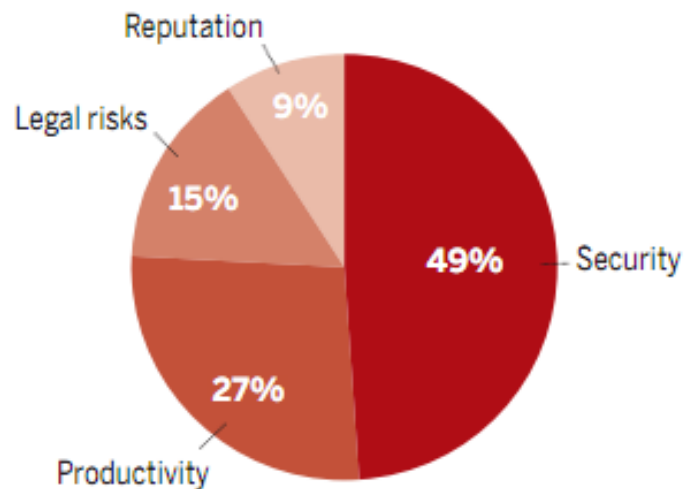


How Many Companies Are About To Start Using Social Media?

(Master New Media, Inc 500 - 2009)

3 – MOLTI VANTAGGI, MOLTI RISCHI

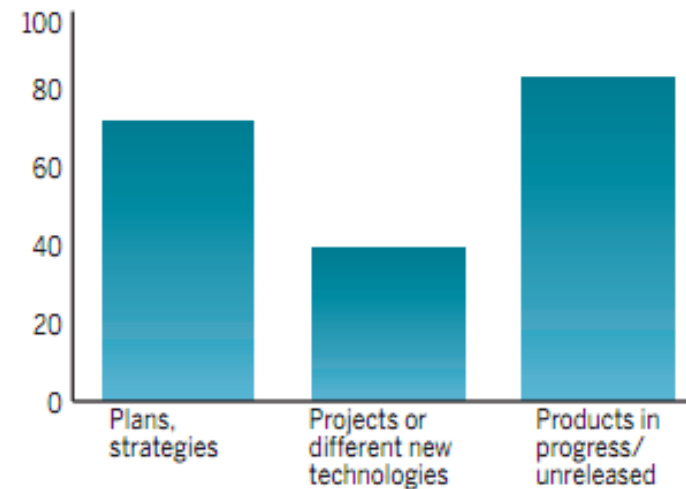
Primary concern about Web 2.0



More than \$1.1 billion was lost by organizations surveyed due to security incidents caused by Web 2.0 technologies.

