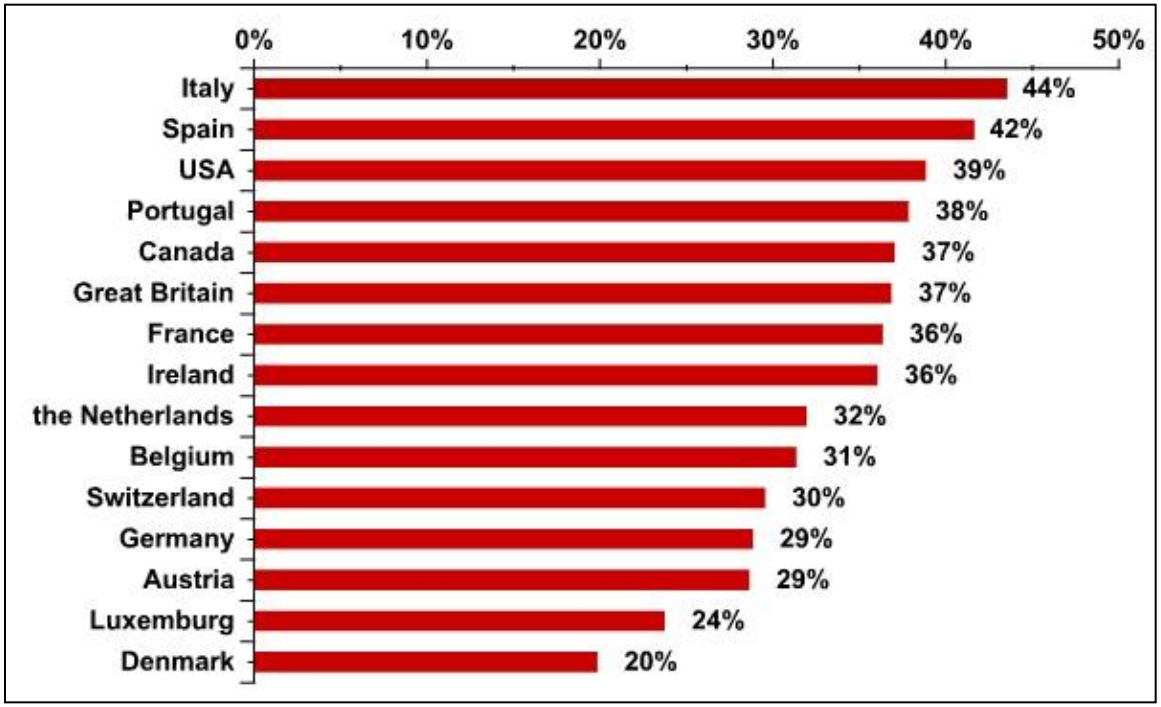
16 novembre – E-privacy

Big Data e Cyber Risk.

Giuseppe Vaciago

Alcuni dati: un primato europeo

In Italia vi sono **38.4 milioni di utenti** nella fascia **11-74 anni** con accesso continuo ad Internet, e quasi **20 milioni** in grado di connettersi con uno smartphone o tablet (Fonte: Audiweb Trends, 2013). Il **44%** dei pc italiani sono attaccati da malware contro il 20% di quelli danesi (Fonte: Kaspersky Lab).



