malabo
ICT Advisory

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

smau
MILANO 22-24 OTTOBRE 2014

Workshop AIPSI Arena Security SMAU
23 ottobre 2014

OAI 2014: un'anteprima sugli attacchi informatici in Italia e nel mondo

Marco R.A. Bozzetti
CEO Malabo Srl
Past President ClubTI Milano – FidaInform
Consiglio Direttivo e Communication Officer AIPSI

Marco R.A. Bozzetti

- **1973 Laurea in Ingegneria elettronica al** Politecnico di Milano
- **1971-85** CREI, Centro Rete Europea Informatica, polo italiano EIN, prima rete europea di ricerca (tipo ARPA) a commutazione di pacchetto
- **1976-80** Olivetti R&D – Ivrea:Responsabile ONE, Olivetti Network Environment, e comitati standard ISO, CCITT (ora ITU-C) , ECMA (chairman VFS)
- **1980-82** Italtel: Responsabile Laboratorio R&D Reti Dati Private, **1982-84** Italtel Telematica : responsabile pianificazione strategica
- **1984-87** Arthur Andersen Management Consultants
- **1987-91** fondatore e Partner Ibimaint System Engineers
- **1988-94**: fondatore e Partner C.A.SI, Consulenti Associati Sicurezza
- **1994-95** Fondatore e Presidente Integration&Engineers nel Gruppo MET
- **1995-2000** CIO Gruppo ENI
- **2001-2005** Fondatore e Presidente ClickICT Srl Gruppo GeaLab
- **Dal 2001** Fondatore e Amministratore Unico Malabo Srl

- ***FTI, Forum delle Tecnologie dell'Informazione (fondatore)***
- ***EITO, European Information Technology Observatory (Co-ideatore e Chief Scientist)***
- ***ClubTI di Milano (Past President)***
- ***FidaInform, Federazione Italiana delle Associazioni Professionali di Information Management (Past President)***
- ***AIPSI-ISSA, Consiglio Direttivo – Comms Officer***
- ***Prospera***

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica
http://www.aipsi.org/

- **Capitolo italiano** di **ISSA**, Information Systems Security Association, (**www.issa.org**)
  - 13.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT
  - ISSA Journal, Webinar, Conferenze, …

- AIPSI è il punto di aggregazione e di trasferimento di know-how sul territorio per i professionisti della sicurezza, sia dipendenti sia liberi professionisti ed imprenditori del settore

- **Primari obiettivi AIPSI**
  - diffondere la cultura e la sensibilizzazione per la sicurezza informatica agli utenti digitali,
  - offrire ai propri Soci qualificati servizi per la loro crescita professionale

- **Sedi territoriali** : Milano, Ancona-Macerata, Roma, Lecce

- Collaborazione con varie associazioni ICT ed Enti per eventi, progetti ed iniziative congiunte: AICA, Anorc, ClubTI Milano e Roma, CSA Italy, FidaInform, Inforav, Polizia Postale, Smau, ecc.

OAI, Osservatorio Attacchi Informatici in Italia

- ***Obiettivi iniziativa***
  - Fornire informazioni sulla reale situazione degli attacchi informatici in Italia
  - Elevata serietà e trasparenza, per acquisire una elevata autorevolezza sui dati e sui commenti forniti
  - Contribuire alla creazione di una cultura della sicurezza informatica in Italia
  - Sensibilizzare i vertici delle aziende/enti sulla sicurezza informatica
  - Indagine via web cui liberamente rispondono i diversi interlocutori: il Rapporto annuale non ha stretta validità statistica ma fornisce chiare e valide indicazioni sulla situazione e sul trend in Italia, basilari per un'efficace analisi dei rischi ICT

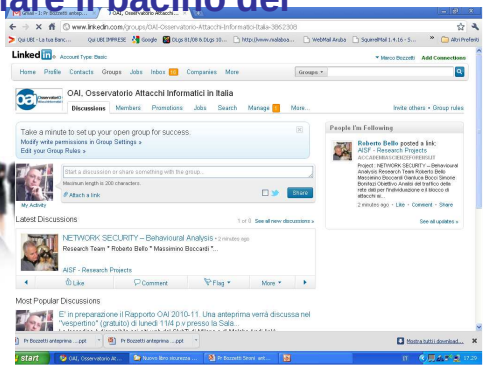
- ***Che cosa fa***
  - Indagine annuale condotta attraverso un questionario on-line indirizzato a CIO, CISO, CSO, ai proprietari/CEO per le piccole aziende
  - Rubrica mensile OAI sulla rivista Office Automation Di Soiel da marzo 2010
  - Gruppo OAI su Linked

- ***Come***
  - Elevata qualità e autorevolezza del Rapporto annuale
  - Assoluta indipendenza anche dagli Sponsor (coprire, parzialmente, i costi di realizzazione)
  - Stretto anonimato sui rispondenti al questionario on line via web
  - Collaborazione con numerose associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori
  - Volontario professionale

Gli attacchi di social engineering

Attacchi ai sistemi di controllo industriale e delle infrastrutture

Hacker, cracker e gli altri: chi sono e perché attaccano



I Rapporti OAI pubblicati e disponibili

Rapporto **OAI 2013**, di 36 pagine in formato A4, fa il punto sugli attacchi informatici in Italia rilevati nel 2012 e nel 1° semestre 2013

Rapporto **OAI 2012**, di 36 p A4, fa il punto sugli attacch nel 2010, 2011 e nel

Scaricabili da

http://www.aipsi.org/

http://www.malaboadvisoring.it/

fa il
nel 2009 e

Ra **OAI 2009** fa il punto sugli attacchi informatici in Italia rilevati nel 2007, nel 2008 e nel 1° quadrimestre 2009

OsservatoriO AttacchInformatici

OAI 2014: la quinta edizione del Rapporto OAI

- Il Rapporto OAI 2014 coprirà gli attacchi rilevati **nel 2013 e nell'intero 2014**
- Sarà pubblicato attorno a **fine febbraio – inizio marzo 2014**
- **Piano di lavoro** previsto
  - Entro metà novembre: revisione del Questionario e sua implementazione sul web
    - Revisione del **Comitato Scientifico**, presieduto dal prof. Stefano Zanero del Politecnico di Milano e ISSA International Board Director
  - Entro fine novembre 2014: acquisizione sponsor e patrocinatori
  - Da novembre 2014 a gennaio 2015: compilazione del questionario
  - Da febbraio 2015: elaborazione dati e preparazione Rapporto OAI 2014
  - Entro fine febbraio – marzo 2015 la pubblicazione del Rapporto OAI 2014 e la sua diffusione:
    - per i primi 4 mesi il download del Rapporto è in esclusiva per gli interlocutori degli Sponsor cui è stato inviato il codice coupon

Sponsorizzazioni, collaborazioni e patrocini OAI 2012-3

Sponsor

accenture
High performance. Delivered.

AICA

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

IBM

ORSYP

LOTTOMATICA GROUP
Responsibly Driving Global Gaming

seeweb

sernet GROUP

Technology Estate

TREND MICRO

e con la collaborazione di

polizia delle comunicazioni

Patrocinatori

AICA

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

ASSOLOMBARDA

ASSOCIAZIONE UTILIZZATORI ESTERI E TECNOLOGIE DELL'INFORMAZIONE

CDTI
Club Dirigenti di Informatica

ti

ti Liguria

Club TI
Club per le tecnologie dell'informazione

CTI per CLUB

FIDA
INFORM

Forum delle Competenze Digitali

FTI
FORUM per la TECNOLOGIA della INFORMAZIONE

IEEE computer society
Italy Chapter

Inforav
Istituto per lo sviluppo e la gestione avanzata dell'informazione

itSMF
ITALIA

Sponsorizzazioni e patrocini OAI 2014 alla data

Sponsor

AICA · aipsi (Associazione Italiana Professionisti Sicurezza Informatica) · DARKTRACE · sernet GROUP · Technology Estate · TREND MICRO

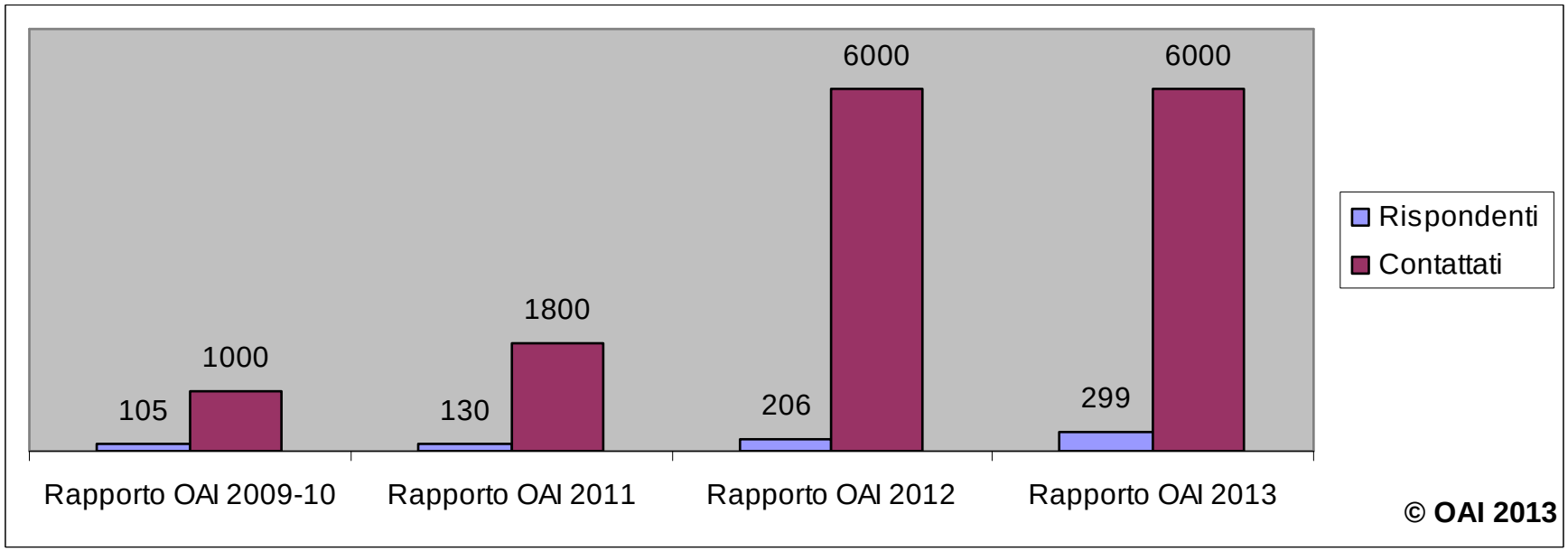
e con la collaborazione di Polizia delle Comunicazioni