Source: McAfee, Web 2.0: A Complex Balancing Act

Confidential information disclosed



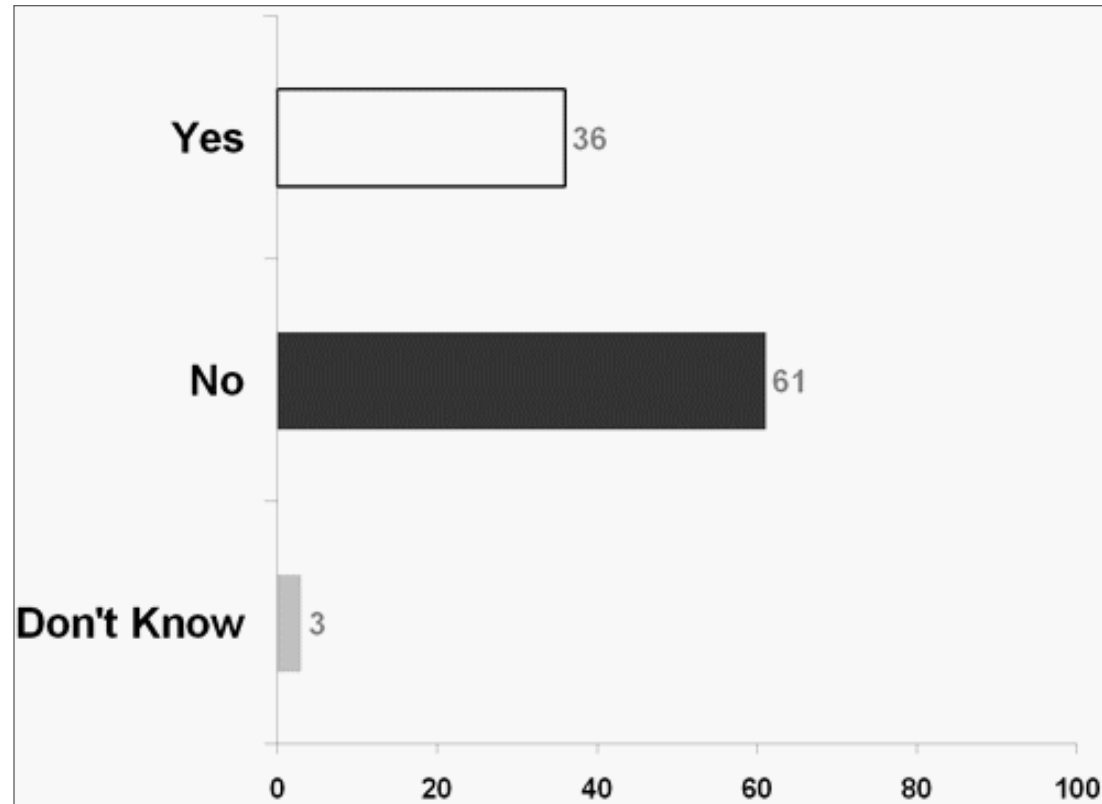
Social network users aren't preoccupied with the real identity of the people they meet online or about the details they share while chatting with strangers. After two hours of conversation, respondents revealed the above data about their company.

Source: BitDefender, Social Networking and the Illusion of Anonymity

Misurazione sul campo delle problematiche

(SC Magazine – Shining the spotlight on Social Media - 2010)

3 – AWARENESS NEL MONDO ENTERPRISE



How Many Companies Have an Official Social Media Policy?

(Master New Media, Inc 500 2009)

3 – PREVISIONI DI DIFFUSIONE DEI SOCIAL MEDIA

*“By **2014**, social networking services will **replace e-mail** as the primary vehicle for interpersonal communications for **20 percent of business users**.”*

*“By **2012**, over **50 percent of enterprises** will use **activity streams** that include **microblogging**.”*

*“Within **five years**, **70 percent of collaboration and communications applications** designed on PCs will be modeled after user experience lessons from **smartphone** collaboration applications.”*

(Gartner - Predicts 2010: Social Software Is an Enterprise Reality)