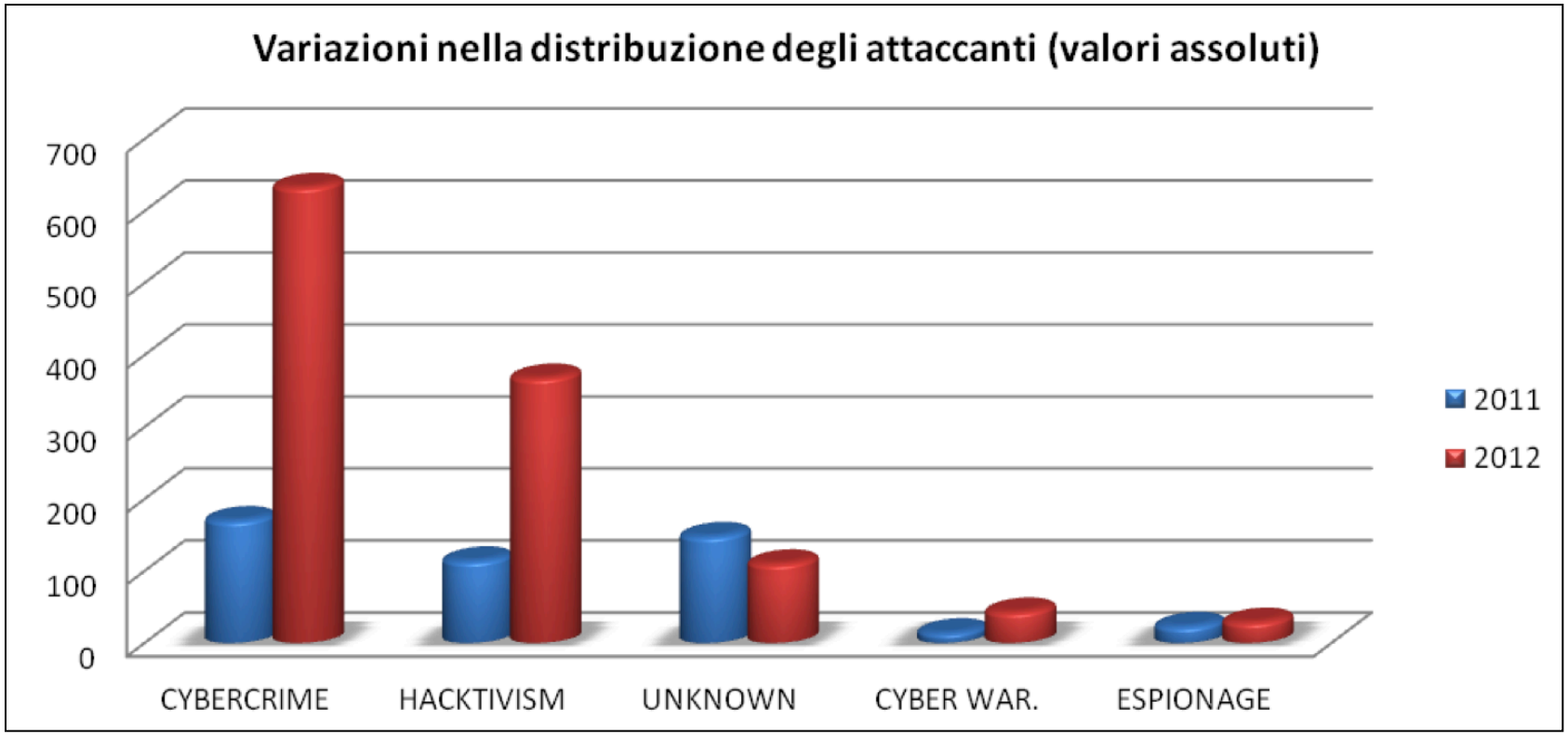
Alcuni dati: un'analisi degli attacchi

Il **rapporto Clusit 2013 identifica un rapido cambiamento del trend:** iniziano ad essere colpiti **tutti i settori industriali** e non solo più il settore governativo o quello dell'industria multimediale

VITTIME PER TIPOLOGIA	2011	2012	Totale	Incremento
Institutions: Gov - Mil - LEAs - Intelligence	153	374	527	244,44%
Others	97	194	291	200,00%
Industry: Entertainment / News	76	175	251	230,26%
Industry: Online Services / Cloud	15	136	151	906,67%
Institutions: Research - Education	26	104	130	400,00%
Industry: Banking / Finance	17	59	76	347,06%
Industry: Software / Hardware Vendor	27	59	86	218,52%
Industry: Telco	11	19	30	172,73%
Gov. Contractors / Consulting	18	15	33	-16,67%
Industry: Security Industry:	17	14	31	-17,65%
Religion	0	14	14	1400,00%
Industry: Health	10	11	21	110,00%
Industry: Chemical / Medical	2	9	11	450,00%
TOTALE	**469**	**1.183**	**1.652**	**252,24**

Alcuni dati: un'analisi degli attacchi

Aumentano gli attacchi per finalità di **cybercrime** rispetto agli attacchi degli attivisti. 1 attacco su 2 è non è per finalità dimostrative.