Patrocinatori

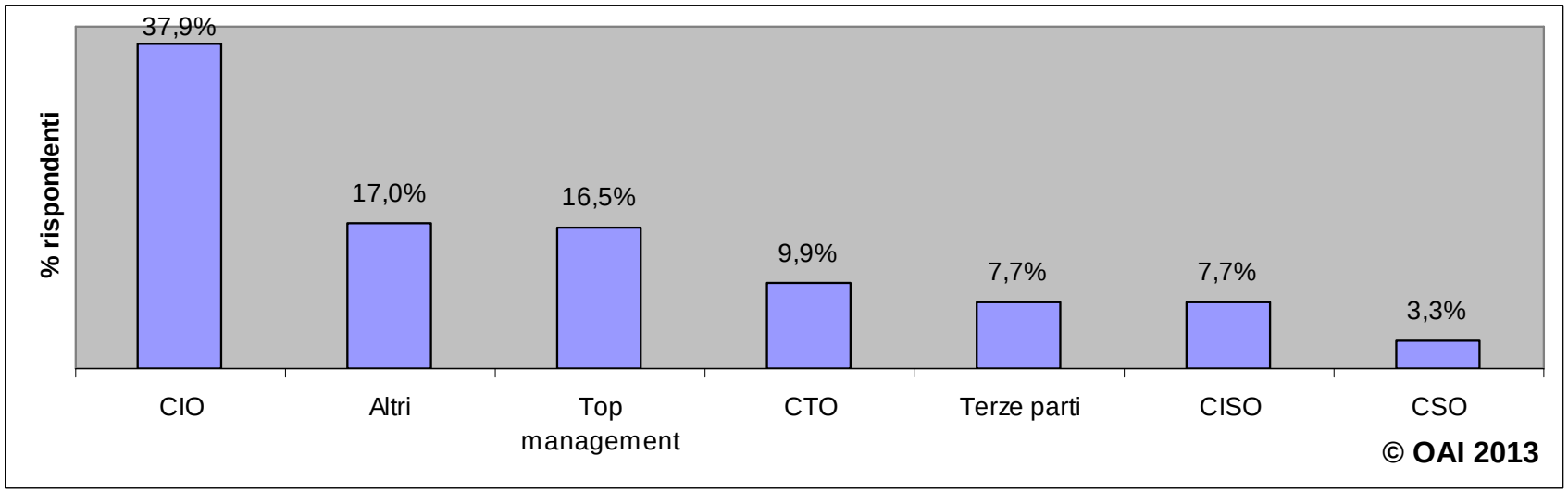
AICA · aipsi (Associazione Italiana Professionisti Sicurezza Informatica) · ASSINTEL Associazione Nazionale Imprese ICT · ASSOLOMBARDA · ASSOCIAZIONE Nazionale Sistemi e Tecnologie dell'Informazione · Club Dirigenti di Informatica · CDTI · ti

Club Ti Club per le tecnologie dell'Informazione · CTI Club · FIDA Informa · Forum delle Competenze Digitali · FTI Forum per la Tecnologia della Informazione · IEEE computer society Italy Chapter · Inforav Istituto per lo sviluppo e la gestione avanzata dell'informazione · itSMF Italia

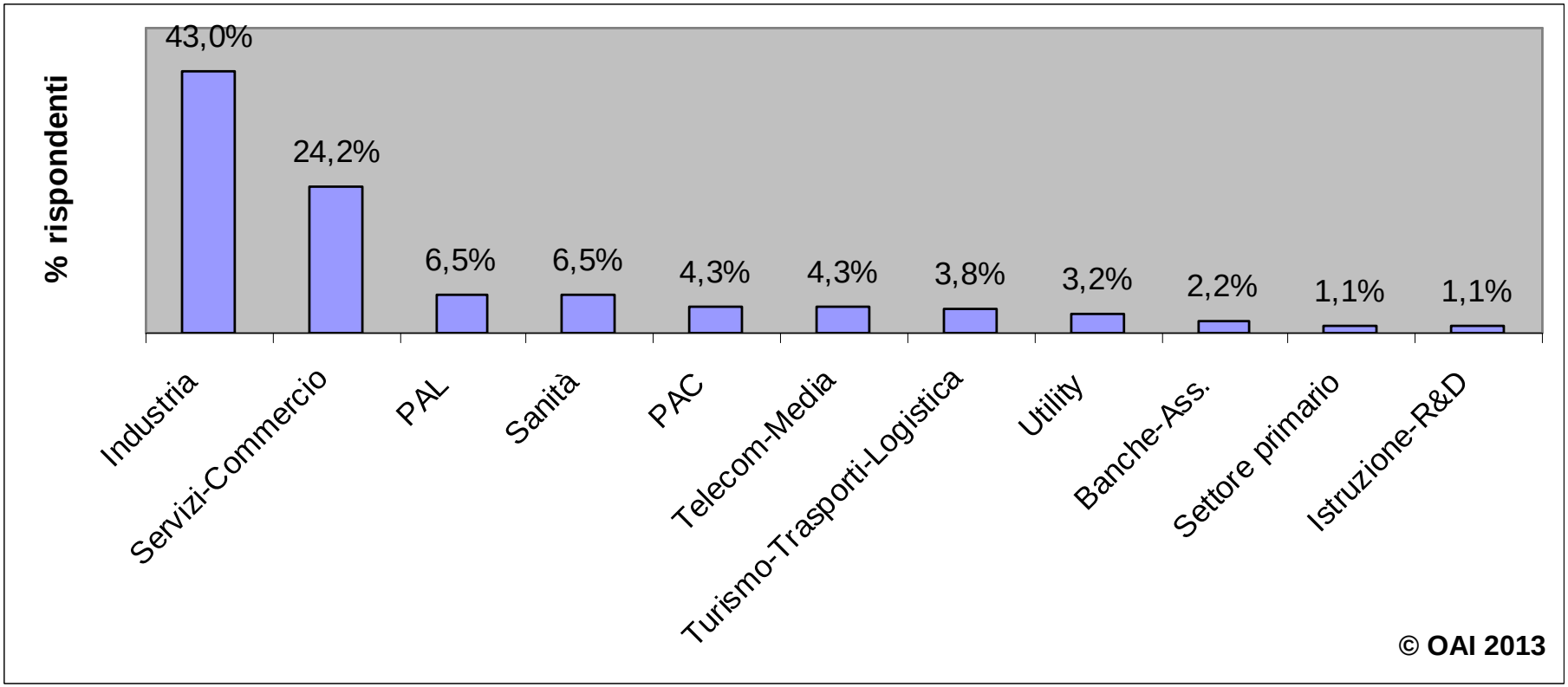
OAI 2009-2013: la crescita del numero di rispondenti



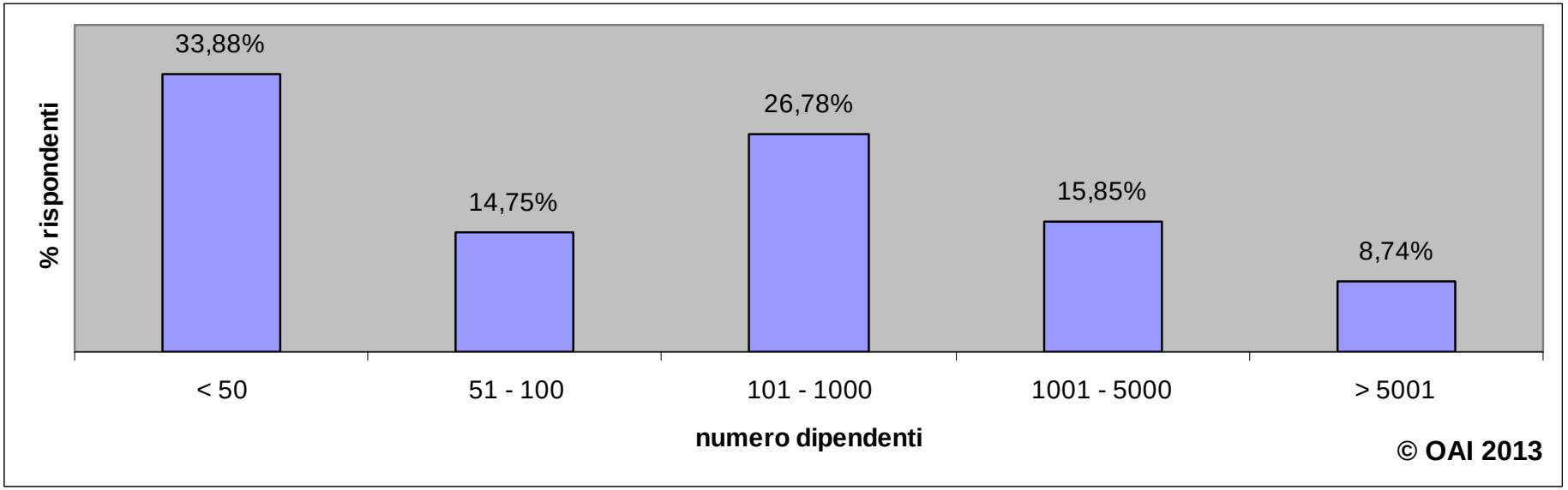
OAI 2013: Ruolo rispondenti



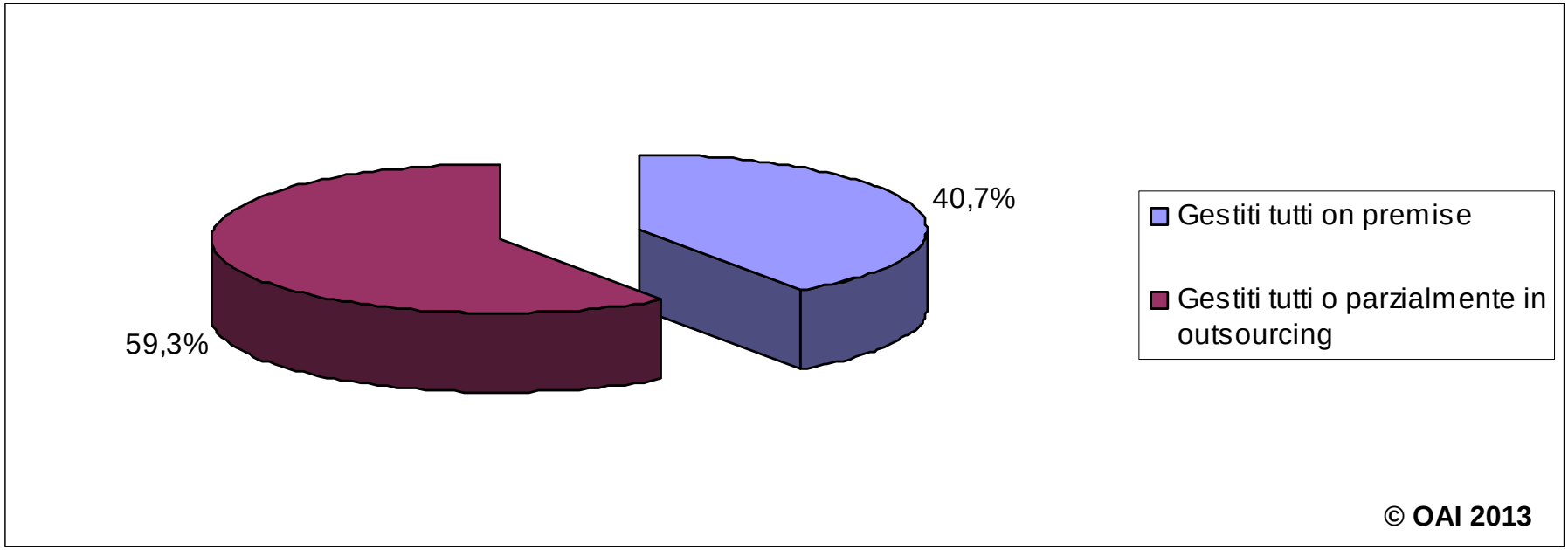
OAI 2013: Settore merceologico di appartenenza