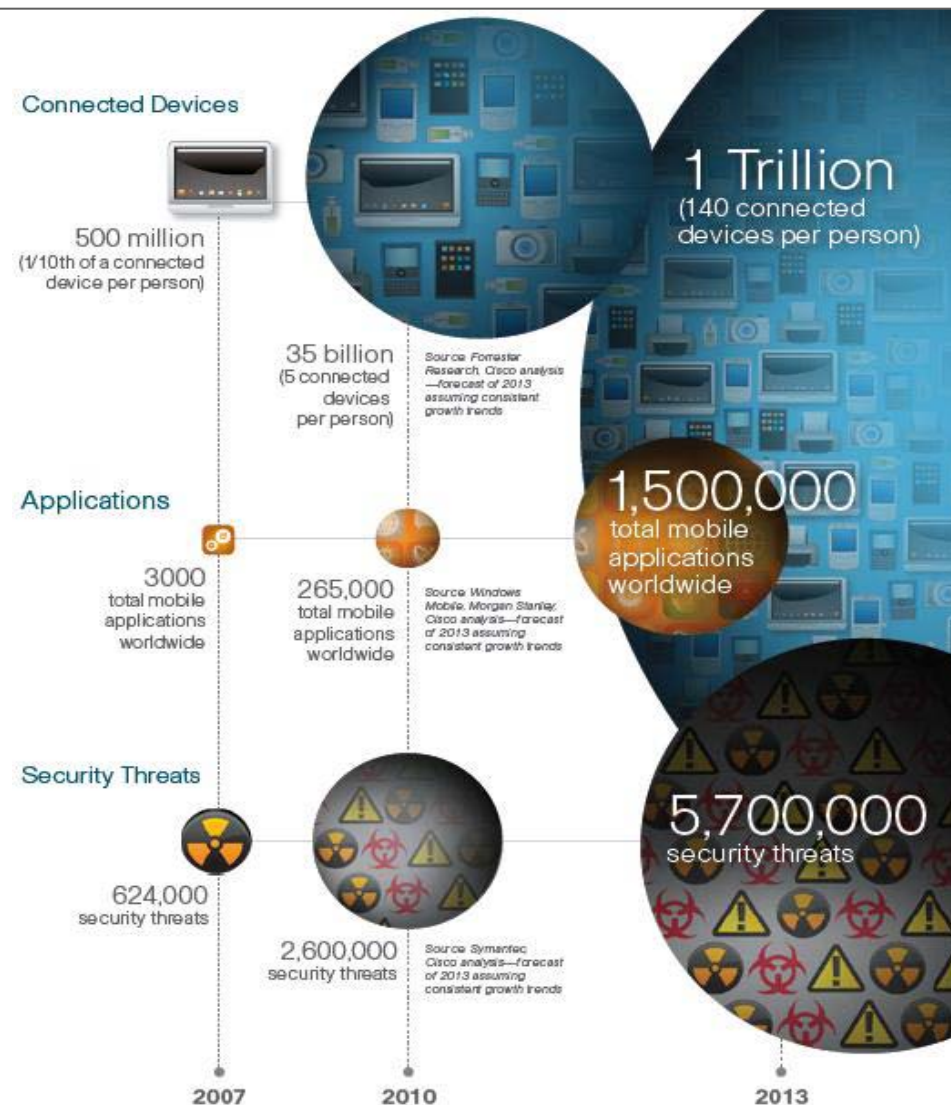


3 – CONSEGUENZE

La prevista diffusione dei Social Media determinerà un **aumento esponenziale** dei **dispositivi** e degli **utenti connessi**, con una crescita corrispondente dei **rischi di sicurezza**, in particolare a causa della proliferazione di **dispositivi mobili** e di servizi **cloud-based**.

Nei **prossimi 3 anni** si stima che **le minacce raddoppieranno**, e che i **rischi** aumenteranno in modo più che proporzionale.

(Cisco 2010 Midyear Security Report)



4 – DEFINIZIONE DI ICT SECURITY

La **Sicurezza Informatica** è la risultante dell'**interazione** tra **tecnologie**, **servizi**, **regolamenti** e **comportamenti** individuali deputati alla **protezione del patrimonio** di un'organizzazione e degli **strumenti informatici** utilizzati per la sua gestione.

Si realizza applicando i seguenti **criteri di protezione** delle informazioni a tutta la catena di **utenti**, **tecnologie** e **processi** coinvolti:

- Autenticità
- Confidenzialità
- Integrità
- Disponibilità
- Tracciabilità

all'interno di un **processo continuativo** di **definizione** e **gestione dei rischi**.

4 – DEFINIZIONE DI RISCHIO

Il rischio si definisce come la *“possibilità di subire un danno, una perdita, come eventualità generica o per il fatto di esporsi a un pericolo”* (Garzanti)

Il **rischio effettivo** si descrive tramite la seguente formula:

$$R = (P \times D) / K$$

dove

P = probabilità dell'accadimento

D = gravità del danno

K = livello di informazione, formazione e preparazione

Con riferimento ai Social Media, quali sono gli **rischi**, e quali sono gli **asset a rischio**? Soprattutto, come si incrementa il **“Fattore K”**? 😊



4 – LE MINACCE DEI SOCIAL MEDIA

Le **minacce generiche** derivanti dall'uso dei Social Media si possono riassumere in:

- Malware (trojan, worms, rootkits, etc)
- Applicazioni di terze parti non trusted
- Spam (in combinazione con malware)
- Phishing & Whaling
- Furto di identità
- Danni alla privacy
- Diffamazione
- Stalking

(La Sicurezza dei Social Media – iDialoghi settembre 2010)



4 – LE MINACCE IN AMBITO BUSINESS

Oltre alle minacce generiche, le **minacce specifiche** derivanti dall'uso dei Social Media **in ambito business** si possono riassumere in:

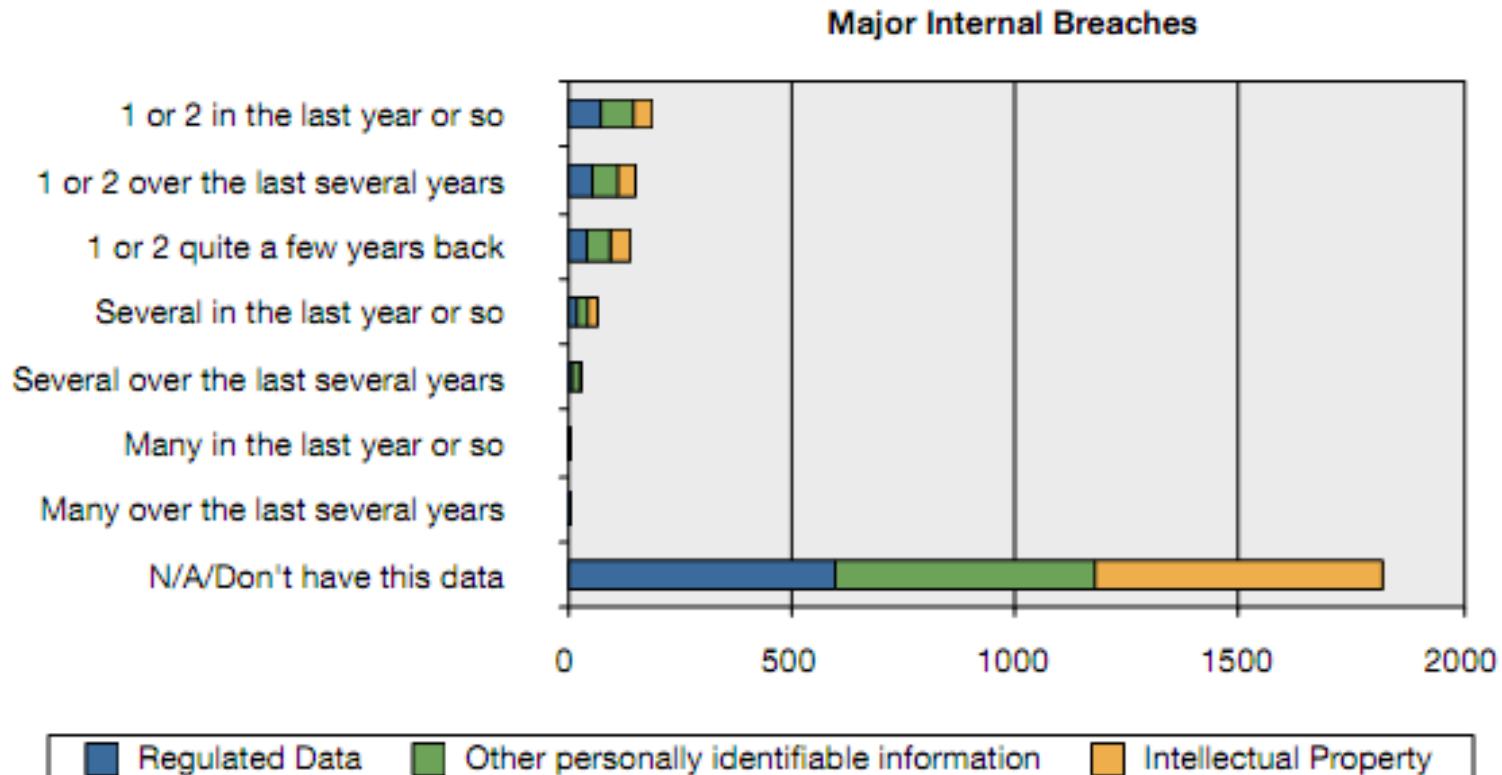
- Danni all'immagine ed alla reputazione
- Perdita di dati riservati / proprietà intellettuale
- Open Source Intelligence (OSInt) da parte di concorrenti
- Danni a terze parti (liabilities / responsabilità)
- Frodi e Social Engineering
- Minore produttività dei collaboratori

I **rimedi** a queste minacce sono **educativi**, **tecnologici** ed **organizzativi**...

e funzionano **solo** se sono applicati **insieme**.