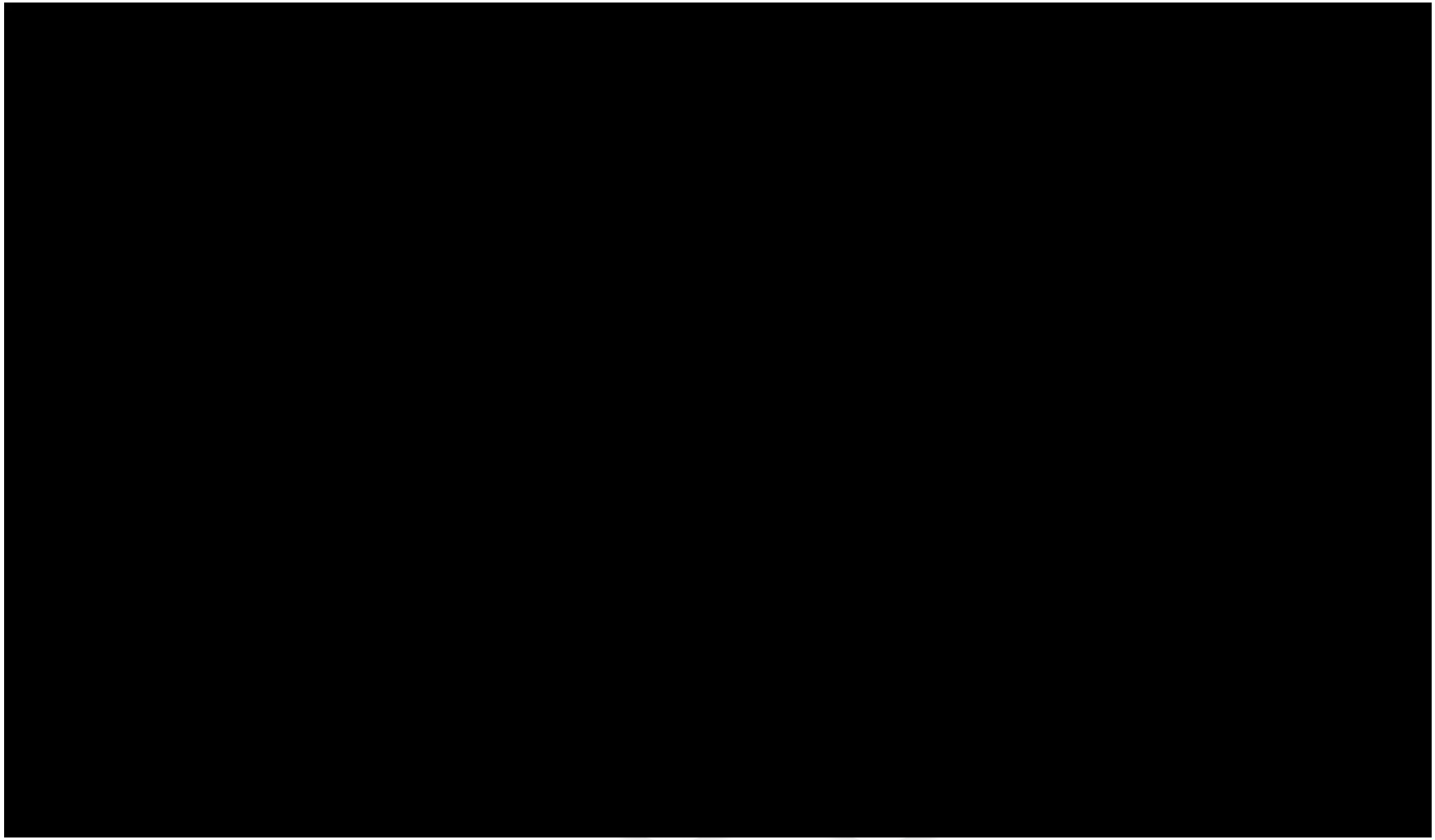


Tipologie di attacchi

- Attività fraudolente poste in essere da insider e outsider
- Attività di “phishing”
- Furto di dati confidenziali, furto di dati e spionaggio industriale
- Accessi non autorizzati da parte dei lavoratori
- Accessi non autorizzati da parte di esterni (hacking)
- Violazioni contrattuali
- Diffamazione e molestie sessuali
- Acquisizione e commercio di materiale pornografico e pedopornografico
- Furto di codici di accesso e pirateria informatica
- Modifica non autorizzata di dati (virus, cavallo di Troia, etc.)
- Furto di risorse informatiche aziendali per fini personali
- Denial of Services
- Abuso dell’utilizzo della posta elettronica e di internet
- Violazione di policy e regolamenti aziendali

Big Data Chronology

Social Media Security and Big Data



Alcuni Casi: “Social Botnet”