OAI 2013: Dimensioni aziende/enti per numero dipendenti

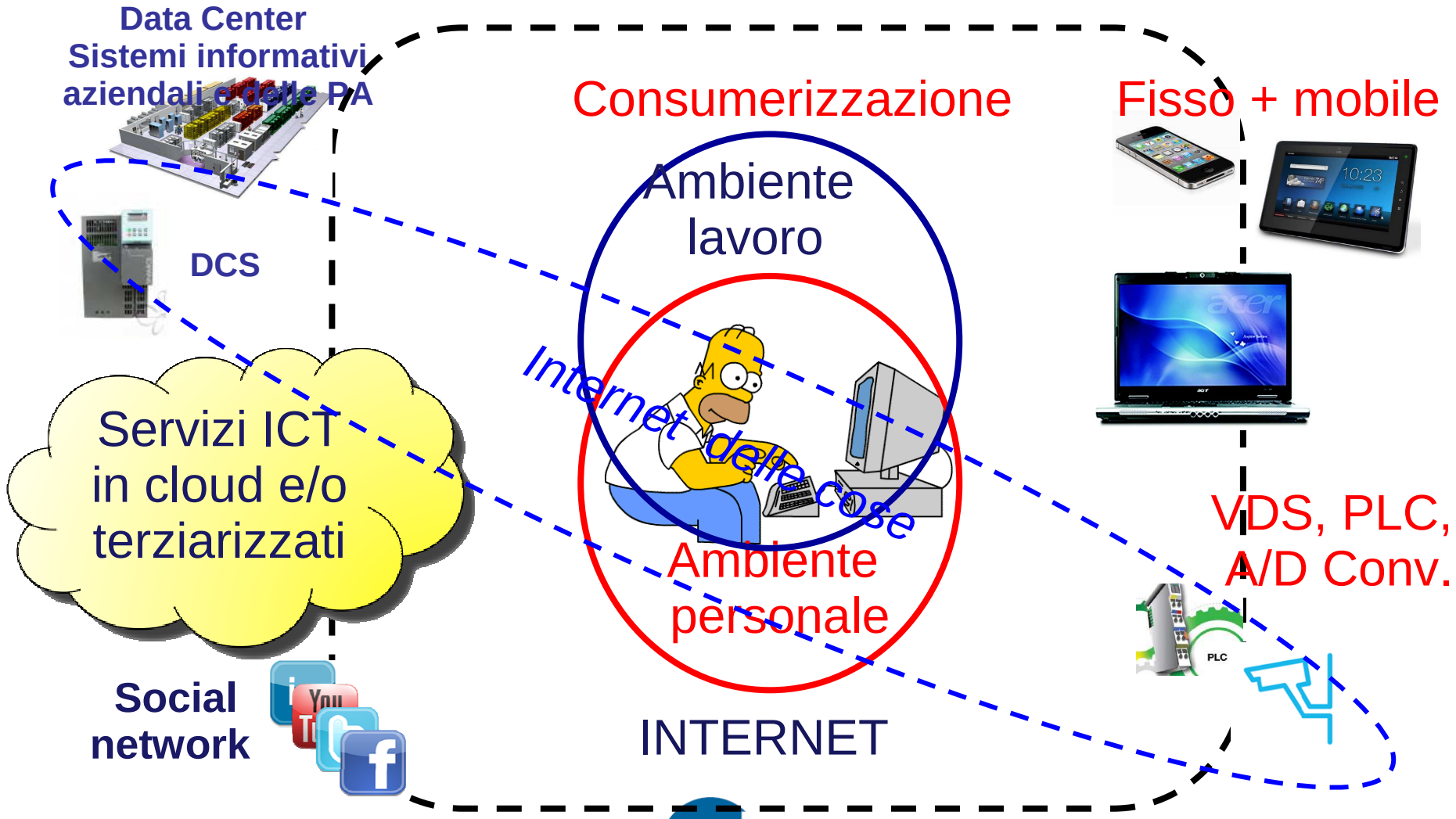


OAI 2013: Modalità di gestione del sistema informativo

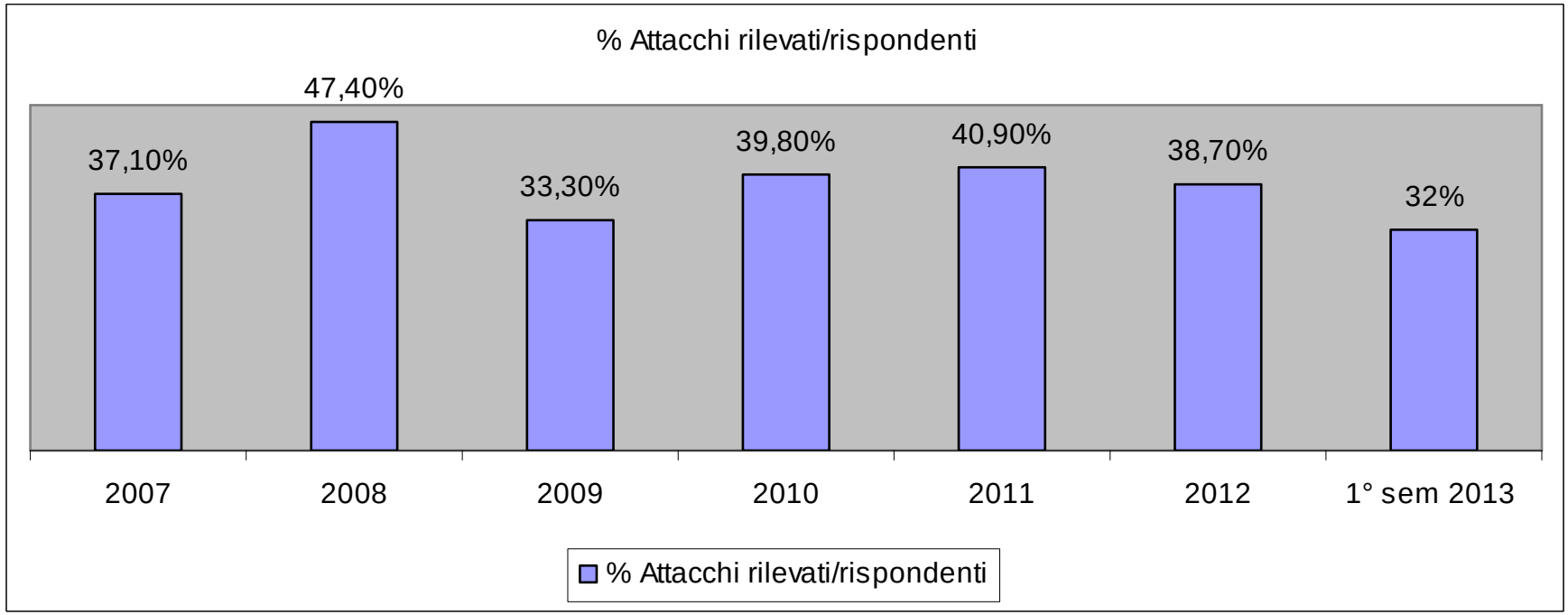


Sicurezza vo cercando ….

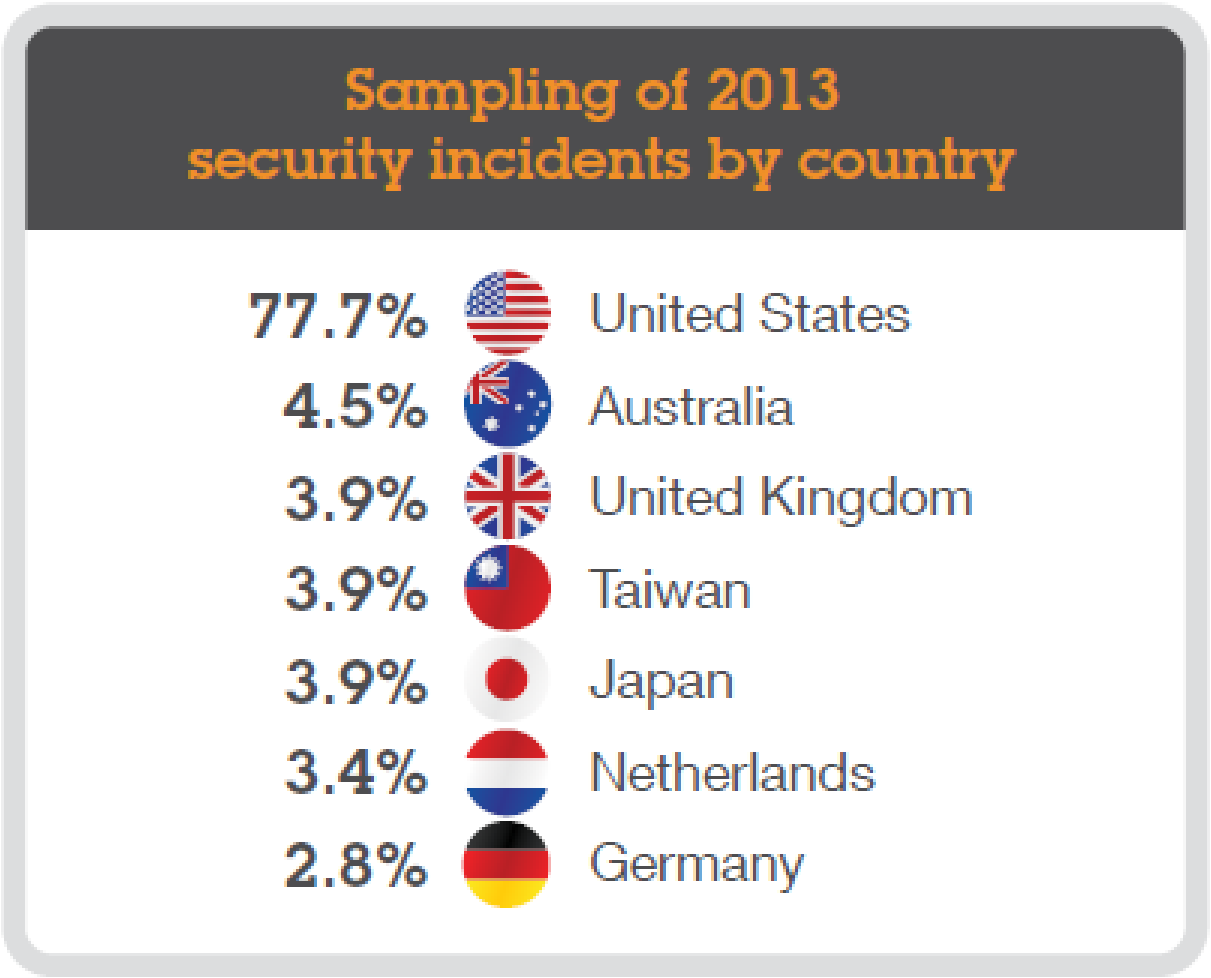
La sicurezza assoluta non esiste – aumenta la complessità