4 – WIKILEAKS DOCET...



How Many Companies Know about their Security Breaches?

(Securosis 2010 Data Security Survey)

4 – OSTACOLI ALLA SICUREZZA DEI SOCIAL MEDIA

- Un numero crescente di minacce si realizza a livello **semantico**, impossibile da monitorare e gestire con strumenti tradizionali;
- **Consumerization of Enterprise IT**: gli utenti utilizzano strumenti propri;
- Per vari motivi, è "**vietato vietare**" (particolarmente in Italia);
- La **normativa** tutela (giustamente) la privacy e le libertà dei collaboratori, **complicando** le attività di monitoraggio;
- La **consapevolezza** dei problemi è ancora **molto bassa**, a tutti i livelli;
- Le **tecnologie** di mitigazione **non sono ancora al passo** con le problematiche (ma si evolvono a gran velocità);
- Le **policy** ed i **comportamenti virtuosi** sono sempre **in ritardo** rispetto alla tecnologia.

5 – IMPLEMENTARE IL “FATTORE K”

Le **4 strategie** da implementare per **ridurre i rischi** e **dare efficacia** ai **rimedi**:

- Rimediare alla mancanza di **procedure** standard, di **policies**, di strumenti organizzativi, di **piani di rientro** ed in generale di **cultura aziendale**;
- Implementare **strumenti tecnologici efficaci** di **monitoraggio e controllo**...
firewall, proxy e antivirus non servono (quasi) più a niente!
- **Responsabilizzare** gli **utenti** e le **strutture aziendali** coinvolte, a qualsiasi titolo, dall'uso dei Social Media. Non è un problema (solo) dell'IT!
- Ridurre i **comportamenti a rischio** contrari alle policies aziendali: secondo Cisco, solo il **10%** degli utenti le rispetta, mentre il **50% non le conosce** ed il restante **40% le aggira!** (*Cisco connected world report - nov 2010*)

5 – LE SOLUZIONI TECNOLOGICHE

Sul “**fronte interno**” (NB non c’è più il perimetro!)

- Strong Authentication + Network Access Control + Next Generation Firewall
- Endpoint protection / Application control / Device control (anche mobile!)
- Data Loss & Leakage prevention / DRM / Encryption end to end

Sul “**fronte esterno**”

- Cloud based antimalware / Reputation based monitoring
- Reputation Management / Brand Management
- OSInt / Analisi e correlazione dei contenuti a livello semantico (testi e immagini)

Tutto questo in un’ottica di **Risk Management, Governance & Compliance!**

5 – LE SOLUZIONI FORMATIVE ED ORGANIZZATIVE

Awareness e Policy

- Fare formazione costante a tutti i livelli (management, utenti, partner);
- Definire regole chiare e condivise specifiche per l'utilizzo dei Social Media;
- Controllare e misurare il loro livello di adozione e la loro efficacia nel tempo;

Organizzazione

- Creare una struttura per la gestione della **Social Media Strategy** che includa ed integri competenze di Marketing, Legali, di HR e di Information Security Management;
- Nominare un **unico responsabile** per la Social Media Strategy che abbia una **visione globale** dei problemi e delle opportunità;
- Scegliere i **consulenti** giusti 😊

6 – CONCLUSIONI

"The most significant risk is usually the unplanned, unmanaged mass-adopted behavior or technology change"

(Sophos - Social media in the enterprise: Great opportunities, great security risks)

Vietare non è solo impossibile, ma anche controproducente: **social** è il nuovo paradigma di comunicazione del **Web 2.0**, indietro non si torna.

Gestire i nuovi scenari di sicurezza derivanti dall'utilizzo dei Social Media in ambito business è una **necessità** ed un'**opportunità**.

Selezionare le **tecnologie più adatte**, **formare** le persone, individuare le **policies** ed i **controlli** più efficaci in ogni contesto specifico ed integrarli nei sistemi di **Governance** esistenti è una **sfida** che accettiamo con piacere...

Parliamone **insieme!**

GRAZIE!

***i*DIALOGHI**

ICT Security & Consulting

web <http://www.idialoghi.com>

e-mail info@idialoghi.com

skype [idialoghi](https://www.skype.com/people/idialoghi)