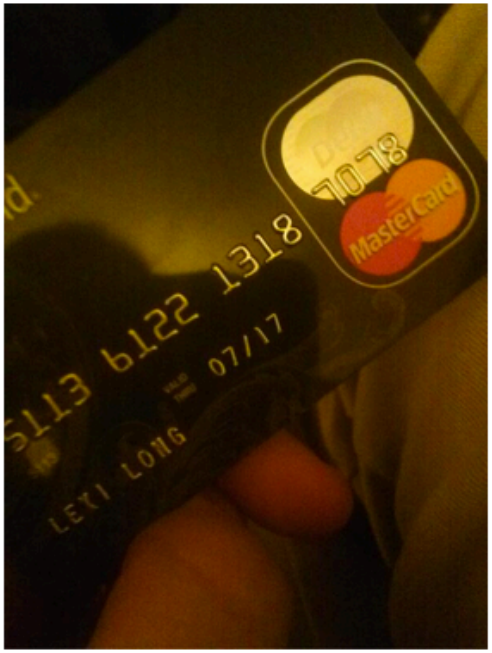
Da una approfondita indagine dell’FBI emerge che nel 2012 più di **11 milioni** di utenti di Facebook sono rimasti affetti da un particolare malware in grado di fare un danno di circa **850 milioni di dollari**.

Alcuni Casi: La “banda della firma digitale”

Un imprenditore “perde” la sua azienda perché il truffatore usando la sua smart card cede a sé stesso e al suo coimputato la totalità delle quote sociali.

Ciò avviene perché il truffatore ottiene la firma digitale dell’imprenditore incarica uno studio commercialista che facendone richiesta a suo nome non è tenuto a portare con sé l’imprenditore al momento della consegna.

Behavioral security



BYOD e Consumerization

Perdità del controllo dei device aziendali

+

Aumento del rischio di introduzione di malware

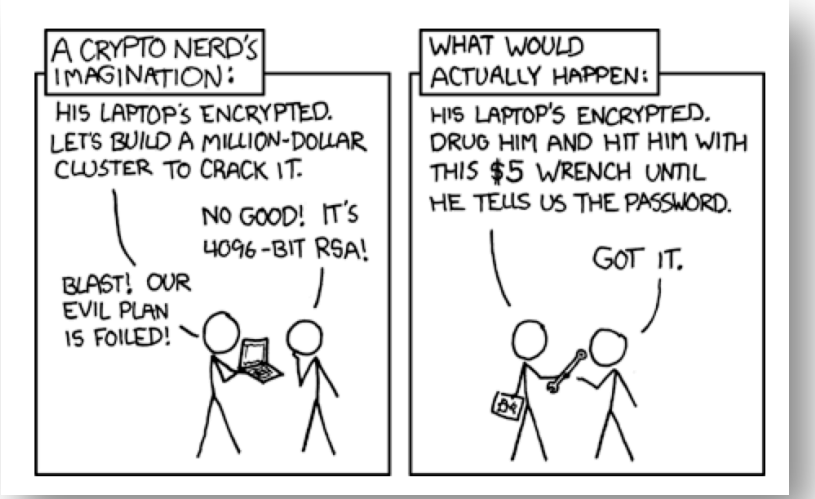
=

Aumento del rischio di perdita di dati aziendali

Cyber security e Human Element

La sicurezza di un sistema è garantita da:

- Protocolli
- Tecnologia
- Elemento umano



Snowden may have persuaded 20 to 25 NSA colleagues to give up their passwords

Reuters says those borrowed creds helped Snowden get access to docs he later leaked.

Alcuni Casi: Una esemplificazione

Sicurezza informatica

Detta in altro modo: la sicurezza non è un prodotto ma un processo.

Inutile spendere milioni di euro di budget nell'IT Security se la vulnerabilità si chiama "UTONTO".

Le attività di controllo

Sistema di Gestione della Digital Forensics

È necessario un sistema di gestione con un approccio di tipo preventivo rispetto alle esigenze di investigazione informatica, fondato su 4 presupposti:

Privacy reato “231” – Occasione persa

Il decreto “femminicidio” non ha ricompreso tra i reati presupposto per la responsabilità dell’impresa il trattamento illecito di dati personali. Inoltre sarebbe comunque mancato l’art. 169 del Codice Privacy che prevede una sanzione alla persona fisica che viola le misure di sicurezza di un sistema informatico.

La normative utili in tema di sicurezza informatica

Grazie per l’attenzione

Avv. Giuseppe Vaciago
giuseppe.vaciago@replegal.it
http://it.linkedin.com/in/vaciago
https://twitter.com/giuseppevaciago