Gli attacchi intenzionali rilevati dai dati OAI 2009-2013



I paesi più attaccati nel 2013



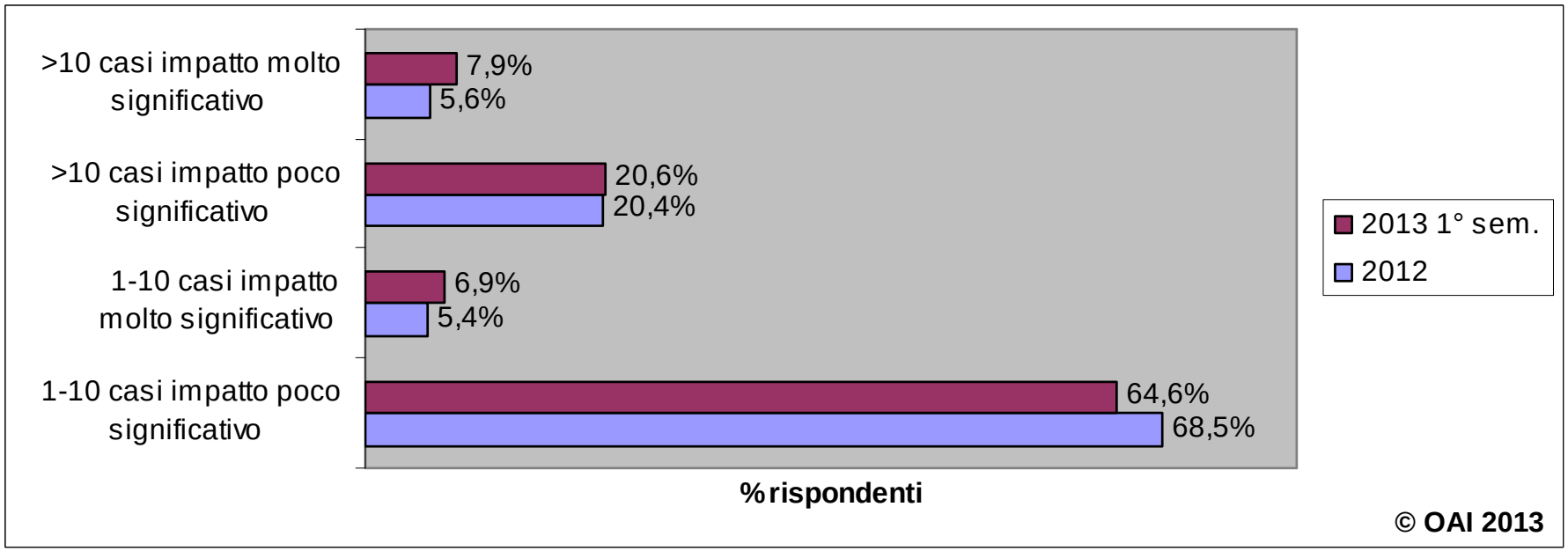
Source: IBM X-Force Report 1Q2014

Imprese in Italia (ultimi dati ISTAT)

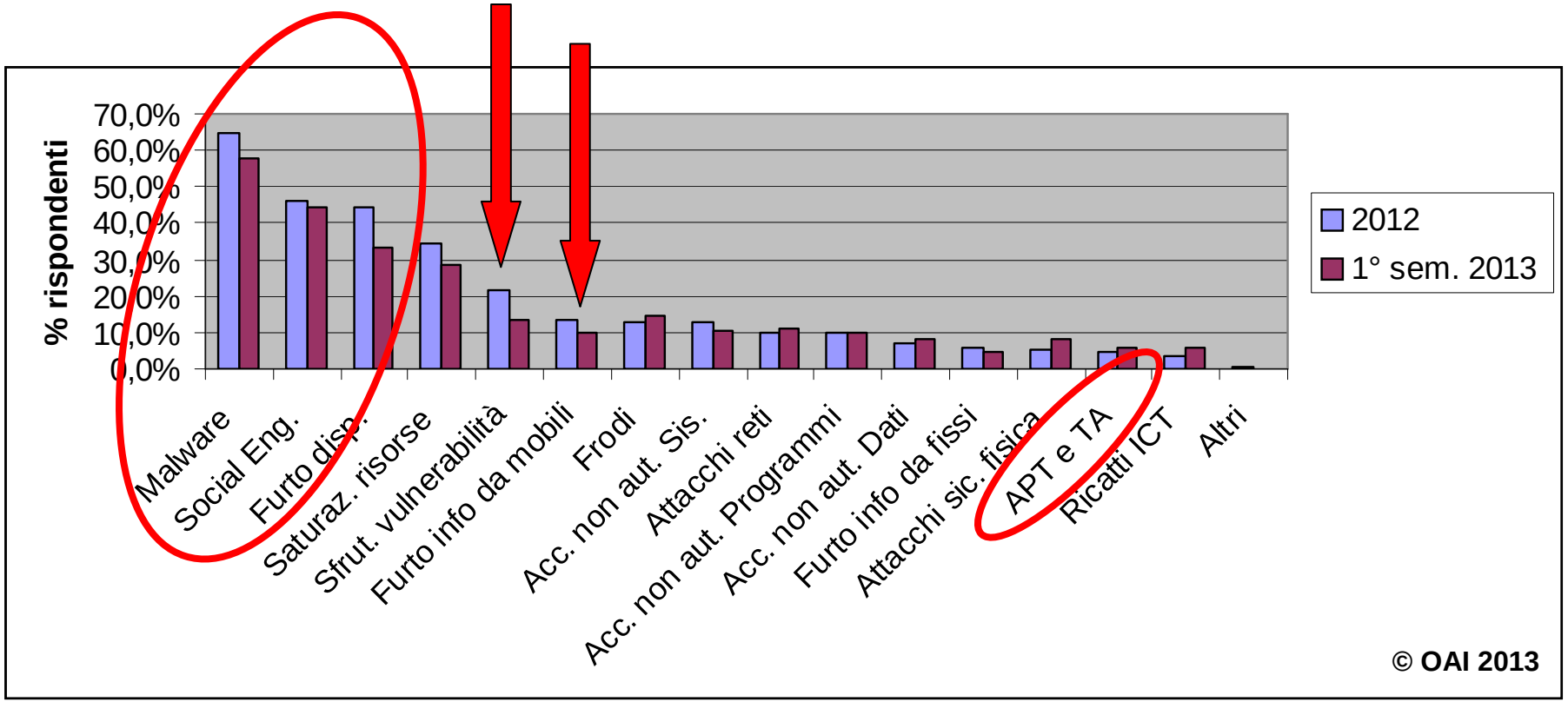
CLASSI DI ADDETTI (a)	Totale	
	Imprese	Addetti
1	**2.655.768**	**2.480.178**
2-9	**1.578.054**	**5.341.753**
10-19	**137.212**	**1.795.963**
20-49	**54.218**	**1.613.195**
50-249	**22.039**	**2.125.788**
250 e più	**3.646**	**3.520.706**
Totale	**4.450.937**	**16.877.583**

ISTAT Imprese e addetti per classi di addetti e settore di attività economica – Anno 2011 (valori assoluti)
Pubblicato 2013

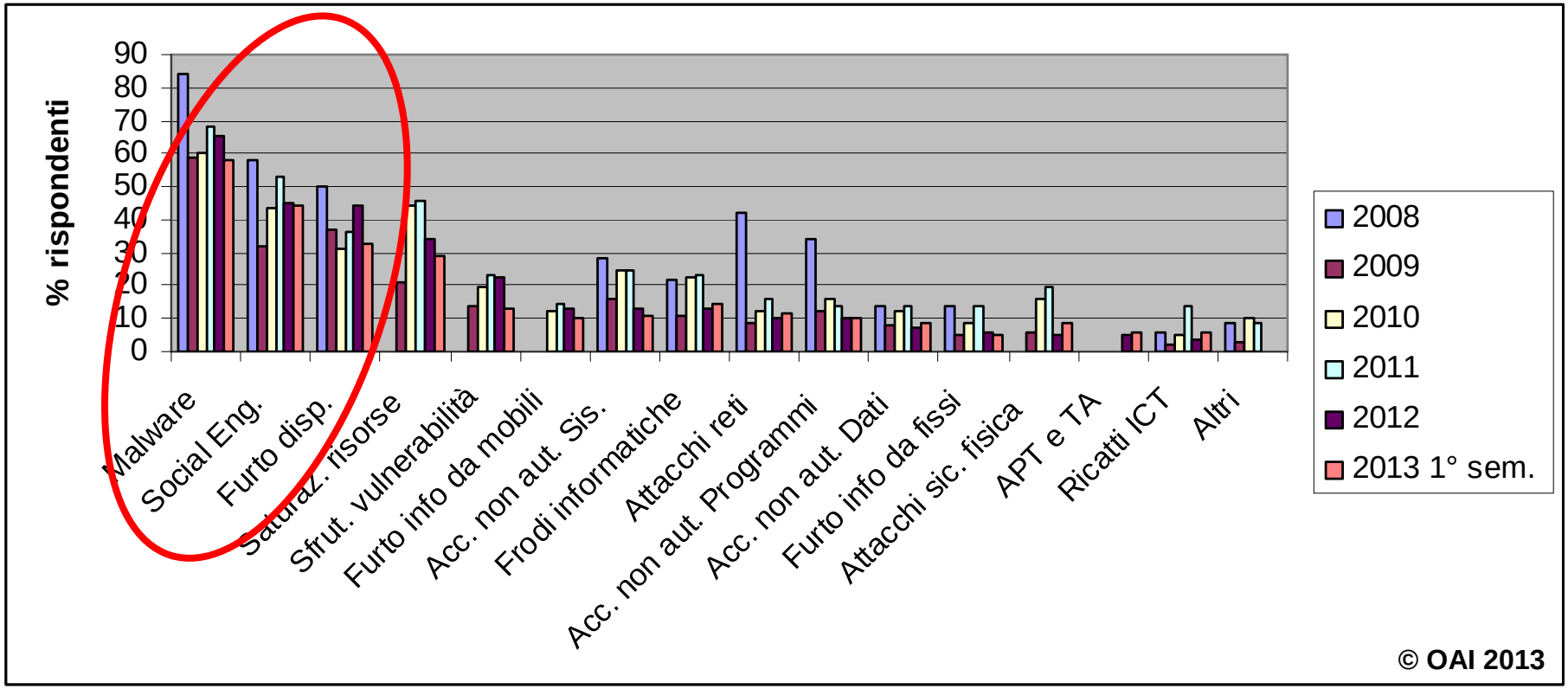
OAI 2013: Impatto dell'attacco



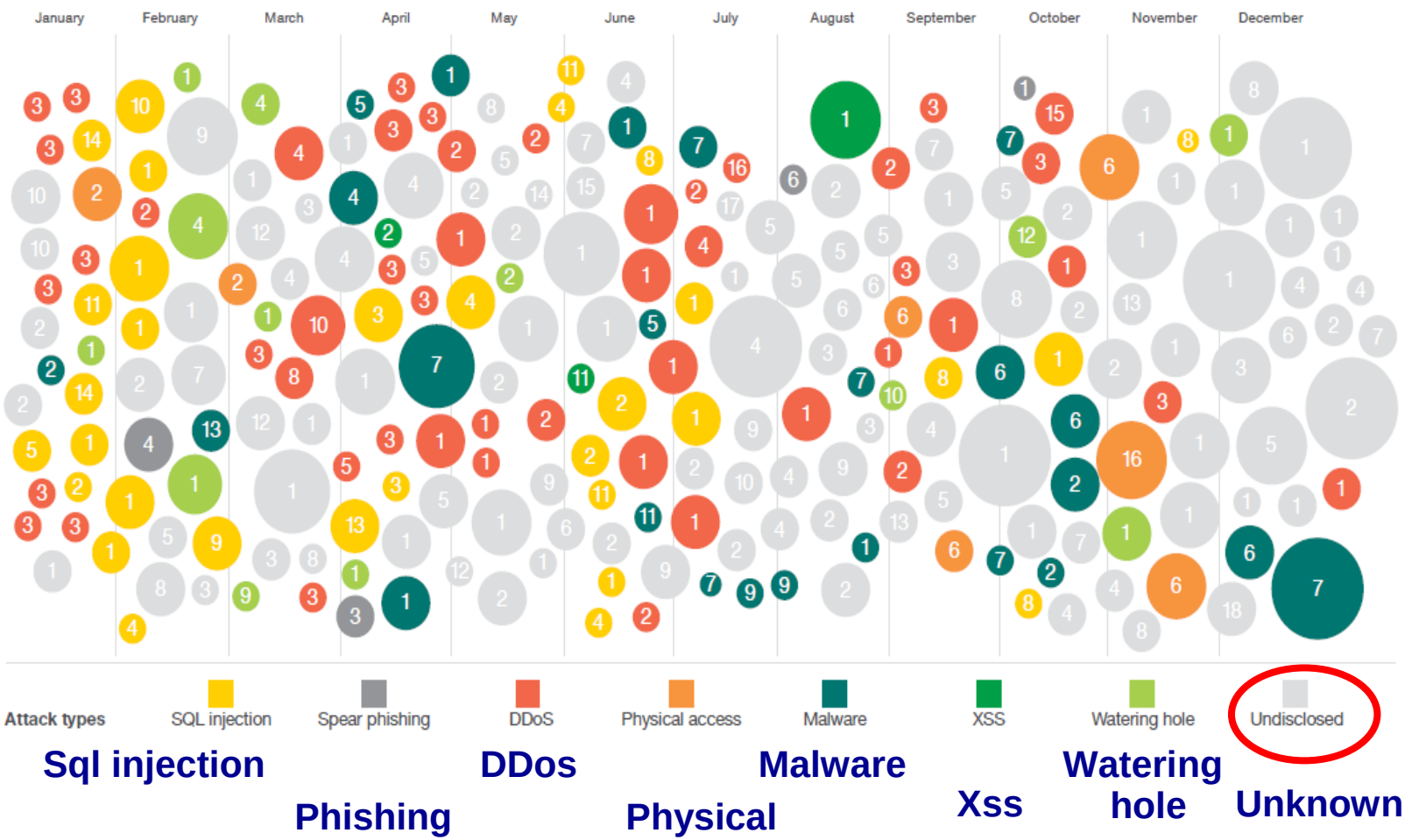
OAI 2013: Diffusione tipologia attacchi subiti 2012 - 1°sem. 2013 (risposte multiple)



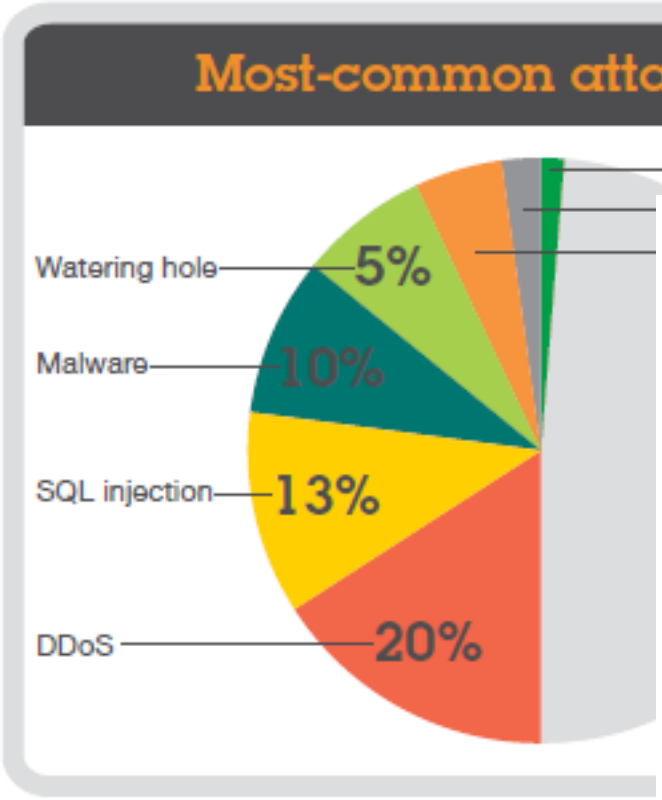
OAI 2013: Confronto diffusione attacchi 2008-1°sem. 2013 (risposte multiple, trend indicativo non statistico)



Attacchi nel 2013 a livello mondiale da IBM Xforce



Worldwide attacks status nel 2013



Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

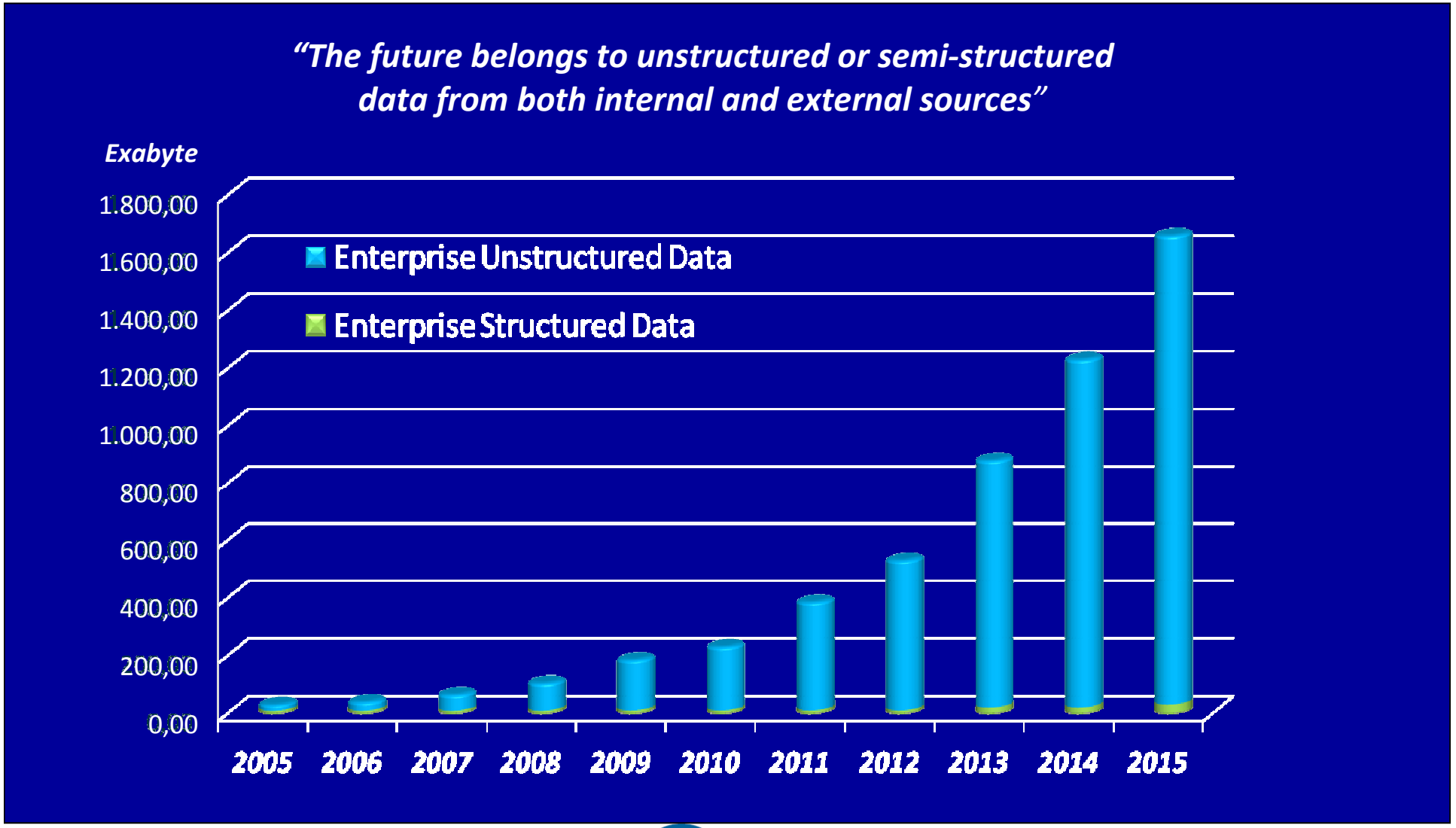
Source: IBM X-Force Report 1Q2014

Attacchi intenzionali:perché?

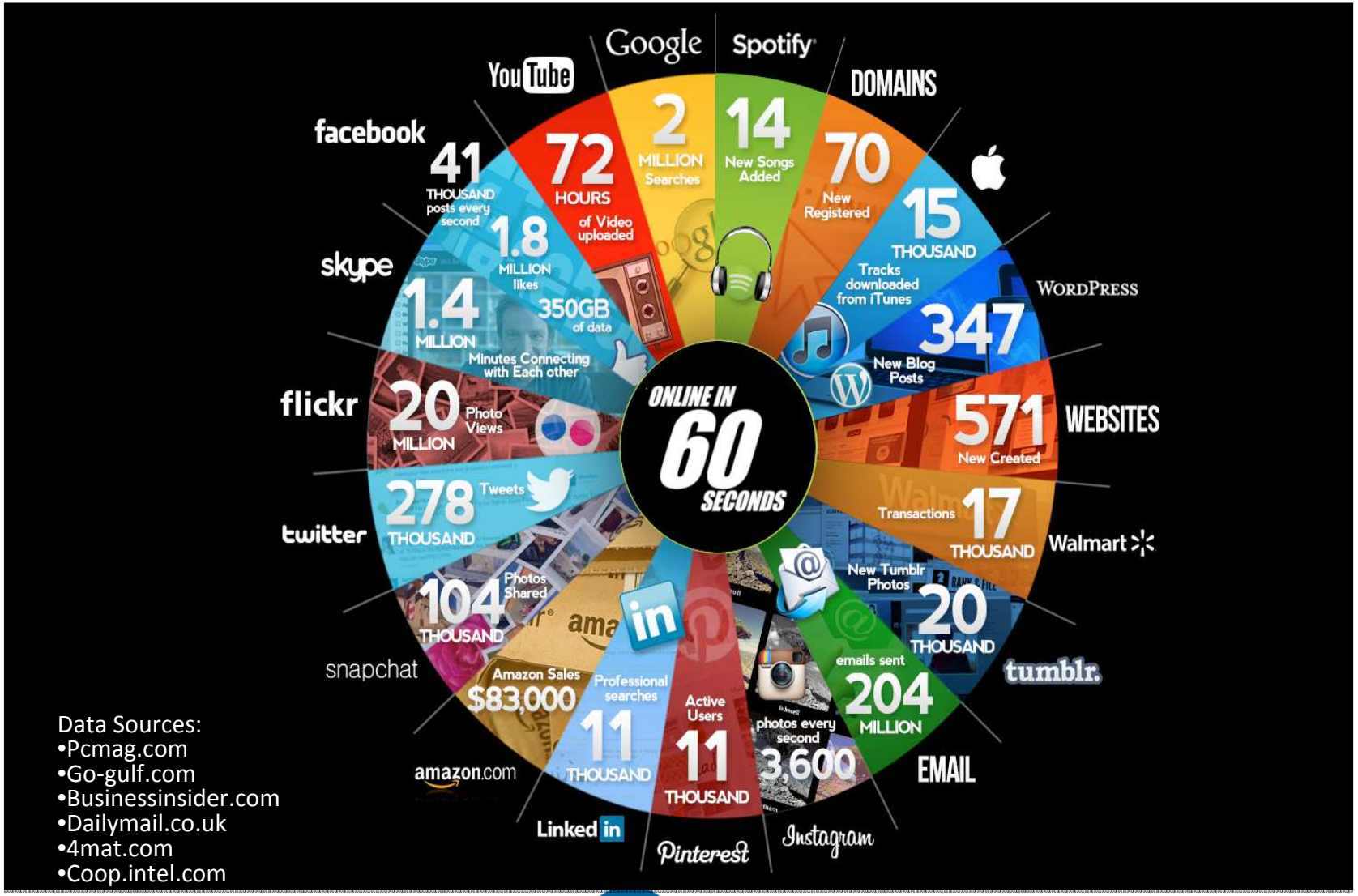
- **Lato target** (mondo digitale):
  - Crescita e pervasività uso ICT
  - innumerevoli vulnerabilità dei sistemi ICT, delle applicazioni, degli utenti, degli operatori

- **Lato attaccanti:**
  - Motivazioni criminali → guadagno economico→frodi, ricatti, furti, spionaggio industriale
    - Basso rischio ed alto guadagno (esentasse)
  - Hacktivism
  - Vendetta-ritorsione individuale
  - Esibizionismo competenze attaccante
  - Terrorismo
  - Cyberwar

L’esplosione dei dati …

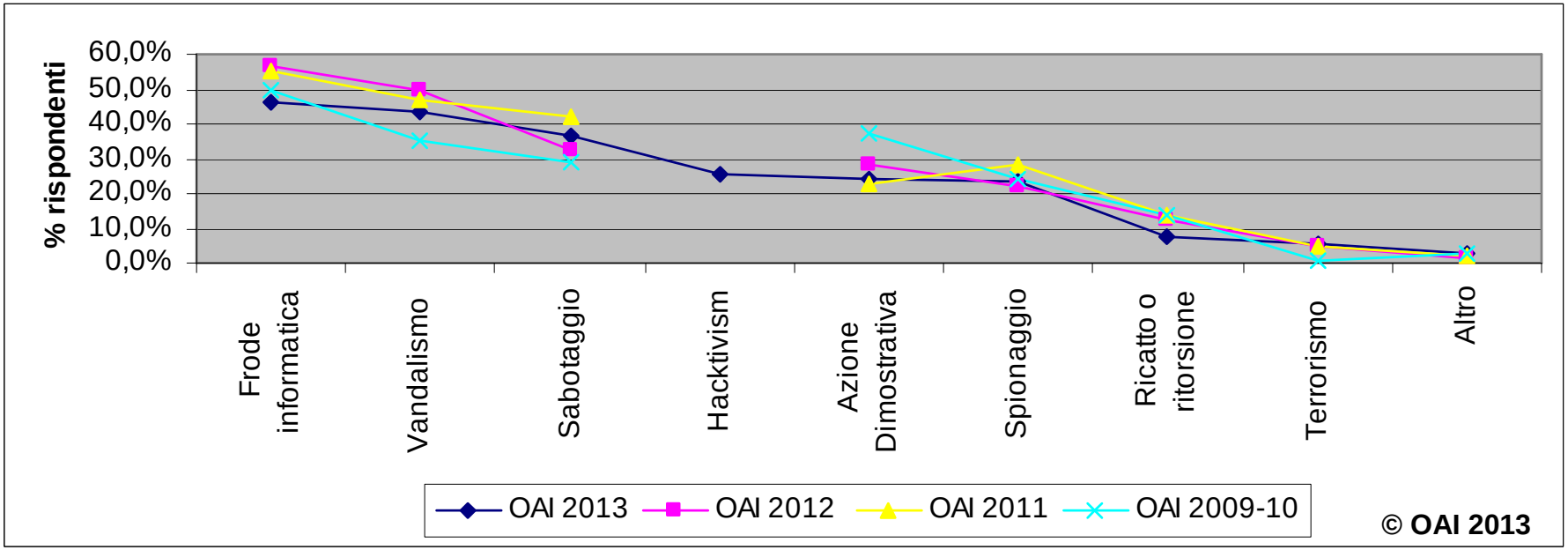


…. prodotti ad una velocità impressionante



Data Sources:
- Pcmag.com
- Go-gulf.com
- Businessinsider.com
- Dailymail.co.uk
- 4mat.com
- Coop.intel.com

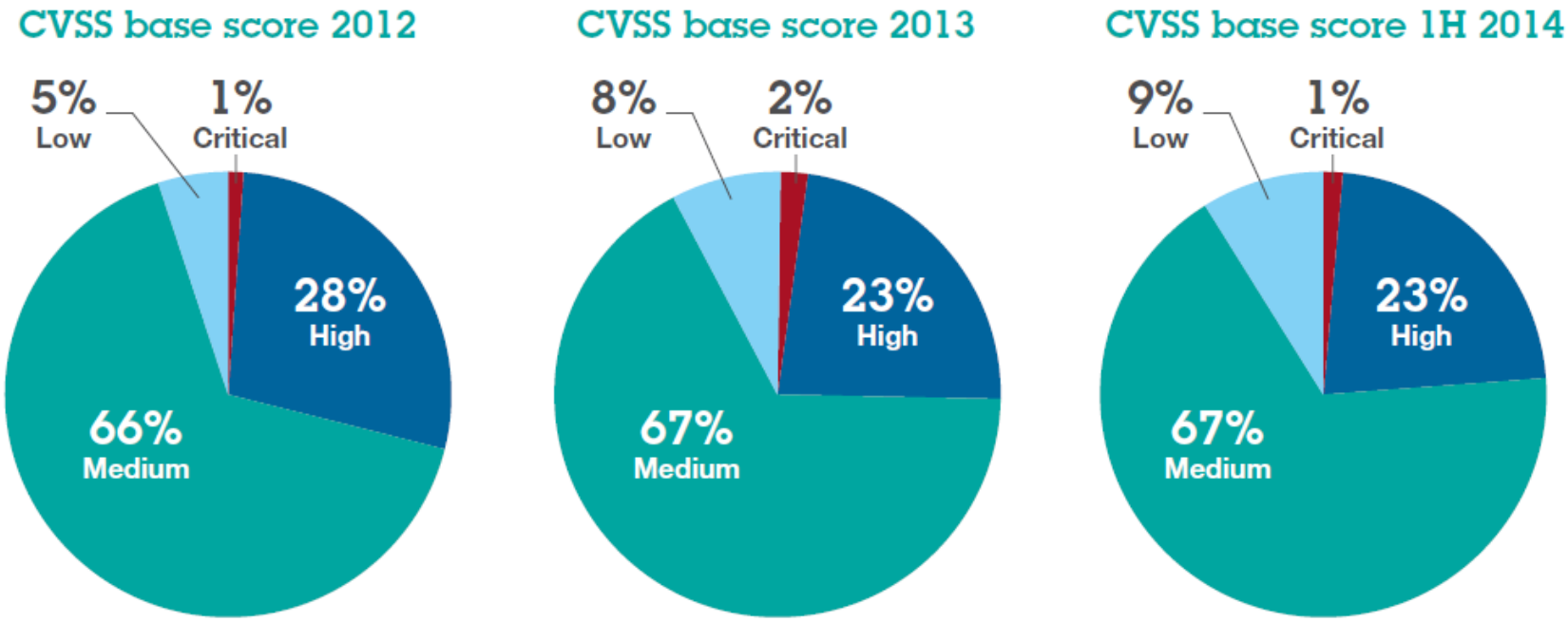
OAI 2009-2013: “attacchi temuti” nei vari Rapporti OAI



Le cause delle crescenti minacce

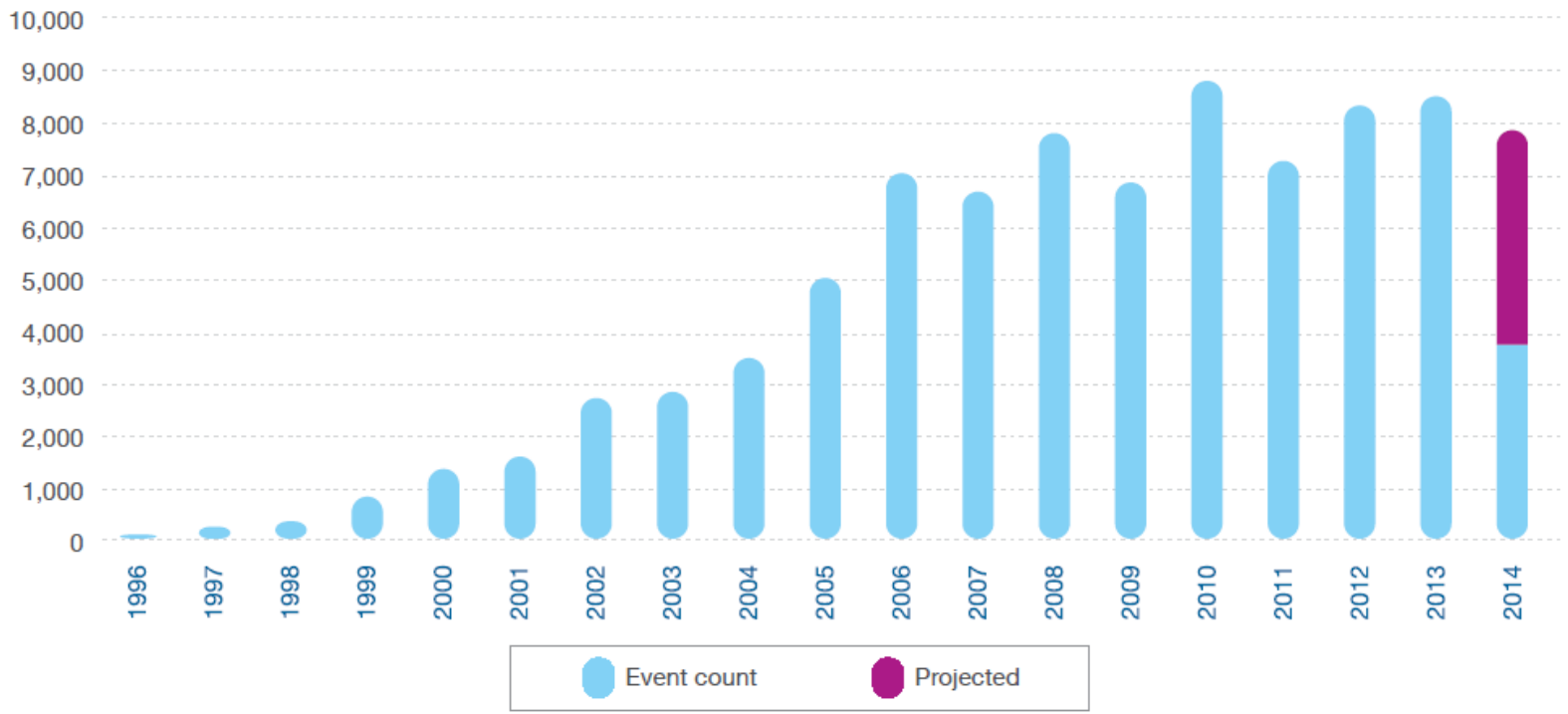
- Tutte si basano sulle **vulnerabilità tecniche e/o umane-organizzative**
  - ***Vulnerabilità tecniche*** (software di base e applicativo, architetture e configurazioni)
    - siti web e piattaforme collaborative
    - Smartphone e tablette → mobilità → **>>14.000 malware**
    - Posta elettronica → spamming e phishing
    - Piattaforme e sistemi virtualizzati
    - Terziarizzazione e Cloud (XaaS)
    - Circa il 40% o più delle vulnerabilità non ha patch di correzione
  - ***Vulnerabilità delle persone***
    - Social Engineering e phishing
    - Utilizzo dei **social network,** anche a livello aziendale
  - ***Vulnerabilità organizzative***
    - Mancanza o non utilizzo procedure organizzative
    - Insufficiente o non utilizzo degli standard e delle best practices
    - Mancanza di formazione e sensibilizzazione
    - Mancanza di controlli e monitoraggi sistematici
    - Analisi dei rischi mancante o difettosa
    - Non efficace controllo dei fornitoriù
    - Limitata o mancante SoD, Separation of Duties

Gravità delle vulnerabilità software scoperte da IBM Xforce 3Q 2014



- CVSS, Common Vulnerability Scoring System: banca mondiale delle vulnerabilità scoperte
- 4 gradi di impatto dell'attacco subito e basato sulla specifica vulnerabilità
  - Critical = impatti catastrofici
  - …
  - Low = impatti trascurabili

Crescita delle vulnerabilità software scoperte



da IBM Xforce 3Q 2014

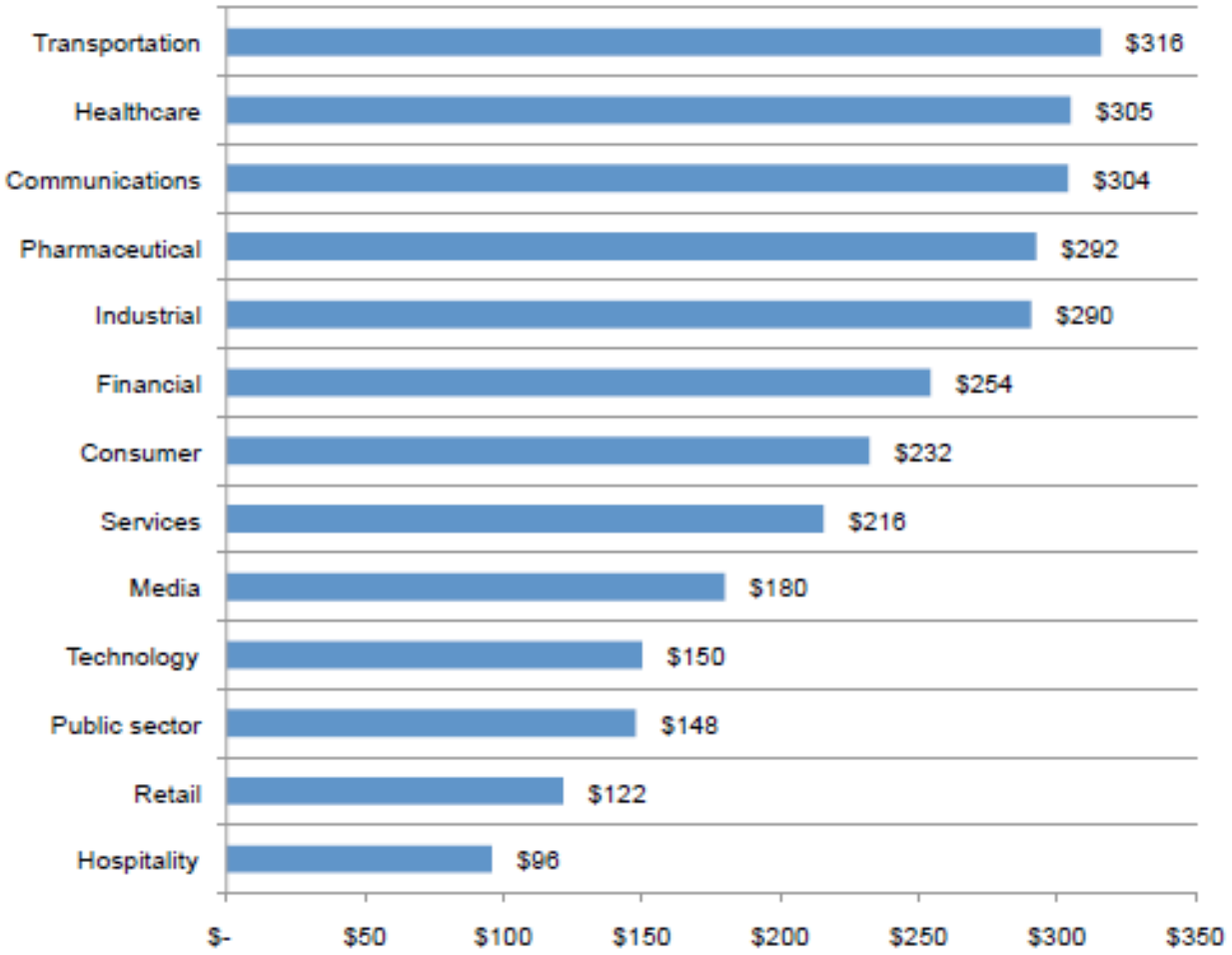
I rischi più critici per gli applicativi web (OWASP Top 10)

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Fonte:OSWAP

OWASP Top 10 Mobile Risks 2014

Ma quanto costa un attacco ?
Data breach cost per capita



OsservatoriO AttacchInformatici

Source: Ponemon Institute Research Report 2013

Targeted Attack (TA) e APT

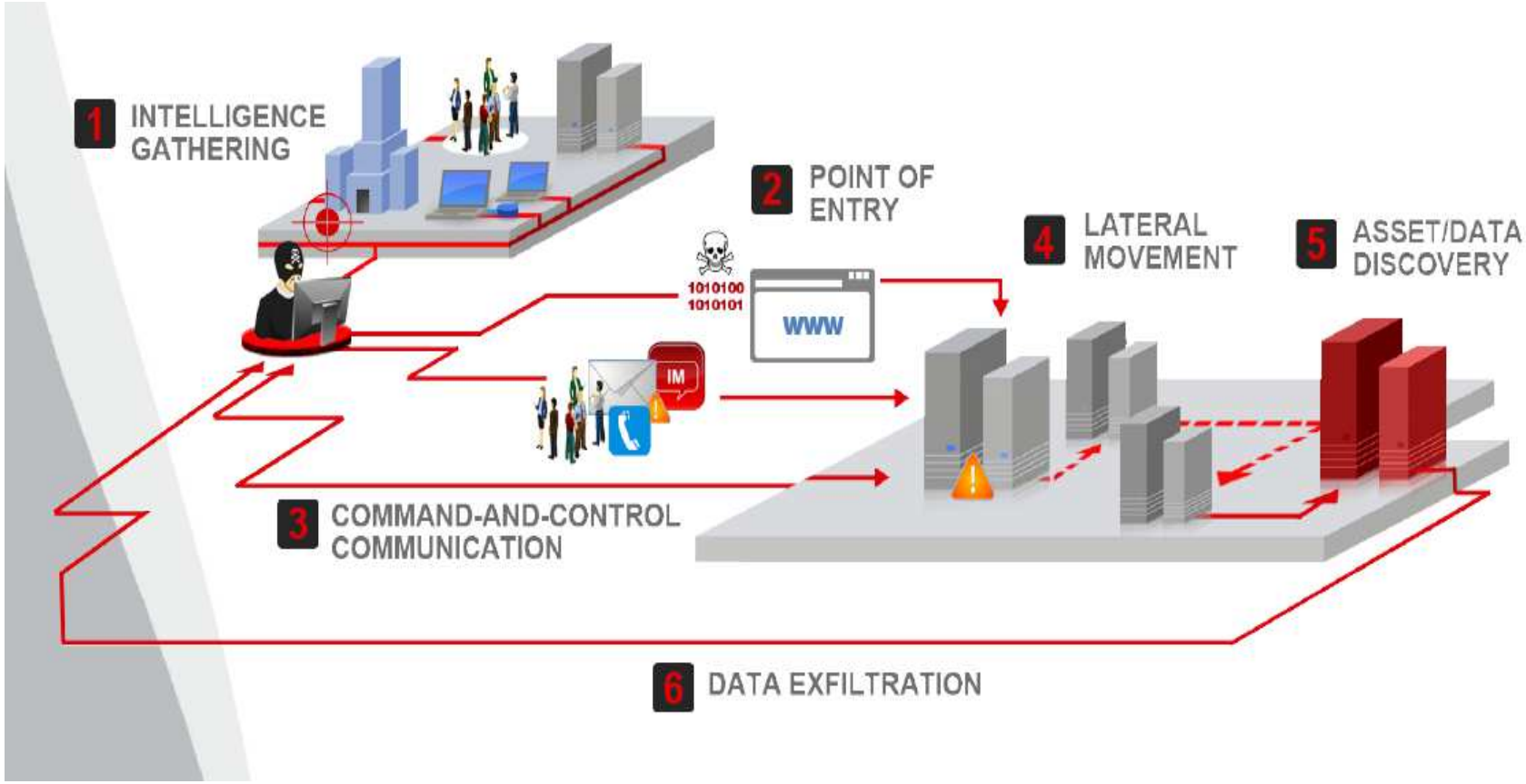
- I **TA**, chiamati anche **targeted attacks**, sono una relativamente nuova classe di attacchi informatici rivolta ad uno specifico obiettivo, o ad un limitato numero di obbiettivi, basato sull' uso di **più strumenti di attacco** con lo scopo primario:
  a) di ottenere informazioni riservate ed importanti → frodi, spionaggio
  b) di seriamente compromettere funzionalità e disponibilità di un sistema informatico o di una sua parte
  c) di seriamente compromettere immagine, credibilità ed autorevolezza dell'obbiettivo attaccato

- **Tipici obiettivi target**: Pubbliche Amministrazioni, Banche ed Istituti finanziari, grandi Corporazioni , infrastrutture nazionali ad alta criticità

- Nell'ambito dei TA una sottoclasse (logica) è costituita dagli **APT**, **Advanced Persistent Threat** attacco mirato ad uno specifico target, usando molteplici e paralleli strumenti di attacco, **persistenti** per essere in grado d**i analizzare le vulnerabilità** esistenti e le possibilità di attacco → **slow and low**

- Sia TA che APT richiedono grandi risorse e competenze →**cyberwar**

Tipiche fasi di un Targeted Attack /APT



Esempi di TA e/o APT

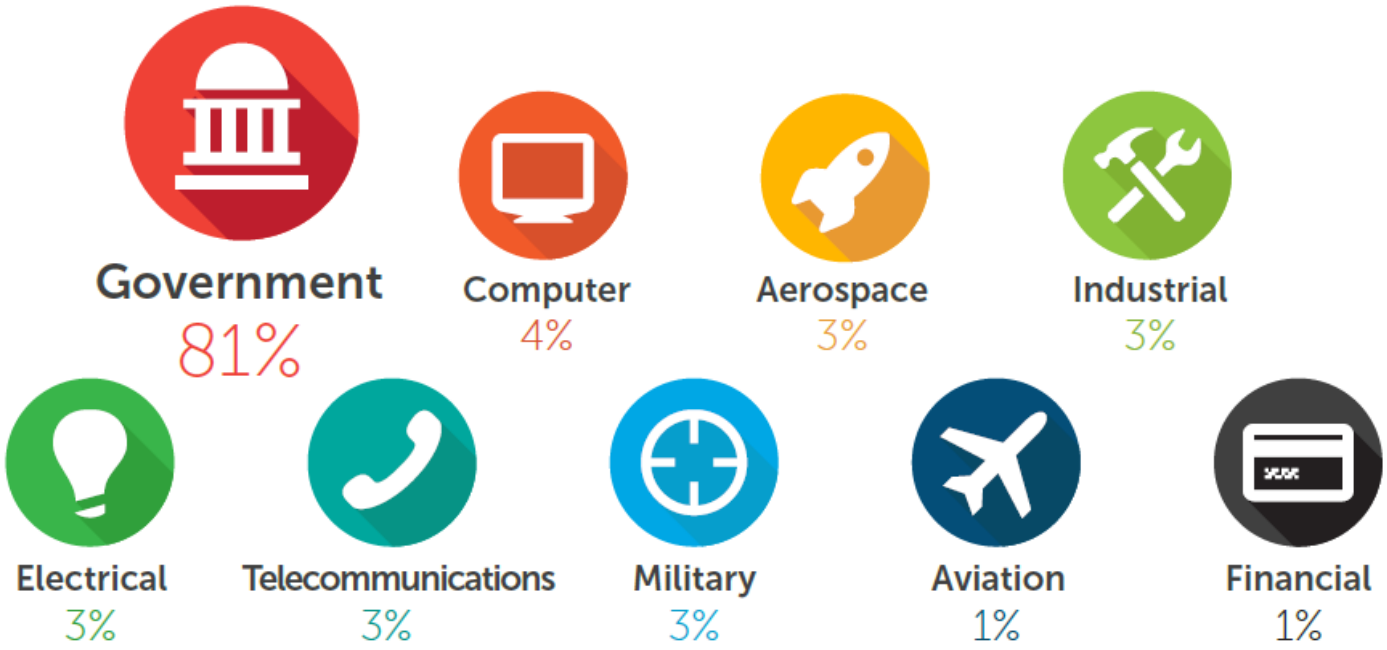
- ***2009-10*** Operazione **Aurora:** attacco a Google (gmail) e ad altri giganti statunitensi dell'ICT dalla Cina via vulnerabilità 0-day su IE e sul sw di controllo versioni codice di Google (Perforce)
- ***2010*** **Stuxnet**: attaccato il centro nucleare iraniano di Bushehr e altre infrastrutture critiche in Cina, India, Indonesia, Pakistan
    - Stuxnet è un codice maligno multicomponente tipo worm che infetta sistemi con sistema operativo Windows, dal vecchio Windows 95 a Windows Server 2003, con installato SIMATIC WinCC, il sistema Siemens per l'automazione dei sistemi SCADA.
    - L'obiettivo del worm è prendere il totale controllo del sistema SCADA attaccato
- ***2011*** **RSA**: attacco a **SecureID** via spear phishing con Excel malevole che attivava codice maligno Poison Ivy con funzionalità backdoor
- ***2011*** **DigiNotar**: CA olandese attaccata creando e diffondendo certificati digitali falsi nei principali browser; un mese dopo **è fallita**
- ***2012*** **Luckycat**: campagna di attacchi in India, Giappone e Tibet ad industrie militari, energia, aerospaziali, .. 90 attacchi compromettendo >233 server via TROJ_WIMMI, VBS_WIMMI, botnet-C&C, Windows Management Instrumentation
- ***2012*** **Flame:** malware modulare e sofisticato di grandi dimensioni (+ 20 M) per ambienti Windows focalizzato allo spionaggio informatico ed al furto di informazioni nei paesi mediorientali
- ***2012*** **Global Payments Inc:** attacco per frode al suo sistema di pagamenti con POS e relative carte di credito, pur essendo certificata PCI-DSS
- **2013-4** **Antifulai:** attacco a vari enti ed aziende giapponesi basato sulla vulnerabilità del word processor Ichitaro, che attivava
- **2014** **Plead**: attacco a varie agenzie governative in Taiwan basato su the RTLO, Right-To-Left Override
- **2014** **Havex**:malware per server di controllo SCADA che opera sulle comunicazioni OPC (Object linking and embedding for Process Control) per attacco ai sistemi di controllo industriale in EU e US

Distribuzione per Paese dei Targeted Attack rilevati nel 2014

Taiwan	62%
Japan	22%
United States	5%
Brazil	1%
China	1%
Israel	1%
Turkey	1%
Others	7%

da Trendmicro Report 3Q 2014

Targeted Attack per settore merceologico



da Trendmicro Report 3Q 2014

Come proteggersi?

- Le misure tecniche ed organizzative “tradizionali” di prevenzione e protezione **possono non essere sufficienti** per individuare e contrastare attacchi come TA e APT
  - ma **sono comunque necessarie**: DMZ, IPS/IDS, antivirus, antispyware, ecc.

- Sistematica **analisi dei comportamenti** anche con tecniche di ***intelligenza artificiale, fuzzy logic***, **statistica bayesiana**, ecc.
  - Sistematico **monitoraggio delle risorse ICT** (reti, OS, middleware, applicazioni), del loro utilizzo ed analisi di eventuali anomale variazioni rispetto alla “normale” media
    - Analisi dei **carichi di traffico**, delle CPU, delle memorie (swapping, …)
    - Analisi dei **log** degli **utenti** e soprattutto degli **operatori di sistema**

- **Scannerizzazione** “intelligente” delle sorgenti di connessioni e di dati

- **Correlazioni *intelligenti* ed *automatiche*** tra gli innumerevoli eventi

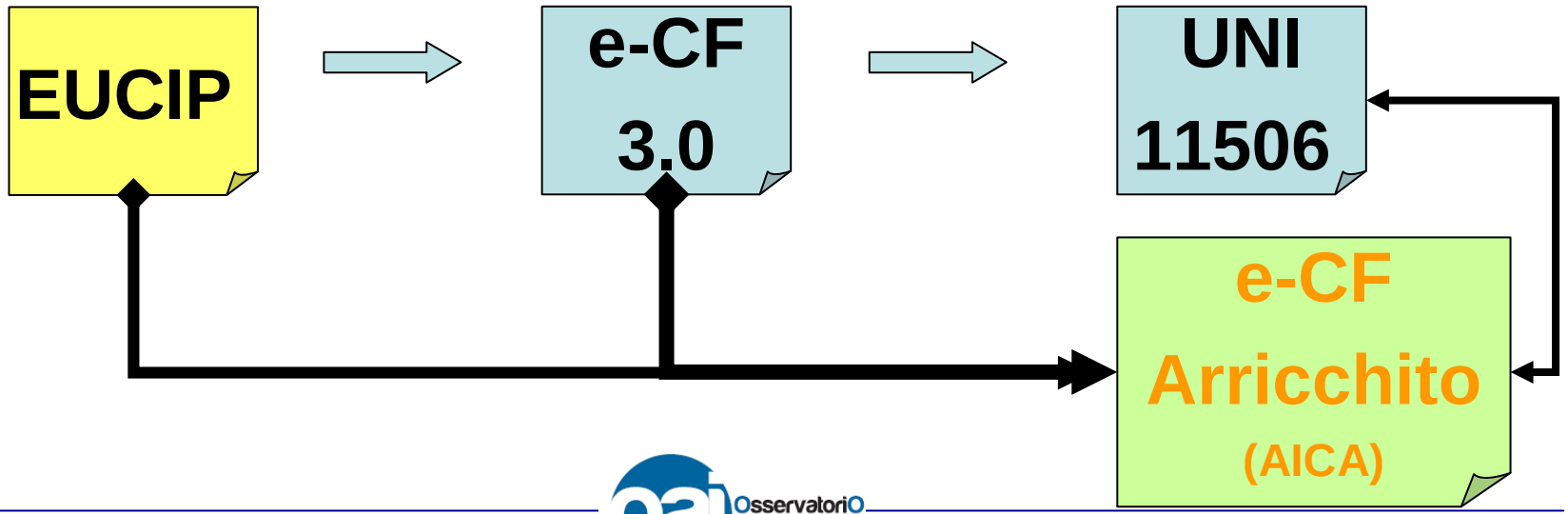
- **Tecniche euristiche** per “problem solving”

D. Lgs. 16 gennaio 2013, n. 13
certificazione delle competenze

Da professionista a *Professionista Certificato*

- Art. 3 Sistema nazionale di certificazione delle competenze
- Art. 17 Riordino della formazione professionale

- UNI 11506: Attività professionali non regolamentate - Figure professionali operanti nel settore Ict - Definizione dei requisiti di conoscenza, abilità e competenze
  - In vigore da settembre 2013



OAI 2014: prossimi passi …

- Da metà – fine novembre 2014 sarà disponibile il **questionario 2014 *totalmente anonimo***.

- Compilatelo numerosi, sarà accessibile da:

http://www.aipsi.org/

http://www.malaboadvisoring.it/

Per chi fosse interessato ad approfondimenti

- **Iscrizione ad AIPSI**

- **Libro “Sicurezza Digitale”**

- **Milano 25-26 novembre 2014: Corsi di formazione manageriali sul governo della Sicurezza Digitale**
  - **Gestire la Sicurezza Digitale in esercizio**
    - rivolto a chi ha responsabilità sulla gestione operativa della sicurezza del sistema informatico,anche in ambiti terziarizzati
  - **Pianificare la Sicurezza Digitale**
    - Rivolto a chi ha responsabilità sulla valutazione dell’efficacia della sicurezza digitale in esercizio e della sua evoluzione, a fronte di esigenze di business e dell’innovazione tecnologica

Riferimenti

marco.bozzetti@gmail.com
www.malaboadvisoring.it
www.aipsi.org